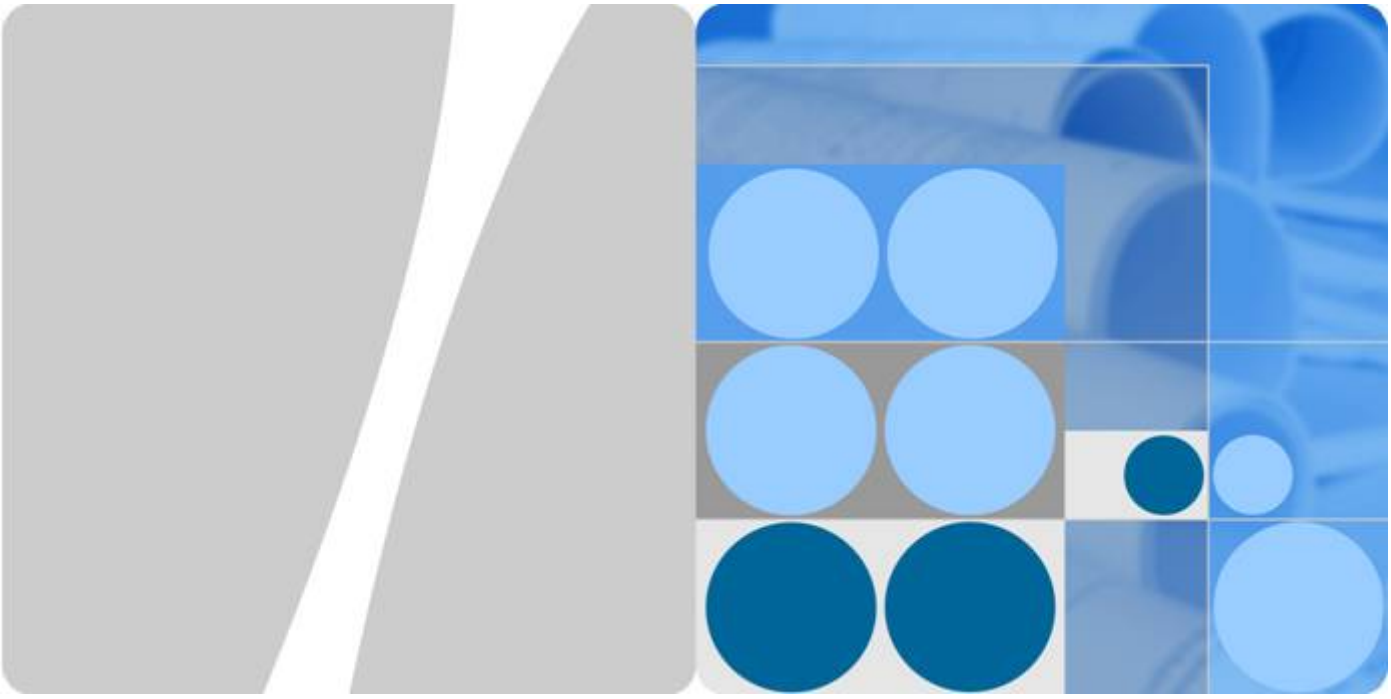


HUAWEI NetEngine5000E Core Router

V800R002C01

Configuration Guide - MPLS

Issue 01

Date 2011-10-15

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Intended Audience

This document provides the basic concepts, configuration procedures, and configuration examples in different application scenarios of the MPLS feature supported by the NE5000E device.

This document describes how to configure the MPLS feature.

This document is intended for:

- Data configuration engineers
- Commissioning engineers
- Network monitoring engineers
- System maintenance engineers

Related Versions (Optional)

The following table lists the product versions related to this document.

Product Name	Version
HUAWEI NetEngine5000E Core Router	V800R002C01

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
 WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injury.

Symbol	Description
CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
TIP	Indicates a tip that may help you solve a problem or save time.
NOTE	Provides additional information to emphasize or supplement important points of the main text.

Command Conventions (Optional)

The command conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[ ]	Items (keywords or arguments) in brackets [ ] are optional.
{ x | y | ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x | y | ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x | y | ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x | y | ...]*	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

Change History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

Changes in Issue 01 (2011-10-15)

The initial commercial release.

Contents

1 MPLS LDP Configuration

About This Chapter

The Multiprotocol Label Switching Label Distribution Protocol (MPLS LDP) defines the messages in and procedures for distributing labels. MPLS LDP is used by Label Switching Routers (LSRs) to negotiate session parameters, distribute labels, and then establish Label Switched Paths (LSPs).

1.9 Configuring LDP over TE

The LDP over TE function is applicable to the network where core devices support TE whereas edge devices support LDP. In this case, a TE tunnel functions as one hop of the entire LDP LSP.

1.10 Configuring the Mode in Which the TTL Field in an IP Packet or an MPLS Packet Is Processed

When an IP packet enters an MPLS domain, you need to set the mode in which the TTL field in the IP packet is processed. When an MPLS packet enters an IP network, you also need to set the mode in which the TTL field in the MPLS packet is processed.

1.11 Maintaining MPLS LDP

This section describes how to maintain MPLS LDP, including resetting LDP and detecting the connectivity of an LSP.

1.12 Configuration Examples

The following sections provide configuration examples for configuring MPLS LDP. Familiarize yourself with the configuration procedures against the networking diagram. Each configuration example consists of the networking requirements, configuration notes, configuration roadmap, configuration procedures, and configuration files.

1.1 MPLS LDP Overview

MPLS LDP is a label distribution protocol. It features simple networking and configurations, supports route-driven establishment of LSPs, and supports high-capacity LSPs, and thus is widely used in Virtual Private Networks (VPNs).

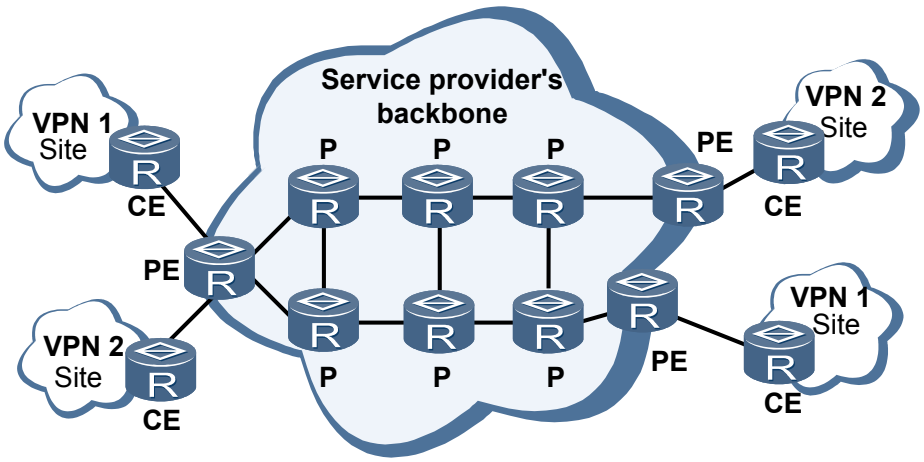
With the prevalence of the Internet in the early 1990s, the IP technology that adopted the longest match for searching routes was simple, whereas became a bottleneck of the forwarding on a network due to limitation of hardware technologies. The Asynchronous Transfer Mode (ATM) technology uses a fixed-length label and maintains a label table of the size much smaller than the size of a routing table. Compared with the IP technology, the ATM technology can provide a higher forwarding rate. The ATM technology has higher performance but is difficult to popularize because of its complex signaling and high deployment costs. The MPLS technology thus emerges to combine the advantages of IP and ATM technologies.

MPLS was initially addressed to improve the forwarding speed of routers. With the development of the Application Specific Integrated Circuit (ASIC) technology, the speed of looking up routes is no longer the bottleneck of the development of networks. Therefore, MPLS loses ground in the high-speed forwarding. MPLS, however, supports a multi-level label stack and is connection-oriented on the forwarding plane and connectionless on the control plane; therefore, MPLS is widely used in VPN, Traffic Engineering (TE), and quality of service (QoS).

LDP is a control protocol of MPLS. Similar to the majority of routing protocols, LDP automatically discovers neighbors and establishes neighbor relationships through multicast Hello messages, or establishes target neighbor relationships through unicast Hello messages. An LDP session is established through parameter negotiation over the TCP connection that is set up between neighbors. Based on an LDP session, LDP distributes label mappings and sets up an LSP according to routes. Data packets are then transmitted over an MPLS network through the LSP.

Actually, LDP runs on Provider (P) routers over a backbone network for forwarding packets and on Provider Edge (PE) routers for deploying LDP over TE.

Figure 1-1 Networking diagram of LDP



1.2 MPLS LDP Features Supported by the NE5000E

The NE5000E supports the LDP session, LDP LSP, LDP fast reroute (FRR),LDP-IGP Synchroniation, LDP generalized TTL security mechanism (GTSM), LDP graceful restart (GR), and LDP over TE.

LDP Session

An LDP session is used by LSRs to distribute labels. LDP sessions are classified into the following types:

- Local LDP session: A local LDP session is established only between adjacent LSRs.
- Remote LDP session: A remote LDP session is established between nonadjacent LSRs or between adjacent LSRs.

A local LDP session and a remote LDP session can be established together.

LDP LSP

An LSP can be established dynamically through LDP. It is recommended that an LSP be established through LDP if an administrator does not need to strictly control the process of establishing an LSP or deploy TE over an MPLS network.

LDP provides a loop detection mechanism to prevent LSP loops.

LDP FRR

The traditional IP FRR cannot effectively protect traffic on an MPLS network. The NE5000E provides the LDP FRR function, which is a solution to port-level traffic protection on an MPLS network.

When a network operates normally, traffic is transmitted through the primary LSP. If the outgoing interface of the primary LSP goes Down, the backup LSP transmits the traffic. In this manner, the uninterrupted traffic forwarding can be ensured in a short period before the network converges. The NE5000E supports LDP FRR in non-load balancing mode over primary and backup LSPs.

LDP FRR depends on IP FRR. After IP FRR is enabled, LDP FRR is automatically enabled.

LDP-IGP Synchroniation

On a network with primary and backup links, if the primary link is faulty, traffic switches from the primary link to the backup link. During this process, traffic is interrupted for about several hundred milliseconds. After the primary link recovers, traffic switches back from the backup link to the primary link. during this process, traffic is interrupted for about 5 seconds.

LDP-IGP synchronization ensures millisecond-level traffic interruption when traffic switches back from the backup link to the primary link.

With LDP-IGP synchronization, if the primary link recovers, the maximum cost of the primary link is advertised to delay IGP route convergence a period of time before LDP successfully establishes the primary LSP. This means that traffic keeps traveling through the backup link in a specified period of time when LDP is establishing the primary LSP and IGP route convergence

is waiting to perform. After LDP successfully establishes the primary LSP, a primary/backup LSP switchback is performed and the primary LSP takes over traffic forwarding, minimizing packet loss.

LDP GTSM

GTSM protects services above the IP layer by checking whether the time-to-live (TTL) value in the IP header is within a specified range. In applications, GTSM is designed to protect the TCP/IP-based control plane (such as routing protocols) against CPU-utilization attacks, such as the CPU overload attack.

For configurations of LDP GTSM, refer to the Core Router *Configuration Guide - Security*.

LDP GR

The GR technology is the key to achieving high availability (HA). Currently, GR has been widely applied to the master/slave switchover and system upgrade.

The NE5000E supports LDP GR, which means that the NE5000E does not reset the interface board during the master/slave switchover. In this manner, the LSP data on the data plane is retained, which ensures uninterrupted forwarding through LSPs, and minimizes the impact on MPLS packet forwarding.

LDP over TE

On the existing network, only certain devices support MPLS TE. In a certain scenario, the core devices support TE and the edge devices support LDP. LDP over TE is thus applied. That is, a TE tunnel functions as one hop along an entire LDP LSP.

Currently, LDP is widely used in the MPLS VPN. You can configure LDP over TE to prevent congestion of VPN traffic on certain nodes.

1.3 Configuring a Local LDP Session

An MPLS LDP session can be configured only when LSR IDs are configured and MPLS LDP is enabled on both ends of the MPLS LDP session.

Applicable Environment

An LDP session is set up based on a TCP connection. After the TCP connection is set up, LSRs negotiate parameters of the LDP session. If the negotiation is successful, an LDP session can be set up.

After the local LDP session is set up, labels can be switched between LSRs and then an LDP LSP can be established.

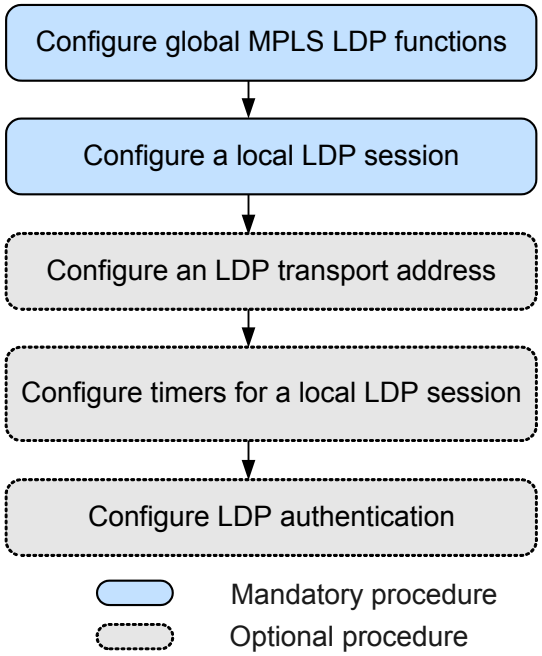
Pre-configuration Tasks

Before configuring a local LDP session, complete the following task:

- Configuring static routes or an IGP to ensure that IP routes between LSRs are reachable

Configuration Procedures

Figure 1-2 Flowchart of the local LDP session configuration



1.3.1 Configuring Global MPLS LDP Functions

You must configure global MPLS LDP functions before configuring all MPLS LDP features. Do as follows on each node in an MPLS domain.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls lsr-id lsr-id
```

The LSR ID of the local node is configured.

When configuring an LSR ID, you need to note the following:

- Configuring an LSR ID is the prerequisite of all MPLS configurations.
- An LSR ID must be manually configured because no default LSR ID is available.
- It is recommended that the IP address of a loopback interface on an LSR be used as the LSR ID.
- To change a set LSR ID, you must run the **undo mpls** command in the system view to delete all MPLS configurations.

CAUTION

Running the **undo mpls** command can delete all MPLS configurations including the established LDP sessions and LSPs.

Step 3 Run:

```
mpls
```

MPLS is enabled globally and the MPLS view is displayed.

By default, MPLS is disabled globally.

Step 4 Run:

```
mpls ldp
```

MPLS LDP is enabled globally and the MPLS LDP view is displayed.

By default, LDP is not enabled globally.

Step 5 (Optional) Run:

```
lsr-id lsr-id
```

The LSR ID is set for an LDP instance.

By default, the LSR ID of the LDP instance is the LSR ID of the local node. It is recommended that the default value be used.

In certain networking schemes such as the BGP/MPLS IP VPN in which VPN instances are applied, if the VPN address space and the public network address space overlap, you need to configure additional LSR IDs for LDP instances to ensure the correct establishment of TCP connections.

Step 6 Run:

```
commit
```

The configurations are committed.

----End

1.3.2 Configuring a Local LDP Session

To configure a local LDP session, you need to globally enable MPLS and MPLS LDP.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The view of the interface on which an LDP session is to be established is displayed.

Step 3 Run:

```
mpls
```

MPLS is enabled on an interface.

Step 4 Run:

```
mpls ldp
```

MPLS LDP is enabled on an interface.

By default, MPLS LDP is disabled on an interface.

NOTE

Disabling MPLS LDP from an interface leads to interruptions of all LDP sessions on the interface and deletions of all LSPs based on these LDP sessions.

Step 5 Run:

```
commit
```

The configurations are committed.

----End

Related Tasks

1.12.1 Example for Configuring Local LDP Sessions

1.3.3 (Optional) Configuring an LDP Transport Address

An LDP session is established over a TCP connection. To set up an LDP session, two LSRs need to confirm the LDP transport address of each other and then set up a TCP connection.

Context

An LDP transport address is used to set up a TCP connection between peers. In this case, a route to the LDP transport address must exist on each peer. Usually, an LSR ID (the loopback interface address) serves as the LDP transport address.

NOTE

- The LDP sessions over multiple links between two LSRs can be established by using the same pair of transport addresses.
- During the configuration of an LDP transport address, an LDP session is interrupted. Therefore, exercising caution when configuring the LDP transport address.

It is recommended that you do not modify an LDP transport address.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The view of the interface on which an LDP session is to be established is displayed.

Step 3 Run:

```
mpls ldp transport-address { interface-type interface-number | interface }
```

The IP address of a specified interface is configured as an LDP transport address.

- *interface-type interface-number*specifies the type and number of an interface. LDP uses the IP address of this specified interface as the transport address to set up a TCP connection.
- **interface** indicates the current interface whose IP address is used by LDP as the transport address for setting up a TCP connection.

By default, an LDP transport address is the LSR ID.

Step 4 Run:

```
commit
```

The configurations are committed.

----End

1.3.4 (Optional) Configuring Timers for a Local LDP Session

Timers of a local LDP session consists of the link Hello hold timer, link Hello send timer, Keepalive hold timer, Keepalive send timer, and Exponential backoff timer.

Context

In a local LDP session, the following timers are used:

- Link Hello send timer: An LSR sends Hello messages at intervals specified by the Hello send timer to the peer LSR. In this manner, the LSR can advertise its presence and set up a Hello adjacency with the peer LSR.
- Link Hello hold timer: LDP peers forming a Hello adjacency periodically send Hello messages to each other to indicate that they expect to maintain the adjacency. If no Hello messages are received before the Hello hold timer expires, the Hello adjacency is torn down.
- Keepalive send timer: LSRs on both ends of an established LDP session start Keepalive send timers and periodically send Keepalive messages to each other to maintain the LDP session.
- Keepalive hold timer: LDP peers start Keepalive hold timers and then periodically send LDP PDUs over an LDP session connection to maintain the LDP session. If the Keepalive hold timers expire and no LDP PDUs are received, the connection is closed and the LDP session is torn down.
- Exponential backoff timer: After the sent LDP Initialization message fails to be processed or the parameters in the Initialization message are refused by the passive role, the active role starts an Exponential backoff timer and periodically attempts to set up an LDP session.

It is recommended that the default value of each timer be adopted.

Procedure

- Configure a link Hello send timer.
  1. Run:
     ```
     system-view
     ```
     The system view is displayed.
  2. Run:
     ```
     interface interface-type interface-number
     ```
     The view of the interface on which an LDP session is to be established is displayed.
  3. Run:

mpls ldp timer hello-send *interval*

A link Hello send timer is configured.

By default, the value of a link Hello send timer is one third the value of a link Hello hold timer.

Actual value of the link Hello send timer = Min{Configured value of the link Hello send timer, 1/3 value of the link Hello hold timer}

4. Run:
commit

The configurations are committed.

- Configure a link Hello hold timer.
  1. Run:
system-view

The system view is displayed.
  2. Run:
interface *interface-type interface-number*

The view of the interface on which an LDP session is to be established is displayed.
  3. Run:
mpls ldp timer hello-hold *interval*

A link Hello hold timer is configured.

By default, the link Hello hold timer is set to 15 seconds.

The value of the Hello hold timer set on the local LSR may not be equal to the value that takes effect. The smaller value between two Hello hold timers set on both ends of the local LDP session can take effect.
  4. Run:
commit

The configurations are committed.
- Configure a Keepalive send timer for a local LDP session.
  1. Run:
system-view

The system view is displayed.
  2. Run:
interface *interface-type interface-number*

The view of the interface on which an LDP session is to be established is displayed.
  3. Run:
mpls ldp timer keepalive-send *interval*

A Keepalive send timer is configured for the local LDP session.

By default, the value of a Keepalive send timer is one third the value of a Keepalive hold timer of the local LDP session.

Actual value of the Keepalive send timer = Min{Configured value of the Keepalive send timer, 1/3 value of the Keepalive hold timer}

4. Run:
   commit

   The configurations are committed.

- Configure a Keepalive hold timer for a local LDP session.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*

     The view of the interface on which an LDP session is to be established is displayed.
  3. Run:
     mpls ldp timer keepalive-hold *interval*

     A Keepalive hold timer is configured for the local LDP session.

     By default, the Keepalive hold timer of the local LDP session is set to 45 seconds.

     The value of the Keepalive hold timer set on the local LSR may not be equal to the value that takes effect. The smaller value between two Keepalive hold timers set on both ends of the local LDP session can take effect.
  4. Run:
     commit

     The configurations are committed.
- Configure an Exponential backoff timer.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     mpls

     The MPLS view is displayed.
  3. Run:
     mpls ldp

     The MPLS LDP view is displayed.
  4. Run:
     backoff timer *init max*

     An Exponential backoff timer is configured.

     The default value of each parameter is as follows:

     - *init*: 15, in seconds
     - *max*: 120, in seconds.

     NOTE

     It is recommended that the initial value be not smaller than 15, and the maximum value be not smaller than 120 for an Exponential backoff timer.
  5. Run:
     commit

The configurations are committed.

----End

1.3.5 (Optional) Configuring LDP Authentication

You can configure LDP authentication to improve security of an LDP session connection. You need to configured LSRs on both ends of an LDP session.

Context

Typically, the MD5 algorithm calculates the digest of a message to avoid the modification of the message. The MD5 message digest is uniquely generated by an irreversible character string conversion algorithm. If the message digest changes in any form during transmission, the message digest received and recalculated is bound to be different, based on which the receiver considers the arriving packet incorrect.

On two peers of an LDP session, the authentication modes can be different and the passwords must be the same.

In MD5 authentication, after simple configurations, a single password is generated and can be switched only through the manual modification. The MD5 algorithm is thus applicable to the networks that require encryption for a short period.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls ldp
```

The MPLS LDP view is displayed.

Step 3 Run:

```
md5-password { plain | cipher } peer-lsr-id password
```

MD5 authentication is enabled and a password is configured.

By default, MD5 authentication is not performed between LDP peers.

Step 4 Run:

```
commit
```

The configurations are committed.

----End

1.3.6 Checking the Configuration

After a local MPLS LDP session is established, you can view information about interfaces enabled with MPLS and MPLS LDP, the LDP protocol, LDP session status, LDP adjacencies, and peers of the LDP session.

Prerequisite

All configurations of a local MPLS LDP session are complete.

Procedure

- Run the **display mpls ldp** [**verbose**] command to check LDP information.
- Run the **display mpls ldp interface** [*interface-type interface-number* | **verbose**] command to check information about an LDP-enabled interface.
- Run the **display mpls ldp session** [**verbose** | *peer-id*] command to check the status of an LDP session.
- Run the **display mpls ldp adjacency** [**interface** *interface-type interface-number* | **remote**] [**peer** *peer-id*] [**verbose**] command to view information about LDP adjacencies.
- Run the **display mpls ldp peer** [**verbose** | *peer-id*] command to check the peer of an LDP session.

----End

Example

Run the **display mpls ldp** command, and you can view global information about LDP, including timers.

```
<HUAWEI> display mpls ldp

                         LDP Global Information
------------------------------------------------------------------------------
 Protocol Version        : V1           Neighbor Liveness    : 600 Sec
 Graceful Restart        : Off          FT Reconnect Timer   : 300 Sec
 MTU Signaling           : On           Recovery Timer       : 300 Sec
                          LDP Instance Information
------------------------------------------------------------------------------
 Instance ID               : 0              VPN-Instance          :
 Instance Status           : Active         LSR ID                : 4.4.4.4
 Hop Count Limit           : 32             Path Vector Limit     : 32
 Loop Detection            : Off
 DU Re-advertise Timer     : 10 Sec         DU Re-advertise Flag  : Off
 DU Explicit Request       : Off            Request Retry Flag    : Off
 Label Distribution Mode   : Ordered        Label Retention Mode  : Liberal
 Graceful-delete           : Off            Graceful-delete Timer : 5 Sec
 Igp-sync-delay Timer      : 10 Sec
 Ipv6-family               : Off
 Local-ipv6-transport-address   :  ::2:2:2:2
------------------------------------------------------------------------------
```

Run the **display mpls ldp interface** [**verbose**] command, and you can view information about LDP-enabled interfaces, including transport addresses and timers.

```
<HUAWEI> display mpls ldp interface

     LDP Interface Information in Public Network
 Codes:LAM(Label Advertisement Mode), IFName(Interface name)
 A '*' before an interface means the entity is being deleted.
------------------------------------------------------------------------------
IFName                Status   LAM    TransportAddress   HelloSent/Rcv
------------------------------------------------------------------------------
Pos3/1/1              Active   DU     1.1.1.9            21411/21409
------------------------------------------------------------------------------
<HUAWEI> display mpls ldp interface verbose

     LDP Interface Information in Public Network
 ------------------------------------------------------------------------------
```

```
 Interface Name : Pos1/0/0
 LDP ID         : 1.1.1.1:0             Transport Address : 1.1.1.1
 Entity Status  : Active                Effective MTU : 1500
 Configured Hello Timer     : 15 Sec
 Negotiated Hello Timer     : 15 Sec
 Configured Keepalive Timer : 45 Sec
 Configured Delay Timer     : 0 Sec
 Label Advertisement Mode   : Downstream Unsolicited
 Hello Message Sent/Rcvd    : 1705/1720 (Message Count)
 ------------------------------------------------------------------------------
```

Run the **display mpls ldp session** [**verbose**] command, and you can view that the LDP session is in the Operational state.

```
<HUAWEI> display mpls ldp session

 LDP Session(s) in Public Network
 Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDD:HH:MM)
 A '*' before a session means the session is being deleted.
------------------------------------------------------------------------------
 PeerID             Status      LAM  SsnRole  SsnAge       KASent/Rcv
------------------------------------------------------------------------------
 2.2.2.9:0          Operational DU   Passive  000:22:40   5426/5426
 3.3.3.9:0          Operational DU   Passive  001:18:33   10185/10182
------------------------------------------------------------------------------
TOTAL: 2 Session(s) Found.
<HUAWEI> display mpls ldp session verbose
               LDP Session(s) in Public Network
 ------------------------------------------------------------------------------
 Peer LDP ID     : 5.5.5.5:0        Local LDP ID   : 3.3.3.3:0
 TCP Connection  : 3.3.3.3 <- 5.5.5.5
 Session State   : Operational          Session Role   : Passive
 Session FT Flag : Off                  MD5 Flag       : Off
 Reconnect Timer : ---                  Recovery Timer : ---
 Negotiated Keepalive Hold Timer   : 45 Sec
 Configured Keepalive Send Timer   : 15 Sec
 Keepalive Message Sent/Rcvd       : 5387/5388 (Message Count)
 Label Advertisement Mode          : Downstream Unsolicited
 Label Resource Status(Peer/Local) : Available/Available
 Session Age                       : 000:22:28  (DDD:HH:MM)
 Addresses received from peer: ( Count: 2 )
  5.5.5.5            10.2.1.2
 ------------------------------------------------------------------------------
```

Run the **display mpls ldp adjacency** command, and you can view information about LDP adjacencies.

```
<HUAWEI> display mpls ldp adjacency

 LDP Adjacency Information
 Codes: R: Remote Adjacency, L: Local Adjacency
 A '*' before an adjacency means the adjacency is being deleted.
 ------------------------------------------------------------------------------
 SN   SourceAddr      PeerID          VrfID     AdjAge(DDD:HH:MM) RcvdHello Type
 ------------------------------------------------------------------------------
 1    2.1.1.2         2.2.2.2         0           000:01:02       703        L
 ------------------------------------------------------------------------------
 TOTAL: 1 Record(s) Found.
```

Run the **display mpls ldp peer** command, and you can view information about the peers of an LDP session.

```
<HUAWEI> display mpls ldp peer

 LDP Peer Information in Public network
 A '*' before a peer means the peer is being deleted.
 ------------------------------------------------------------------------------
 PeerID                TransportAddress   DiscoverySource
 ------------------------------------------------------------------------------
```

```
 2.2.2.9:0             2.2.2.9           Pos3/1/1
 ------------------------------------------------------------------------------
TOTAL: 1 Peer(s) Found.
```

1.4 Configuring a Remote LDP Session

A remote MPLS LDP session can be set up only when LSR IDs are configured and MPLS LDP is enabled on both ends of the MPLS LDP session.

Applicable Environment

A remote LDP session is applicable to LDP over TE. On an MPLS network, if core devices support TE whereas edge devices support LDP, a remote LDP session needs to be set up between the two edge LSRs. In the LDP over TE function, a TE tunnel functions as one hop along the entire LDP LSP.

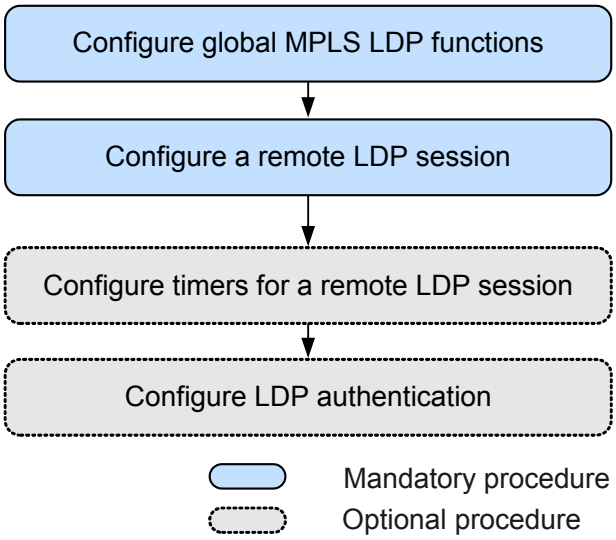
Pre-configuration Tasks

Before configuring a remote LDP session, complete the following task:

- Configuring static routes or an IGP to ensure that IP routes between LSRs are reachable

Configuration Procedures

Figure 1-3 Flowchart of the remote LDP session configuration



Related Tasks

1.12.2 Example for Configuring a Remote LDP Session

1.4.1 Configuring Global MPLS LDP Functions

You must configure global MPLS LDP functions before configuring all MPLS LDP features. Do as follows on each node in an MPLS domain.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls lsr-id lsr-id
```

The LSR ID of the local node is configured.

When configuring an LSR ID, you need to note the following:

- Configuring an LSR ID is the prerequisite of all MPLS configurations.
- An LSR ID must be manually configured because no default LSR ID is available.
- It is recommended that the IP address of a loopback interface on an LSR be used as the LSR ID.
- To change a set LSR ID, you must run the **undo mpls** command in the system view to delete all MPLS configurations.

CAUTION

Running the **undo mpls** command can delete all MPLS configurations including the established LDP sessions and LSPs.

Step 3 Run:

```
mpls
```

MPLS is enabled globally and the MPLS view is displayed.

By default, MPLS is disabled globally.

Step 4 Run:

```
mpls ldp
```

MPLS LDP is enabled globally and the MPLS LDP view is displayed.

By default, LDP is not enabled globally.

Step 5 (Optional) Run:

```
lsr-id lsr-id
```

The LSR ID is set for an LDP instance.

By default, the LSR ID of the LDP instance is the LSR ID of the local node. It is recommended that the default value be used.

In certain networking schemes such as the BGP/MPLS IP VPN in which VPN instances are applied, if the VPN address space and the public network address space overlap, you need to configure additional LSR IDs for LDP instances to ensure the correct establishment of TCP connections.

Step 6 Run:

```
commit
```

The configurations are committed.

----End

1.4.2 Configuring a Remote LDP Session

To configure a remote LDP session, you need to specify the name and IP address of the remote peer.

Context

A remote LDP session can be established between nonadjacent LSRs or between adjacent LSRs.

A local LDP session and a remote LDP session can be configured together between two LSRs.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls ldp remote-peer remote-peer-name
```

A remote MPLS LDP peer is created and the remote MPLS LDP peer view is displayed.

Step 3 Run:

```
remote-ip ip-address
```

The IP address is assigned to the remote MPLS LDP peer.

The remote MPLS LDP peer must use the LSR ID as the IP address.

NOTE

- The IP address of a remote LDP peer must be the LSR ID of the remote LDP peer. When an LDP LSR ID is different from an MPLS LSR ID, the LDP LSR ID must be adopted.
- Modifying or deleting a configured IP address of a remote MPLS LDP peer leads to the deletion of the remote LDP session.

Step 4 (Optional) You can select either of the following modes to prohibit labels from being distributed to a remote MPLS LDP peer:

- Run:

  ```
  remote-ip ip-address pwe3
  ```

  The local LSR is prohibited from distributing labels to a specified remote MPLS LDP peer.
- Run the following commands to prohibit labels from being distributed to all remote MPLS LDP peers.
  - Run:

    ```
    quit
    ```

    Return to the system view.
  - Run:

    ```
    mpls ldp
    ```

    The MPLS LDP view is displayed.

- Run:

  ```
  remote-peer pwe3
  ```

The local LSR is prohibited from distributing labels to all remote MPLS LDP peers.

By default, a local LSR is allowed to distribute labels to the remote MPLS LDP peers.

NOTE

When a remote LDP session provides services for a VPN, you can run the preceding commands to prohibit labels from being distributed to the remote MPLS LDP peers, which can save system resources. When TE services are transmitted over a backbone network in the LDP over TE scenario, it is not recommended that you perform this configuration.

Step 5 Run:

```
commit
```

The configurations are committed.

----End

1.4.3 (Optional) Configuring Timers for a Remote LDP Session

LDP timers consists of the target Hello hold timer, target Hello send timer, Keepalive hold timer, Keepalive send timer, and Exponential backoff timer.

Context

In a remote LDP session, the following timers are used:

- Target Hello send timer: An LSR sends Hello messages at intervals specified by the Hello send timer to the peer LSR. In this manner, the LSR can advertise its existence and set up a Hello adjacency with the peer LSR.
- Target Hello hold timer: LDP peers forming a Hello adjacency periodically send Hello messages to each other to indicate that they expect to maintain the adjacency. If the Hello hold timer expires and no Hello messages are received, the Hello adjacency is torn down.
- Keepalive send timer: LSRs on both ends of an established LDP session start Keepalive send timers and periodically send Keepalive messages to each other to maintain the LDP session.
- Keepalive hold timer: LDP peers start Keepalive hold timers and periodically send LDP PDUs over an LDP session connection to maintain the LDP session. If the Keepalive hold timers expire and no LDP PDUs are received, the connection is closed and the LDP session is torn down.
- Exponential backoff timer: After the sent LDP Initialization message fails to be processed or the parameters in the Initialization message are refused by the passive role, the active role starts an Exponential backoff timer and periodically attempts to set up an LDP session.

It is recommended that the default value of each timer be adopted.

Procedure

- Configure a target Hello send timer.
  1. Run:

     ```
     system-view
     ```

     The system view is displayed.

2. Run:
   mpls ldp remote-peer *remote-peer-name*

   The remote MPLS LDP peer view is displayed.
3. Run:
   mpls ldp timer hello-send *interval*

   A target Hello send timer is configured.

   By default, the value of a target Hello send timer is one third the value of a target Hello hold timer.

   Actual value of the target Hello send timer = Min{Configured value of the target Hello send timer, 1/3 value of the target Hello hold timer}
4. Run:
   commit

   The configurations are committed.

- Configure a target Hello hold timer.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     mpls ldp remote-peer *remote-peer-name*

     The remote MPLS LDP peer view is displayed.
  3. Run:
     mpls ldp timer hello-hold *interval*

     A target Hello hold timer is configured.

     By default, the target Hello hold timer is set to 45 seconds.

     The value of the Hello hold timer set on the local LSR may not be equal to the value that takes effect. The smaller value between two Hello hold timers set on both ends of the remote LDP session can take effect.
  4. Run:
     commit

     The configurations are committed.
- Configure a Keepalive send timer for a remote LDP session.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     mpls ldp remote-peer *remote-peer-name*

     The remote MPLS LDP peer view is displayed.
  3. Run:
     mpls ldp timer keepalive-send *interval*

     A Keepalive send timer for a remote LDP session is configured.

By default, the value of a Keepalive send timer is one third the value of a Keepalive hold timer.

Actual value of the Keepalive send timer = Min{Configured value of the Keepalive send timer, 1/3 value of the Keepalive hold timer}

4. Run:
   commit

   The configurations are committed.

- Configure a Keepalive hold timer for a remote LDP session.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     mpls ldp remote-peer *remote-peer-name*

     The remote MPLS LDP peer view is displayed.
  3. Run:
     mpls ldp timer keepalive-hold *interval*

     A Keepalive hold timer for a remote LDP session is configured.

     By default, the Keepalive hold timer of the remote LDP session is set to 45 seconds.

     The value of the Keepalive hold timer set on the local LSR may not be equal to the value that takes effect. The smaller value between two Keepalive hold timers set on both ends of the remote LDP session can take effect.
  4. Run:
     commit

     The configurations are committed.
- Configure an Exponential backoff timer.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     mpls

     The MPLS view is displayed.
  3. Run:
     mpls ldp

     The MPLS LDP view is displayed.
  4. Run:
     backoff timer *init max*

     An Exponential backoff timer is configured.

     By default, its initial value is 15 and its maximum value is 120, in seconds.

     NOTE

     It is recommended that the initial value be not smaller than 15 and the maximum value be not smaller than 120 for an Exponential backoff timer.

5. Run:
   commit

   The configurations are committed.

----End

1.4.4 (Optional) Configuring LDP Authentication

You can configure LDP authentication to improve security of an LDP session connection. You need to configured LSRs on both ends of an LDP session.

Context

Typically, the MD5 algorithm calculates the digest of a message to avoid the modification of the message. The MD5 message digest is uniquely generated by an irreversible character string conversion algorithm. If the message digest changes in any form during transmission, the message digest received and recalculated is bound to be different, based on which the receiver considers the arriving packet incorrect.

On two peers of an LDP session, the authentication modes can be different and the passwords must be the same.

In MD5 authentication, after simple configurations, a single password is generated and can be switched only through the manual modification. The MD5 algorithm is thus applicable to the networks that require encryption for a short period.

Procedure

Step 1 Run:
system-view

The system view is displayed.

Step 2 Run:
mpls ldp

The MPLS LDP view is displayed.

Step 3 Run:
md5-password { **plain** | **cipher** } *peer-lsr-id password*

MD5 authentication is enabled and a password is configured.

By default, MD5 authentication is not performed between LDP peers.

Step 4 Run:
commit

The configurations are committed.

----End

1.4.5 Checking the Configuration

After a remote MPLS LDP session is established, you can view information about the LDP protocol, LDP session status, LDP adjacencies,, and remote peers of the LDP session.

Prerequisite

All configurations of a remote MPLS LDP session are complete.

Procedure

- Run the **display mpls ldp** [**all**] [**verbose**] command to check LDP information.
- Run one of the following commands to check the LDP session status:
  - **display mpls ldp session** [**verbose** | *peer-id*]
  - **display mpls ldp session** [**all**] [**verbose**]
- Run the **display mpls ldp adjacency** [**interface** *interface-type interface-number* | **remote**] [**peer** *peer-id*] [**verbose**] command to view information about LDP adjacencies.
- Run one of the following commands to check information about the peer of an LDP session:
  - **display mpls ldp peer** [**verbose** | *peer-id*]
  - **display mpls ldp peer** [**all**] [**verbose**]
- Run the **display mpls ldp remote-peer** [*remote-peer-name*] command to check a remote peer of an LDP session.

----End

Example

Run the **display mpls ldp** command, and you can view global information about LDP, including timers.

```
<HUAWEI> display mpls ldp

                          LDP Global Information
------------------------------------------------------------------------------
 Protocol Version        : V1           Neighbor Liveness    : 600 Sec
 Graceful Restart        : Off          FT Reconnect Timer   : 300 Sec
 MTU Signaling           : On           Recovery Timer       : 300 Sec
                          LDP Instance Information
------------------------------------------------------------------------------
 Instance ID               : 0              VPN-Instance          :
 Instance Status           : Active         LSR ID                : 4.4.4.4
 Hop Count Limit           : 32             Path Vector Limit     : 32
 Loop Detection            : Off
 DU Re-advertise Timer     : 10 Sec         DU Re-advertise Flag  : Off
 DU Explicit Request       : Off            Request Retry Flag    : Off
 Label Distribution Mode   : Ordered        Label Retention Mode  : Liberal
 Graceful-delete           : Off            Graceful-delete Timer : 5 Sec
 Igp-sync-delay Timer      : 10 Sec
 Ipv6-family               : Off
 Local-ipv6-transport-address   :  ::2:2:2:2
------------------------------------------------------------------------------
```

Run the **display mpls ldp session** [**verbose**] command, and you can view that the LDP session is in the Operational state.

```
<HUAWEI> display mpls ldp session

 LDP Session(s) in Public Network
 Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDD:HH:MM)
 A '*' before a session means the session is being deleted.
------------------------------------------------------------------------------
 PeerID            Status      LAM  SsnRole  SsnAge       KASent/Rcv
------------------------------------------------------------------------------
 2.2.2.9:0         Operational DU   Passive  000:22:40   5426/5426
 3.3.3.9:0         Operational DU   Passive  001:18:33   10185/10182
```

```
--------------------------------------------------------------------------
TOTAL: 2 Session(s) Found.
<HUAWEI> display mpls ldp session verbose
              LDP Session(s) in Public Network
 --------------------------------------------------------------------------
 Peer LDP ID     : 5.5.5.5:0        Local LDP ID   : 3.3.3.3:0
 TCP Connection  : 3.3.3.3 <- 5.5.5.5
 Session State   : Operational          Session Role   : Passive
 Session FT Flag : Off                  MD5 Flag       : Off
 Reconnect Timer : ---                  Recovery Timer : ---
 Negotiated Keepalive Hold Timer   : 45 Sec
 Configured Keepalive Send Timer   : 15 Sec
 Keepalive Message Sent/Rcvd       : 5387/5388 (Message Count)
 Label Advertisement Mode          : Downstream Unsolicited
 Label Resource Status(Peer/Local) : Available/Available
 Session Age                       : 000:22:28  (DDD:HH:MM)
 Addresses received from peer: ( Count: 2 )
  5.5.5.5            10.2.1.2
 --------------------------------------------------------------------------
```

Run the **display mpls ldp adjacency** command, and you can view information about LDP adjacencies.

```
<HUAWEI> display mpls ldp adjacency

LDP Adjacency Information
 Codes: R: Remote Adjacency, L: Local Adjacency
 A '*' before an adjacency means the adjacency is being deleted.
 ------------------------------------------------------------------------------
 SN   SourceAddr      PeerID          VrfID     AdjAge(DDDD:HH:MM) RcvdHello Type
 ------------------------------------------------------------------------------
 1    11.11.11.1      1.1.1.1         0           0000:01:19       956        L
 2    20.20.20.1      2.2.2.2         0           0000:01:19       949        L
 3    1.1.1.1         1.1.1.1         0           0000:01:19       315        R
 4    2.2.2.2         2.2.2.2         0           0000:01:19       313        R
 ------------------------------------------------------------------------------
 TOTAL: 4 Record(s) Found.
```

Run the **display mpls ldp peer** command or the **display mpls ldp remote-peer** command, and you can view information about the peers of LDP sessions.

```
<HUAWEI> display mpls ldp peer

 LDP Peer Information in Public network
 A '*' before a peer means the peer is being deleted.
 --------------------------------------------------------------------------
 PeerID                TransportAddress   DiscoverySource
 --------------------------------------------------------------------------
 3.3.3.9:0             3.3.3.9            Remote Peer : 3.3.3.9
 --------------------------------------------------------------------------
TOTAL: 1 Peer(s) Found.
<HUAWEI> display mpls ldp remote-peer
                        LDP Remote Entity Information
 ------------------------------------------------------------------------------
 Remote Peer Name: rtc
 Remote Peer IP    : 3.3.3.9             LDP ID        : 1.1.1.9:0
 Transport Address : 1.1.1.9             Entity Status : Active

 Configured Keepalive Hold Timer : 45 Sec
 Configured Keepalive Send Timer : 15 Sec
 Configured Hello Hold Timer     : 45 Sec
 Negotiated Hello Hold Timer     : 45 Sec
 Configured Hello Send Timer     : 15 Sec
 Configured Delay Timer          : ----
 Hello Packet sent/received      : 6347/6307
 ------------------------------------------------------------------------------
 TOTAL: 1 Remote-Peer(s) Found.
```

1.5 Configuring an LDP LSP

LDP is a label distribution protocol used in an MPLS domain for setting up LSPs.

Applicable Environment

It is recommended that an LSP be established through LDP if an administrator does not need to strictly control the process of establishing an LSP or deploy TE over an MPLS network.

The supported a maximum number of LSPs varies with the capacity and performance of a device. Establishing a large number of LSPs may lead the unstable operation of a device.

An LSP can be established only when eligible routes exist on LSRs and match the LSP setup policy. LDP can be triggered only by routes filtered by the policy and then set up LSPs. In this manner, the number of LSPs can be controlled.

The NE5000E provides the following policies for controlling the number of LSPs:

- Policies for setting up ingress LSPs or egress LSPs are as follows:
  - All IGP routes can trigger the establishment of LSPs.
  - Host routes can trigger the establishment of LSPs.
  - An IP prefix list can trigger the establishment of LSPs.
  - Establishment of LSPs is not triggered.
- To control the number of transit LSPs on a transit LSR, an IP prefix list can be adopted to filter routes and only the routes matching the filtering policy can be used to set up transit LSPs.

To correctly detect the path MTU (Maximum Transmission Unit), an LSR must obtain the MTU of each link connected to it. In this case, the LDP MTU signaling function needs to be configured.

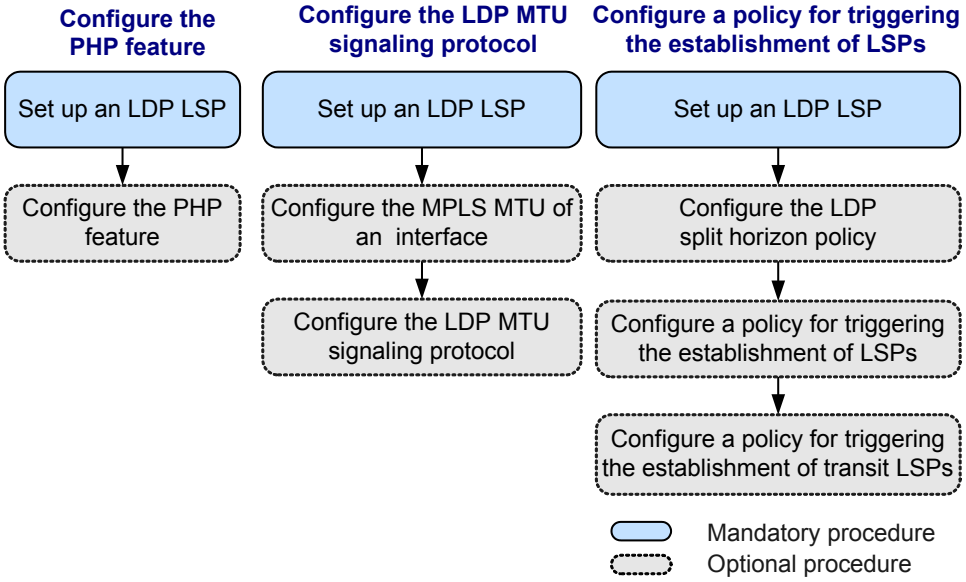
Pre-configuration Tasks

Before configuring an LDP LSP, complete the following task:

- **Configuring a Local LDP Session**

Configuration Procedures

Figure 1-4 Flowchart of the LDP LSP configuration



Related Tasks

1.12.3 Example for Establishing LSPs Through LDP

1.12.4 Example for Configuring Transit LSPs Through an IP Prefix List

1.5.1 Setting Up an LDP LSP

An LDP LSP can be automatically set up only when an LDP session is established.

Context

Complete the task of **Configuring a Local LDP Session** between adjacent LSRs along an LSP to be set up. After the local LDP session is established, an LDP LSP can be set up automatically.

1.5.2 (Optional) Configuring the PHP Feature

After the penultimate hop popping (PHP) function is configured, you can configure the label to be distributed to the penultimate hop on the egress node.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Step 3 Run:

```
label advertise { explicit-null | implicit-null | non-null }
```

The label distributed to the penultimate hop is configured.

According to the specified parameters, you can configure the egress to allocate different labels to the penultimate hop.

- By default, **implicit-null** is configured, indicating that the PHP feature is supported. That is, the egress node distributes an implicit null label being 3 to the penultimate hop.
- When **explicit-null** is configured, it indicates that the PHP feature is not supported. That is, the egress node distributes an explicit null label to the penultimate hop.The IPv4 explicit null label is 0,
- When **non-null** is configured, it indicates that the PHP feature is not supported. That is, the egress node distributes a normal label whose value is equal to or larger than 16 to the penultimate hop.

NOTE

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

Step 4 Run:

```
commit
```

The configurations are committed.

----End

1.5.3 (Optional) Configuring the MPLS MTU of an Interface

To configure the MPLS MTU of an interface, you need to configure each node along an LSP.

Context

LDP can automatically calculate the minimum value among MTUs on all outbound interfaces of each LSP. Then MPLS can use the minimum MTU to determine the size of MPLS packets to be forwarded on the ingress node. By doing this, the ingress node can avoid sending large MPLS packets, which prevents forwarding failures on a transit node.

The relationship between the MPLS MTU and the interface MTU of an interface is as follows:

- If no MPLS MTU is set, the interface MTU is used as the MPLS MTU.
- If an MPLS MTU is set, the smaller value between the MPLS MTU and the interface MTU is used as the effective interface MTU.

NOTE

The MPLS MTU of an interface can take effect only after the MTU signalling is enabled.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The view of the interface enabled with MPLS is displayed.

Step 3 Run:

```
mpls mtu mtu
```

An MPLS MTU is set for an interface.

Step 4 Run:

```
commit
```

The configurations are committed.

----End

1.5.4 (Optional) Configuring the LDP MTU Signaling Protocol

By configuring the LDP MTU signaling protocol, you can determine that a send Label Mapping message carries an MTU TLV.

Context

The value of an MTU determines the maximum number of bytes that can be transmitted by the sender at a time. If the MTU exceeds the maximum number of bytes supported by the receiver or a transit device, packets are then fragmented or even discarded, thus imposing heavy burden on network transmission. After the LDP MTU signaling protocol is configured, packets smoothly pass through each transit device and reach receivers without packet reassembly.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls ldp
```

The MPLS LDP view is displayed.

Step 3 Run:

```
mtu-signalling [apply-tlv]
```

The function that a send Label Mapping message carries an MTU TLV is enabled.

By default, the function that a send Label Mapping message carries an MTU TLV is enabled.

Step 4 Run:

```
commit
```

The configurations are committed.

----End

1.5.5 (Optional) Configuring the LDP Split Horizon Policy

By configuring an LDP split horizon policy, you can restrain an LSR from distributing labels to specified downstream LDP peers.

Context

By default, LSPs distribute labels to both upstream and downstream LDP peers, which speeds up convergence of an LDP LSP. For the digital subscriber line access multiplexers (DSLAMs) accessing to an MPLS network, it is recommended that a split horizon policy be configured for LDP peers so that these LDP peers distribute labels to only upstream LDP peers, which saves memory.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls ldp
```

The MPLS LDP view is displayed.

Step 3 Run:

```
outbound peer { peer-id | all } split-horizon
```

A split horizon policy is configured for LDP peers. That is, LSRs are restrained from distributing labels to specified downstream LDP peers.

By default, no split horizon policy is configured for LDP peers. That is, LSRs distribute labels to both upstream and downstream LDP peers.

Step 4 Run:

```
commit
```

The configurations are committed.

----End

1.5.6 (Optional) Configuring a Policy for Triggering the Establishment of LSPs

By configuring a policy for triggering the establishment of up LSPs, you can use eligible routes to trigger LDP to set up LSPs.

Context

To set up ingress LSPs and egress LSPs on a public network, you can use one of the following policies to use eligible routes to trigger the establishment of LSPs:

NOTE

LSPs can be set up only when each LSR along the LSP has a route exactly matching the FEC.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Step 3 Run:

```
lsp-trigger { all | host | ip-prefix prefix-name | none }
```

A policy for triggering the establishment of LSPs is configured. Any of the following policies can be configured:

- **host**: is the default policy and allows 32-bit host addresses to trigger LDP to establish LSPs.
- **all**: allows IGP routes to trigger LDP to establish LSPs. In addition, neither public network BGP routes or default routes trigger LDP to establish LSPs.
- **ip-prefix**: allows FECs filtered by an IP address prefix list to trigger LDP to establish LSPs.
- **none**: disables LDP from being triggered to establish LSPs.

NOTE

If the triggering policy is changed from **all** to **host**, the LSPs whose establishment is triggered by the host routes are not reestablished.

Step 4 Run:

```
commit
```

The configurations are committed.

----End

1.5.7 (Optional) Configuring a Policy for Triggering the Establishment of Transit LSPs

By configuring a policy for triggering the establishment of transit LSPs, you can use the routes that meet the specified requirements to trigger LDP to set up transit LSPs.

Context

After MPLS LDP is enabled, LDP LSPs are automatically set up. In this case, a large number of transit LSPs may be set up, which wastes resources. By configuring a policy for triggering the establishment of transit LSPs, you can allow the routes meeting the filtering requirements to trigger the establishment of transit LSPs, and restrain the local LSR from sending Label Mapping message of the routes not meeting the filtering requirements to the upstream peer. This can effectively reduce the number of LSPs and thus save network resources.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls ldp
```

The MPLS LDP view is displayed.

Step 3 Run:

```
propagate mapping for ip-prefix ip-prefix-name
```

A policy for triggering the establishment of transit LSPs is configured.

By default, when LDP sets up transit LSPs, no received routes are filtered.

Step 4 Run:

```
commit
```

The configurations are committed.

----End

1.5.8 Checking the Configuration

After an LDP LSP is successfully set up, you can view information about LDP and LDP LSPs, and LSPs.

Prerequisite

All configurations of an LDP LSP are complete.

Procedure

- Run the **display mpls ldp** [**all**] [**verbose**] command to check information about LDP.
- Run the **display mpls ldp lsp** [**all**] command to check information about LDP LSPs.
- Run the **display mpls lsp** [**verbose**] command to check information about LSPs.

----End

Example

After the configurations, run one of the preceding commands, and you can view the following results.

Run the **display mpls ldp** command, and you can view information about LDP.

```
<HUAWEI> display mpls ldp

                          LDP Global Information
------------------------------------------------------------------------------
 Protocol Version        : V1           Neighbor Liveness    : 600 Sec
 Graceful Restart        : Off          FT Reconnect Timer   : 300 Sec
 MTU Signaling           : On           Recovery Timer       : 300 Sec
                         LDP Instance Information
------------------------------------------------------------------------------
 Instance ID               : 0             VPN-Instance          :
 Instance Status           : Active        LSR ID                : 4.4.4.4
 Hop Count Limit           : 32            Path Vector Limit     : 32
 Loop Detection            : Off
 DU Re-advertise Timer     : 10 Sec        DU Re-advertise Flag  : Off
 DU Explicit Request       : Off           Request Retry Flag    : Off
```

```
 Label Distribution Mode    : Ordered        Label Retention Mode  : Liberal
 Graceful-delete            : Off            Graceful-delete Timer : 5 Sec
 Igp-sync-delay Timer       : 10 Sec
 Ipv6-family                : Off
 Local-ipv6-transport-address   :  ::2:2:2:2
------------------------------------------------------------------------------
```

Run the **display mpls ldp lsp** command or the **display mpls lsp** command, and you can view that an LDP LSP is successfully set up.

```
<HUAWEI> display mpls ldp lsp

 LDP LSP Information
 ------------------------------------------------------------------------------
 DestAddress/Mask   In/OutLabel    UpstreamPeer    NextHop          OutInterface
 ------------------------------------------------------------------------------
*1.1.1.1/32         Liberal/25                    DS/2.2.2.2
 1.1.1.1/32         3/NULL         2.2.2.2        127.0.0.1         Loop1
 2.2.2.2/32         NULL/3         -              10.1.1.2          Eth3/0/1
 2.2.2.2/32         16/3           2.2.2.2        10.1.1.2          Eth3/0/1
 3.2.1.0/24         NULL/3         -              10.1.1.2          Eth3/0/1
 3.2.1.0/24         17/3           2.2.2.2        10.1.1.2          Eth3/0/1
 3.3.1.0/24         NULL/3         -              10.1.1.2          Eth3/0/1
 3.3.1.0/24         18/3           2.2.2.2        10.1.1.2          Eth3/0/1
*10.1.1.0/24        Liberal/3                     DS/2.2.2.2
 10.1.1.0/24        3/NULL         2.2.2.2        10.1.1.1          Eth3/0/1
 10.2.1.0/24        NULL/3         -              10.1.1.2          Eth3/0/1
 10.2.1.0/24        19/3           2.2.2.2        10.1.1.2          Eth3/0/1
*10.5.1.0/24        Liberal/26                    DS/2.2.2.2
 10.5.1.0/24        3/NULL         2.2.2.2        10.5.1.1          Eth3/0/0
 10.6.1.0/24        3/NULL         2.2.2.2        10.6.1.1          Eth3/0/2
 ------------------------------------------------------------------------------
 TOTAL: 12 Normal LSP(s) Found.
 TOTAL: 3 Liberal LSP(s) Found.
 TOTAL: 0 Frr LSP(s) Found.
 A '*' before an LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stale
 A '*' before a UpstreamPeer means the session is in GR state
 A '*' before a DS means the session is in GR state
 A '*' before a NextHop means the LSP is FRR LSP
<HUAWEI> display mpls lsp
------------------------------------------------------------------------------
                LSP Information: LDP LSP
------------------------------------------------------------------------------
FEC                In/Out Label  In/Out IF                     Vrf Name
3.3.3.9/32         NULL/1025     -/Pos1/0/0
```

1.6 Configuring Static BFD to Detect an LDP LSP

By configuring static BFD to detect an LDP LSP, you can detect faults on the LDP LSP.

Applicable Environment

BFD implements fast detection at the millisecond level. If you need to fast determine whether LDP LSPs are faulty, you can establish BFD sessions.

When configuring static BFD to detect an LDP LSP, note the following points:

- You can bind a BFD session to an LDP LSP only on the ingress.
- A maximum number of 16 BFD sessions are bound to an LDP LSP.
- The LDP LSP can be set up only through the triggering of host routes.

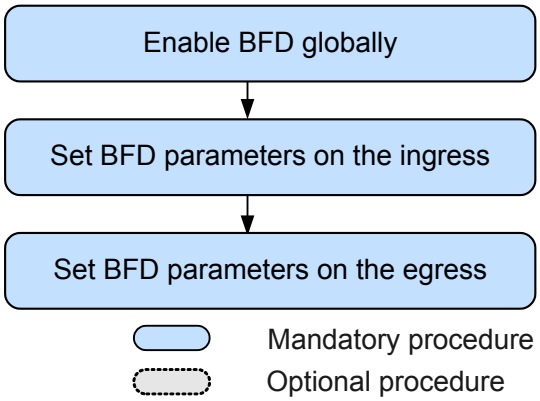
Pre-configuration Tasks

Before configuring static BFD to detect an LDP LSP, complete the following tasks:

- Configuring network layer parameters to ensure that the network layer is reachable
- Enabling MPLS LDP on each node and setting up an LDP session
- Configuring an LDP LSP

Configuration Procedures

Figure 1-5 Flowchart of configuring static BFD to detect an LSP LSP



Related Tasks

1.12.5 Example for Configuring Static BFD for LDP LSP

1.6.1 Enabling BFD Globally

BFD must be enabled globally before configurations relevant to BFD are performed.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bfd
```

BFD is enabled globally on the local node and the BFD view is displayed.

Configurations relevant to BFD can be performed only after the **bfd** command is run globally.

Step 3 Run:

```
commit
```

The configurations are committed.

----End

1.6.2 Setting BFD Parameters on the Ingress

By setting BFD parameters on the ingress, you can set up a BFD session to detect an LDP LSP.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bfd session-name bind ldp-lsp peer-ip ip-address [ nexthop ip-address [ interface interface-type interface-number ] ]
```

A BFD session is bound to a dynamic LSP.

Step 3 Run:

```
discriminator local discr-value
```

The local discriminator of the BFD session is created.

Step 4 Run:

```
discriminator remote discr-value
```

The remote discriminator of the BFD session is created.

NOTE

The local discriminators and remote discriminators of the two ends on a BFD session must be correctly associated. That is, the local discriminator of the local device and the remote discriminator of the remote device are the same, and the remote discriminator of the local device and the local discriminator of the remote device are the same. Otherwise, the BFD session cannot be correctly set up. In addition, the local and remote discriminators cannot be modified after being successfully configured.

Step 5 (Optional) Run:

```
min-tx-interval interval
```

The local minimum interval for sending BFD packets is set.

By default, the minimum interval for sending BFD control packets is 10 ms.

When the reverse tunnel is an IP link, the local parameters cannot be configured.

Actual local interval for sending BFD packets = MAX { Local sending interval, Remote receiving interval }

Actual local interval for receiving BFD packets = MAX { Remote sending interval, Local receiving interval }

Local detection interval = Local receiving interval x Remote BFD detection multiplier

For example: assume that the locally-configured interval for sending BFD packets is 200 ms, the interval for receiving BFD packets is 300 ms, the detection multiplier is 4, and the remotely-configured interval for sending BFD packets is 100 ms, the interval for receiving BFD packets is 600 ms, the detection multiplier is 5.

- The actual local interval for sending BFD packets is 600 ms (MAX { 200 ms, 600 ms }), the actual local interval for receiving BFD packets is 300 ms (MAX { 100 ms, 300 ms }), and the detection interval is 1500 ms (300 ms x 5).

- The actual remote interval for sending BFD packets is 300 ms (MAX { 100 ms, 300 ms }), the actual remote interval for receiving BFD packets is 600 ms (MAX { 200 ms, 600 ms}), and the detection interval is 2400 ms (600 ms x 4).

Step 6 (Optional) Run:**min-rx-interval** *interval* The local minimum interval for receiving BFD packets is set.

By default, the minimum interval for receiving BFD control packets is 10 ms.

When the reverse tunnel is an IP link, the local parameters cannot be configured.

Step 7 (Optional) Run:

```
detect-multiplier multiplier
```

The local BFD detection multiplier is set.

By default, the value is 3.

Step 8 Run:

```
commit
```

The configurations are committed.

----End

1.6.3 Setting BFD Parameters on the Egress

By setting BFD parameters on the egress, you can set up a BFD session to detect an LDP LSP.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 The IP link, LSP, or TE tunnel can be used as the reverse tunnel to inform the ingress of a fault. If there is a reverse LSP or a TE tunnel, you need to use the reverse LSP or the TE tunnel; otherwise, you can choose an IP link. If the configured reverse tunnel requires BFD detection, you can configure a pair of BFD sessions for it. Perform one of the following configurations as required:

- For an IP link, run:

  ```
  bfd session-name bind peer-ip ip-address [ vpn-instance vpn-name ] [ source-ip ip-address ]
  ```

- For a dynamic LSP, run:

  ```
  bfd session-name bind ldp-lsp peer-ip ip-address [ nexthop ip-address [ interface interface-type interface-number ] ]
  ```

- For MPLS TE, run:

  ```
  bfd session-name bind mpls-te interface tunnel interface-number [ te-lsp ]
  ```

Step 3 Run:

```
discriminator local discr-value
```

The local discriminator of the BFD session is created.

Step 4 Run:

```
discriminator remote discr-value
```

The remote discriminator of the BFD session is created.

NOTE

The local discriminators and remote discriminators of the two ends on a BFD session must be correctly associated. That is, the local discriminator of the local device and the remote discriminator of the remote device are the same, and the remote discriminator of the local device and the local discriminator of the remote device are the same. Otherwise, the BFD session cannot be correctly set up. In addition, the local and remote discriminators cannot be modified after being successfully configured.

Step 5 (Optional) Run:

min-tx-interval *interval*

The local minimum interval for sending BFD packets is set.

By default, the minimum interval for sending BFD control packets is 10 ms.

When the reverse tunnel is an IP link, the local parameters cannot be configured.

Actual local interval for receiving BFD packets = MAX { Local sending interval, Remote receiving interval }.

Actual local interval for receiving BFD packets = MAX { Remote sending interval, Local receiving interval }

Local detection period = Local receiving interval x Remote BFD detection multiplier

For example: assume that the locally-configured interval for sending BFD packets is 200 ms, the interval for receiving BFD packets is 300 ms, the detection multiplier is 4, and the remotely-configured interval for sending BFD packets is 100 ms, the interval for receiving BFD packets is 600 ms, the detection multiplier is 5.

- The actual local interval for sending BFD packets is 600 ms (MAX { 200 ms, 600 ms }), the actual local interval for receiving BFD packets is 300 ms (MAX { 100 ms, 300 ms }), and the detection interval is 1500 ms (300 ms x 5).
- The actual remote interval for sending BFD packets is 300 ms (MAX { 100 ms, 300 ms }), the actual remote interval for receiving BFD packets is 600 ms (MAX { 200 ms, 600 ms}), and the detection interval is 2400 ms (600 ms x 4).

Step 6 (Optional) Run:

min-rx-interval *interval*

The local minimum interval for receiving BFD packets is set.

By default, the minimum interval for receiving BFD control packets is 10 ms.

When the reverse tunnel is an IP link, the local parameters cannot be configured.

Step 7 (Optional) Run:

detect-multiplier *multiplier*

The local BFD detection multiplier is set.

By default, the value is 3.

Step 8 Run:

commit

The configurations are committed.

----End

1.6.4 Checking the Configuration

After BFD is successfully configured to detect an LDP LSP, you can view the configurations of the BFD session such as the session type and status.

Prerequisite

The configurations of static BFD in detection of an LDP LSP are complete.

Procedure

- Run the **display bfd session** { **all** | **static** | **dynamic** | **discriminator** *discr-value* } [**verbose**] [**for-lsp**] command to check information about BFD sessions.
- Run the **display bfd statistics session** { **all** | **static** | **dynamic** | **discriminator** *discr-value* | **peer-ip** *peer-ip* } [**for-ip** | **for-lsp**] command to check information about BFD sessions.

----End

Example

```
<HUAWEI> display bfd session all verbose
--------------------------------------------------------------------------------
  (One Hop) State : Up                      Name : 1to4
--------------------------------------------------------------------------------
  Local Discriminator    : 1                Remote Discriminator   : 2
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type          : LDP_LSP
  Bind Session Type      : Static
  Bind Peer IP Address   : 4.4.4.9
  NextHop Ip Address     : 10.1.1.2
  Bind Interface         : Pos1/0/0
  Tunnel ID              : 0
  FSM Board Id           : 1                TOS-EXP                : 7
  Min Tx Interval (ms)   : 10               Min Rx Interval (ms)   : 10
  Actual Tx Interval (ms): 2000             Actual Rx Interval (ms): 2000
  Local Detect Multi     : 3                Detect Interval (ms)   : 30
  Echo Passive           : Disable          Acl Number             : -
  Destination Port       : 3784             TTL                    : 1
  Proc Interface Status  : Disable          Process PST            : Enable
  WTR Interval (ms)      : -                Local Demand Mode      : Disable
  Active Multi           : 3
  Last Local Diagnostic  : No Diagnostic
  Bind Application       : No Application Bind
  Session TX TmrID       : 94               Session Detect TmrID   : 95
  Session Init TmrID     : -                Session WTR TmrID      : -
  Session Echo Tx TmrID  : -
  Session Description    : -
--------------------------------------------------------------------------------

     Total UP/DOWN Session Number : 1/0
```

Run the **display bfd statistics session all** command, and you can view statistics about all BFD sessions.

```
<HUAWEI> display bfd statistics session all
--------------------------------------------------------------------------------
  State : Up                     Name : atob
--------------------------------------------------------------------------------
  Session Type                        : Static
  Bind Type                           : IP
  Local/Remote Discriminator          : 10/20
  Received Packets                    : 1710577
  Sent Packets                        : 1710593
```

```
  Received Bad Packets               : 0
  Sent Failed Packets                : 0
  Down Count                         : 0
  ShortBreak Count                   : 0
  Sent Lsp Ping Count                : 0
  Create Time                        : 2009/09/27 07:20:06
  Last Down Time                     : 0000/00/00 00:00:00
  Total Time From Last DOWN          : -D:--H:--M:--S
  Total Time From Create             : 0D:09H:03M:47S
------------------------------------------------------------------------------

     Total Session Number :  1
```

1.7 Configuring Synchronization Between LDP and IGP

By configuring synchronization between LDP and IGP, you can shorten traffic interruption when the traffic is switched from the backup link to the primary link and achieve the millisecond-level switchover.

Applicable Environment

You can configure synchronization between LDP and IGP to solve the problem of traffic loss after the primary LSP fails on the network where primary and backup links exist. The details are as follows:

- When the primary link fails, IGP traffic and LSP traffic are switched to the backup link. When the primary link recovers from a fault, LSP traffic is discarded because IGP converges faster than LDP and thus IGP traffic is switched to the primary LSP earlier than LDP traffic.
- When the primary link becomes normal and an LDP session between nodes along the primary link fails, LSP traffic is discarded because LSP traffic is switched from the primary link to the backup link, whereas IGP traffic is still transmitted through the primary link.

NOTE

IGP that supports synchronization with LDP includes OSPF and IS-IS.

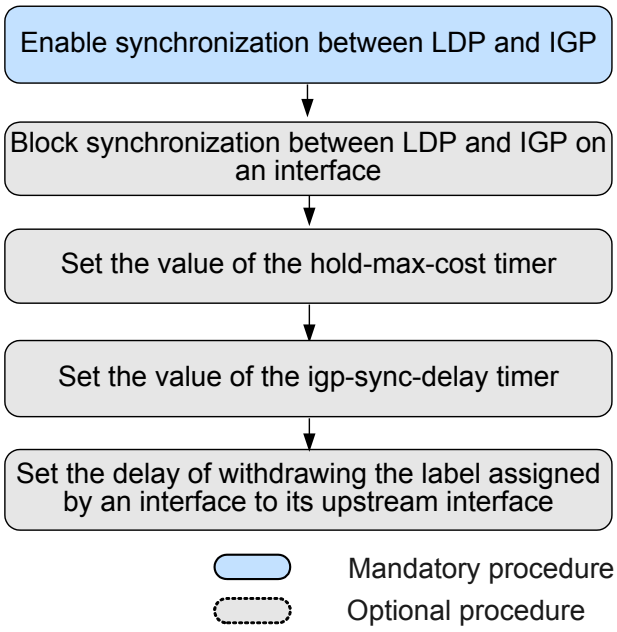
Pre-configuration Tasks

Before configuring synchronization between LDP and IGP, complete the following tasks:

- Configuring basic IGP (OSPF or IS-IS) functions
- Enabling MPLS globally and on each interface
- Enabling MPLS LDP globally and on each interface

Configuration Procedure

Figure 1-6 Flowchart for configuring synchronization between LDP and IGP



Related Tasks

1.12.6 Example for Configuring LDP-IGP Synchronization

1.7.1 Enabling LDP-IGP Synchronization

LDP-IGP synchronization needs to be enabled on interfaces on both ends of a link between a node where a primary LSP and a backup LSP diverge from each other and its LDP peer on the primary LSP. LDP-IGP synchronization is enabled either on an interface or in an IGP process.

Procedure

- Enable LDP-IGP synchronization in the interface view.

  If OSPF is used for IGP, do as follows on the interfaces on both ends of the link between the node where the primary LSP and the backup LSP diverge from each other and its LDP peer on the primary LSP:

  1. Run:

     system-view

     The system view is displayed.
  2. Run:

     interface *interface-type interface-number*

     The interface view is displayed.
  3. Run:

     ospf ldp-sync

     LDP-IGP synchronization is enabled on the protected interface.

If IS-IS is used, do as follows on the interfaces on both ends of the link between the node where the primary LSP and the backup LSP diverge from each other and its LDP peer on the primary LSP:

1. Run:
   system-view

   The system view is displayed.
2. Run:
   interface *interface-type interface-number*

   The interface view is displayed.
3. Run:
   isis enable *process-id*

   IS-IS is enabled.
4. Run:
   isis ldp-sync

   Synchronization between LDP and IS-IS is enabled on the protected interface.

- Enable LDP-IGP synchronization in an IGP process.

  If OSPF is used for IGP, do as follows on the interfaces on both ends of the link between the node where the primary LSP and the backup LSP diverge from each other and its LDP peer on the primary LSP:

  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     ospf [*process-id*]

     A specified OSPF process is started and the OSPF view is displayed.

     process-id specifies an OSPF process. If *process-id* is not specified, the default OSPF process ID of the system is 1. Run the **ospf** [*process-id* | **vpn-instance** *vpn-instance-name*] * command to associate an OSPF process with a VPN instance and run OSPF in the VPN instance. If a VPN instance is specified, the OSPF process belongs to the specified VPN instance. If no VPN instance is specified, the OSPF process belongs to a public network instance.
  3. Run:
     area *area-id*

     The OSPF area view is displayed.
  4. Run:
     ldp-sync enable

     LDP-IGP synchronization is enabled.
  5. Run:
     commit

     The configuration is committed.

  If IS-IS is used, do as follows on the interfaces on both ends of the link between the node where the primary LSP and the backup LSP diverge from each other and its LDP peer on the primary LSP:

1. Run:
   system-view

   The system view is displayed.
2. Run:
   isis [*process-id*]

   A specified IS-IS process is started and the IS-IS view is displayed.

   process-id specifies an IS-IS process. If *process-id* is not specified, the default IS-IS process ID of the system is 1. Run the **isis** [*process-id*] [**vpn-instance** *vpn-instance-name* | **vpn6-instance** *vpn6-instance-name*] * command to associate an IS-IS process with a VPN instance.
3. Run:
   ldp-sync enable

   LDP-IS-IS synchronization is enabled.
4. Run:
   commit

   The configuration is committed.

----End

1.7.2 (Optional)Blocking Synchronization Between LDP and IGP on an Interface

If you do not want to run synchronization between LDP and IGP on certain interfaces, you can block the function on these interfaces.

Context

After the **ldp-sync enable** command is run in an IGP process, the following situations occur:

- On a P2P network, the interfaces whose neighbor status is Up implement synchronization between LDP and IGP.
- On a broadcast network, if the IGP is OSPF, the interfaces (whose neighbor status is Up) connecting the DR and a non-DR (or BDR) implement synchronization between LDP and IGP; if the IGP is IS-IS, the interfaces (whose neighbor status is Up) connecting the DIS and a non-DIS implement synchronization between LDP and IGP.

For the interfaces on a device bearing key services, you must ensure that this device detours around the backup path. You can block synchronization between LDP and IGP on a specified interface of the NE5000E.

Procedure

- If OSPF is used for IGP, do as follows on the interfaces on both ends of the link between the node where the primary LSP and the backup LSP diverge from each other and its LDP peer on the primary LSP.
  1. Run:
     system-view

     The system view is displayed.

2. Run:
   interface *interface-type interface-number*

   The view of an OSPF interface is displayed.
3. Run:
   ospf ldp-sync block

   Synchronization between LDP and OSPF is blocked on the interface.
4. Run:
   commit

   The configuration is committed.

- If IS-IS is used for IGP, do as follows on the interfaces on both ends of the link between the node where the primary LSP and the backup LSP diverge from each other and its LDP peer on the primary LSP.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*

     The view of an IS-IS interface is displayed.
  3. Run:
     isis ldp-sync block

     Synchronization between LDP and IS-IS is blocked on the interface.
  4. Run:
     commit

     The configuration is committed.

----End

1.7.3 (Optional) Setting the Hold-max-cost Timer Value

When an LDP session on a primary LSP fails, traffic is transmitted along a backup LSP within the timeout period of the hold-max-cost timer before the LDP session on the primary LSP recovers.

Context

Select parameters based on networking requirements:

- If an IGP carries only LDP services, configure the parameter **infinite** to ensure that a selected IGP route is kept consistent with the LDP LSP.
- If an IGP carries multiple types of services including LDP services, set the value of the parameter *value* to ensure that a teardown of LDP sessions does not affect IGP route selection or other services.

Procedure

- If OSPF is used, do as follows on the interfaces on both ends of a link between a node where the primary LSP and the backup LSP diverge from each other and its LDP peer on the primary LSP:

1. Run:
   system-view

   The system view is displayed.
2. Run:
   interface *interface-type interface-number*

   The interface view is displayed.
3. Run:
   ospf timer ldp-sync hold-max-cost { *value* | **infinite** }

   The value of the hold-max-cost timer is set.

   The value of the hold-max-cost timer equals the interval at which the local node sends an LSA to advertise the maximum cost. The maximum cost is 65535.

   By default, the local device running an IGP keeps advertising the maximum cost by sending Link State PDUs (LSPs).

- If IS-IS is used, do as follows on the nodes of both ends of a link between a node where the primary LSP and the backup LSP diverge from each other and its LDP peer on the primary LSP:

  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     isis [*process-id*]

     A specified IS-IS process is restarted and the IS-IS view is displayed.
  3. Run:
     timer ldp-sync hold-max-cost { **infinite** | *interval* }

     The time is set for all interfaces in the IS-IS process take to wait for leaving the LDP-IGP synchronization state.

     By default, IS-IS keeps advertising the maximum cost by sending LSPs.

  Do as follows on the interfaces of both ends of a link between a node where the primary LSP and the backup LSP diverge from each other and the LDP peer on the primary LSP:

  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*

     The interface view is displayed.
  3. Run:
     isis timer ldp-sync hold-max-cost { *value* | **infinite** }

     The value of the hold-max-cost timer is set.

     The value of the hold-max-cost timer equals the interval at which the local node advertises the maximum cost in LSAs. The maximum cost is 16777213.

By default, an IGP keeps advertising the maximum cost in Link State PDUs.

----End

1.7.4 (Optional) Setting the Value of the igp-sync-delay Timer

When an LDP session is re-established on a faulty link, LDP starts the igp-sync-delay timer to wait for the establishment of an LSP. After the igp-sync-delay timer times out, LDP notifies the IGP that synchronization between LDP and IGP is complete.

Procedure

- Do as follows in the MPLS LDP view.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     mpls ldp

     The MPLS LDP view is displayed.
  3. Run:
     igp-sync-delay timer *value*

     The value of the igp-sync-delay timer is set.

     By default, the value of the delay timer is 10s.
- Do as follows in the interface view.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*

     The interface view is displayed.
  3. Run:
     mpls ldp timer igp-sync-delay *value*

     The value of the igp-sync-delay timer is set.

----End

1.7.5 (Optional) Setting the Delay Time for Withdrawing an Upstream Label

To prevent traffic interruption after LDP traffic is switched to the backup LSP, you can set the delay time for withdrawing upstream labels

Context

After LDP-IGP is enabled on an LDP device and an LDP session on the LDP device becomes Down, the LDP device withdraws a label assigned to its upstream device, and then deletes the entire LSP. After LDP traffic is switched to a backup LSP, the primary LSP needs to be re-established. As a result, the duration of traffic interruption is long.

Delaying the withdrawal of a label assigned to an upstream device ensures that LDP does not withdraw the upstream label during IGP convergence. This prevents traffic interruption.

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Run:

mpls ldp

The MPLS LDP view is displayed.

Step 3 Run:

graceful-delete timer

The delay time for withdrawing an upstream label is set.

The default delay time is 2 seconds.

----End

1.7.6 Checking the Configuration

After configuring synchronization between LDP and IGP on an interface, you can view the synchronization status of interfaces enabled with synchronization between LDP and IGP.

Prerequisite

All configurations of synchronization between LDP and IGP are complete.

Procedure

- Run the **display mpls ldp** command to check the global LDP configuration.
- Run the **display isis** [*process-id* | **vpn-instance** *vpn-instance-name*] **ldp-sync interface** command to check synchronization status of interfaces configured with synchronization between LDP and IS-IS.
- Run the **display ospf ldp-sync interface** { **all** | *interface-type interface-number* } command to check synchronization status of interfaces configured with synchronization between LDP and OSPF.

----End

Example

Run the **display mpls ldp** command, and you can view the time of waiting for the establishment of the LSP after the LDP session is set up and the delay of withdrawing the label assigned by an interface to its upstream interface after the LDP session becomes Down.

```
<HUAWEI> display mpls ldp

                          LDP Global Information
------------------------------------------------------------------------------
 Protocol Version        : V1           Neighbor Liveness    : 600 Sec
 Graceful Restart        : Off          FT Reconnect Timer   : 300 Sec
 MTU Signaling           : On           Recovery Timer       : 300 Sec
```

```
                        LDP Instance Information
------------------------------------------------------------------------------
 Instance ID               : 0              VPN-Instance          :
 Instance Status           : Active         LSR ID                : 4.4.4.4
 Hop Count Limit           : 32             Path Vector Limit     : 32
 Loop Detection            : Off
 DU Re-advertise Timer     : 10 Sec         DU Re-advertise Flag  : Off
 DU Explicit Request       : Off            Request Retry Flag    : Off
 Label Distribution Mode   : Ordered        Label Retention Mode  : Liberal
 Graceful-delete           : Off            Graceful-delete Timer : 5 Sec
 Igp-sync-delay Timer      : 10 Sec
 Ipv6-family               : Off
 Local-ipv6-transport-address   :  ::2:2:2:2
------------------------------------------------------------------------------
```

Run the **display ospf ldp-sync interface** { **all** | *interface-type interface-number* } command, and you can find that the interface status becomes **Sync-Achieved**.

```
<HUAWEI> display ospf ldp-sync interface Pos 1/0/0
 Interface gigabitethernet1/0/0
 HoldMaxCost Timer: 50
 LDP State: Up             OSPF Sync State: Sync-Achieved
```

Run the **display isis ldp-sync interface** command, and you can find that the interface status becomes **Sync-Achieved**.

```
<HUAWEI> display isis ldp-sync interface
             Ldp Sync interface information for ISIS( 1 )
------------------------------------------------------------------------
Interface              HoldMaxCostTimer   LDP State   Sync State
------------------------------------------------------------------------
GigabitEthernet1/0/0   infinite           Down        Sync-Achieved
------------------------------------------------------------------------
```

1.8 Configuring the LDP GR Helper

You can configure a device to function as a GR Helper to help a neighbor with the LDP GR process.

Applicable Environment

In LDP GR, a Restarter, with the help of the Helper, ensures uninterrupted forwarding during the active main board/standby main board (AMB/SMB) switchover or on the Restarter.

Without GR, during the AMB/SMB switchover or the upgrade of the system, the peers may delete LSPs because an LDP session goes Down. This causes short-time traffic interruption. With LDP GR, you can ensure that the labels are the same after the exceptional master/slave switchover or restart of a protocol. In addition, the LDP session and LSP can be restored after the AMB/SMB switchover or system upgrade. In this manner, the MPLS forwarding is uninterrupted.

By default, NSR is adopted on a device installed with double main control boards.

NOTE

Currently, LDP supports only the GR Helper.

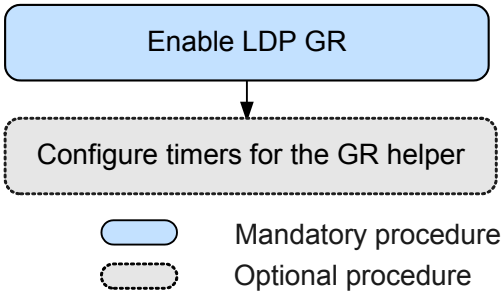
Pre-configuration Tasks

Before configuring LDP GR, complete the following tasks:

- Configuring IGP GR
- Configuring a local LDP session

Configuration Procedures

Figure 1-7 Flowchart of the LDP GR configuration



Related Tasks

1.12.7 Example for Configuring LDP GR

1.8.1 Enabling LDP GR

You need to enable LDP GR on both the GR Restarter and the GR Helper.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls ldp
```

LDP is enabled on the local LSR and the MPLS LDP view is displayed.

Step 3 Run:

```
graceful-restart
```

LDP GR is enabled.

By default, LDP GR is disabled.

NOTE

- Enabling or disabling LDP GR can lead reestablishment of an LDP session.
- During the LDP GR, the **undo mpls ldp** command and the **reset mpls ldp** command cannot be run.

Step 4 Run:

```
commit
```

The configurations are committed.

----End

1.8.2 (Optional) Configuring Timers for the GR Helper

By configuring timers for the GR Helper, you can set the values of an LDP Reconnect timer and an LDP Recovery timer.

Context

Timers associated with LDP GR are as follows:

- Reconnect timer: indicates the timer for reconnecting an LDP session. After the master/slave switchover on the GR Restarter, the GR Helper detects that the LDP session between the GR Helper and the GR Restarter fails to be set up. In this case, the GR Helper starts a Reconnect timer to wait for reestablishing an LDP session.
  - If an LDP session is not set up between the GR Helper and GR Restarter after the Reconnect timer expires, the GR Helper immediately deletes the MPLS forwarding entries associated with the GR Restarter and exits from the GR process.
  - If the LDP session is reestablished before the Reconnect timer expires, the GR Helper deletes the Reconnect timer and starts a Recovery timer.
- Recovery timer: indicates the timer for restoring an LSP. After the LDP session is reestablished, the GR Helper starts a Recovery timer to wait for the LSP to be restored.
  - If the Recovery timer expires, the GR Helper regards that the neighbor GR process ends and then deletes the LSP that is not restored.
  - If all LSPs are restored before the Recovery timer expires, the GR Helper regards the neighbor GR process ends after the Recovery timer expires.
- Neighbor-liveness timer: indicates the duration of the LDP GR process.

NOTE

Modifying the value of an LDP GR-associated timer leads to the reestablishment of an LDP session.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls ldp
```

The MPLS LDP view is displayed.

Step 3 Run:

```
graceful-restart timer reconnect timer
```

The value of a Reconnect timer is set.

The value of the Reconnect timer that takes effect is the smaller value between the Neighbor-liveness timer set on the GR Helper and the Reconnect timer set on the GR Restarter.

By default, the Reconnect timer is set to 300 seconds.

Step 4 Run:

```
graceful-restart timer recovery timer
```

The value of a Recovery timer is set.

The value of the Recovery timer that takes effect is the smaller value between the Recovery timer set on the GR Helper and the Recovery timer set on the GR Restarter.

By default, the Recovery timer is set to 300 seconds.

Step 5 Run:

graceful-restart timer neighbor-liveness *timer*

The value of a Neighbor-liveness timer is set.

When the reconnection time of an LDP session is negotiated in an LDP GR process, the value of the Neighbor-liveness timer is the smaller value between the Neighbor-liveness timer set on the GR Helper and the Reconnect timer set on the GR Restarter.

By default, the Neighbor-liveness is set to 600 seconds.

Step 6 Run:

commit

The configurations are committed.

----End

1.8.3 Checking the Configuration

After the configurations of LDP GR, you can view information about the LDP protocol, and the LDP session.

Procedure

- Run the **display mpls ldp** [**all**] [**verbose**] command to check information about LDP.
- Run the **display mpls ldp session** [**all**] [**verbose**] command to check information about LDP sessions.

----End

Example

After the configurations, run one of the preceding commands, and you can view the following results:

- Run the **display mpls ldp** command, and you can view that the GR status is On, which indicates that LDP GR is enabled.

```
<HUAWEI> display mpls ldp

                          LDP Global Information
------------------------------------------------------------------------------
 Protocol Version        : V1           Neighbor Liveness    : 600 Sec
 Graceful Restart        : On           FT Reconnect Timer   : 300 Sec
 MTU Signaling           : On           Recovery Timer       : 300 Sec
                         LDP Instance Information
------------------------------------------------------------------------------
 Instance ID               : 0              VPN-Instance          :
 Instance Status           : Active         LSR ID                : 4.4.4.4
 Hop Count Limit           : 32             Path Vector Limit     : 32
 Loop Detection            : Off
 DU Re-advertise Timer     : 10 Sec         DU Re-advertise Flag  : Off
 DU Explicit Request       : Off            Request Retry Flag    : Off
 Label Distribution Mode   : Ordered        Label Retention Mode  : Liberal
 Graceful-delete           : Off            Graceful-delete Timer : 5 Sec
 Igp-sync-delay Timer      : 10 Sec
```

```
 Ipv6-family                : Off
 Local-ipv6-transport-address   :  ::2:2:2:2
--------------------------------------------------------------------------
```

- Run the **display mpls ldp session verbose** command, and you can view the value of the Session FT Flag field is On.

```
              LDP Session(s) in Public Network
------------------------------------------------------------------------------
Peer LDP ID     : 5.5.5.5:0        Local LDP ID   : 3.3.3.3:0
TCP Connection  : 3.3.3.3 <- 5.5.5.5
Session State   : Operational          Session Role   : Passive
Session FT Flag : On                   MD5 Flag       : Off
Reconnect Timer : 300 Sec              Recovery Timer : 300 Sec
Negotiated Keepalive Timer        : 45 Sec
Keepalive Message Sent/Rcvd       : 5387/5388 (Message Count)
Label Advertisement Mode          : Downstream Unsolicited
Label Resource Status(Peer/Local) : Available/Available
Session Age                       : 000:22:28  (DDD:HH:MM)
Addresses received from peer: ( Count: 2 )
 5.5.5.5             10.2.1.2
------------------------------------------------------------------------------
```

1.9 Configuring LDP over TE

The LDP over TE function is applicable to the network where core devices support TE whereas edge devices support LDP. In this case, a TE tunnel functions as one hop of the entire LDP LSP.

Applicable Environment

LDP over TE is a technology through which LDP LSPs can be set up across an RSVP TE domain and provide services for a VPN. According to existing VPN applications, to carry out MPLS TE, a carrier has difficulties in deploying TE on an entire network. In this situation, as shown in **Figure 1-1**, the carrier can plan a core area where TE is deployed, and implement LDP on PEs at the edge of the TE area.

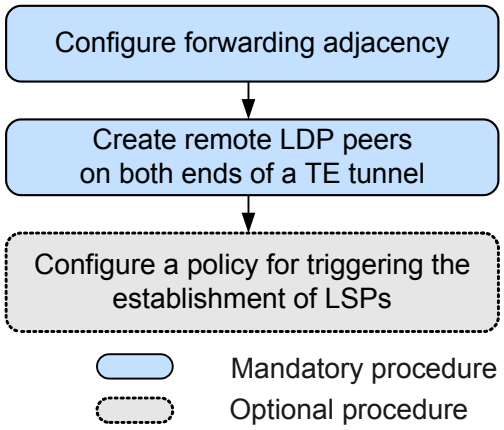
Pre-configuration Tasks

Before configuring LDP over TE, complete the following tasks:

- Configuring an IGP to ensure connectivity between LSRs on the network layer
- Enabling MPLS on each LSR and interface
- Enabling MPLS LDP on each LSR at the edge of the TE area and each interface outside the TE area
- Setting up an RSVP-TE tunnel along the TE nodes
- Assign an IP address to the tunnel and configure IGP to advertise the route
- Configuring virtual TE interfaces

Configuration Procedures

Figure 1-8 Flowchart of the LDP over TE configuration



Related Tasks

1.12.8 Example for Configuring LDP over TE

1.9.1 Configuring Forwarding Adjacency

The forwarding adjacency is configured on the ingress of a CR-LSP. The forwarding adjacency allows a route of a CR-LSP to be advertised to neighbors so that these neighbors can use this CR-LSP.

Context

A routing protocol performs bidirectional detection on a link. The forwarding adjacency needs to be enabled on both ends of a tunnel. The forwarding adjacency allows a node to advertise a CR-LSP route to other nodes. Another tunnel for transferring data packets in the reverse direction needs to be configured.

NOTE

MPLS LDP must be enabled on the tunnel interface view before the forwarding adjacency is enabled.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The view of the MPLS TE tunnel interface is displayed.

Step 3 Run:

```
mpls te igp advertise [ hold-time value ]
```

The forwarding adjacency is configured.

By default, the forwarding adjacency is disabled.

Step 4 Run:

```
mpls te igp metric { absolute | relative } value
```

The IGP metric value of the MPLS TE tunnel is configured.

NOTE

A proper IGP metric value ensures that the CR-LSP route is advertised and used correctly. The metric value of a CR-LSP must be smaller than the metric value of an unwanted IGP route.

Step 5 Run:

```
quit
```

The system view is displayed.

Step 6 Run:

```
ospf [ process-id ]
```

The OSPF view is displayed.

Step 7 Run:

```
enable traffic-adjustment advertise
```

The forwarding adjacency is enabled in the OSPF process.

Step 8 Run:

```
commit
```

The configuration is committed.

----End

1.9.2 Creating Remote LDP Peers on Both Ends of a TE Tunnel

You need to configure both ends of a TE tunnel as remote LDP peers.

Context

NOTE

- The virtual interfaces on the TE tunnel must be enabled with LDP.
- If the destination address of the TE tunnel is not the LSR ID of the egress, the interface with the destination address must be enabled with LDP.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls ldp remote-peer remote-peer-name
```

The remote MPLS LDP peer view is displayed.

Step 3 Run:

```
remote-ip ip-address
```

An IP address is assigned to the remote LDP peer.

Step 4 Run:

```
commit
```

The configurations are committed.

----End

1.9.3 (Optional) Configuring a Policy for Triggering the Establishment of LSPs

By configuring a policy for triggering the establishment of up LSPs, you can use eligible routes to trigger LDP to set up LSPs.

Context

To set up ingress LSPs and egress LSPs on a public network, you can use one of the following policies to use eligible routes to trigger the establishment of LSPs:

NOTE

LSPs can be set up only when each LSR along the LSP has a route exactly matching the FEC.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Step 3 Run:

```
lsp-trigger { all | host | ip-prefix prefix-name| none }
```

A policy for triggering the establishment of LSPs is configured.

- By default, the triggering policy is **host**, indicating that 32-bit host IP routes trigger LDP to set up LSPs.
- If the triggering policy is **all**, it indicates that all static routes or IGP routes trigger LDP to set up LSPs. The Border Gateway Protocol (BGP) routes, however, cannot trigger LDP to set up LSPs.
- If the triggering policy is **ip-prefix**, it indicates that only the forwarding equivalence class (FEC) entries filtered through an IP prefix list can trigger LDP to set up LSPs.
- If the triggering policy is **none**, LDP is not triggered to set up LSPs.

NOTE

If the triggering policy is changed from **all** to **host**, the LSPs whose establishment is triggered by the host routes are not reestablished.

Step 4 Run:

```
commit
```

The configurations are committed.

----End

1.9.4 Checking the Configuration

After the configurations of LDP over TE, you can view information about an LDP LSP on the ingress.

Prerequisite

All configurations of LDP over TE are complete.

Procedure

- Run the **display mpls ldp lsp** [*destination-address mask-length*] command to check information about the LDP LSP on the ingress node.

----End

Example

After the configurations, run the preceding command, and you can view the following results:

Run the **display mpls ldp lsp** command on the ingress of the LDP LSP, and you can view that the outgoing interface of the TE tunnel.

```
<HUAWEI> display mpls ldp lsp

 LDP LSP Information
 -------------------------------------------------------------------------------
 DestAddress/Mask   In/OutLabel    UpstreamPeer    NextHop          OutInterface
 -------------------------------------------------------------------------------
*1.1.1.1/32         Liberal/25                    DS/2.2.2.2
 1.1.1.1/32         3/NULL         2.2.2.2        127.0.0.1         Loop1
 2.2.2.2/32         NULL/3         -              10.1.1.2          Eth3/0/1
 2.2.2.2/32         16/3           2.2.2.2        10.1.1.2          Tunnel1
 3.2.1.0/24         NULL/3         -              10.1.1.2          Eth3/0/1
 3.2.1.0/24         17/3           2.2.2.2        10.1.1.2          Eth3/0/1
 3.3.1.0/24         NULL/3         -              10.1.1.2          Eth3/0/1
 3.3.1.0/24         18/3           2.2.2.2        10.1.1.2          Eth3/0/1
*10.1.1.0/24        Liberal/3                     DS/2.2.2.2
 10.1.1.0/24        3/NULL         2.2.2.2        10.1.1.1          Eth3/0/1
 10.2.1.0/24        NULL/3         -              10.1.1.2          Eth3/0/1
 10.2.1.0/24        19/3           2.2.2.2        10.1.1.2          Eth3/0/1
*10.5.1.0/24        Liberal/26                    DS/2.2.2.2
 10.5.1.0/24        3/NULL         2.2.2.2        10.5.1.1          Eth3/0/0
 10.6.1.0/24        3/NULL         2.2.2.2        10.6.1.1          Eth3/0/2
 -------------------------------------------------------------------------------
 TOTAL: 12 Normal LSP(s) Found.
 TOTAL: 3 Liberal LSP(s) Found.
 TOTAL: 0 Frr LSP(s) Found.
 A '*' before an LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stale
 A '*' before a UpstreamPeer means the session is in GR state
 A '*' before a DS means the session is in GR state
 A '*' before a NextHop means the LSP is FRR LSP
```

1.10 Configuring the Mode in Which the TTL Field in an IP Packet or an MPLS Packet Is Processed

When an IP packet enters an MPLS domain, you need to set the mode in which the TTL field in the IP packet is processed. When an MPLS packet enters an IP network, you also need to set the mode in which the TTL field in the MPLS packet is processed.

1.10.1 Establishing the Configuration Task

Before setting the mode in which the TTL field in an IP packet or an MPLS packet is processed, familiarize yourself with the applicable environment, pre-configuration tasks, and required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

By default, the NE5000E processes the TTL field by the following means:

- When an IP packet enters an MPLS domain, the ingress copies the IP TTL to the MPLS TTL.
- When an MPLS packet leaves the MPLS domain, the egress or the penultimate hop copies the MPLS TTL to the IP TTL.

In an actual MPLS network, there may be multiple devices of other vendors that do not process the TTL filed. In this case, you need to adjust the TTL processing mode on the NE5000E based on the configuration of the devices of other vendors. The rules are as follows:

- If the ingress is not enabled with the TTL copy function, that is, it does not copy the IP TTL to the MPLS TTL but directly uses the MPLS TTL (255), you need to disable the TTL copy function on the egress or the penultimate hop.
- If the ingress is enabled with the TTL copy function, you need to enable the TTL copy function on the egress or the penultimate hop.
- If the TTL copy function is disabled on the egress or the penultimate hop, you need to disable the TTL copy function on the ingress.
- If the TTL copy function is enabled on the egress or the penultimate hop, you need to enable the TTL copy function the ingress.

Pre-configuration Tasks

Before setting the mode in which the TTL field in an IP packet or an MPLS packet is processed, complete the following task:

- Configuring MPLS

Data Preparation

To setting the mode in which the TTL field in an IP packet or an MPLS packet is processed, you need the following data.

No.	Data
1	Path in which an ICMP response packet is returned

1.10.2 Configuring the Mode in Which the TTL Field in an IP Packet or an MPLS Packet Is Processed

In an MPLS domain, the TTL processing modes must be the same on the ingress, egress, and penultimate hop.

Context

To prevent routing loops in IP networks, the TTL field is defined in an IP packet. In the same way, to prevent routing loops in MPLS networks, the TTL field is defined in an MPLS packet. When an IP packet is transmitting across an MPLS domain, the processing modes of the IP TTL and MPLS TTL need to be taken into consideration.

- If the ingress is not enabled with the TTL copy function, that is, it does not copy the IP TTL to the MPLS TTL but directly uses the MPLS TTL (255), you need to disable the TTL copy function on the egress or the penultimate hop.
- If the ingress is enabled with the TTL copy function, you need to enable the TTL copy function on the egress or the penultimate hop.
- If the TTL copy function is disabled on the egress or the penultimate hop, you need to disable the TTL copy function on the ingress.
- If the TTL copy function is enabled on the egress or the penultimate hop, you need to enable the TTL copy function on the ingress.

Procedure

- Run:
  ```
  system-view
  ```
  The system view is displayed.
- Run:
  ```
  mpls
  ```
  The MPLS view is displayed.
- Run:
  ```
  ttl ip-mpls propagate
  ```
  The TTL processing mode is set.

  By default, the TTL copy function is enabled. In actual networking, the TTL processing modes must be the same on the ingress, egress, and penultimate hop.

----End

1.11 Maintaining MPLS LDP

This section describes how to maintain MPLS LDP, including resetting LDP and detecting the connectivity of an LSP.

1.11.1 Resetting LDP

Resetting LDP makes new configurations take effect.

Context

CAUTION

Resetting LDP affects the establishment of an LSP. You must confirm whether to reset LDP before running a reset command.

Procedure

- To reset all LDP peers in global LDP instances, run the **reset mpls ldp** command in the user view to validate new configurations.
- To reset a specified LDP peer, run the **reset mpls ldp peer** *peer-id* command in the user view to validate new configurations.
- To reset all GR-capable LDP peers in global LDP instances, run the **reset mpls ldp graceful** command in the user view to validate new configurations, achieving non-interrupted service transmission during a restart.
- To reset a specified GR-capable LDP peer, run the **reset mpls ldp peer** *peer-id* **graceful** command in the user view to validate new configurations, achieving non-interrupted service transmission during a restart.

----End

1.11.2 Detecting Connectivity and Reachability of an LSP

By running a ping or tracert command, you can detect connectivity and reachability of an LSP.

Context

Run one of the following commands to perform MPLS ping or MPLS tracert detection.

Procedure

- Run the **ping lsp** [**-a** *source-ip* | **-c** *count* | **-exp** *exp-value* | **-h** *ttl-value* | **-m** *interval* | **-r** *reply-mode* | **-s** *packet-size* | **-t** *time-out* | **-v**] * **ip** *destination-address mask-length* [*ip-address*] command in any view to perform MPLS ping detection.
- Run the **tracert lsp** [**-a** *source-ip* | **-exp** *exp-value* | **-h** *ttl-value* | **-r** *reply-mode* | **-t** *time-out*] * { **ip** *destination-address mask-length* [*ip-address*] command in any view to perform MPLS tracert detection.

----End

1.12 Configuration Examples

The following sections provide configuration examples for configuring MPLS LDP. Familiarize yourself with the configuration procedures against the networking diagram. Each configuration

example consists of the networking requirements, configuration notes, configuration roadmap, configuration procedures, and configuration files.

1.12.1 Example for Configuring Local LDP Sessions

This section provides an example for configuring local LDP sessions, including enabling MPLS and MPLS LDP on each LSR and interface.

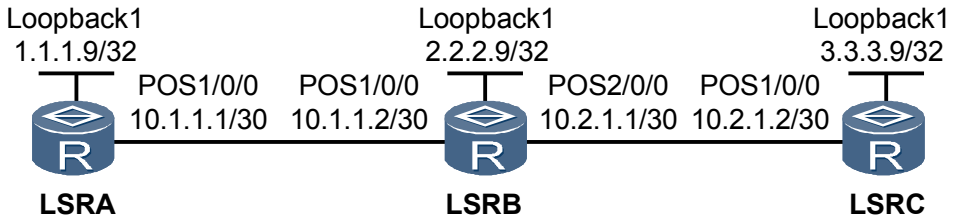
Networking Requirements

CAUTION

On a single NE5000E, an interface is numbered in the format of slot number/card number/interface number. On an NE5000E cluster, the interface is numbered in the format of chassis ID/slot number/card number/interface number. This requires the chassis ID to be specified along with the slot number.

As shown in **Figure 1-9**, all of LSR A, LSR B, and LSR C function as core devices or edge devices on a backbone network. To deploy MPLS LDP services on the backbone network, you need to configure local LDP sessions. After local LDP sessions are set up between LSR A and LSR B, and between LSR B and LSR C, each pair of LSRs can distribute labels to each other and then LDP LSPs can be set up.

Figure 1-9 Networking diagram of configuring local LDP sessions



Configuration Notes

When configuring local LDP sessions, note the following:

- An LSR ID must be configured before you run other MPLS commands.
- An LSR ID of an LSR must be manually configured because no default LSR ID is available.
- It is recommended that the IP address of a reachable loopback interface on an LSR be configured as the LSR ID.

Configuration Roadmap

The configuration roadmap is as follows:

1. Assign an IP address to each interface, and configure OSPF to advertise the route to the segment of each interface and the host route to each LSR ID.
2. Enable MPLS and MPLS LDP globally on each LSR.
3. Enable MPLS on interfaces of each LSR.
4. Enable MPLS LDP on the interfaces of both ends of each local LDP session.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each interface on each LSR as shown in **Figure 1-9**, OSPF process ID, and OSPF area ID
- LSR ID of each LSR

Procedure

Step 1 Assign an IP address to each interface, and configure OSPF to advertise the route to the segment of each interface and the host route to each LSR ID.

According to **Figure 1-9**, assign an IP address to each interface, including the loopback interface, and configure OSPF to advertise the route to the segment of each interface and the host route to each LSR ID. The configuration details are not mentioned here.

Step 2 Enable MPLS and MPLS LDP globally on each LSR.

Configure LSR A.

```
<LSRA> system-view
[~LSRA] mpls lsr-id 1.1.1.9
[~LSRA] mpls
[~LSRA-mpls] quit
[~LSRA] mpls ldp
[~LSRA-mpls-ldp] commit
[~LSRA-mpls-ldp] quit
```

Configure LSR B.

```
<LSRB> system-view
[~LSRB] mpls lsr-id 2.2.2.9
[~LSRB] mpls
[~LSRB-mpls] quit
[~LSRB] mpls ldp
[~LSRB-mpls-ldp] commit
[~LSRB-mpls-ldp] quit
```

Configure LSR C.

```
<LSRC> system-view
[~LSRC] mpls lsr-id 3.3.3.9
[~LSRC] mpls
[~LSRC-mpls] quit
[~LSRC] mpls ldp
[~LSRC-mpls-ldp] commit
[~LSRC-mpls-ldp] quit
```

Step 3 Enable MPLS and MPLS LDP on the interfaces of each LSR.

Configure LSR A.

```
[~LSRA] interface pos 1/0/0
[~LSRA-Pos1/0/0] mpls
[~LSRA-Pos1/0/0] mpls ldp
```

```
[~LSRA-Pos1/0/0] commit
[~LSRA-Pos1/0/0] quit
```

Configure LSR B.

```
[~LSRB] interface pos 1/0/0
[~LSRB-Pos1/0/0] mpls
[~LSRB-Pos1/0/0] mpls ldp
[~LSRB-Pos1/0/0] commit
[~LSRB-Pos1/0/0] quit
[~LSRB] interface pos 2/0/0
[~LSRB-Pos2/0/0] mpls
[~LSRB-Pos2/0/0] mpls ldp
[~LSRB-Pos2/0/0] commit
[~LSRB-Pos2/0/0] quit
```

Configure LSR C.

```
[~LSRC] interface pos 1/0/0
[~LSRC-Pos1/0/0] mpls
[~LSRC-Pos1/0/0] mpls ldp
[~LSRC-Pos1/0/0] commit
[~LSRC-Pos1/0/0] quit
```

Step 4 Verify the configuration.

After the configuration, run the **display mpls ldp session** command on an LSR. You can view that the status of the local LDP session between LSR A and LSR B, or between LSR B and LSR C is **Operational**.

Take the display on LSR A as an example.

```
<LSRA> display mpls ldp session

 LDP Session(s) in Public Network
 Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDD:HH:MM)
 A '*' before a session means the session is being deleted.
------------------------------------------------------------------------------
 PeerID             Status      LAM  SsnRole  SsnAge       KASent/Rcv
------------------------------------------------------------------------------
2.2.2.9:0          Operational DU   Passive  0000:00:22  91/91
------------------------------------------------------------------------------
TOTAL: 1 Session(s) Found.
```

----End

Configuration Files

- Configuration file of LSR A

```
#
sysname LSRA
#
mpls lsr-id 1.1.1.9
#
mpls
#
mpls ldp
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.1.1.1 255.255.255.252
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
```

```
ospf 1
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.3
#
return
```

- Configuration file of LSR B

```
#
sysname LSRB
#
mpls lsr-id 2.2.2.9
#
mpls
#
mpls ldp
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.1.1.2 255.255.255.252
 mpls
 mpls ldp
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.2.1.1 255.255.255.252
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 2.2.2.9 0.0.0.0
  network 10.1.1.0 0.0.0.3
  network 10.2.1.0 0.0.0.3
#
return
```

- Configuration file of LSR C

```
#
sysname LSRC
#
mpls lsr-id 3.3.3.9
#
mpls
#
mpls ldp
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.2.1.2 255.255.255.252
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 3.3.3.9 0.0.0.0
  network 10.2.1.0 0.0.0.3
#
return
```

Related Tasks

1.3.2 Configuring a Local LDP Session

1.12.2 Example for Configuring a Remote LDP Session

This section describes how to configure a remote LDP session. A remote LDP session applies to VPN services.

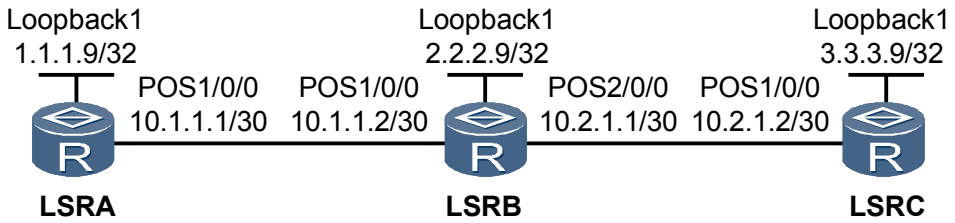
Networking Requirements

CAUTION

On a single NE5000E, an interface is numbered in the format of slot number/card number/interface number. On an NE5000E cluster, the interface is numbered in the format of chassis ID/slot number/card number/interface number. This requires the chassis ID to be specified along with the slot number.

As shown in **Figure 1-10**, LSR A and LSR C are at the edge of a backbone network. To deploy VPN services over the backbone network, you need to set up a remote LDP session between LSR A and LSR C, which can transmit VPN services.

Figure 1-10 Networking diagram of configuring a remote LDP session



Configuration Notes

When configuring a remote LDP session, note the following:

- An LSR ID must be configured before you run other MPLS commands.
- An LSR ID of an LSR must be manually configured because no default LSR ID is available.
- It is recommended that the IP address of a reachable loopback interface on an LSR be configured as the LSR ID.
- The IP address of a remote LDP peer must be the LSR ID of the remote LDP peer. When an LDP LSR ID is different from an MPLS LSR ID, the LDP LSR ID must be adopted.

Configuration Roadmap

The configuration roadmap is as follows:

1. Assign an IP address to each interface, and configure OSPF to advertise the route to the segment of each interface and the host route to each LSR ID.
2. Enable MPLS and MPLS LDP globally on each LSR.
3. Specify the name and IP address of the remote peer on LSRs of both ends of a remote LDP session.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each interface as shown in **Figure 1-10**, OSPF process ID, and OSPF area ID
- LSR ID of each LSR
- Name and IP address of each remote peer of a remote LDP session

Procedure

Step 1 Assign an IP address to each interface.

According to **Figure 1-10**, assign an IP address to each interface, including the loopback interface, and configure OSPF to advertise the route to the segment of each interface and the host route to each LSR ID. The configuration details are not mentioned here.

Step 2 Enable MPLS and MPLS LDP globally on each LSR.

Configure LSR A.

```
<LSRA> system-view
[~LSRA] mpls lsr-id 1.1.1.9
[~LSRA] mpls
[~LSRA-mpls] quit
[~LSRA] mpls ldp
[~LSRA-mpls-ldp] commit
[~LSRA-mpls-ldp] quit
```

Configure LSR C.

```
<LSRC> system-view
[~LSRC] mpls lsr-id 3.3.3.9
[~LSRC] mpls
[~LSRC-mpls] quit
[~LSRC] mpls ldp
[~LSRC-mpls-ldp] commit
[~LSRC-mpls-ldp] quit
```

Step 3 Specify the name and IP address of the remote peer on LSRs of both ends of a remote LDP session.

Configure LSR A.

```
[~LSRA] mpls ldp remote-peer LSRC
[~LSRA-mpls-ldp-remote-LSRC] remote-ip 3.3.3.9
[~LSRA-mpls-ldp-remote-LSRC] commit
[~LSRA-mpls-ldp-remote-LSRC] quit
```

Configure LSR C.

```
[~LSRC] mpls ldp remote-peer LSRA
[~LSRC-mpls-ldp-remote-LSRA] remote-ip 1.1.1.9
[~LSRC-mpls-ldp-remote-LSRA] commit
[~LSRC-mpls-ldp-remote-LSRA] quit
```

Step 4 Verify the configuration.

After the configuration, run the **display mpls ldp session** command on an LSR. You can view that the status of the remote LDP session between LSR A and LSR C is **Operational**.

Take the display on LSR A as an example.

```
<LSRA> display mpls ldp session

 LDP Session(s) in Public Network
 Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDD:HH:MM)
 A '*' before a session means the session is being deleted.
------------------------------------------------------------------------------
 PeerID            Status      LAM  SsnRole  SsnAge       KASent/Rcv
------------------------------------------------------------------------------
3.3.3.9:0          Operational DU   Passive  0000:00:01  6/6
------------------------------------------------------------------------------
TOTAL: 1 Session(s) Found.
```

Run the **display mpls ldp remote-peer** command on either of the LSRs on both ends of the remote LDP session. You can view information about the remote peer of the LSR.

Take the display on LSR A as an example.

```
<LSRA> display mpls ldp remote-peer
                        LDP Remote Entity Information
 ------------------------------------------------------------------------------
 Remote Peer Name: LSRC
 Remote Peer IP    : 3.3.3.9             LDP ID        : 1.1.1.9:0
 Transport Address : 1.1.1.9             Entity Status : Active

 Configured Keepalive Hold Timer : 45 Sec
 Configured Keepalive Send Timer : 15 Sec
 Configured Hello Hold Timer     : 45 Sec
 Negotiated Hello Hold Timer     : 45 Sec
 Configured Hello Send Timer     : 15 Sec
 Configured Delay Timer          : ----
 Hello Packet sent/received      : 6347/6307
 ------------------------------------------------------------------------------
 TOTAL: 1 Remote-Peer(s) Found.
```

----End

Configuration Files

- Configuration file of LSR A

```
#
sysname LSRA
#
mpls lsr-id 1.1.1.9
#
mpls
#
mpls ldp
#
mpls ldp remote-peer LSRC
 remote-ip 3.3.3.9
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.1.1.1 255.255.255.252
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
ospf 1
```

```
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.3
#
return
```

- Configuration file of LSR B

```
#
sysname LSRB
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.1.1.2 255.255.255.252
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.2.1.1 255.255.255.252
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 2.2.2.9 0.0.0.0
  network 10.1.1.0 0.0.0.3
  network 10.2.1.0 0.0.0.3
#
return
```

- Configuration file of LSR C

```
#
sysname LSRC
#
mpls lsr-id 3.3.3.9
#
mpls
#
mpls ldp
#
mpls ldp remote-peer LSRA
 remote-ip 1.1.1.9
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.2.1.2 255.255.255.252
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 3.3.3.9 0.0.0.0
  network 10.2.1.0 0.0.0.3
#
return
```

Related Tasks

1.4 Configuring a Remote LDP Session

1.12.3 Example for Establishing LSPs Through LDP

This section provides an example for establishing LSPs through LDP, which consists of establishing a local LDP session and modifying the policy for triggering the establishment of an LSP on each LSR.

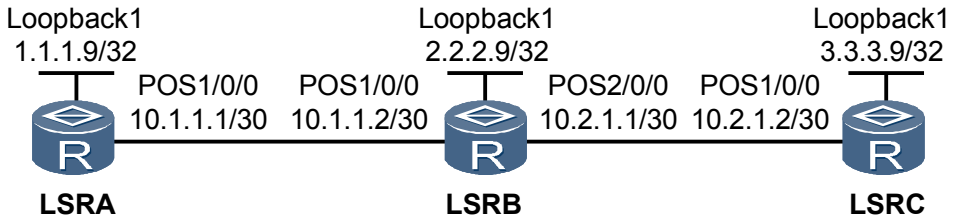
Networking Requirements

CAUTION

On a single NE5000E, an interface is numbered in the format of slot number/card number/interface number. On an NE5000E cluster, the interface is numbered in the format of chassis ID/slot number/card number/interface number. This requires the chassis ID to be specified along with the slot number.

As shown in **Figure 1-11**, LSR A, LSR B, and LSR C all function as core devices or edge devices on a backbone network. On this network, after local LDP sessions are set up between LSR A and LSR B, and between LSR B and LSR C, each pair of LSRs can distribute labels to each other and then LDP LSPs can be set up. In this manner, MPLS services can be deployed.

Figure 1-11 Networking diagram of establishing LSPs through LDP



Configuration Notes

When establishing LSPs through LDP, note the following:

- An LSP can be established only when a route exactly matches the FEC associated with the LSP on an LSR.
- By default, the triggering policy is **host**. That is, the route to the host IP address with a 32-bit mask triggers LDP to establish an LSP.
- If the triggering policy is **all**, thus allowing all IGP routes to trigger LDP to trigger LDP to establish LSPs. In addition, neither public network BGP routes or default routes trigger LDP to establish LSPs.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure local LDP sessions.
2. Modify the policy for triggering the establishment of an LSP on each LSR.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each interface on each LSR as shown in **Figure 1-11**, OSPF process ID, and OSPF area ID
- Policy for triggering the establishment of an LSP

Procedure

Step 1 Configure an LDP LSP.

After you complete the task described in the **Example for Configuring Local LDP Sessions**, each LSR triggers LDP to establish an LSP according to the default triggering policy, that is, the route to the host IP address with a 32-bit mask.

Run the **display mpls ldp lsp** command on an LSR. You can view that all host routes successfully trigger LDP to establish LSPs.

Take the display on LSR A as an example.

```
[~LSRA] display mpls ldp lsp

 LDP LSP Information
 ------------------------------------------------------------------------------
 DestAddress/Mask   In/OutLabel    UpstreamPeer    NextHop          OutInterface
 ------------------------------------------------------------------------------
 1.1.1.9/32         3/NULL         2.2.2.9         127.0.0.1        Loop1
*1.1.1.9/32         Liberal/3                      DS/2.2.2.2
 2.2.2.9/32         NULL/3         -               10.1.1.2         Pos1/0/0
 2.2.2.9/32         1024/3         2.2.2.9         10.1.1.2         Pos1/0/0
 3.3.3.9/32         NULL/1025      -               10.1.1.2         Pos1/0/0
 3.3.3.9/32         1025/1025      3.3.3.9         10.1.1.2         Pos1/0/0
 ------------------------------------------------------------------------------
 TOTAL: 5 Normal LSP(s) Found.
 TOTAL: 1 Liberal LSP(s) Found.
 TOTAL: 0 Frr LSP(s) Found.
 A '*' before an LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stale
 A '*' before a UpstreamPeer means the session is in GR state
 A '*' before a DS means the session is in GR state
 A '*' before a NextHop means the LSP is FRR LSP
```

NOTE

By default, it is recommended that the default triggering policy be adopted. That is, use the route to the host IP address with a 32-bit mask trigger LDP to establish an LSP. Alternatively, you can perform the following procedures to modify the LDP LSP triggering policy as required.

Step 2 Change the policy for triggering the establishment of LDP LSPs.

Change the triggering policy to **all** on each LSP, thus allowing static routes and IGP routes in a routing table to trigger LDP to establish LSPs.

Configure LSR A.

```
[~LSRA] mpls
[~LSRA-mpls] lsp-trigger all
[~LSRA-mpls] commit
[~LSRA-mpls] quit
```

Configure LSR B.

```
[~LSRB] mpls
[~LSRB-mpls] lsp-trigger all
[~LSRB-mpls] commit
[~LSRB-mpls] quit
```

Configure LSR C.

```
[~LSRC] mpls
[~LSRC-mpls] lsp-trigger all
[~LSRC-mpls] commit
[~LSRC-mpls] quit
```

Step 3 Verify the configuration.

After the configuration, run the **display mpls ldp lsp** command on an LSR. You can view information about LDP LSPs. Take the display on LSR A as an example.

```
[~LSRA] display mpls ldp lsp

LDP LSP Information
 ------------------------------------------------------------------------------
 DestAddress/Mask   In/OutLabel   UpstreamPeer    NextHop     OutInterface
 ------------------------------------------------------------------------------
 1.1.1.9/32         3/NULL        2.2.2.9         127.0.0.1   InLoop0
*1.1.1.9/32         Liberal
 2.2.2.9/32         NULL/3        -               10.1.1.2    Pos1/0/0
 2.2.2.9/32         1024/3        2.2.2.9         10.1.1.2    Pos1/0/0
 3.3.3.9/32         NULL/1025     -               10.1.1.2    Pos1/0/0
 3.3.3.9/32         1025/1025     2.2.2.9         10.1.1.2    Pos1/0/0
 10.1.1.0/30        3/NULL        2.2.2.9         10.1.1.1    Pos1/0/0
*10.1.1.0/30        Liberal
 10.2.1.0/30        NULL/3        -               10.1.1.2    Pos1/0/0
 10.2.1.0/30        1026/3        2.2.2.9         10.1.1.2    Pos1/0/0
 ------------------------------------------------------------------------------
 TOTAL: 8 Normal LSP(s) Found.
 TOTAL: 2 Liberal LSP(s) Found.
 TOTAL: 0 Frr LSP(s) Found.
 A '*' before an LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stale
 A '*' before a UpstreamPeer means the session is in GR state
 A '*' before a NextHop means the LSP is FRR LSP
```

----End

Configuration Files

- Configuration file of LSR A

```
#
sysname LSRA
#
mpls lsr-id 1.1.1.9
#
mpls
  lsp-trigger all
#
mpls ldp
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.1.1.1 255.255.255.252
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.3
#
return
```

- Configuration file of LSR B

```
#
 sysname LSRB
#
 mpls lsr-id 2.2.2.9
#
 mpls
  lsp-trigger all
#
mpls ldp
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.1.1.2 255.255.255.252
 mpls
 mpls ldp
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.2.1.1 255.255.255.252
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 2.2.2.9 0.0.0.0
  network 10.1.1.0 0.0.0.3
  network 10.2.1.0 0.0.0.3
#
return
```

- Configuration file of LSR C

```
#
sysname LSRC
#
mpls lsr-id 3.3.3.9
#
mpls
  lsp-trigger all
#
mpls ldp
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.2.1.2 255.255.255.252
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 3.3.3.9 0.0.0.0
  network 10.2.1.0 0.0.0.3
#
return
```

Related Tasks

1.5 Configuring an LDP LSP

1.12.4 Example for Configuring Transit LSPs Through an IP Prefix List

This section provides an example for configuring transit LSPs, which consists of establishing local LDP sessions and configuring an IP prefix list to filter routes on each transit LSR.

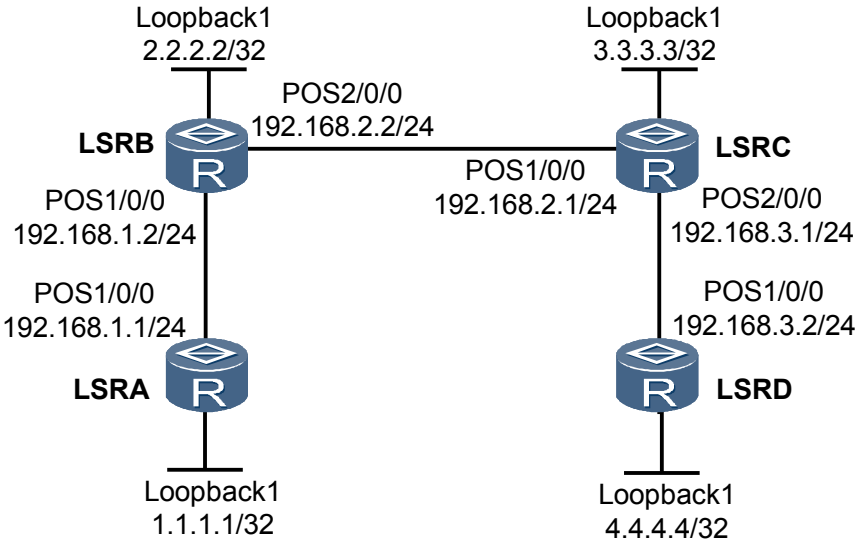
Networking Requirements

CAUTION

On a single NE5000E, an interface is numbered in the format of slot number/card number/interface number. On an NE5000E cluster, the interface is numbered in the format of chassis ID/slot number/card number/interface number. This requires the chassis ID to be specified along with the slot number.

After MPLS LDP is enabled on each interface, LDP LSPs can be automatically established. In this case, a large number of transit LSPs may be established, which wastes resources. As shown in **Figure 1-12**, after a policy for triggering the establishment of transit LSPs is configured, LSR B allows the establishment of transit LSPs according to only the routes to 4.4.4.4/32.

Figure 1-12 Networking diagram of configuring transit LSPs through the prefix list



Configuration Notes

When configuring transit LSPs through the prefix list, note the following:

By default, LDP does not filter the received routing information to establish transit LSPs.

Configuration Roadmap

The configuration roadmap is as follows:

1. Assign an IP address to each interface, and configure OSPF to advertise the route to the segment of each interface and the host route to each LSR ID.
2. Configure the IP prefix list according to the requirements for controlling LSPs.
3. Enable MPLS and MPLS LDP globally on each LSR, and configure a policy of triggering the establishment of LSPs.
4. Filter the transit LSP routes by using the IP prefix list on transit LSR B.
5. Enable MPLS and MPLS LDP on each interface.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each interface as shown in **Figure 1-12**, OSPF process ID, and OSPF area ID
- Policy for triggering the establishment of LSPs
- IP prefix list name, and the routes to be filtered on the transit node

Procedure

Step 1 Assign an IP address to each interface, and configure OSPF to advertise the route to the segment of each interface and the host route to each LSR ID.

According to **Figure 1-12**, assign an IP address to each interface, including the loopback interface, and configure OSPF to advertise the route to the segment of each interface and the host route to each LSR ID. The configuration details are not mentioned here.

Step 2 Configure the IP prefix list on transit LSR B.

Configure the IP prefix list on transit LSR B. Thus, only the routes to 4.4.4.4/32 of LSR D can be used to establish transit LSPs.

```
[~LSRB]ip ip-prefix FilterOnTransit permit 4.4.4.4 32
[~LSRB]commit
```

Step 3 Enable MPLS and MPLS LDP on each LSR and interface, and configure a policy for triggering the establishment of LSPs.

Configure LSR A.

```
[~LSRA] mpls lsr-id 1.1.1.1
[~LSRA] mpls
[~LSRA-mpls] lsp-trigger all
[~LSRA-mpls] quit
[~LSRA] mpls ldp
[~LSRA-mpls-ldp] quit
[~LSRA] interface pos 1/0/0
[~LSRA-Pos1/0/0] mpls
[~LSRA-Pos1/0/0] mpls ldp
[~LSRA-Pos1/0/0] commit
[~LSRA-Pos1/0/0] quit
```

Configure LSR B.

```
[~LSRB] mpls lsr-id 2.2.2.2
[~LSRB] mpls
[~LSRB-mpls] lsp-trigger all
[~LSRB-mpls] quit
[~LSRB] mpls ldp
[~LSRB-mpls-ldp] propagate mapping for ip-prefix FilterOnTransit
```

```
[~LSRB-mpls-ldp] quit
[~LSRB] interface pos 1/0/0
[~LSRB-Pos1/0/0] mpls
[~LSRB-Pos1/0/0] mpls ldp
[~LSRB-Pos1/0/0] quit
[~LSRB] interface pos 2/0/0
[~LSRB-Pos2/0/0] mpls
[~LSRB-Pos2/0/0] mpls ldp
[~LSRB-Pos2/0/0] commit
[~LSRB-Pos2/0/0] quit
```

The configurations of LSR C and LSR D are similar to those of LSR A, and the configuration details are not mentioned here.

Step 4 Verify the configuration.

Run the **display mpls ldp lsp** command. You can view the establishment of LSPs.

Display LDP LSPs established on LSR A.

```
[~LSRA] display mpls ldp lsp

 LDP LSP Information
 -------------------------------------------------------------------------------
 DestAddress/Mask   In/OutLabel    UpstreamPeer    NextHop          OutInterface
 -------------------------------------------------------------------------------
 1.1.1.1/32         3/NULL         2.2.2.2         127.0.0.1        Loop1
 2.2.2.2/32         NULL/3         -               192.168.1.2      Pos1/0/0
 2.2.2.2/32         1025/3         2.2.2.2         192.168.1.2      Pos1/0/0
 4.4.4.4/32         NULL/1025      -               192.168.1.2      Pos1/0/0
 4.4.4.4/32         1026/1026      4.4.4.4         192.168.1.2      Pos1/0/0
 192.168.1.0/24     3/NULL         2.2.2.2         192.168.1.1      Pos1/0/0
*192.168.1.0/24     Liberal/26                     DS/2.2.2.2
 192.168.2.0/24     NULL/3         -               192.168.1.2      Pos1/0/0
 192.168.2.0/24     1027/3         3.3.3.3         192.168.1.2      Pos1/0/0
-------------------------------------------------------------------------------
 TOTAL: 8 Normal LSP(s) Found.
 TOTAL: 1 Liberal LSP(s) Found.
 TOTAL: 0 Frr LSP(s) Found.
 A '*' before an LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stale
 A '*' before a UpstreamPeer means the session is in GR state
 A '*' before a DS means the session is in GR state
 A '*' before a NextHop means the LSP is FRR LSP
```

The command output shows that each LSR, only LDP LSPs with LSR B being the transit node and routes to 4.4.4.4/32 and other LDP LSPs, on which LSR B is not the transit node, are set up after the policy for triggering the establishment of LSPs is configured.

----End

Configuration Files

- Configuration file of LSR A

```
#
sysname LSRA
#
mpls lsr-id 1.1.1.1
#
mpls
  lsp-trigger all
#
mpls ldp
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
```

```
 ip address 192.168.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

- Configuration file of LSR B

```
#
sysname LSRB
#
mpls lsr-id 2.2.2.2
#
mpls
  lsp-trigger all
#
mpls ldp
#
ipv4-family
propagate mapping for ip-prefix FilterOnTransit
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 192.168.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 192.168.2.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
ip ip-prefix FilterOnTransit index 10 permit 4.4.4.4 32
#
return
```

- Configuration file of LSR C

```
#
sysname LSRC
#
mpls lsr-id 3.3.3.3
#
mpls
  lsp-trigger all
#
mpls ldp
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 192.168.2.2 255.255.255.0
```

```
 mpls
 mpls ldp
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 192.168.3.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
return
```

- Configuration file of LSR D

```
#
sysname LSRD
#
mpls lsr-id 4.4.4.4
#
mpls
  lsp-trigger all
#
mpls ldp
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 192.168.3.2 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 192.168.3.0 0.0.0.255
#
Return
```

Related Tasks

1.5 Configuring an LDP LSP

1.12.5 Example for Configuring Static BFD for LDP LSP

This section describes how to configure static BFD for LDP LSP, including the procedure such as enabling MPLS and MPLS LDP in the system and interface views and enabling BFD on two ends of a link to be detected.

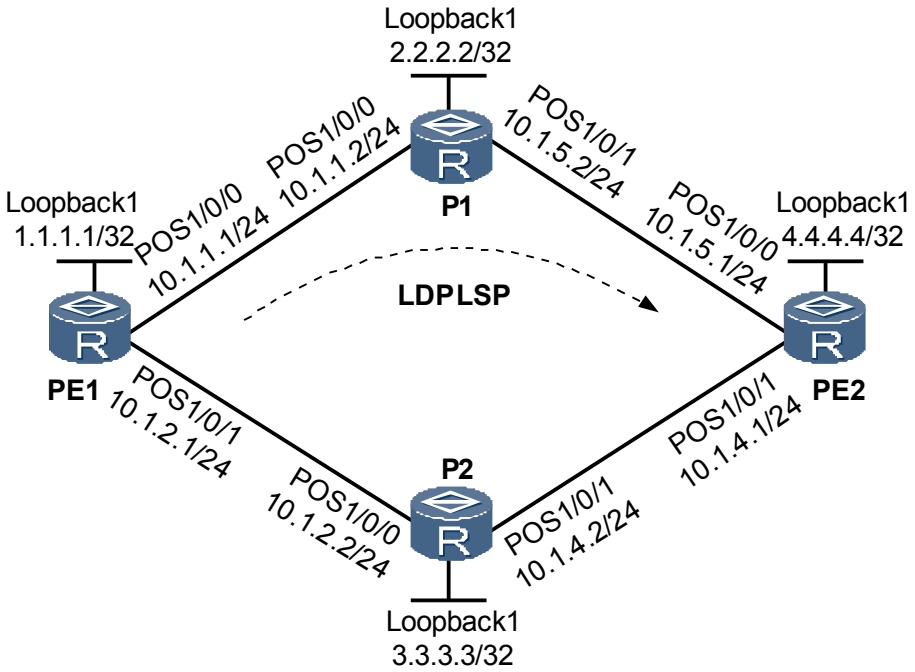
Networking Requirements

CAUTION

On a single NE5000E, an interface is numbered in the format: slot number/card number/interface number. On the NE5000E cluster, an interface is numbered in the format: chassis ID/slot number/card number/interface number. If the slot number is specified, the chassis ID of the slot must also be specified.

On the network shown in **Figure 1-13**, an LDP LSP is set up over a path PE1 -> P1 -> PE2. The opposite path PE2 -> P1 -> PE1 is an IP path. Static BFD is required to detect faults in the LDP LSP.

Figure 1-13 Networking diagram for static BFD for LDP LSP



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure OSPF on the MPLS domain and ensure the connectivity between nodes at the network layer.
2. Set up an LDP LSP along the path PE1 -> P1 -> PE2.
3. Configure a BFD session and bind the BFD session to the LDP LSP on PE1.
4. Configure a BFD session and bind the BFD session to the IP path on PE2, allowing PE2 to notify PE1 of a fault if BFD detects a fault in the LDP LSP.

Data Preparation

To complete the configuration, you need the following data:

- IP address of every interface
- OSPF process ID
- BFD configuration name and local and remote discriminators

Procedure

Step 1 Assign an IP address to every interface and configure OSPF.

Assign an IP address and its mask to every interface such as a loopback interface shown in **Figure 1-13**.

Configure OSPF on every node to advertise every host and segment route. The configuration procedure is not provided.

After completing the configurations, ping every node using a specific LSR ID. The ping is successful. Run the **display ip routing-table** command on every node. Routes to nodes in routing tables are reachable.

```
<PE1> display ip routing-table
Route Flags: R - relay, D - download for forwarding
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 14       Routes : 15

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.9/32  Direct  0    0           D   127.0.0.1       InLoopBack0
        2.2.2.9/32  OSPF    10   2           D   10.1.1.2        Pos1/0/0
        3.3.3.9/32  OSPF    10   2           D   10.1.2.2        Pos1/0/1
        4.4.4.9/32  OSPF    10   3           D   10.1.2.2        Pos1/0/1
                    OSPF    10   3           D   10.1.1.2        Pos1/0/0
      10.1.1.0/24   Direct  0    0           D   10.1.1.1        Pos1/0/0
      10.1.1.1/32   Direct  0    0           D   127.0.0.1       InLoopBack0
      10.1.1.2/32   Direct  0    0           D   10.1.1.2        Pos1/0/0
      10.1.2.0/24   Direct  0    0           D   10.1.2.1        Pos1/0/1
      10.1.2.1/32   Direct  0    0           D   127.0.0.1       InLoopBack0
      10.1.2.2/32   Direct  0    0           D   10.1.2.2        Pos1/0/1
      10.1.4.0/24   OSPF    10   2           D   10.1.2.2        Pos1/0/1
      10.1.5.0/24   OSPF    10   2           D   10.1.1.2        Pos1/0/0
     127.0.0.0/8    Direct  0    0           D   127.0.0.1       InLoopBack0
     127.0.0.1/32   Direct  0    0           D   127.0.0.1       InLoopBack0
```

Step 2 Set up an LDP LSP along the path PE1 -> P1 -> PE2.

Configure PE1.

```
<PE1> system-view
[~PE1] mpls lsr-id 1.1.1.9
[~PE1] mpls
[~PE1-mpls] quit
[~PE1] mpls ldp
[~PE1-mpls] quit
[~PE1]interface pos 1/0/0
[~PE1-Pos1/0/0] mpls
[~PE1-Pos1/0/0] mpls ldp
[~PE1-Pos1/0/0] quit
[~PE1] commit
```

Configure P1.

```
<P1> system-view
```

```
[~P1] mpls lsr-id 2.2.2.9
[~P1] mpls
[~P1-mpls] quit
[~P1] mpls ldp
[~P1-mpls] quit
[~P1]interface pos 1/0/0
[~P1-Pos1/0/0] mpls
[~P1-Pos1/0/0] mpls ldp
[~P1-Pos1/0/0] quit
[~P1]interface pos 1/0/1
[~P1-Pos1/0/1] mpls
[~P1-Pos1/0/1] mpls ldp
[~P1-Pos1/0/1] quit
[~P1] commit
```

Configure PE2.

```
<PE2> system-view
[~PE2] mpls lsr-id 4.4.4.9
[~PE2] mpls
[~PE2-mpls] quit
[~PE2] mpls ldp
[~PE2-mpls] quit
[~PE2]interface pos 1/0/0
[~PE2-Pos1/0/0] mpls
[~PE2-Pos1/0/0] mpls ldp
[~PE2-Pos1/0/0] quit
[~PE2] commit
```

Run the **display mpls ldp lsp** command. An LDP LSP destined for 4.4.4.9/32 has been established on PE1.

```
<PE1> display mpls ldp lsp

 LDP LSP Information
 ------------------------------------------------------------------------------
 DestAddress/Mask   In/OutLabel     UpstreamPeer    NextHop     OutInterface
 ------------------------------------------------------------------------------
 1.1.1.9/32         3/NULL          2.2.2.9         127.0.0.1   InLoop0
*1.1.1.9/32         Liberal
 2.2.2.9/32         NULL/3          -               10.1.1.2    S0/0/0
 2.2.2.9/32         1024/3          2.2.2.9         10.1.1.2    S0/0/0
 4.4.4.9/32         NULL/1025       -               10.1.1.2    S0/0/0
 4.4.4.9/32         1025/1025       2.2.2.9         10.1.1.2    S0/0/0
 ------------------------------------------------------------------------------
 TOTAL: 5 Normal LSP(s) Found.
 TOTAL: 1 Liberal LSP(s) Found.
 TOTAL: 0 Frr LSP(s) Found.
 A '*' before an LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stale
 A '*' before a UpstreamPeer means the session is in GR state
 A '*' before a NextHop means the LSP is FRR LSP
```

Step 3 Enable BFD globally on two nodes at the two ends of a link to be detected.

Configure PE1.

```
<PE1> system-view
[~PE1] bfd
[~PE1-bfd] quit
[~PE1] commit
```

Configure P2.

```
<PE2> system-view
[~PE2] bfd
[~PE2-bfd] quit
[~PE2] commit
```

Step 4 Configure a BFD session and bind the BFD session to the LDP LSP on the ingress.

Configure PE1.

```
<PE1> system-view
[~PE1] bfd 1to4 bind ldp-lsp peer-ip 4.4.4.9 nexthop 10.1.1.2 interface pos 1/0/0
[~PE1-bfd-lsp-session-1to4] discriminator local 1
[~PE1-bfd-lsp-session-1to4] discriminator remote 2
[~PE1-bfd-lsp-session-1to4] process-pst
[~PE1-bfd-lsp-session-1to4] commit
[~PE1-bfd-lsp-session-1to4] quit
```

Step 5 Configure a BFD session and bind the BFD session to the IP path on the egress, allowing the egress to notify the ingress of a fault if BFD detects a fault in the LDP LSP.

Configure PE2.

```
<PE2> system-view
[~PE2] bfd 4to1 bind peer-ip 1.1.1.9
[~PE2-bfd-session-4ot1] discriminator local 2
[~PE2-bfd-session-4ot1] discriminator remote 1
[~PE2-bfd-session-4ot1] commit
[~PE2-bfd-session-4ot1] quit
```

Step 6 Verify the configuration.

After completing the configuration, run the **display bfd session all verbose** command on the ingress. The **State** field displays **Up** and the **BFD Bind Type** field displays **LDP_LSP**.

```
<PE1> display bfd session all verbose
-------------------------------------------------------------------------------
  (One Hop) State : Up                     Name : 1to4
-------------------------------------------------------------------------------
  Local Discriminator    : 1               Remote Discriminator   : 2
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type          : LDP_LSP
  Bind Session Type      : Static
  Bind Peer IP Address   : 4.4.4.9
  NextHop Ip Address     : 10.1.1.2
  Bind Interface         : Pos1/0/0
  Tunnel ID              : 0
  FSM Board Id           : 1               TOS-EXP                : 7
  Min Tx Interval (ms)   : 10              Min Rx Interval (ms)   : 10
  Actual Tx Interval (ms): 2000            Actual Rx Interval (ms): 2000
  Local Detect Multi     : 3               Detect Interval (ms)   : 30
  Echo Passive           : Disable         Acl Number             : -
  Destination Port       : 3784            TTL                    : 1
  Proc Interface Status  : Disable         Process PST            : Enable
  WTR Interval (ms)      : -               Local Demand Mode      : Disable
  Active Multi           : 3
  Last Local Diagnostic  : No Diagnostic
  Bind Application       : No Application Bind
  Session TX TmrID       : 94              Session Detect TmrID   : 95
  Session Init TmrID     : -               Session WTR TmrID      : -
  Session Echo Tx TmrID  : -
  Session Description    : -
-------------------------------------------------------------------------------

     Total UP/DOWN Session Number : 1/0
```

Run the **display bfd session all verbose** command on the egress. The **(Multi Hop) State** field displays **Up** and the **BFD Bind Type** field displays **Peer IP Address**.

```
<PE2> display bfd session all verbose
-------------------------------------------------------------------------------
  (Multi Hop) State : Up                     Name : 4to1
-------------------------------------------------------------------------------
  Local Discriminator    : 2               Remote Discriminator   : 1
  Session Detect Mode    : Asynchronous Mode Without Echo Function
```

```
  BFD Bind Type           : Peer IP Address
  Bind Session Type       : Static
  Bind Peer IP Address    : 1.1.1.9
  Bind Interface          : -
  FSM Board Id            : 6                 TOS-EXP                 : 7
  Min Tx Interval (ms)    : 10                Min Rx Interval (ms)    : 10
  Actual Tx Interval (ms): 2000               Actual Rx Interval (ms): 2000
  Local Detect Multi      : 3                 Detect Interval (ms)    : 30
  Echo Passive            : Disable           Acl Number              : -
  Proc Interface Status   : Disable           Process PST             : Disable
  WTR Interval (ms)       : -                 Local Demand Mode       : Disable
  Active Multi            : 3
  Last Local Diagnostic   : No Diagnostic
  Bind Application        : No Application Bind
  Session TX TmrID        : 75                Session Detect TmrID    : 76
  Session Init TmrID      : -                 Session WTR TmrID       : -
  Session Echo Tx TmrID   : -
  Session Description     : -
--------------------------------------------------------------------------------

     Total UP/DOWN Session Number : 1/0
```

----End

Configuration Files

- Configuration file of PE1

```
#
 sysname PE1
#
 bfd
#
 mpls lsr-id 1.1.1.9
 mpls
#
mpls ldp
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface Pos1/0/1
 undo shutdown
 link-protocol ppp
 ip address 10.1.2.1 255.255.255.0
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
#
bfd 1to4 bind ldp-lsp peer-ip 4.4.4.9 nexthop 10.1.1.2 interface Pos1/0/0
 discriminator local 1
 discriminator remote 2
 process-pst
 #
return
```

- Configuration file of PE2

```
#
 sysname PE2
```

```
#
 bfd
#
 mpls lsr-id 4.4.4.9
 mpls
#
mpls ldp
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.1.5.1 255.255.255.0
 mpls
 mpls ldp
#
interface Pos1/0/1
 undo shutdown
 link-protocol ppp
 ip address 10.1.4.1 255.255.255.0
#
interface LoopBack1
 ip address 4.4.4.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 10.1.5.0 0.0.0.255
  network 10.1.4.0 0.0.0.255
  network 4.4.4.9 0.0.0.0
#
bfd 4to1 bind peer-ip 1.1.1.9
 discriminator local 2
 discriminator remote 1
#
return
```

- Configuration file of P1

```
#
 sysname P1
#
 mpls lsr-id 2.2.2.9
 mpls
#
mpls ldp
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Pos1/0/1
 undo shutdown
 link-protocol ppp
 ip address 10.1.5.2 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 2.2.2.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.5.0 0.0.0.255
return
```

- Configuration file of P2

```
#
 sysname P2
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.1.2.2 255.255.255.0
#
interface Pos1/0/1
 undo shutdown
 link-protocol ppp
 ip address 10.1.4.2 255.255.255.0
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 3.3.3.9 0.0.0.0
  network 10.1.4.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
return
```

Related Tasks

1.6 Configuring Static BFD to Detect an LDP LSP

1.12.6 Example for Configuring LDP-IGP Synchronization

This exmample describes how to configure synchronization between LDP and an IGP (OSPF).

Networking Requirements

CAUTION

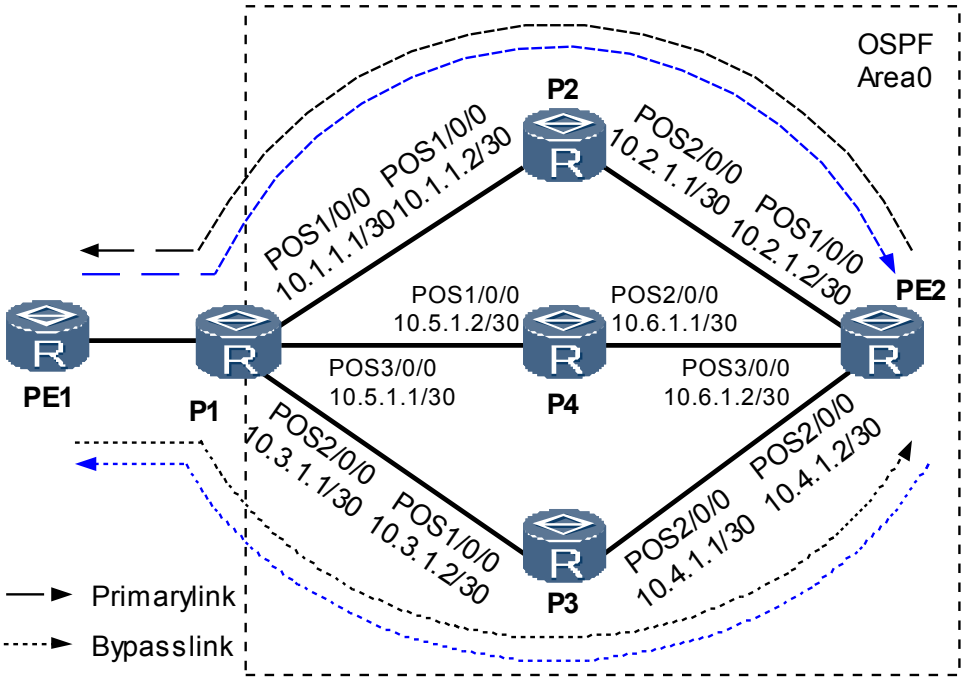
On a single NE5000E, an interface is numbered in the format: slot number/card number/interface number. On the NE5000E cluster, an interface is numbered in the format: chassis ID/slot number/card number/interface number. If the slot number is specified, the chassis ID of the slot must also be specified.

On the network shown in **Figure 1-14**, three links are set up between PE1 and PE2. The path PE1 -> P1 -> P2 -> PE2 functions as the primary path. P3 functions a backup device because P4 operates important services. Therefore, the path PE1 -> P1 -> P3 -> PE2 functions as a backup path.

LDP-IGP synchronization is configured on the interfaces on both ends of the link between P1 and P2. On a network with both a primary LSP and a backup LSPs, after the primary LSP recovers, LDP-IGP synchronization minimizes the traffic interruption period to be at the millisecond level.

Setting a delay time for deleting upstream labels prevents traffic interruption if LDP traffic is switched to a backup path.

Figure 1-14 Networking diagram for configuring synchronization between LDP and IGP



Device	Loopback Address	Device	Loopback Address
P1	1.1.1.9/32	P4	4.4.4.9/32
P2	2.2.2.9/32	PE2	5.5.5.9/32
P3	3.3.3.9/32		

Configuration Notes

When configuring LDP-IGP synchronization, note the following point:

To ensure that an LDP session can be properly re-established, configure the hold-max-cost timer to adjust the interval at which OSPF sending an LSA to advertise the maximum cost. In this manner, traffic is transmitted through the backup LSP before the LDP session on the primary LSP is re-established.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic OSPF functions on P1, P2, P3, and P4 to interconnect these devices.
2. Establish LDP sessions between neighboring nodes and LSPs between P1 and PE2.
3. Set the priorities of equal-cost routes on P1 to ensure that the path PE1 -> P1 -> P2 ->PE2 functions as the primary LSP.
4. Enable synchronization between LDP and IGP in the OSPF process on P1.
5. Block synchronization between LDP and IGP on the interfaces on both ends of the link between P1 and P4.

6. Set the values of hold-max-cost and delay timers on the interfaces on both ends of the link between P1 and P2.

Data Preparation

To complete the configuration, you need the following data:

- IP addresses of the interfaces on each node as shown in **Figure 1-14**, OSPF process ID, and OSPF area ID
- Priories of equal-cost routes on P1
- Values of hold-max-cost and igp-sync-delay timers

Procedure

Step 1 Configure an IP address for each interface. The configuration procedure is not provided.

Configure an IP address for each interface shown in **Figure 1-14**, including the IP address of each loopback interface, and configure OSPF to advertise network segments to which the interfaces are connected and LSR ID host routes. For details, see Example for Configuring Basic OSPF Functions.

After completing the configuration, run the **display ip routing-table** command on each node. All nodes learn the routes from each other and that there are three equal-cost routes from P1 to address 5.5.5.9/32. In this example, the IP routing table on P1 is displayed.

```
[~P1] display ip routing-table
Route Flags: R - relay, D - download for forwarding
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 18        Routes : 18
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
        1.1.1.9/32  Direct  0    0           D   127.0.0.1       InLoopBack0
        2.2.2.9/32  OSPF    10   2           D   10.1.1.2        Pos1/0/0
        3.3.3.9/32  OSPF    10   4           D   10.1.1.2        Pos1/0/0
        5.5.5.9/32  OSPF    10   3           D   10.1.1.2        Pos1/0/0
                    OSPF    10   3           D   10.3.1.2        Pos2/0/0
                    OSPF    10   3           D   10.5.1.2        Pos3/0/0
       10.1.1.0/30  Direct  0    0           D   10.1.1.1        Pos1/0/0
       10.1.1.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
       10.1.1.2/32  Direct  0    0           D   10.1.1.2        Pos1/0/0
       10.2.1.0/30  OSPF    10   2           D   10.1.1.2        Pos1/0/0
       10.3.1.0/30  Direct  0    0           D   10.3.1.1        Pos2/0/0
       10.3.1.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
       10.3.1.2/32  Direct  0    0           D   10.3.1.2        Pos2/0/0
       10.4.1.0/30  OSPF    10   3           D   10.1.1.2        Pos2/0/0
       10.5.1.0/30  Direct  0    0           D   10.5.1.1        Pos3/0/0
       10.5.1.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
       10.5.1.2/32  Direct  0    0           D   10.5.1.2        Pos4/0/0
       10.6.1.0/30  OSPF    10   3           D   10.1.1.2        Pos3/0/0
      127.0.0.0/20  Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

Step 2 Set the priorities of equal-cost routes on P1 to ensure that the path PE1 -> P1 -> P2 ->PE2 functions as the primary LSP.

```
[~P1] ospf
[~P1-ospf-1] nexthop 10.1.1.2 weight 1
[~P1-ospf-1] nexthop 10.3.1.2 weight 2
[~P1-ospf-1] nexthop 10.5.1.2 weight 2
[~P1-ospf-1] commit
[~P1-ospf-1] quit
```

After completing the preceding configuration, run the **display ip routing-table** command on P1. There is only one route to address 5.5.5.9/32 and the outgoing interface of the route is changed

to POS 1/0/0. Therefore, the path PE1 -> P1 -> P2 -> PE2 becomes the primary LSP and the path PE1 -> P1 -> P3 -> PE2 becomes the backup LSP.

```
[~P1] display ip routing-table
Route Flags: R - relay, D - download for forwarding
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 18       Routes : 18
Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface
        1.1.1.9/32  Direct 0    0           D  127.0.0.1       InLoopBack0
        2.2.2.9/32  OSPF   10   2           D  10.1.1.2        Pos1/0/0
        3.3.3.9/32  OSPF   10   4           D  10.1.1.2        Pos1/0/0
        5.5.5.9/32  OSPF   10   3           D  10.1.1.2        Pos1/0/0
       10.1.1.0/30  Direct 0    0           D  10.1.1.1        Pos1/0/0
       10.1.1.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
       10.1.1.2/32  Direct 0    0           D  10.1.1.2        Pos1/0/0
       10.2.1.0/30  OSPF   10   2           D  10.1.1.2        Pos1/0/0
       10.3.1.0/30  Direct 0    0           D  10.3.1.1        Pos2/0/0
       10.3.1.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
       10.3.1.2/32  Direct 0    0           D  10.3.1.2        Pos2/0/0
       10.4.1.0/30  OSPF   10   3           D  10.1.1.2        Pos2/0/0
       10.5.1.0/30  Direct 0    0           D  10.5.1.1        Pos3/0/0
       10.5.1.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
       10.5.1.2/32  Direct 0    0           D  10.5.1.2        Pos4/0/0
       10.6.1.0/30  OSPF   10   3           D  10.1.1.2        Pos3/0/0
      127.0.0.0/20  Direct 0    0           D  127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
```

Step 3 Enable MPLS and MPLS LDP on each node and interfaces of each node.

Configure P1.

```
[~P1] mpls lsr-id 1.1.1.9
[~P1] mpls
[~P1-mpls] quit
[~P1] mpls ldp
[~P1-mpls-ldp] quit
[~P1] interface pos 1/0/0
[~P1-Pos1/0/0] mpls
[~P1-Pos1/0/0] mpls ldp
[~P1-Pos1/0/0] quit
[~P1] interface pos 2/0/0
[~P1-Pos2/0/0] mpls
[~P1-Pos2/0/0] mpls ldp
[~P1-Pos2/0/0] commit
[~P1-Pos2/0/0] quit
```

Configure P2.

```
[~P2] mpls lsr-id 2.2.2.9
[~P2] mpls
[~P2-mpls] quit
[~P2] mpls ldp
[~P2-mpls-ldp] quit
[~P2] interface pos 1/0/0
[~P2-Pos1/0/0] mpls
[~P2-Pos1/0/0] mpls ldp
[~P2-Pos1/0/0] quit
[~P2] interface pos 2/0/0
[~P2-Pos2/0/0] mpls
[~P2-Pos2/0/0] mpls ldp
[~P2-Pos2/0/0] commit
[~P2-Pos2/0/0] quit
```

Configure P3.

```
[~P3] mpls lsr-id 3.3.3.9
[~P3] mpls
[~P3-mpls] quit
```

```
[~P3] mpls ldp
[~P3-mpls-ldp] quit
[~P3] interface pos 1/0/0
[~P3-Pos1/0/0] mpls
[~P3-Pos1/0/0] mpls ldp
[~P3-Pos1/0/0] quit
[~P3] interface pos 2/0/0
[~P3-Pos2/0/0] mpls
[~P3-Pos2/0/0] mpls ldp
[~P3-Pos2/0/0] commit
[~P3-Pos2/0/0] quit
```

Configure PE2.

```
[~PE2] mpls lsr-id 5.5.5.9
[~PE2] mpls
[~PE2-mpls] quit
[~PE2] mpls ldp
[~PE2-mpls-ldp] quit
[~PE2] interface pos 1/0/0
[~PE2-Pos1/0/0] mpls
[~PE2-Pos1/0/0] mpls ldp
[~PE2-Pos1/0/0] quit
[~PE2] interface pos 2/0/0
[~PE2-Pos2/0/0] mpls
[~PE2-Pos2/0/0] mpls ldp
[~PE2-Pos2/0/0] commit
[~PE2-Pos2/0/0] quit
```

After completing the preceding configuration is complete, run the **display mpls ldp session** command on each node to check LDP session information. The command output shows that **Status** is displayed as **Operational**. In this example, LDP session information on P1 is displayed.

```
[~P1] display mpls ldp session
               LDP Session(s) in Public Network
------------------------------------------------------------------------------
 Peer-ID           Status      LAM  SsnRole  SsnAge      KA-Sent/Rcv
------------------------------------------------------------------------------
2.2.2.9:0          Operational DU   Passive  0000:00:56  227/227
3.3.3.9:0          Operational DU   Passive  0000:00:56  227/227
5.5.5.9:0          Operational DU   Passive  0000:00:56  227/227
------------------------------------------------------------------------------
TOTAL: 3 Session(s) Found.
 LAM : Label Advertisement Mode      SsnAge Unit : DDD:HH:MM
```

Step 4 Enable synchronization between LDP and IGP on P1.

Configure P1.

```
[~P1] ospf 1
[~P1-ospf-1] area 0
[~P1-ospf-1-area-0.0.0.1] ldp-sync enable
[~P1-ospf-1-area-0.0.0.1] commit
[~P1-ospf-1-area-0.0.0.1] quit
[~P1-ospf-1] quit
```

Step 5 Block LDP-IGP synchronization on an interface of P1.

Configure P1.

```
[~P1] ospf 1
[~P1] interface pos 3/0/0
[~P1-Pos3/0/0] ospf ldp-sync block
[~P1-Pos3/0/0] commit
[~P1-Pos3/0/0] quit
```

Step 6 Set the value of the hold-max-cost timer on the interfaces on both ends of the link between P1 and P2.

Configure P1.

```
[~P1] interface pos 1/0/0
[~P1-Pos1/0/0] ospf timer ldp-sync hold-max-cost 9
[~P1-Pos1/0/0] commit
[~P1-Pos1/0/0] quit
```

Configure P2.

```
[~P2] interface pos 1/0/0
[~P2-Pos1/0/0] ospf timer ldp-sync hold-max-cost 9
[~P2-Pos1/0/0] commit
[~P2-Pos1/0/0] quit
```

Step 7 Set the value of the delay timer on the interfaces on both ends of the link between P1 and P2.

Configure P1.

```
[~P1] interface pos 1/0/0
[~P1-Pos1/0/0] mpls ldp timer igp-sync-delay 6
[~P1-Pos1/0/0] commit
[~P1-Pos1/0/0] quit
```

Configure P2.

```
[~P2] interface pos 1/0/0
[~P2-Pos1/0/0] mpls ldp timer igp-sync-delay 6
[~P2-Pos1/0/0] commit
[~P2-Pos1/0/0] quit
```

Step 8 Verify the configuration.

After completing the preceding configuration, run the **display ospf ldp-sync** command on P1. The interface status is **Sync-Achieved**.

```
[~P1] display ospf ldp-sync interface pos 1/0/0
 Interface POS1/0/0
 HoldMaxCost Timer: 9
 LDP State: Up             OSPF Sync State: Sync-Achieved
```

----End

Configuration Files

- Configuration file of P1

```
#
sysname P1
#
mpls lsr-id 1.1.1.9
#
mpls
#
mpls ldp
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.1.1.1 255.255.255.252
 ospf ldp-sync
 ospf timer ldp-sync holdmaxcost 9
 mpls ldp timer igp-sync-delay 6
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.3.1.1 255.255.255.252
#
interface Pos3/0/0
```

```
 undo shutdown
 link-protocol ppp
 ip address 10.5.1.1 255.255.255.252
 ospf ldp-sync block
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
ospf 1
 nexthop 10.1.1.2 weight 1
 nexthop 10.3.1.2 weight 2
 nexthop 10.5.1.2 weight 2
 area 0.0.0.0
  ldp-sync enable
  network 1.1.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.3
  network 10.3.1.0 0.0.0.3
  network 10.5.1.0 0.0.0.3
#
return
```

- Configuration file of P2

```
#
sysname P2
#
mpls lsr-id 2.2.2.9
#
mpls
#
mpls ldp
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.1.1.2 255.255.255.252
 ospf ldp-sync
 ospf timer ldp-sync holdmaxcost 9
 mpls ldp timer igp-sync-delay 6
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.2.1.1 255.255.255.252
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 2.2.2.9 0.0.0.0
  network 10.1.1.0 0.0.0.3
  network 10.2.1.0 0.0.0.3
#
return
```

- Configuration file of P3

```
#
sysname P3
#
mpls lsr-id 3.3.3.9
#
mpls
#
mpls ldp
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.3.1.2 255.255.255.252
#
```

```
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.4.1.1 255.255.255.252
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 3.3.3.9 0.0.0.0
  network 10.3.1.0 0.0.0.3
  network 10.4.1.0 0.0.0.3
#
return
```

- Configuration file of P4

```
#
sysname P4
#
mpls lsr-id 4.4.4.9
#
mpls
#
mpls ldp
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.5.1.2 255.255.255.252
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.6.1.1 255.255.255.252
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 4.4.4.9 0.0.0.0
  network 10.5.1.0 0.0.0.3
  network 10.6.1.0 0.0.0.3
#
return
```

- Configuration file of PE2

```
#
sysname PE2
#
mpls lsr-id 5.5.5.9
#
mpls
#
mpls ldp
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.2.1.2 255.255.255.252
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.4.1.2 255.255.255.252
#
interface Pos3/0/0
 undo shutdown
 link-protocol ppp
```

```
 ip address 10.6.1.2 255.255.255.252
#
interface LoopBack1
 ip address 5.5.5.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 5.5.5.9 0.0.0.0
  network 10.2.1.0 0.0.0.3
  network 10.4.1.0 0.0.0.3
  network 10.6.1.0 0.0.0.3
#
return
```

Related Tasks

1.7 Configuring Synchronization Between LDP and IGP

1.12.7 Example for Configuring LDP GR

This section describes how to configure LDP GR, including enabling MPLS and MPLS LDP on each LSR and interface and enabling LDP GR on a GR Restarter and its neighbor.

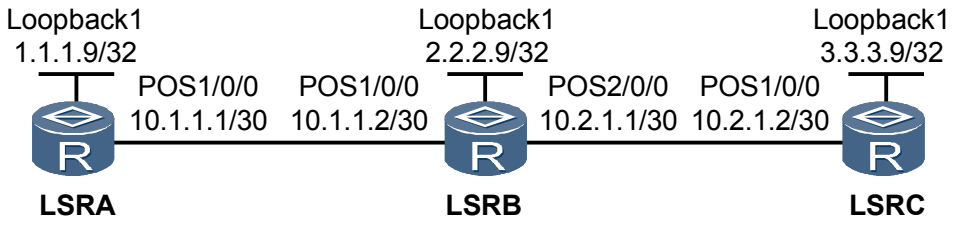
Networking Requirements

CAUTION

On a single NE5000E, an interface is numbered in the format of slot number/card number/interface number. On an NE5000E cluster, the interface is numbered in the format of chassis ID/slot number/card number/interface number. This requires the chassis ID to be specified along with the slot number.

As shown in **Figure 1-15**, LSR A, LSR B, and LSR C are devices with a single main control board. Without GR, during the master/slave switchover or upgrade of the system, the LSPs are deleted because the neighbor goes Down, which causes short traffic interruption. In this case, you can configure LDP GR to ensure that the labels are the same before and after the master/slave switchover or the restart of a protocol, and the LDP sessions and LSPs are reestablished after the master/slave switchover or upgrade of the system. In this manner, the MPLS forwarding is uninterrupted and traffic is unaffected.

Figure 1-15 Networking diagram of configuring LDP GR



Configuration Notes

When configuring LDP GR, note the following:

- Enabling or disabling LDP GR causes an LDP session to be reestablished.
- Changing the value of an LDP GR timer also causes an LDP session to be reestablished.

Configuration Roadmap

The configuration roadmap is as follows:

1. Assign an IP address to each interface, and configure OSPF to advertise the route to the segment of each interface and the host route to each LSR ID.
2. Enable MPLS and MPLS LDP globally on each LSR.
3. Enable MPLS and MPLS LDP on each interface.
4. Configure LDP GR.
5. Set LDP GR parameters on a GR Restarter.

Data Preparation

To complete the configuration, you need the following data:

- IP address of the interface on each LSR as shown in **Figure 1-15**, OSPF process ID, OSPF area ID
- OSPF GR interval
- LDP reconnecting time
- LDP neighbor-liveness time
- LDP recovery time

Procedure

Step 1 Assign an IP address to each interface, and configure OSPF to advertise the route to the segment of each interface and the host route to each LSR ID. The configuration details are not mentioned here.

Step 2 Enable MPLS and MPLS LDP globally on each LSR.

Configure LSR A.

```
[~LSRA] mpls lsr-id 1.1.1.9
[~LSRA] mpls
[~LSRA-mpls] quit
[~LSRA] mpls ldp
[~LSRA-mpls-ldp] commit
[~LSRA-mpls-ldp] quit
```

Configure LSR B.

```
[~LSRB] mpls lsr-id 2.2.2.9
[~LSRB] mpls
[~LSRB-mpls] quit
[~LSRB] mpls ldp
[~LSRB-mpls-ldp] commit
[~LSRB-mpls-ldp] quit
```

Configure LSR C.

```
[~LSRC] mpls lsr-id 3.3.3.9
[~LSRC] mpls
[~LSRC-mpls] quit
[~LSRC] mpls ldp
[~LSRC-mpls-ldp] commit
[~LSRC-mpls-ldp] quit
```

Step 3 Enable MPLS and MPLS LDP on each interface.

Configure LSR A.

```
[~LSRA] interface pos 1/0/0
[~LSRA-Pos1/0/0] mpls
[~LSRA-Pos1/0/0] mpls ldp
[~LSRA-Pos1/0/0] commit
[~LSRA-Pos1/0/0] quit
```

Configure LSR B.

```
[~LSRB] interface pos 1/0/0
[~LSRB-Pos1/0/0] mpls
[~LSRB-Pos1/0/0] mpls ldp
[~LSRB-Pos1/0/0] commit
[~LSRB-Pos1/0/0] quit
[~LSRB] interface pos 2/0/0
[~LSRB-Pos2/0/0] mpls
[~LSRB-Pos2/0/0] mpls ldp
[~LSRB-Pos2/0/0] commit
[~LSRB-Pos2/0/0] quit
```

Configure LSR C.

```
[~LSRC] interface pos 1/0/0
[~LSRC-Pos1/0/0] mpls
[~LSRC-Pos1/0/0] mpls ldp
[~LSRC-Pos1/0/0] commit
[~LSRC-Pos1/0/0] quit
```

After the preceding configurations, local LDP sessions are successfully set up between LSR A and LSR B, and between LSR B and LSR C.

Run the **display mpls ldp session** command on an LSR. You can view information about the established LDP session. Take the display on LSR A as an example.

```
[~LSRA] display mpls ldp session

 LDP Session(s) in Public Network
 Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDD:HH:MM)
 A '*' before a session means the session is being deleted.
------------------------------------------------------------------------------
 PeerID             Status      LAM  SsnRole  SsnAge       KASent/Rcv
------------------------------------------------------------------------------
2.2.2.9:0          Operational DU   Passive  000:00:02   9/9
------------------------------------------------------------------------------
TOTAL: 1 Session(s) Found.
```

Step 4 Configure LDP GR.

Configure LSR A.

```
[~LSRA] mpls ldp
[~LSRA-mpls-ldp] graceful-restart
Warning: All the related sessions will be deleted if the operation is performed!
 Continue? [Y/N]:y
[~LSRA-mpls-ldp] commit
[~LSRA-mpls-ldp] quit
```

Configure LSR B.

```
[~LSRB] mpls ldp
[~LSRB-mpls-ldp] graceful-restart
Warning: All the related sessions will be deleted if the operation is performed!
 Continue? [Y/N]:y
[~LSRB-mpls-ldp] commit
[~LSRB-mpls-ldp] quit
```

Configure LSR C.

```
[~LSRC] mpls ldp
[~LSRC-mpls-ldp] graceful-restart
Warning: All the related sessions will be deleted if the operation is performed!
 Continue? [Y/N]:y
[~LSRC-mpls-ldp] commit
[~LSRC-mpls-ldp] quit
```

Step 5 Verify the configuration.

After the preceding configuration, run the **display mpls ldp session verbose** command on an LSR. You can view that the **Session FT Flag** field indicates **On**. Take the display on LSR A as an example.

```
[~LSRA] display mpls ldp session verbose
              LDP Session(s) in Public Network
 ------------------------------------------------------------------------------
 Peer LDP ID     : 2.2.2.9:0        Local LDP ID   : 1.1.1.9:0
 TCP Connection  : 1.1.1.9 <- 2.2.2.9
 Session State   : Operational          Session Role   : Active
 Session FT Flag : On                  MD5 Flag       : Off
 Reconnect Timer : 300                  Recovery Timer : 300
 Negotiated Keepalive Hold Timer   : 45 Sec
 Configured Keepalive Send Timer   : 15 Sec
 Keepalive Message Sent/Rcvd       : 1/1 (Message Count)
 Label Advertisement Mode          : Downstream Unsolicited
 Label Resource Status(Peer/Local) : Available/Available
 Session Age                       : 000:01:39  (DDD:HH:MM)
 Addresses received from peer: ( Count: 1 )
 2.2.2.9
 ------------------------------------------------------------------------------
```

Alternatively, run the **display mpls ldp peer verbose** command on an LSR. You can view that the **Peer FT Flag** field indicates **On**. Take the display on LSR A as an example.

```
[~LSRA] display mpls ldp peer verbose

        LDP Peer Information in Public network
 ------------------------------------------------------------------
 Peer LDP ID         : 2.2.2.9:0
 Peer Max PDU Length : 4096           Peer Transport Address : 2.2.2.9:0
 Peer Loop Detection : Off            Peer Path Vector Limit : 0
 Peer FT Flag        : On             Peer Keepalive Timer   : 45 Sec
 Recovery Timer      : 300            Reconnect Timer        : 300
 Peer Type : Local
 Peer Label Advertisement Mode : Downstream Unsolicited
 Distributed    ID             : 0

Peer Discovery Source         : Pos1/0/0
 ------------------------------------------------------------------------------
```

----End

Configuration Files

- Configuration file of LSR A

```
#
sysname LSRA
#
```

```
mpls lsr-id 1.1.1.9
#
mpls
#
mpls ldp
 graceful-restart
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.1.1.1 255.255.255.252
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.3
#
return
```

- Configuration file of LSR B

```
#
sysname LSRB
#
mpls lsr-id 2.2.2.9
#
mpls
#
mpls ldp
 graceful-restart
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.1.1.2 255.255.255.252
 mpls
 mpls ldp
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
ip address 10.2.1.1 255.255.255.252
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#
ospf 1
area 0.0.0.0
  network 2.2.2.9 0.0.0.0
  network 10.1.1.0 0.0.0.3
  network 10.2.1.0 0.0.0.3
#
return
```

- Configuration file of LSR C

```
#
sysname LSRC
#
mpls lsr-id 3.3.3.9
#
mpls
#
mpls ldp
 graceful-restart
```

```
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.2.1.2 255.255.255.252
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
ospf 1
area 0.0.0.0
  network 3.3.3.9 0.0.0.0
  network 10.2.1.0 0.0.0.3
#
Return
```

Related Tasks

1.8 Configuring the LDP GR Helper

1.12.8 Example for Configuring LDP over TE

This section describes how to configure LDP over TE, including the setup of a TE tunnel and a remote LDP peer.

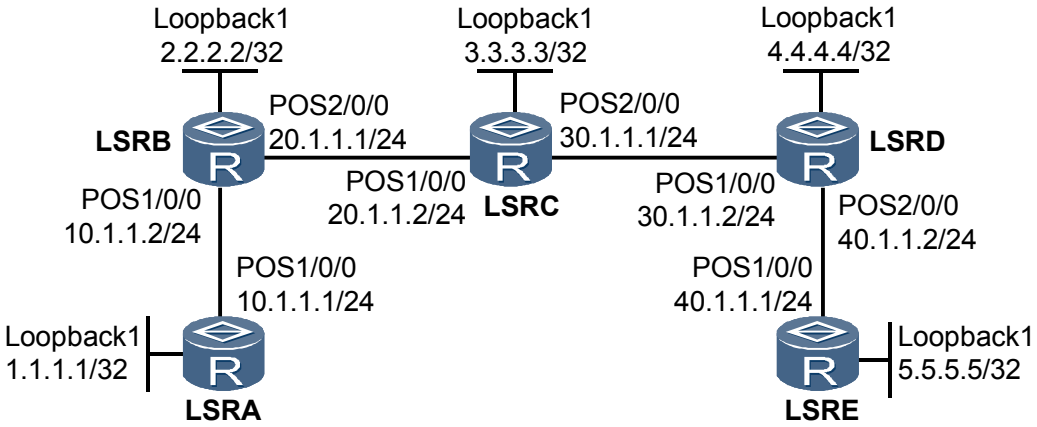
Networking Requirements

CAUTION

On a single NE5000E, an interface is numbered in the format: slot number/card number/interface number. On an NE5000E cluster, the interface is numbered in the format: chassis ID/slot number/card number/interface number. This requires the chassis ID to be specified along with the slot number.

On the network shown in **Figure 1-16**, LSR B and LSR D are at the edge of a backbone network. It is required that LDP over TE be deployed on this network, allowing an LDP LSP to across an RSVP-TE area. In this manner, LDP services can be transmitted between LSR A and LSR B, and between LSR D and LSR E. In addition, TE services are transmitted between LSR B, LSR C, and between LSR C and LSR D. A TE tunnel destined for LSR D is set up on LSR B, and an RSVP tunnel destined for LSR B is set up on LSR D. This requires that traffic between LSR A and LSR E be transmitted through the tunnel. LDP over TE can transmit VPN services.

Figure 1-16 Networking diagram of LDP over TE



Configuration Notes

When configuring LDP over TE, note that the tunnel destination address must be the LSR ID of the egress.

Configuration Roadmap

The configuration roadmap is as follows:

1. Assign an IP address to each interface; configure the loopback address as the LSR ID; configure an IGP to advertise the routes.
2. Enable OSPF TE in a TE-aware area and set up an MPLS TE tunnel.
3. Enable MPLS LDP in each non-TE-aware area and configure remote LDP peers at the edge of the TE-aware area.
4. Configure the forwarding adjacency.

Data Preparation

To complete the configuration, you need the following data:

- OSPF process ID and OSPF area ID
- Policy for triggering the establishment of LSPs
- Name and IP address of each remote LDP peer of LSR B and LSR D
- Link bandwidth attributes of the tunnel
- Tunnel interface number, IP address, destination address, tunnel ID, RSVP-TE tunnel signaling protocol, tunnel bandwidth, TE metric value, link cost on LSR B and LSR D

Procedure

Step 1 Assign an IP address to each interface.

Assign an IP address to each interface, including the loopback interface on each LSR shown in **Figure 1-16**. The configuration procedure is not provided.

Step 2 Configure OSPF to advertise the route to the segment of each interface and the host route to each LSR ID. The configuration procedure is not provided.

Step 3 Enable MPLS on each LSR. Enable LDP to set up LDP sessions between LSR A and LSR B, and between LSR D and LSR E. Enable RSVP TE to establish RSVP neighbor relationships between LSR B and LSR C, and between LSR C and LSR D.

Configure LSR A.

```
[~LSRA] mpls lsr-id 1.1.1.1
[~LSRA] mpls
[~LSRA-mpls] lsp-trigger all
[~LSRA-mpls] quit
[~LSRA] mpls ldp
[~LSRA-mpls-ldp] quit
[~LSRA] interface pos 1/0/0
[~LSRA-Pos1/0/0] mpls
[~LSRA-Pos1/0/0] mpls ldp
[~LSRA-Pos1/0/0] commit
[~LSRA-Pos1/0/0] quit
```

Configure LSR B.

```
[~LSRB] mpls lsr-id 2.2.2.2
[~LSRB] mpls
[~LSRB-mpls] mpls te
[~LSRB-mpls] lsp-trigger all
[~LSRB-mpls] mpls rsvp-te
[~LSRB-mpls] mpls te cspf
[~LSRB-mpls] quit
[~LSRB] mpls ldp
[~LSRB-mpls-ldp] quit
[~LSRB] interface pos 1/0/0
[~LSRB-Pos1/0/0] mpls
[~LSRB-Pos1/0/0] mpls ldp
[~LSRB-Pos1/0/0] quit
[~LSRB] interface pos 2/0/0
[~LSRB-Pos2/0/0] mpls
[~LSRB-Pos2/0/0] mpls te
[~LSRB-Pos2/0/0] mpls rsvp-te
[~LSRB-Pos2/0/0] commit
[~LSRB-Pos2/0/0] quit
```

Configure LSR C.

```
[~LSRC] mpls lsr-id 3.3.3.3
[~LSRC] mpls
[~LSRC-mpls] mpls te
[~LSRC-mpls] mpls rsvp-te
[~LSRC-mpls] quit
[~LSRC] interface pos 1/0/0
[~LSRC-Pos1/0/0] mpls
[~LSRC-Pos1/0/0] mpls te
[~LSRC-Pos1/0/0] mpls rsvp-te
[~LSRC-Pos1/0/0] quit
[~LSRC] interface pos 2/0/0
[~LSRC-Pos2/0/0] mpls
[~LSRC-Pos2/0/0] mpls te
[~LSRC-Pos2/0/0] mpls rsvp-te
[~LSRC-Pos2/0/0] commit
[~LSRC-Pos2/0/0] quit
```

Configure LSR D.

```
[~LSRD] mpls lsr-id 4.4.4.4
[~LSRD] mpls
[~LSRD-mpls] mpls te
[~LSRD-mpls] lsp-trigger all
[~LSRD-mpls] mpls rsvp-te
```

```
[~LSRD-mpls] mpls te cspf
[~LSRD-mpls] quit
[~LSRD] mpls ldp
[~LSRD-mpls-ldp] quit
[~LSRD] interface pos 1/0/0
[~LSRD-Pos1/0/0] mpls
[~LSRD-Pos1/0/0] mpls te
[~LSRD-Pos1/0/0] mpls rsvp-te
[~LSRD-Pos1/0/0] quit
[~LSRD] interface pos 2/0/0
[~LSRD-Pos2/0/0] mpls
[~LSRD-Pos2/0/0] mpls ldp
[~LSRD-Pos2/0/0] commit
[~LSRD-Pos2/0/0] quit
```

Configure LSR E.

```
[~LSRE] mpls lsr-id 5.5.5.5
[~LSRE] mpls
[~LSRE-mpls] lsp-trigger all
[~LSRE-mpls] quit
[~LSRE] mpls ldp
[~LSRE-mpls-ldp] quit
[~LSRE] interface pos 1/0/0
[~LSRE-Pos1/0/0] mpls
[~LSRE-Pos1/0/0] mpls ldp
[~LSRE-Pos1/0/0] commit
[~LSRE-Pos1/0/0] quit
```

After the preceding configurations, the local LDP sessions are successfully set up between LSR A and LSR B, and between LSR D and LSR E.

Run the **display mpls ldp session** command on LSR A, LSR B, LSR D, or LSR E. You can view information about the established LDP session. Take the display on LSR A as an example.

```
[~LSRA] display mpls ldp session
               LDP Session(s) in Public Network
------------------------------------------------------------------------------
 Peer-ID           Status      LAM  SsnRole  SsnAge      KA-Sent/Rcv
------------------------------------------------------------------------------
2.2.2.2:0          Operational DU   Passive  0000:00:22  91/91
------------------------------------------------------------------------------
TOTAL: 1 Session(s) Found.
 LAM : Label Advertisement Mode      SsnAge Unit : DDD:HH:MM
```

Run the **display mpls ldp peer** command on an LSR. You can view information about the established LDP peer. Take the display on LSR A as an example.

```
[~LSRA] display mpls ldp peer
         LDP Peer Information in Public network
 ------------------------------------------------------------------------------
 Peer-ID             Transport-Address  Discovery-Source     Did
 ------------------------------------------------------------------------------
 2.2.2.2:0           2.2.2.2            Pos1/0/0             0
 ------------------------------------------------------------------------------
 TOTAL: 1 Peer(s) Found.
```

Run the **display mpls lsp** command on an LSR. You can view information about LDP LSPs and RSVP tunnels are not set up. Take the display on LSR A as an example.

```
[~LSRA] display mpls lsp
------------------------------------------------------------------------------
                LSP Information: LDP LSP
------------------------------------------------------------------------------
FEC                In/Out Label  In/Out IF                      Vrf Name
1.1.1.1/32         3/NULL        Pos1/0/0/-
2.2.2.2/32         NULL/3        -/Pos1/0/0
2.2.2.2/32         1024/3        -/Pos1/0/0
10.1.1.0/24        3/NUL         Pos1/0/0/-
```

```
20.1.1.0/24        NULL/3        -/Pos1/0/0
20.1.1.0/24        1025/3        -/Pos1/0/0
```

Step 4 Configure a remote LDP session between LSR B and LSR D.

Configure LSR B.

```
[~LSRB] mpls ldp remote-peer LSRD
[~LSRB-mpls-ldp-remote-lsrd] remote-ip 4.4.4.4
[~LSRB-mpls-ldp-remote-lsrd] commit
[~LSRB-mpls-ldp-remote-lsrd] quit
```

Configure LSR D.

```
[~LSRD] mpls ldp remote-peer LSRB
[~LSRD-mpls-ldp-remote-lsrb] remote-ip 2.2.2.2
[~LSRD-mpls-ldp-remote-lsrb] commit
[~LSRD-mpls-ldp-remote-lsrb] quit
```

After the preceding configurations, a remote LDP session is set up between LSR B and LSR D. Run the **display mpls ldp remote-peer** command on LSR B or LSR D. You can view information about the remote session entity. Take the display on LSR B as an example.

```
[~LSRB] display mpls ldp remote-peer LSRD
                        LDP Remote Entity Information
 ------------------------------------------------------------------------------
 Remote Peer Name: LSRD
 Remote Peer IP: 4.4.4.4            LDP ID: 2.2.2.2:0
 Transport Address: 2.2.2.2         Entity Status: Active
 Configured Keepalive Timer: 45 Sec     Configured Hello Timer: 45 Sec
 Negotiated Hello Timer: 45 Sec         Hello Packet sent/received: 425/382
 ------------------------------------------------------------------------------
 TOTAL: 1 Remote-Peer(s) Found.
```

Step 5 Configure bandwidth attributes on each outgoing interface along the link of the TE tunnel.

Configure LSR B.

```
[~LSRB] interface pos 2/0/0
[~LSRB-Pos2/0/0] mpls te bandwidth max-reservable-bandwidth 20000
[~LSRB-Pos2/0/0] mpls te bandwidth bc0 20000
[~LSRB-Pos2/0/0] commit
[~LSRB-Pos2/0/0] quit
```

Configure LSR C.

```
[~LSRC] interface pos 1/0/0
[~LSRC-Pos1/0/0] mpls te bandwidth max-reservable-bandwidth 20000
[~LSRC-Pos1/0/0] mpls te bandwidth bc0 20000
[~LSRC-Pos1/0/0] quit
[~LSRC] interface pos 2/0/0
[~LSRC-Pos2/0/0] mpls te bandwidth max-reservable-bandwidth 20000
[~LSRC-Pos2/0/0] mpls te bandwidth bc0 20000
[~LSRC-Pos2/0/0] commit
[~LSRC-Pos2/0/0] quit
```

Configure LSR D.

```
[~LSRD] interface pos 1/0/0
[~LSRD-Pos1/0/0] mpls te bandwidth max-reservable-bandwidth 20000
[~LSRD-Pos1/0/0] mpls te bandwidth bc0 20000
[~LSRD-Pos1/0/0] commit
[~LSRD-Pos1/0/0] quit
```

Step 6 Configure a tunnel from LSR B to LSR D.

On LSR B, enable the forwarding adjacency on the tunnel interface and adjust the metric value of the forwarding adjacency to ensure that traffic destined for LSR D or LSR E passes through the tunnel.

```
[~LSRB] interface tunnel 1
[~LSRB-Tunnel1] ip address 2.2.2.2 32
[~LSRB-Tunnel1] tunnel-protocol mpls te
[~LSRB-Tunnel1] destination 4.4.4.4
[~LSRB-Tunnel1] mpls te tunnel-id 100
[~LSRB-Tunnel1] mpls te bandwidth ct0 10000
[~LSRB-Tunnel1] mpls te igp advertise
[~LSRB-Tunnel1] mpls te igp metric absolute 1
[~LSRB-Tunnel1] quit
[~LSRB] ospf 1
[~LSRB-ospf-1] area 0
[~LSRB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[~LSRB-ospf-1-area-0.0.0.0] quit
[~LSRB-ospf-1] enable traffic-adjustment advertise
[~LSRB-Tunnel1] commit
```

Step 7 Configure a tunnel from LSR D to LSR B.

On LSR D, enable the forwarding adjacency on the tunnel interface and adjust the metric value of the forwarding adjacency to ensure that traffic destined for LSR A or LSR B passes through the tunnel.

```
[~LSRD] interface tunnel 1
[~LSRD-Tunnel1] ip address 4.4.4.4 32
[~LSRD-Tunnel1] tunnel-protocol mpls te
[~LSRD-Tunnel1] destination 2.2.2.2
[~LSRD-Tunnel1] mpls te tunnel-id 101
[~LSRD-Tunnel1] mpls te tunnel-id 100
[~LSRD-Tunnel1] tunnel bandwidth ct0 10000
[~LSRD-Tunnel1] mpls te igp advertise
[~LSRD-Tunnel1] mpls te igp metric absolute 1
[~LSRD-Tunnel1] quit
[~LSRD] ospf 1
[~LSRD-ospf-1] area 0
[~LSRD-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[~LSRD-ospf-1-area-0.0.0.0] quit
[~LSRD-ospf-1] enable traffic-adjustment advertise
[~LSRD-Tunnel1] commit
```

Step 8 Verify the configuration.

After the preceding configurations, the tunnels are successfully set up. Run the **display interface tunnel** command on LSR B. You can view information about these tunnels.

```
[~LSRB] display interface tunnel
Tunnel1 current state : UP
Line protocol current state : UP
Last up time: 2007-10-29, 16:35:10
Description : HUAWEI, Tunnel 1 Interface (ifindex: 109, vr: 0)
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 2.2.2.2/32
Encapsulation is TUNNEL, loopback not set
Tunnel destination 4.4.4.4
Tunnel up/down statistics 1
Tunnel protocol/transport MPLS/MPLS, ILM is available
    300 seconds output rate 0 bits/sec, 0 packets/sec
    0 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets output,  0 bits
    0 output error
    ct0:0 packets output,  0 bytes
        0 output error
```

Run the **display ip routing-table** command on LSR B to check routing information. You can view that the outgoing interfaces destined for LSR D and LSR E are tunnel interfaces.

```
[~LSRB] display ip routing-table
Route Flags: R - relied, D - download for forwarding
------------------------------------------------------------------------------
Routing Table : _public_
```

```
         Destinations : 13       Routes : 13
Destination/Mask    Proto  Pre  Cost   Flags NextHop         Interface
        1.1.1.1/32  OSPF   15   10        D  10.1.1.1        Pos1/0/0
        2.2.2.2/32  Direct 0    0         D  127.0.0.1       InLoopBack0
        3.3.3.3/32  OSPF   15   10        D  20.1.1.2        Pos2/0/0
        4.4.4.4/32  OSPF   15   1         D  2.2.2.2         Tunnel1
        5.5.5.5/32  OSPF   15   11        D  2.2.2.2         Tunnel1
      127.0.0.0/8   Direct 0    0         D  127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0         D  127.0.0.1       InLoopBack0
       20.1.1.0/24  Direct 0    0         D  20.1.1.1        Pos2/0/0
       20.1.1.1/32  Direct 0    0         D  127.0.0.1       InLoopBack0
       30.1.1.0/24  OSPF   15   11        D  2.2.2.2         Tunnel1
       10.1.1.0/24  Direct 0    0         D  10.1.1.2        Pos1/0/0
       10.1.1.2/32  Direct 0    0         D  127.0.0.1       InLoopBack0
       40.1.1.0/24  OSPF   15   11        D  2.2.2.2         Tunnel1
```

Run the **display mpls lsp** command on LSR B, LSR C, or LSR D to check information about LSPs. You can view information about RSVP LSPs. Take the display on LSR B as an example.

```
[~LSRB] display mpls lsp
------------------------------------------------------------------------------
                  LSP Information: RSVP LSP
------------------------------------------------------------------------------
FEC                 In/Out Label  In/Out IF                      Vrf Name
4.4.4.4/32          NULL/1024     -/Pos2/0/0
------------------------------------------------------------------------------
                  LSP Information: LDP LSP
------------------------------------------------------------------------------
FEC                 In/Out Label  In/Out IF                      Vrf Name
3.3.3.3/32          1024/NULL     -/-
1.1.1.1/32          NULL/3        -/Pos1/0/0
1.1.1.1/32          1028/3        -/Pos1/0/0
4.4.4.4/32          NULL/3        -/Tun1/0/0
4.4.4.4/32          1025/3        -/Tun1/0/0
5.5.5.5/32          NULL/1029     -/Tun1/0/0
5.5.5.5/32          1026/1029     -/Tun1/0/0
30.1.1.0/24         NULL/3        -/Tun1/0/0
30.1.1.0/24         1027/3        -/Tun1/0/0
```

Check the routing table on LSR A, and you can view that the cost values change after the forwarding adjacency is configured.

```
[~LSRA] display ip routing-table
Route Flags: R - relied, D - download for forwarding
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 12       Routes : 12
Destination/Mask    Proto  Pre  Cost    Flags NextHop         Interface
        1.1.1.1/32  Direct 0    0         D   127.0.0.1       InLoopBack0
        2.2.2.2/32  OSPF   15   10        D   10.1.1.2        Pos1/0/0
        3.3.3.3/32  OSPF   15   20          D  10.1.1.2        Pos1/0/0
        4.4.4.4/32  OSPF   15   11          D  10.1.1.2         Pos1/0/0
        5.5.5.5/32  OSPF   15   21          D  10.1.1.2        Pos1/0/0
      127.0.0.0/8   Direct 0    0           D  127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
       20.1.1.0/24  OSPF   15   20          D  10.1.1.2        Pos1/0/0
       30.1.1.0/24  OSPF   15   21          D  10.1.1.2        Pos1/0/0
       10.1.1.0/24  Direct 0    0           D  10.1.1.1        Pos1/0/0
       10.1.1.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
       40.1.1.0/24  OSPF   15   21          D  10.1.1.2        Pos1/0/0
```

----End

Configuration Files

- Configuration file of LSR A

```
#
sysname LSRA
```

```
#
mpls lsr-id 1.1.1.1
#
mpls
  lsp-trigger all
#
mpls ldp
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 10.1.1.0 0.0.0.255
  mpls-te enable
#
return
```

- Configuration file of LSR B

```
#
sysname LSRB
#
mpls lsr-id 2.2.2.2
#
mpls
  mpls te
  mpls te cspf
  lsp-trigger all
  mpls rsvp-te
#
mpls ldp
#
mpls ldp remote-peer lsrd
 remote-ip 4.4.4.4
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 20.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 20000
 mpls te bandwidth bc0 20000
 mpls rsvp-te
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 mpls
 mpls ldp
#
interface Tunnel1
 ip address 2.2.2.2 32
 tunnel-protocol mpls te
 destination 4.4.4.4
 mpls te tunnel-id 100
```

```
 mpls te bandwidth ct0 10000
 mpls te igp advertise
 mpls te igp metric absolute 1
#
ospf 1
 enable traffic-adjustment advertise
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
  mpls-te enable
#
return
```

- Configuration file of LSR C

```
#
sysname LSRC
#
mpls lsr-id 3.3.3.3
#
mpls
  mpls te
  mpls rsvp-te
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 20.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 20000
 mpls te bandwidth bc0 20000
 mpls rsvp-te
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 30.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 20000
 mpls te bandwidth bc0 20000
 mpls rsvp-te
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 20.1.1.0 0.0.0.255
  network 30.1.1.0 0.0.0.255
  mpls-te enable
#
return
```

- Configuration file of LSR D

```
#
sysname LSRD
#
mpls lsr-id 4.4.4.4
#
mpls
  mpls te
  mpls te cspf
  lsp-trigger all
  mpls rsvp-te
#
mpls ldp
#
```

```
mpls ldp remote-peer lsrb
 remote-ip 2.2.2.2
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 30.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 20000
 mpls te bandwidth bc0 20000
 mpls rsvp-te
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 40.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 mpls
 mpls ldp
#
interface Tunnel1
 ip address 4.4.4.4 32
 tunnel-protocol mpls te
 destination 2.2.2.2
 mpls te tunnel-id 101
 mpls te bandwidth ct0 10000
 mpls te igp advertise
 mpls te igp metric absolute 1
#
ospf 1
 enable traffic-adjustment advertise
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 30.1.1.0 0.0.0.255
  network 40.1.1.0 0.0.0.255
  mpls-te enable
#
return
```

- Configuration file of LSR E

```
#
sysname LSRE
#
mpls lsr-id 5.5.5.5
#
mpls
  lsp-trigger all
#
mpls ldp
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 40.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 5.5.5.5 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 5.5.5.5 0.0.0.0
  network 40.1.1.0 0.0.0.255
  mpls-te enable
```

```
#
return
```

Related Tasks

1.9 Configuring LDP over TE

2 MPLS TE Configuration

About This Chapter

This chapter describes the principles for Multiprotocol Label Switching Traffic Engineering (MPLS TE), Resource Reservation Protocol (RSVP) TE tunnels, RSVP signaling parameter adjustment, RSVP authentication, tunnel parameter adjustment, measures for adjusting TE forwarding, bandwidth flood threshold, tunnel re-optimization, Differentiated Service (DS) TE, MPLS TE fast reroute (FRR), MPLS TE Auto FRR, Constraints-routed label switched path (CR-LSP), RSVP graceful restart (GR), static bidirectional forwarding detection (BFD) for CR-LSP, dynamic BFD for CR-LSP, MPLS TE distribution, and how to configure MPLS TE, and provides configuration examples.

The IGP shortcut and forwarding adjacency are configured to allow a CR-LSP to participate in IGP route calculation. This adjusts the MPLS TE traffic forwarding.

2.8 Adjusting the Threshold for Flooding Bandwidth Information
If the link bandwidth changes slightly, the threshold for flooding bandwidth information is set on the ingress or a transit node of a CR-LSP, which reduces flooding attempts and saves network resources.

2.9 Configuring MPLS TE Manual FRR
MPLS TE manual FRR is a local protection mechanism and protects traffic on a link or a node along a CR-LSP.

2.10 Configuring MPLS TE Auto FRR
MPLS TE Auto FRR is a local protection mechanism that protects traffic on a link or a node on a CR-LSP.

2.11 Configuring CR-LSP Backup
CR-LSP backup is configured to provide end-to-end protection for a CR-LSP.

2.12 Configuring an RSVP GR Helper
An RSVP GR Helper is configured to allow devices along an RSVP-TE tunnel to retain RSVP sessions during a master/slave switchover.

2.13 Configuring Static BFD for CR-LSP
By configuring static BFD for CR-LSP, you can detect a static CR-LSP or an RSVP CR-LSP.

2.14 Configuring the Static BFD for TE
This section describes how to configure the static BFD for TE to detect faults on the TE tunnel.

2.15 Maintaining MPLS TE
This section describes how to remove MPLS TE information and debug MPLS TE.

2.16 Configuration Examples
This section provides MPLS TE configuration examples.

2.1 MPLS TE Overview

The Multiprotocol Label Switching Traffic Engineering (MPLS TE) technology integrates the MPLS technology with TE. It reserves resources by setting up label switched paths (LSPs) over a specified path in an attempt to prevent network congestion and balance network traffic.

TE

Congestion is a major cause for the poor performance of a backbone network. A network may be congested because of insufficient resources or be partially congested because of network resource imbalance. TE prevents congestion caused by load imbalance.

TE dynamically monitors network traffic and loads on network elements, and adjusts parameters of traffic management, routing, and resource constraints in real time.

MPLS TE

The MPLS TE technology integrates the MPLS technology with TE. MPLS TE reserves resources by setting up LSPs over a specified path in an attempt to prevent network congestion and balance network traffic.

An LSP with a higher priority preempts resources such as bandwidth of an LSP with a lower priority. This ensures bandwidth requirements for services with a higher priority if resources are insufficient.

In addition, if an LSP fails or a node is congested, MPLS TE uses fast reroute (FRR) function and backup paths to protect traffic.

A network administrator uses MPLS TE to deploy LSPs to properly allocate network resources, preventing network congestion. Administrators can use designated offline utility to analyze traffic over the increasing number of LSPs.

2.2 MPLS TE Features Supported by the NE5000E

On the NE5000E, RSVP-TE signaling is used to set up TE tunnels, and a variety of attributes are used to adjust parameters for TE tunnels and traffic forwarding. In addition, traffic protection mechanisms are available, such as TE FRR and CR-LSP backup, improving tunnel reliability.

NOTE

This section describes MPLS TE features supported by the NE5000E. For more information about MPLS TE features, see the chapter "MPLS TE" in the *HUAWEI NetEngine5000E Core Router Feature Description - MPLS*.

RSVP-TE Tunnels

RSVP-TE signaling is used to set up RSVP-TE tunnels or adapt RSVP-TE tunnels to changing network conditions.

The RSVP-TE features on the NE5000E are described as follows:

- Collecting and advertising TE link information

  RSVP-TE uses an extended Interior Gateway Protocol (IGP) to collect and advertise TE link information and set up a traffic engineering database (TEDB). The extended IGP is

either Open Shortest Path First (OSPF) TE or Intermediate System-to-Intermediate System (IS-IS) TE. An extended IGP periodically floods link information, and also floods link information if a link goes Up or Down, link attributes change, or the reservable bandwidth on a link changes to a certain extent. The bandwidth flooding is triggered by setting a flood threshold or using a command.

- Path calculation

  On the NE5000E, the path of a TE tunnel is calculated using Constrained Shortest Path First (CSPF). If multiple reachable paths share the same weight, one path is selected based on the configured tie-breaking policy.

  In addition to reservable bandwidth and the administrative group attribute for a link, the following attributes can be set for a tunnel:

  - Tunnel bandwidth
  - Affinity property
  - Explicit path
  - Maximum hop limit
  - Shared risk link group (SRLG)

- Establishing an RSVP-TE tunnel

  NE5000Es can be configured to record information about routes and labels during the establishment of an RSVP-TE tunnel. The NE5000Es preempt bandwidth of other RSVP-TE tunnels with lower setup and holding priorities before establishing an RSVP-TE tunnel if resources are insufficient.

  If the NE5000E fails to establish an RSVP-TE tunnel, it attempts to re-establish the RSVP-TE tunnel periodically.

- Signaling mechanism

  NE5000EThe NE5000E reserves resources using RSVP-TE in either fixed filter (FF) or shared-explicit (SE) styles. The NE5000E supports RSVP extensions, such as confirmation and retransmission of RSVP messages, summary refresh (Srefresh), and the Hello mechanism. The RSVP extensions help the NE5000E relieve network loads and improve network reliability. In addition, the NE5000E supports RSVP authentication, improving network security.

- Traffic forwarding

  A tunnel policy is used to import Virtual Private Network (VPN) traffic to TE tunnels; policy-based routing, IGP shortcut, or forwarding adjacency is used to import non-VPN traffic to TE tunnels.

- Optimizing and adjusting tunnels

  After TE tunnels have been set up, the tunnels are adjusted and optimized using the following features:

  - Tunnel re-optimization: automatically triggers re-optimization of a CR-LSP. The NE5000E resends a request for calculating a better path for a CR-LSP. After the new CR-LSP has been established, the NE5000E switches traffic to the new CR-LSP.
  - Route pinning: pins the path of a tunnel that has been set up. This prevents the path from being changed even if a better path is calculated.

Reliability

The NE5000E supports the following reliability features applied to MPLS TE tunnels:

- FRR

  FRR is a local protection mechanism in RSVP-TE. FRR protects CR-LSP links and nodes against faults. Either manual or Auto FRR is performed to manually or automatically establish a bypass tunnel.

- CR-LSP backup

  CR-LSP backup protects an entire RSVP-TE CR-LSP from end to end. If a primary CR-LSP fails, traffic switches to a backup CR-LSP. If both the primary and backup CR-LSPs cannot be established, a best-effort path will be established, allowing traffic to switch to the best-effort path.

- BFD

  Bidirectional Forwarding Detection (BFD) detects a CR-LSP fault in milliseconds. BFD is applicable to a network that requires rapid detection but does not provide a hardware detection mechanism.

- RSVP GR

  RSVP graceful restart (GR) is a status recovery mechanism for RSVP-TE tunnels. If a switchover is triggered by faults or operations on the control plane, RSVP GR guarantees proper data transmission on the forwarding plane and restores the correct RSVP-TE CR-LSP status on the control plane. The NE5000E supports FRR and manual re-optimization during the GR process.

- RSVP NSR

  With the growth of IP-/MPLS-based bearer networks and Metropolitan Area Networks (MANs), operators require higher availability. Non-Stop Routing (NSR), a high availability (HA) solution, becomes more and more popular with operators.

  RSVP implements NSR by synchronizing data on the slave control board with that on the master control board. If a fault occurs, a switchover is triggered. NSR ensures that the slave control board rapidly takes over services on the original master control board after switchover, but neighbors does not detect the fault on the local node. For details about RSVP NSR configurations, see the *NE5000E Configuration Guide - Reliability*.

2.3 Configuring an RSVP-TE Tunnel

MPLS TE reserves resources for RSVP-TE tunnels. These tunnels are established along specified paths, not passing through congested nodes, balancing traffic on a network.

Applicable Environment

The dynamic RSVP-TE signaling protocol adjusts a path of a TE tunnel, adapting to network topology changes. To help implement advanced features such as TE FRR or CR-LSP backup, using the RSVP-TE signaling protocol to set up an MPLS TE tunnel is recommended.

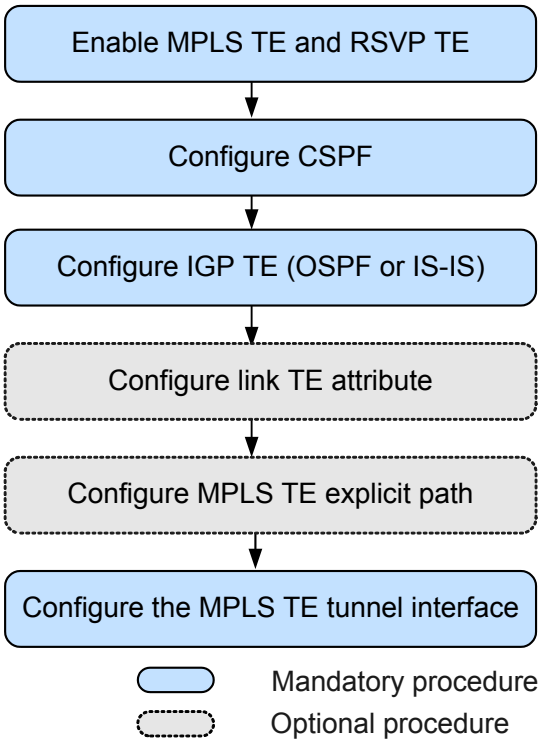
Pre-configuration Tasks

Before configuring an RSVP-TE tunnel, complete the following tasks:

- Configuring OSPF or IS-IS to ensure reachability between label switching routers (LSRs)
- Setting the LSR ID for every LSR
- Enabling MPLS in the system and interface views on every LSR

Configuration Procedures

Figure 2-1 Flowchart for configuring an RSVP-TE tunnel



2.3.1 Enabling MPLS TE and RSVP-TE

MPLS TE and RSVP-TE must be enabled on each LSR in an MPLS domain before TE features are configured.

Context

NOTE

- If MPLS TE is disabled in the MPLS view, MPLS TE enabled in the interface view is also disabled, all CR-LSPs configured on this interface go Down, and all configurations associated with these CR-LSPs are deleted.
- If MPLS TE is disabled in the interface view, all CR-LSPs on the interface go Down.
- If RSVP-TE is disabled on an LSR, RSVP-TE is also disabled on all interfaces on this LSR.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Step 3 Run:

```
mpls te
```

MPLS TE is enabled globally.

Step 4 Run:

```
mpls rsvp-te
```

RSVP-TE is enabled.

Step 5 Run:

```
quit
```

The system view is displayed.

Step 6 Run:

```
interface interface-type interface-number
```

The view of the interface on which the MPLS TE tunnel is established is displayed.

Step 7 Run:

```
mpls rsvp-te
```

MPLS TE is enabled on the interface.

Step 8 Run:

```
mpls rsvp-te
```

RSVP-TE is enabled on the interface.

Step 9 Run:

```
commit
```

The configurations are committed.

----End

2.3.2 Configuring CSPF

CSPF is configured to calculate the shortest path destined for a specified node.

Context

Configuring CSPF on all nodes along a path ensures that the ingress calculates a complete path.

CSPF calculates only the shortest path to reach the tunnel destination. During path computation, if there are multiple paths with the same weight, the optimal path is selected using the tie-breaking function.

The tie-breaking function is performed in one of the following modes:

- Most-fill: selects a link with the largest ratio of the used bandwidth to the maximum reservable bandwidth. This mode ensures that bandwidth resources are used effectively.
- Least-fill: selects a link with the smallest ratio of the used bandwidth to the maximum reservable bandwidth. This mode ensures that bandwidth resources of links are used evenly.
- Random: selects a link at random. This mode allows CR-LSPs to distribute evenly over links regardless of bandwidth.

NOTE

Tie-breaking selects a link based on a bandwidth ratio. If ratios are the same in the situation where no reservable bandwidth is available or the same bandwidth is used on every link, the link that is discovered firstly is used, even if **least-fill** or **most-fill** is configured.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Step 3 Run:

```
mpls te cspf
```

CSPF is enabled on the local node.

CSPF is disabled by default.

Step 4 (Optional) Run:

```
mpls te cspf preferred-igp { isis | ospf }
```

A preferred IGP is configured.

Step 5 Run:

```
mpls te tie-breaking { least-fill | most-fill | random }
```

A tie-breaking mode for calculating a path for a CR-LSP is configured.

The default tie-breaking mode is **random**.

Step 6 Run:

```
quit
```

The system view is displayed.

Step 7 Run:

```
interface tunnel tunnel-number
```

The view of the MPLS TE tunnel interface is displayed.

Step 8 Run:

```
mpls te tie-breaking { least-fill | most-fill | random }
```

The tie-breaking function for calculating a path is configured for the current tunnel.

The tie-breaking mode is configured either the tunnel interface view or MPLS view. If the tie-breaking mode configured in both the tunnel interface and MPLS views, the configuration in the tunnel interface view takes effect.

Step 9 Run:

```
commit
```

The configurations are committed.

----End

2.3.3 Configuring IGP TE (OSPF or IS-IS)

After IGP TE is configured on each LSR in an MPLS domain, a TEDB is generated on the MPLS network.

Context

IGP TE is configured in either of the following modes as needed on a network:

NOTE

If neither OSPF TE nor IS-IS TE is configured, no TE link state advertisement (LSA) or TE Link State PDU (LSP) is generated on the network, and no TEDB is generated.

- Configure OSPF TE.

  An OSPF area does not support TE by default.

  OSPF TE uses Opaque Type 10 LSAs to carry TE attributes. Therefore, the OSPF Opaque capability must be enabled on each LSR. In addition, TE LSAs are generated only when at least one OSPF neighbor is in the FULL state.

- Configure IS-IS TE.

  By default, an IS-IS process does not support TE.

  IS-IS TE uses the sub-Time-Live-Value (sub-TLV) in the IS-reachable TLV (22) to carry TE attributes. Therefore, the IS-IS wide metric attribute must be configured, and its value is narrow, wide, compatible, or wide-compatible. By default, IS-IS sends or receives packets carrying a route metric that is expressed in Narrow mode.

Procedure

- Configure OSPF TE.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     ospf [*process-id*]

     The OSPF view is displayed.
  3. Run:
     opaque-capability enable

     The OSPF Opaque capability is enabled.

     NOTE

     This step is necessary only on an Area Border Router (ABR) in multiple OSPF areas.
  4. Run:
     area *area-id*

     The OSPF area view is displayed.
  5. Run:
     mpls-te enable [**standard-complying**]

     TE is enabled in the OSPF area.
  6. Run:

commit

The configurations are committed.

- Configure IS-IS TE.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     isis [*process-id*]

     The IS-IS view is displayed.
  3. Run:
     cost-style { **wide** | **compatible** | **wide-compatible** }

     The IS-IS wide metric attribute is configured.
  4. Run:
     traffic-eng [**level-1** | **level-2** | **level-1-2**]

     IS-IS TE is enabled.

     If no level is specified when IS-IS TE is enabled, IS-IS TE is valid for both Level-1 and Level-2 routers.
  5. Run:
     commit

     The configurations are committed.

----End

2.3.4 (Optional) Configuring TE Attributes for a Link

Configuring TE attributes, such as the link bandwidth, administrative group attribute, affinity property, and SRLS allows you to select a required link for a CR-LSP.

Context

TE attributes of a link are as follows:

- Link bandwidth

  The link bandwidth attribute must be set if the CR-LSP bandwidth needs to be limited. The default maximum reservable link bandwidth is 0 bit/s.

  NOTE

  If no bandwidth is set for a link, the CR-LSP bandwidth will be higher than the maximum reservable link bandwidth. As a result, the CR-LSP cannot be set up.

- Administrative group attribute and affinity property

  The affinity property determines attributes for links to be used by an MPLS TE tunnel. The affinity property, together with the link administrative group attribute, is used to determine which link a tunnel uses. The administrative group attribute and affinity property are configured on the ingress of a CR-LSP.

  The default values of the administrative group, affinity property, and mask are all 0x0.

- SRLG

A shared risk link group (SRLG) is a set of links which are likely to fail concurrently when sharing a physical resource (for example, an optical fiber). Links in an SRLG at the same risk of faults. If one of the links fails, other links in the SRLG also fail.

An SRLG enhances CR-LSP reliability on an MPLS TE network enabled with CR-LSP hot standby or TE FRR. Two or more links are at the same risk if they share physical resources. Assume that links on an interface and its sub-interfaces are in an SRLG. This means sub-interfaces share risks with their interface. These sub-interfaces will go Down if the interface goes Down. If the links of a primary tunnel and a backup or bypass tunnel are in one SRLG, the links of a backup or bypass tunnel share risks with the links of the primary tunnel. The backup or bypass tunnel will go Down if the primary tunnel goes Down.

Procedure

- Configure link bandwidth.

  In real world situations, the bandwidth value is set on outbound interfaces along links of a TE tunnel that requires sufficient bandwidth.

  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*

     The view of the MPLS TE-enabled interface is displayed.
  3. Run:
     mpls te bandwidth max-reservable-bandwidth *bandwidth*

     The maximum reservable link bandwidth is set.
  4. Run:
     mpls te bandwidth bc0 *bc0-bandwidth*

     The BC bandwidth is set for the link.

     NOTE

     - The maximum reservable link bandwidth cannot be greater than the actual link bandwidth. A maximum of 80% of the link bandwidth is recommended for the maximum reservable link bandwidth.
     - The BC0 bandwidth cannot be greater than the maximum reservable link bandwidth.
  5. Run:
     commit

     The configurations are committed.

- Configure the administrative group attribute and affinity property.

  NOTE

  - The modified administrative group attribute takes effect only on LSPs that will be established, not on LSPs that have been set up.
  - After the modified affinity property is committed, the system will recalculate a path for the TE tunnel, and the established LSPs in this TE tunnel will be affected.

  1. Run:
     system-view

The system view is displayed.

2. Run:
   interface *interface-type interface-number*

   The view of the interface on which the MPLS TE tunnel is established is displayed.
3. Run:
   mpls te link administrative group *value*

   The administrative group attribute is configured for the link.
4. Run:
   quit

   The system view is displayed.
5. Run:
   interface tunnel *tunnel-number*

   The view of the MPLS TE tunnel interface is displayed.
6. Run:
   mpls te affinity property *properties* [**mask** *mask-value*] [**secondary** | **best-effort**]

   The affinity property is configured for the MPLS TE tunnel.
7. Run:
   commit

   The configurations are committed.

- Configure an SRLG.

  NOTE

  On the ingress of a hot-standby CR-LSP or a TE FRR tunnel, perform Steps 1 to 3. On the interface of each SRLG member, perform Step 5 and Step 6.

  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     mpls

     The MPLS view is displayed.
  3. Run:
     mpls te srlg path-calculation [**preferred** | **strict**]

     The SRLG path calculation mode is configured.

     NOTE

     - If **strict** is configured, CSPF uses an SRLG as a constraint when calculating a path for a bypass or backup CR-LSP.
     - If **preferred** is configured, CSPF uses an SRLG as a constraint when calculating a path for a bypass or backup CR-LSP for the first time; if calculation fails, CSPF no longer uses the SRLG as a constraint.
  4. Run:
     quit

     The system view is displayed.

5. Run:
   interface *interface-type interface-number*

   The view of the interface on which the MPLS TE tunnel is established is displayed.
6. Run:
   mpls te srlg *srlg-number*

   The link on which the interface resides joins the SRLG.

   On a network with hot standby or TE FRR, the SRLG attribute needs to be configured for the outbound interface of the ingress on a tunnel and other members of the SRLG. A link joins an SRLG after the SRLG attribute is configured on an outbound interface of the link.
7. Run:
   commit

   The configuration is committed.

----End

2.3.5 (Optional) Configuring an Explicit Path

An explicit path is configured on the ingress of an MPLS TE tunnel, specifying the nodes through which the MPLS TE tunnel passes or bypasses.

Context

An explicit path consists of a series of nodes. These nodes are arranged in the sequence by configuration and form a vector path. An IP address for an explicit path is an interface IP address on every node. The loopback IP address of the egress node is usually used as the destination address of an explicit path.

Two adjacent nodes are connected in either of the following modes on an explicit path:

- Strict: A hop is directly connected to its next hop.
- Loose: Other nodes may exist between a hop and its next hop.

The strict and loose modes are used either separately or together.

TE tunnels are classified into the following types:

- Intra-area tunnel: indicates a TE tunnel in a single OSPF or IS-IS area, but not an autonomous system (AS) running the Border Gateway Protocol (BGP).
- Inter-area tunnel: indicates a TE tunnel traversing multiple OSPF or IS-IS areas, but not BGP ASs.

A strict explicit path is used to establish an inter-area TE tunnel, on which a next hop can be only an Area Border Router (ABR) or an Autonomous System Boundary Router (ASBR).

Procedure

Step 1 Run:
system-view

The system view is displayed.

Step 2 Run:

```
explicit-path path-name
```

An explicit path is created and the explicit path view is displayed.

Step 3 Run:

```
next hop ip-address [ include [ strict | loose ] | exclude ]
```

The next-hop address is specified for the explicit path.

include strict are used by default, meaning a tunnel must pass through a specified node.

include indicates that a tunnel does pass through a specified node; **exclude** indicates that a tunnel does not pass through a specified node.

Step 4 (Optional) Run:

```
add hop ip-address1 [ include [ strict | loose ] | exclude ] { after | before } ip-address2
```

A node is added to the explicit path.

include strict are used by default, meaning a tunnel must pass through a specified node.

Step 5 (Optional) Run:

```
modify hop ip-address1 ip-address2 [ include [ strict | loose ] | exclude ]
```

The address of a node on an explicit path is changed.

include strict are used by default, meaning a tunnel must pass through a specified node.

Step 6 (Optional) Run:

```
delete hop ip-address
```

A node is deleted from an explicit path.

Step 7 (Optional) Run:

```
list hop [ ip-address ]
```

Information about nodes on an explicit path is displayed.

Step 8 Run:

```
commit
```

The configurations are committed.

----End

2.3.6 Configuring an MPLS TE Tunnel Interface

An MPLS TE tunnel is set up and managed on a tunnel interface. Therefore, the tunnel interface is configured on the ingress of an MPLS TE tunnel.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

A tunnel interface is created and the tunnel interface view is displayed.

Step 3 Run either of the following commands to configure the IP address of the tunnel interface:

- To assign an IP address to the tunnel interface, run:
  ip address *ip-address* { *mask* | *mask-length* } [**sub**]

  The primary IP address must be configured before the secondary IP address is configured for the tunnel interface.
- To configure the tunnel interface to borrow an IP address of another interface, run:
  ip address unnumbered interface *interface-type interface-number*

The tunnel interface must use an IP address before forwarding traffic. An MPLS TE tunnel is unidirectional; therefore, its peer address is irrelevant to traffic forwarding. A tunnel interface does not need to be assigned an IP address but uses the local LSR ID as its IP address.

Step 4 Run:
tunnel-protocol mpls te

MPLS TE is configured as a tunnel protocol.

Step 5 Run:
destination *ip-address*

The destination address of a tunnel is configured, which is usually the LSR ID of the egress.

Various types of tunnels require specific destination addresses. If a tunnel protocol is changed to MPLS TE from another protocol, a configured destination address is deleted automatically and a new destination address needs to be configured.

Step 6 Run:
mpls te bandwidth ct0 *ct0-bw-value*

The bandwidth is configured for an MPLS TE tunnel.

The bandwidth used by the tunnel cannot be greater than the maximum reservable link bandwidth.

The default bandwidth type is CT0.

The bandwidth used by a tunnel does not need to be set if only a path needs to be configured for an MPLS TE tunnel.

If the set bandwidth is higher than 28630 kbit/s, the available bandwidth assigned to the MPLS TE tunnel may not be precise, but the MPLS TE tunnel can be set up successfully.

Step 7 Run:
mpls te path explicit-path *path-name* [**secondary**]

An explicit path is configured for an MPLS TE tunnel.

An explicit path does not need to be configured if only the bandwidth needs to be set for an MPLS TE tunnel.

Step 8 (Optional) Run:
mpls te resv-style { **ff** | **se** }

A resource reservation style is configured.

The default resource reservation style is shared explicit (SE).

The SE style is used in make-before-break, and the fixed filter (FF) style is seldom used.

Step 9 Run:

```
commit
```

The configurations are committed.

----End

2.3.7 Checking the Configuration

After configuring the RSVP-TE tunnel, you can view statistics about the RSVP-TE tunnel and the tunnel status.

Prerequisite

The configurations of an RSVP-TE tunnel are complete.

Procedure

- Run the **display mpls te link-administration bandwidth-allocation** [**interface** *interface-type interface-number*] command to check information about the allocated link bandwidth.
- Run the **display ospf** [*process-id*] **mpls-te** [**area** *area-id*] [**self-originated**] command to check information about OSPF TE.
- Run either of the following commands to check the IS-IS TE status:
  - **display isis traffic-eng advertisements** [{ **level-1** | **level-2** | **level-1-2** } | { *lsp-id* | **local** }] * [*process-id* | [**vpn-instance** *vpn-instance-name*]]
  - **display isis traffic-eng statistics** [*process-id* | [**vpn-instance** *vpn-instance-name*]]
- Run the **display explicit-path** [*path-name*] [**verbose**] command to check the configured explicit path.
- Run the **display mpls te cspf destination** *ip-address* [**affinity** *properties* [**mask** *mask-value*] | **bandwidth** { **ct0** *ct0-bandwidth* | **ct1** *ct1-bandwidth* | **ct2** *ct2-bandwidth* | **ct3** *ct3-bandwidth* | **ct4** *ct4-bandwidth* | **ct5** *ct5-bandwidth* | **ct6** *ct6-bandwidth* | **ct7** *ct7-bandwidth* }* | **explicit-path** *path-name* | **hop-limit** *hop-limit-number* | **metric-type** { **igp** | **te** } | **priority** *setup-priority* | **srlg-strict** *exclude-path-name* | **tie-breaking** { **random** | **most-fill** | **least-fill** }]* command to check the path that is calculated using CSPF based on specified conditions.
- Run the **display mpls te cspf tedb** { **all** | **area** *area-id* | **interface** *ip-address* | **network-lsa** | **node** [*router-id*] } command to check information about TEDBs that meet specified conditions and can be used by CSPF to calculate a path.
- Run the **display mpls rsvp-te** [**interface** [*interface-type interface-number*]] command to check RSVP information.
- Run the **display mpls rsvp-te established** [**interface** *interface-type interface-number peer-ip-address*] command to check information about the established RSVP-TE CR-LSPs.
- Run the **display mpls rsvp-te peer** [**interface** *interface-type interface-number*] command to check the parameters of an RSVP neighbor.
- Run the **display mpls rsvp-te reservation** [**interface** *interface-type interface-number peer-ip-address*] command to check information about RSVP resource reservation.
- Run the **display mpls rsvp-te request** [**interface** *interface-type interface-number peer-ip-address*] command to check information about RSVP resource reservation requests.

- Run the **display mpls rsvp-te sender** [**interface** *interface-type interface-number peer-ip-address*] command to check information about an RSVP sender.
- Run the **display mpls rsvp-te statistics** { **global** | **interface** [*interface-type interface-number*] } command to check RSVP-TE statistics.
- Run the **display mpls te link-administration admission-control** [**interface** *interface-type interface-number* | **stale-interface** *interface-index*] command to check tunnels set up on the local node.
- Run the **display mpls te tunnel** [**destination** *ip-address*] [**lsp-id** *lsr-id session-id local-lsp-id* | **lsr-role** { **all** | **egress** | **ingress** | **remote** | **transit** }] [**name** *tunnel-name*] [{ **incoming-interface** | **interface** | **outgoing-interface** } *interface-type interface-number*] [**verbose**] command to check information about a tunnel.
- Run the **display mpls te tunnel statistics** or **display mpls lsp statistics** command to check tunnel statistics.
- Run the **display mpls te tunnel-interface** [**tunnel** *tunnel-number*] command to check information about a tunnel interface on the ingress of a tunnel.

----End

Example

Run the following command to check the previous configurations.

Run the **display mpls te tunnel-interface** command. The tunnel is Up. For example:

```
<HUAWEI> display mpls te tunnel-interface
    Tunnel Name       : Tunnel1
    Tunnel State Desc : CR-LSP is Up
    Tunnel Attributes   :
    Active LSP          : Primary LSP
    Traffic Switch      : Primary LSP -> Hot-Standby LSP
    Session ID          : 1
    Ingress LSR ID      : 1.1.1.1              Egress LSR ID: 4.4.4.4
    Admin State         : UP                   Oper State   : UP
    Signaling Protocol  : RSVP
    FTid                : 1
    Tie-Breaking Policy : None                 Metric Type  : None
    BypassBW Flag       : Not Supported
    BypassBW Type       : -                    Bypass BW    : -
    Bfd Cap             : None                 Retry Int    : -
    Reopt               : Disabled             Reopt Freq   : -
    Auto BW             : Disabled
    Current Collected BW: -                    Auto BW Freq : -
    Min BW              : -                    Max BW       : -
    Tunnel Group        : -
    Interfaces Protected: -
    Excluded IP Address : -
    Is On Radix-Tree    : -                    Referred LSP Count: -
    Primary Tunnel      : -                    Pri Tunn Sum : -
    Backup Tunnel       : -
    Group Status        : -                    Oam Status   : -
    IPTN InLabel        : -
    BackUp Type         : None                 BestEffort   : Disabled
    SRLG Disjoing       : NA
    Secondary HopLimit  : -
    BestEffort HopLimit : -
    Secondary Explicit Path Name: -
    Secondary Affinity Prop/Mask: -
    BestEffort Affinity Prop/Mask: 0x0/0x0
    IsConfigLspConstraint: -

    Primary LSP ID      : 1.1.1.1:116
    LSP State           : FRR INUSE            LSP Type     : Primary
```

```
Setup Priority      : 7                     Hold Priority: 7
IncludeAll          : 0x0
IncludeAny          : 0x0
ExcludeAny          : 0x0
Affinity Prop/Mask  : 0x0/0x0               Resv Style   :  SE
Configured Bandwidth Information:
CT0 Bandwidth(Kbit/sec): 50000          CT1 Bandwidth(Kbit/sec): 0
CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
Actual Bandwidth Information:
CT0 Bandwidth(Kbit/sec): 50000          CT1 Bandwidth(Kbit/sec): 0
CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
Explicit Path Name  : pri-path              Hop Limit           : -
Record Route        : Enabled               Record Label : Enabled
Route Pinning       : Disabled
FRR Flag            : Enabled
IdleTime Remain     : -
BFD Status          : -
```

2.4 Adjusting RSVP Signaling Parameters

RSVP-TE supports diverse signaling parameters, which meet requirements for reliability and network resources, and requirements of certain MPLS TE advanced features.

Applicable Environment

RSVP TE supports diversified signaling parameters, which meet requirements of reliability and network resources, and certain MPLS TE advanced features.

Before starting each configuration task, understand configuration objectives and possible impacts on networks.

Pre-configuration Tasks

Before adjusting RSVP signaling parameters, complete the following task:

- **Enabling MPLS TE and RSVP-TE**

Configuration Procedures

You can perform one or more configuration tasks (excluding "Checking the Configuration") as required.

2.4.1 Configuring the RSVP Hello Extension

The RSVP Hello extension rapidly detects connectivity between RSVP neighbors.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Step 3 Run:

```
mpls rsvp-te hello
```

The RSVP Hello extension is enabled on the local node.

The RSVP Hello extension is disabled by default.

Step 4 Run:

```
mpls rsvp-te hello-lost times
```

The maximum number of Hello messages that can be discarded is set.

If a default number of four consecutive Hello messages are not received, a node regards its neighbor as Down or a link as faulty. As a result, one of the following changes may occur:

- If RSVP GR is configured, RSVP GR starts to restore the TE tunnel.
- If RSVP GR is not configured, one of the following situations may occur:
  - If TE FRR is configured, traffic switches to a bypass tunnel.
  - If TE FRR is not configured, the TE tunnel is torn down and re-established.

Step 5 Run:

```
mpls rsvp-te timer hello interval
```

The interval at which Hello messages are refreshed is set.

The default interval at which Hello messages are refreshed is 3 seconds.

NOTE

If the refresh interval is changed, the modification takes effect after the previous refresh timer expires.

Step 6 Run:

```
quit
```

The system view is displayed.

Step 7 Run:

```
interface interface-type interface-number
```

The view of an RSVP-enabled interface is displayed.

Step 8 Run:

```
mpls rsvp-te hello
```

The RSVP Hello extension is enabled on an interface.

The RSVP Hello extension rapidly detects reachability of RSVP neighbors. For details, see RFC 3209.

Step 9 Run:

```
commit
```

The configurations are committed.

----End

2.4.2 Configuring an RSVP Timer

Configuring an RSVP timer is to set the interval at which Path and Resv messages are refreshed and the timeout multiplier associated with the RSVP blocked state.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Step 3 Run:

```
mpls rsvp-te timer refresh interval
```

The interval at which Path and Resv messages are refreshed is set.

The default interval is 30 seconds.

NOTE

If the refresh interval is modified, the modification takes effect after the previous refresh timer expires. Do not set a long refresh interval or frequently modify a refresh interval.

Step 4 Run:

```
mpls rsvp-te keep-multiplier number
```

The PSB and RSB timeout multiplier is set.

The default timeout multiplier is 3.

Step 5 Run:

```
commit
```

The configurations are committed.

----End

2.4.3 Configuring RSVP-TE Srefresh

Enabling Summary Refresh (Srefresh) on interfaces connecting two RSVP neighboring nodes reduces the network cost and improves the network performance. After Srefresh is enabled, retransmission of Srefresh messages will be automatically enabled on interfaces.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Srefresh enabled in the MPLS view takes effect on an entire device. Enabling Srefresh in the MPLS view is applicable to a TE FRR network. Srefresh is enabled globally on the Point of Local Repair (PLR) and Merge Point (MP). This allows efficient usage of network resources and improves Srefresh reliability.

Step 3 Run:

```
mpls rsvp-te srefresh
```

Srefresh is enabled.

Step 4 Run:

```
commit
```

The configuration is committed.

----End

2.4.4 Enabling RSVP-TE Reservation Confirmation

RSVP-TE reservation confirmation configured on the egress of a tunnel verifies that resources are successfully reserved.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Step 3 Run:

```
mpls rsvp-te resvconfirm
```

RSVP-TE reservation confirmation is enabled.

RSVP-TE reservation confirmation is disabled by default.

After receiving a Path message, a receiver initiates reservation confirmation by sending a Resv message carrying an object that requests for reservation confirmation.

NOTE

Receiving ResvConf messages does not mean that resource reservation is successful. It means that, however, resources are reserved successfully only on the farthest upstream node where this Resv message arrives. These resources may be preempted by other applications later.

Step 4 Run:

```
commit
```

The configuration is committed.

----End

2.4.5 Changing the PSB and RSB Timeout Multiplier

The PSB and RSB timeout multiplier is used to set the maximum number of signaling packets that can be be discarded in a poor signaling environment.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Step 3 Run:

```
mpls rsvp-te keep-multiplier number
```

The PSB and RSB timeout multiplier is set.

The default timeout multiplier is 3.

NOTE

Setting the PSB and RSB timeout multiplier to a value equal to or larger than 5 is recommended. This prevents the PSB and RSB from aging and being deleted if the PSB and RSB fail to recover in the case of a large number of services.

Step 4 Run:

```
commit
```

The configuration is committed.

----End

2.4.6 Checking the Configuration

After adjusting RSVP signaling parameters, you can view the refresh parameters, RSVP reservation confirmation status, RSVP Hello extension status, and RSVP timer parameters.

Prerequisite

The configurations of adjusting RSVP signaling parameters are complete.

Procedure

- Run the **display mpls rsvp-te** [**interface** [*interface-type interface-number*]] command to check RSVP-TE configurations.
- Run the **display mpls rsvp-te psb-content** [*ingress-lsr-id tunnel-id lsp-id*] command to check information about the RSVP-TE PSB.
- Run the **display mpls rsvp-te rsb-content** [*ingress-lsr-id lsp-id tunnel-id*] command to check information about the RSVP-TE RSB.
- Run the **display mpls rsvp-te statistics** { **global** | **interface** [*interface-type interface-number*] } command to check RSVP-TE statistics.

----End

Example

Run the following commands to check the previous configurations.

Run the **display mpls rsvp-te** command, and you can view RSVP-TE configurations. For example:

```
<HUAWEI> display mpls rsvp-te
LSR ID: 1.1.1.1
 Resv Confirmation Request: DISABLE
 RSVP Hello Extension: DISABLE
 Hello interval: 3 sec                 Max Hello misses: 4
 Path and Resv message refresh interval: 30 sec
 Path and Resv message refresh retries count: 3
 Blockade Multiplier: 4
 Graceful-Restart Capability: None
```

Run the **display mpls rsvp-te psb-content** command, and you can view information about the RSVP-TE PSB. For example:

```
<HUAWEI> display mpls rsvp-te psb-content
==============================================================
                      The PSB Content
==============================================================
 Tunnel Addr: 4.4.4.4                      Exist time: 1h 45m 36s
 Tunnel ExtID: 1.1.1.1                     Session ID: 1
 Ingress LSR ID: 1.1.1.1                   Local LSP ID: 116
 Previous Hop: ----                        Next Hop: 2.1.1.2
 Incoming / Outgoing Interface: ---- / Pos3/1/1
 InLabel: NULL                             OutLabel: 17
 Send Message ID: 0                        Recv Message ID: 0
 Session Attribute-
   SetupPrio: 7                            HoldPrio: 7
   SessionAttrib: SE Style desired
                  Local Protect desired
                  Node Protect desired
                  Label Record desired
   FRR Flag: No protection                 Local RRO Flag: 0x0
 ERO Information-
      L-Type          ERO-IPAddr          ERO-PrefixLen
   ERHOP_STRICT       2.1.1.2             32
   ERHOP_STRICT       3.1.1.2             32
   ERHOP_STRICT       4.1.1.2             32
   ERHOP_STRICT       4.4.4.4             32
 RRO Information-
   -----
 SenderTspec Information-
   Token bucket rate: 6250000
   Token bucket size: 1000
   Peak data rate: 6250000
   Minimum policed unit: 0
   Maximum packet size: 1500
 CT-BandWidth Information:
   CT0 Bandwidth (Bytes/sec):  6250000    CT1 Bandwidth (Bytes/sec):  0
   CT2 Bandwidth (Bytes/sec):  0          CT3 Bandwidth (Bytes/sec):  0
   CT4 Bandwidth (Bytes/sec):  0          CT5 Bandwidth (Bytes/sec):  0
   CT6 Bandwidth (Bytes/sec):  0          CT7 Bandwidth (Bytes/sec):  0
 Path Message arrive on Unknown(0x0) from PHOP 0.0.0.0
 Path Message sent to NHOP 2.1.1.2 on Pos3/1/1
 Resource Reservation OK

 LSP Statistics Information:
   SendPacketCounter: 155                  RecvPacketCounter: 365
   SendPathCounter: 155                    RecvPathCounter: 0
   SendResvCounter: 0                      RecvResvCounter: 365
```

Run the **display mpls rsvp-te rsb-content** command, and you can view information about the RSVP-TE RSB. For example:

```
<HUAWEI> display mpls rsvp-te rsb-content
============================================================
                      The RSB Content
============================================================
 Tunnel Addr: 1.1.1.1                Session Tunnel ID: 10
 Tunnel ExtID: 2.2.2.2
 Next Hop: 100.1.1.2                 Reservation Style: SE STYLE
 Reservation Incoming Interface: GigabitEthernet1/0/0
 Reservation Interface: GigabitEthernet1/0/0
 Message ID : 0
 Filter Spec Information-
   The filter number: 1
   Ingress LSR ID: 2.2.2.2         Local LSP ID: 1024    OutLabel: 3
   RRO Information-
   RRO-CType: IPV4   RRO-IPAddress: 100.1.1.2          RRO-IPPrefixLen: 32
   RRO-CType: LABEL  RRO-Label: 3
   RRO-CType: IPV4   RRO-IPAddress: 1.1.1.1            RRO-IPPrefixLen: 32
 FlowSpec Information-
   Token bucket rate: 125
   Token bucket size: 1000
   Peak data rate: 125
   Minimum policed unit: 0
   Maximum packet size: 1500
   Bandwidth guarantees: 0
   Delay guarantees: 0
   Qos Service is Controlled
 Resv Message arrive on GigabitEthernet1/0/0 from NHOP 100.1.1.2
```

Run the **display mpls rsvp-te statistics global** command, and you can view RSVP-TE statistics. For example:

```
<HUAWEI> display mpls rsvp-te statistics global
  LSR ID: 1.1.1.1                        LSP Count: 1
  PSB Count: 1                           RSB Count: 1
  RFSB Count: -
 FRR statistics information:
  PLR AvailLsps: 0                       PLR InuseLsps: 0
  MP AvailLsps: 0                        MP InuseLsps: 0
 Total Statistics Information:
  PSB CleanupTimeOutCounter: 0           RSB CleanupTimeOutCounter: 0
  SendPacketCounter: 3172                RecPacketCounter: 2558
  SendCreatePathCounter: 3172            RecCreatePathCounter: 0
  SendRefreshPathCounter: 1326           RecRefreshPathCounter: 6229
  SendCreateResvCounter: 0               RecCreateResvCounter: 2558
  SendRefreshResvCounter: 1326           RecRefreshResvCounter: 6229
  SendResvConfCounter: 0                 RecResvConfCounter: 0
  SendHelloCounter: 0                    RecHelloCounter: 0
  SendAckCounter: 0                      RecAckCounter: 0
  SendPathErrCounter: 0                  RecPathErrCounter: 0
  SendResvErrCounter: 0                  RecResvErrCounter: 0
  SendPathTearCounter: 0                 RecPathTearCounter: 0
  SendResvTearCounter: 0                 RecResvTearCounter: 0
  SendSrefreshCounter: 0                 RecSrefreshCounter: 0
  SendAckMsgCounter: 0                   RecAckMsgCounter: 0
  SendChallengeMsgCounter: 0             RecChallengeMsgCounter: 0
  SendResponseMsgCounter: 0              RecResponseMsgCounter: 0
  SendErrMsgCounter: 0                   RecErrMsgCounter: 0
  SendRecoveryPathMsgCounter: 0          RecRecoveryPathMsgCounter: 0
  SendGRPathMsgCounter: 0                RecGRPathMsgCounter: 0
  ResourceReqFaultCounter: 0
  Bfd neighbor count: 0                  Bfd session count: 0
```

2.5 Configuring RSVP Authentication

RSVP authentication is configured to protect a node against malicious attacks and improve network security.

Applicable Environment

RSVP authentication prevents the following problems:

- An unauthorized node attempts to set up an RSVP neighbor relationship with the local node.
- A remote node constructs forged RSVP messages to set up an RSVP neighbor relationship with the local node, and initiates attacks to the local node.

RSVP key authentication cannot prevent anti-replay attacks or RSVP message mis-sequence during network congestion. RSVP message mis-sequence causes authentication termination between RSVP neighbors. The handshake and message window functions, together with RSVP key authentication, can prevent the preceding problems.

CR-LSP flapping may lead to frequent re-establishment of RSVP neighbor relationships. As a result, the handshake function is repeatedly performed and RSVP authentication is prolonged. An RSVP authentication lifetime is set to resolve the preceding problems. If no CR-LSP exists, RSVP neighbors still retain their neighbor relationship until the RSVP authentication lifetime expires.

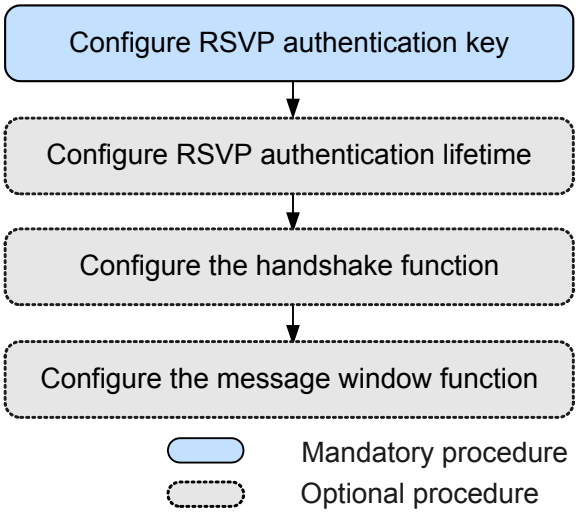
Pre-configuration Tasks

Before configuring RSVP authentication, complete the following task:

- **Configuring an RSVP-TE Tunnel**

Configuration Procedures

Figure 2-2 Flowchart for configuring RSVP authentication



2.5.1 Configuring an RSVP Authentication Mode

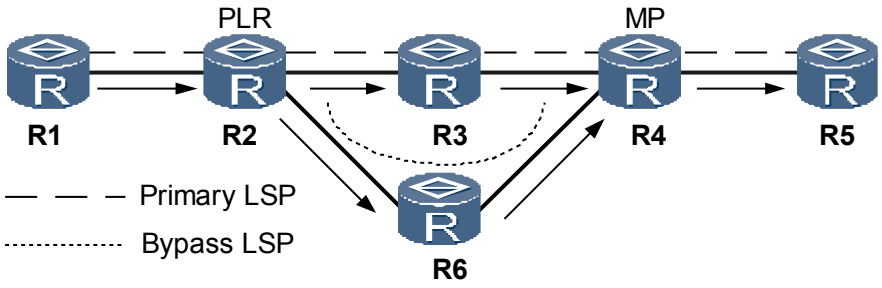
RSVP authentication modes are configured between RSVP neighboring nodes or between interfaces of RSVP neighboring nodes. The keys on both ends to be authenticated must be the same; otherwise, RSVP authentication fails and packets received by RSVP neighboring nodes are discarded.

Context

RSVP authentication in the key mode is used to prevent an unauthorized node from establishing an RSVP neighbor relationship with the local node or prevent a remote node from constructing forged packets to establish an RSVP neighbor relationship with the local node.

The NE5000E supports RSVP key authentication in the following modes, shown in the **Figure 2-3**.

Figure 2-3 Schematic diagram for RSVP key authentication



- Local interface–based authentication

  Local interface–based authentication is performed between LSRs and is applicable to inter-domain MPLS TE FRR. Local interface-based authentication is performed between interfaces connecting a Point of Local Repair (PLR) and a Merge Point (MP).

  - Local interface–based authentication is recommended on a network configured with inter–domain MPLS TE FRR.
  - Local interface- or neighbor interface-based authentication can be used on a network that is not configured with inter-domain MPLS TE FRR.

- Neighbor node–based authentication

  Neighbor node-based authentication is performed between LSRs. The neighbor node-based authentication takes effect on an entire device. Neighbor node-based authentication is usually performed between a PLR and an MP based on LSR IDs.

  Neighbor node-based authentication is recommended on a network with non-inter-domain MPLS TE FRR.

- Neighbor interface–based authentication

  Neighbor interface-based authentication is performed between interfaces connecting two LSRs. Neighbor interface-based authentication is performed between interfaces connecting R2 and R3 shown in the **Figure 2-3**.

  Local interface- or neighbor address-based authentication can be used on a network that is not configured with inter-domain MPLS TE FRR.

Each pair of RSVP neighbors must use the same key; otherwise, RSVP authentication fails and all the received RSVP messages are discarded.

Table 2-1 shows differences between local interface-based authentication, neighbor node-based authentication, and neighbor address-based authentication.

Table 2-1 Principle for RSVP authentication mode selection

RSVP Key Authentication	Local Interface-based Authentication	Neighbor Node-based Authentication	Neighbor Interface-based Authentication
Authentication mode	Local interface-based authentication	RSVP neighbor-based authentication	RSVP neighbor interface-based authentication
Priority	High	Medium	Low
Applicable environment	Any network	Non-inter-area network	Networks where MPLS TE FRR is enabled and primary CR-LSPs are in the FRR Inuse state
Advantages	N/A	Simplex configuration	N/A

Procedure

- Configure RSVP key authentication in neighbor address-based mode.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*

     The view of the interface on which the MPLS TE tunnel is established is displayed.
  3. Run:
     mpls rsvp-te authentication { **cipher** | **plain** } *auth-key*

     The key for RSVP authentication is configured.
  4. Run:
     commit

     The configuration is committed.
- Configure RSVP key authentication in neighbor-based mode.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     mpls

     The MPLS view is displayed.
  3. Run:
     mpls rsvp-te peer *peer-address*

     The RSVP neighbor view is displayed.
  4. Run:
     mpls rsvp-te authentication { **cipher** | **plain** } *auth-key*

The key for RSVP authentication is configured.

5. Run:
   commit

   The configuration is committed.

----End

2.5.2 (Optional) Setting RSVP Authentication Lifetime

The RSVP authentication lifetime is set. This prevents RSVP authentication from being prolonged in the situation that CR-LSP flapping causes frequent re-establishment of RSVP neighbor relationships and repeatedly-performed handshake.

Context

RSVP neighbors retain an RSVP neighbor relationship within a set RSVP authentication lifetime if no CR-LSP exists. Configuring the RSVP authentication lifetime does not affect existing CR-LSPs.

Procedure

Step 1 Run:
system-view

The system view is displayed.

Step 2 Run:
interface *interface-type interface-number*

The view of an RSVP-enabled interface is displayed.

Step 3 Run:
mpls rsvp-te authentication lifetime *lifetime*

The RSVP authentication lifetime is set.

lifetime is in the format of HH:MM:SS and ranges from 00:00:01 to 23:59:59. The default lifetime is 00:30:00, that is, 30 minutes.

Step 4 Run:
commit

The configuration is committed.

----End

2.5.3 (Optional) Configuring the Handshake Function

The handshake function helps RSVP key authentication prevent anti-replay attacks.

Procedure

Step 1 Run:
system-view

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The view of the interface on which the MPLS TE tunnel is established is displayed.

Step 3 Run:

```
mpls rsvp-te authentication handshake local-secret
```

The handshake function is enabled.

local-secret is valid only on a local node; therefore, *local-secret* values configured on two RSVP neighboring nodes can be different.

NOTE

The task of **Configuring an RSVP Authentication Mode** must be complete before the RSVP handshake function is configured.

After the handshake function is configured on a node and its RSVP neighbors, if the node receives RSVP messages from a neighbor that has not established an RSVP authentication relationship with the node, the node sends a Challenge message carrying *local-secret* to the neighbor. After receiving the Challenge message, the neighbor replies with a Response message carrying *local-secret* the same as that in the Challenge message. If the node detects that *local-secret* carried in the Response message is the same as the locally configured *local-secret*, the node determines to establish an RSVP authentication relationship with the neighbor.

Step 4 Run:

```
commit
```

The configuration is committed.

----End

2.5.4 (Optional) Configuring the Message Window Function

The message window function prevents RSVP message mis-sequence. RSVP message mis-sequence terminates RSVP authentication between neighboring nodes.

Context

The message window function prevents RSVP message mis-sequence.

The default window size is 1. This allows a local device to store only the largest sequence number of the latest RSVP message sent by a neighbor.

If the window size is larger than 1, the local device stores several latest valid sequence numbers.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The view of the interface on which the MPLS TE tunnel is established is displayed.

Step 3 Run:

```
mpls rsvp-te authentication window-size window-size
```

The message window function is configured. This means the number of valid sequence numbers of received RSVP messages that can be stored is set.

NOTE

The task of **Configuring an RSVP Authentication Mode** must be complete before the message window function is configured.

If RSVP is enabled on an Eth-Trunk or IP-Trunk interface, only one neighbor relationship is established on the trunk interface between RSVP neighbors. This means any trunk member interface receives RSVP messages in a random order, resulting in message mis-sequence. An RSVP message window size is configured to address this problem. Setting the window size to a value larger than 32 is recommended. If the size of a sliding window is too small, received RSVP messages with sequence numbers beyond the window size will be discarded, resulting in termination of an RSVP neighbor relationship.

Step 4 Run:

```
commit
```

The configuration is committed.

----End

2.5.5 Checking the Configuration

After configuring RSVP authentication, you can view information about RSVP authentication.

Prerequisite

The configurations of RSVP authentication are complete.

Procedure

Step 1 Run the **display mpls rsvp-te** [**interface** *interface-type interface-number*] command to check RSVP-TE configurations on an interface.

Step 2 Run the **display mpls rsvp-te peer** [**interface** *interface-type interface-number* | *peer-address*] command to check RSVP-TE neighbor information on an RSVP-TE-enabled interface.

----End

Example

Run the following command to check the previous configurations.

Run the **display mpls rsvp-te peer** command, and you can view information about RSVP-TE neighbors on an RSVP-TE-enabled interface. For example:

```
<HUAWEI> display mpls rsvp-te peer
Interface GigabitEthernet3/0/1
 Neighbor Addr: 10.1.1.2
 SrcInstance: 0x97B6198F                NbrSrcInstance: 0x0
 PSB Count: 1                           RSB Count: 0
 Hello Type Sent: NONE                  Neighbor Hello Extension: DISABLE
 SRefresh Enable: NO
 Authentication: ENABLE
 Authentication Algorithm: HMAC-MD5
```

```
 WindowsSize: 32
 Last valid seq # rcvd: NULL

Remote Node id Neighbor
 Neighbor Addr: 2.2.2.2
 SrcInstance: 0x97B6198F                NbrSrcInstance: 0x0
 PSB Count: 0                           RSB Count: 0
 Hello Type Sent: NONE                  Neighbor Hello Extension: DISABLE
 SRefresh Enable: NO
 Authentication: DISABLE
 Last valid seq # rcvd: NULL
```

2.6 Adjusting Parameters for Establishing an MPLS TE Tunnel

Multiple attributes are used to establish MPLS TE tunnels flexibly.

Applicable Environment

During the establishment of an MPLS TE tunnel, specific configurations are required. This section describes these specific configurations.

Context

Before adjusting parameters for establishing an MPLS TE tunnel, complete the following task:

- **Configuring an RSVP-TE tunnel**

Configuration Procedures

You can perform one or more configuration tasks (excluding "Checking the Configuration") as required.

2.6.1 Configuring an MPLS TE Explicit Path

An explicit path is configured on the ingress of an MPLS TE tunnel, specifying the nodes through which the MPLS TE tunnel passes or bypasses.

Context

An explicit path consists of a series of nodes. These nodes are arranged in the sequence by configuration and form a vector path. An IP address for an explicit path is an interface IP address on every node. The loopback IP address of the egress node is usually used as the destination address of an explicit path.

Two adjacent nodes are connected in either of the following modes on an explicit path:

- Strict: A hop is directly connected to its next hop.
- Loose: Other nodes may exist between a hop and its next hop.

The strict and loose modes are used either separately or together.

TE tunnels are classified into the following types:

- Intra-area tunnel: indicates a TE tunnel in a single OSPF or IS-IS area, but not an autonomous system (AS) running the Border Gateway Protocol (BGP).
- Inter-area tunnel: indicates a TE tunnel traversing multiple OSPF or IS-IS areas, but not BGP ASs.

A strict explicit path is used to establish an inter-area TE tunnel, on which a next hop can be only an Area Border Router (ABR) or an Autonomous System Boundary Router (ASBR).

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
explicit-path path-name
```

An explicit path is created and the explicit path view is displayed.

Step 3 Run:

```
next hop ip-address [ include [ strict | loose ] | exclude ]
```

The next-hop address is specified for the explicit path.

include strict are used by default, meaning a tunnel must pass through a specified node.

include indicates that a tunnel does pass through a specified node; **exclude** indicates that a tunnel does not pass through a specified node.

Step 4 (Optional) Run:

```
add hop ip-address1 [ include [ strict | loose ] | exclude ] { after | before } ip-address2
```

A node is added to the explicit path.

include strict are used by default, meaning a tunnel must pass through a specified node.

Step 5 (Optional) Run:

```
modify hop ip-address1 ip-address2 [ include [ strict | loose ] | exclude ]
```

The address of a node on an explicit path is changed.

include strict are used by default, meaning a tunnel must pass through a specified node.

Step 6 (Optional) Run:

```
delete hop ip-address
```

A node is deleted from an explicit path.

Step 7 (Optional) Run:

```
list hop [ ip-address ]
```

Information about nodes on an explicit path is displayed.

Step 8 Run:

```
commit
```

The configurations are committed.

----End

2.6.2 Setting Priority Values for an MPLS TE Tunnel

The priority values are set on the ingress of an MPLS TE tunnel. Preemption is performed based on the setup and holding priorities during the establishment of MPLS TE tunnel.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The view of the MPLS TE tunnel interface is displayed.

Step 3 Run:

```
mpls te priority setup-priority [ hold-priority ]
```

The priority values are set for the MPLS TE tunnel.

Both the setup and holding priority values range from 0 to 7. The smaller the value, the higher the priority.

Both the default setup and the holding priority values are 7. If only the setup priority value is set, ensure that the setup priority value is the same the holding priority value.

NOTE

The setup priority value must be equal to or larger than the holding priority value. This means the setup priority is equal to or lower than the holding priority.

Step 4 Run:

```
commit
```

The configuration is committed.

----End

2.6.3 Setting the Hop Limit for a CR-LSP

The hop limit set on an ingress is the maximum number of hops on a path along which a CR-LSP is to be set up. The hop limit is a constraint during path selection.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The view of the MPLS TE tunnel interface is displayed.

Step 3 Run:

```
mpls te hop-limit hop-limit-value [ best-effort | secondary ]
```

The hop limit of a CR-LSP is set.

Step 4 Run:

```
commit
```

The configuration is committed.

----End

2.6.4 Configuring Route and Label Record

An ingress is configured to allow routes and labels able or unable to be recorded along a path over which an RSVP-TE CR-LSP will be established.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The view of the MPLS TE tunnel interface is displayed.

Step 3 Run:

```
mpls te record-route [ label ]
```

Routes and labels are able to be recorded during the establishment of a CR-LSP.

Routes and labels are not recorded by default.

Step 4 Run:

```
commit
```

The configuration is committed.

----End

2.6.5 Configuring Route Pinning

Route pinning is configured on the ingress of a CR-LSP to lock the path of the CR-LSP, prohibiting re-optimization or rerouting.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The view of the MPLS TE tunnel interface is displayed.

Step 3 Run:

```
mpls te record-route [ label ]
```

Routes and labels are able to be recorded during the establishment of a CR-LSP.

Step 4 Run:

```
mpls te route-pinning
```

Route pinning is enabled.

By default, route pinning is disabled.

Step 5 Run:

```
commit
```

The configuration is committed.

----End

2.6.6 Setting Switching and Deletion Delays

The switching and deletion delays are set to ensure that a CR-LSP is deleted only after a new CR-LSP has been set up, preventing traffic interruption.

Context

MPLS TE uses a make-before-break mechanism. If attributes of an MPLS TE tunnel such as bandwidth or path change, a new CR-LSP with new attributes is established. Such a CR-LSP is called a Modified CR-LSP. The new CR-LSP needs to be established before the original CR-LSP, also called the primary CR-LSP, is torn down. This prevents data loss and additional bandwidth consumption during traffic switching.

If a forwarding entry associated with the new CR-LSP does not take effect after the original CR-LSP has been deleted, temporary traffic interruption occurs.

The switching and deletion delays can be set on the ingress of the CR-LSP to prevent the preceding problem.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Step 3 Run:

```
mpls te switch-delay switch-time delete-delay delay-time
```

The switching and deletion delays are set.

By default, the switching delay time is 5 seconds and the deletion delay time is 7 seconds.

Step 4 Run:

```
commit
```

The configuration is committed.

----End

2.6.7 Checking the Configuration

After adjusting the establishment of the MPLS TE tunnel, you can view information about the tunnel interface.

Prerequisite

The configurations of adjusting the establishment of the MPLS TE tunnel are complete.

Procedure

Step 1 Run the **display mpls te tunnel-interface** [**tunnel** *tunnel-number*] command to check information about a tunnel interface on the ingress of a tunnel.

----End

Example

Run the following command to check the previous configurations.

Run the **display mpls te tunnel-interface** command, and you can view information about the tunnel interface. For example:

```
<HUAWEI> display mpls te tunnel-interface
    Tunnel Name       : Tunnel1
    Tunnel State Desc : CR-LSP is Up
    Tunnel Attributes   :
    Active LSP          : Primary LSP
    Traffic Switch      : Primary LSP -> Hot-Standby LSP
    Session ID          : 1
    Ingress LSR ID      : 1.1.1.1               Egress LSR ID: 4.4.4.4
    Admin State         : UP                    Oper State   : UP
    Signaling Protocol  : RSVP
    FTid                : 1
    Tie-Breaking Policy : None                  Metric Type  : None
    BypassBW Flag       : Not Supported
    BypassBW Type       : -                     Bypass BW    : -
    Bfd Cap             : None                  Retry Int    : -
    Reopt               : Disabled              Reopt Freq   : -
    Auto BW             : Disabled
    Current Collected BW: -                     Auto BW Freq : -
    Min BW              : -                     Max BW       : -
    Tunnel Group        : -
    Interfaces Protected: -
    Excluded IP Address : -
    Is On Radix-Tree    : -                     Referred LSP Count: -
    Primary Tunnel      : -                     Pri Tunn Sum : -
    Backup Tunnel       : -
    Group Status        : -                     Oam Status   : -
    IPTN InLabel        : -
    BackUp Type         : None                  BestEffort   : Disabled
    SRLG Disjoing       : NA
    Secondary HopLimit  : -
    BestEffort HopLimit : -
    Secondary Explicit Path Name: -
    Secondary Affinity Prop/Mask: -
    BestEffort Affinity Prop/Mask: 0x0/0x0
    IsConfigLspConstraint: -

    Primary LSP ID      : 1.1.1.1:116
    LSP State           : FRR INUSE             LSP Type     : Primary
    Setup Priority      : 7                     Hold Priority: 7
    IncludeAll          : 0x0
    IncludeAny          : 0x0
```

```
ExcludeAny          : 0x0
Affinity Prop/Mask  : 0x0/0x0              Resv Style    :  SE
Configured Bandwidth Information:
CT0 Bandwidth(Kbit/sec): 50000          CT1 Bandwidth(Kbit/sec): 0
CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
Actual Bandwidth Information:
CT0 Bandwidth(Kbit/sec): 50000          CT1 Bandwidth(Kbit/sec): 0
CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
Explicit Path Name  : pri-path              Hop Limit           : -
Record Route        : Enabled              Record Label : Enabled
Route Pinning       : Disabled
FRR Flag            : Enabled
IdleTime Remain     : -
BFD Status          : -
```

2.7 Adjusting Parameters for Forwarding MPLS TE Traffic

The IGP shortcut and forwarding adjacency are configured to allow a CR-LSP to participate in IGP route calculation. This adjusts the MPLS TE traffic forwarding.

Applicable Environment

MPLS TE traffic forwarding adjustment is to change a path through which IP or MPLS traffic passes or to allow a specified type of traffic to pass through an MPLS TE tunnel.

This section describes several measures to adjust MPLS TE traffic forwarding.

Context

The configuration described in this section should be used together with CSPF and a dynamic signaling protocol such as RSVP-TE.

Before adjusting parameters for MPLS TE forwarding, complete the following task:

- **Configuring an RSVP-TE Tunnel**

Configuration Procedures

You can perform one or more configuration tasks (excluding "Checking the Configuration") as required.

2.7.1 Configuring the IGP Shortcut

IGP shortcut is configured on the ingress of a CR-LSP. IGP shortcut prevents a route of a CR-LSP from being advertised to neighbors so that the neighbors cannot use this CR-LSP.

Context

NOTE

IGP shortcut and forwarding adjacency cannot be configured together.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The view of the MPLS TE tunnel interface is displayed.

Step 3 Run:

```
mpls te igp shortcut [ ospf ]
```

The OSPF shortcut is configured.

By default, the OSPF shortcut is not configured.

Step 4 Run:

```
mpls te igp metric { absolute | relative } value
```

The IGP metric of the TE tunnel is configured.

By default, the metric value used by a TE tunnel is the same as that of an IGP path.

Either of the following parameters is set when configuring the metric value used by a TE tunnel during IGP shortcut path calculation:

- If **absolute** is configured, the TE tunnel metric value is equal to the configured metric value.
- If **relative** is configured, the TE tunnel metric value is equal to the sum of the IGP route metric value and relative TE tunnel metric value.

Step 5 Run the following commands:

- Run:

  ```
  quit
  ```

  The system view is displayed.
- Run:

  ```
  ospf [ process-id ]
  ```

  The OSPF view is displayed.
- Run:

  ```
  enable traffic-adjustment
  ```

  Traffic adjustment is enabled.

Step 6 Run:

```
commit
```

The configuration is committed.

----End

2.7.2 Configuring Forwarding Adjacency

The forwarding adjacency is configured on the ingress of a CR-LSP. The forwarding adjacency allows a route of a CR-LSP to be advertised to neighbors so that these neighbors can use this CR-LSP.

Context

A routing protocol performs bidirectional detection on a link. The forwarding adjacency needs to be enabled on both ends of a tunnel. The forwarding adjacency allows a node to advertise a CR-LSP route to other nodes. Another tunnel for transferring data packets in the reverse direction needs to be configured.

NOTE

MPLS LDP must be enabled on the tunnel interface view before the forwarding adjacency is enabled.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The view of the MPLS TE tunnel interface is displayed.

Step 3 Run:

```
mpls te igp advertise [ hold-time value ]
```

The forwarding adjacency is configured.

By default, the forwarding adjacency is disabled.

Step 4 Run:

```
mpls te igp metric { absolute | relative } value
```

The IGP metric value of the MPLS TE tunnel is configured.

NOTE

A proper IGP metric value ensures that the CR-LSP route is advertised and used correctly. The metric value of a CR-LSP must be smaller than the metric value of an unwanted IGP route.

Step 5 Run:

```
quit
```

The system view is displayed.

Step 6 Run:

```
ospf [ process-id ]
```

The OSPF view is displayed.

Step 7 Run:

```
enable traffic-adjustment advertise
```

The forwarding adjacency is enabled in the OSPF process.

Step 8 Run:

```
commit
```

The configuration is committed.

----End

2.8 Adjusting the Threshold for Flooding Bandwidth Information

If the link bandwidth changes slightly, the threshold for flooding bandwidth information is set on the ingress or a transit node of a CR-LSP, which reduces flooding attempts and saves network resources.

Applicable Environment

To synchronize data between TEDBs in an IGP area, OSPF TE or IS-IS TE needs to be configured to update TEDB information and flood bandwidth information if the remaining bandwidth changes on an MPLS interface.

If a great number of tunnels using reserved bandwidth are set up on a node, the node will update TEDB information and flood bandwidth information frequently. Assume that the bandwidth of a link is 100 Mbit/s. If 100 TE tunnels with the bandwidth of 1 Mbit/s are set up for every link, flooding will be performed 100 times.

The following mechanism helps a node reduce the number of attempts to update TEDB information and flood bandwidth information:

- OSPF TE or IS-IS TE floods link bandwidth information to all nodes within a domain and update TEDB information if the ratio of the reserved bandwidth for an MPLS TE tunnel to the remaining bandwidth in the TEDB is equal to or larger than the set threshold.
- OSPF TE or IS-IS TE floods link bandwidth information to all nodes within the domain and updates the TEDB information if the ratio of the released bandwidth for an MPLS TE tunnel to the remaining bandwidth in the TEDB is equal to or larger than the set threshold on a link.

The default flooding threshold is 10%. The value is set using a command line.

The bandwidth flooding threshold is the ratio of the link bandwidth used or released by a TE tunnel to the link bandwidth remained in the TEDB.

If the link bandwidth changes slightly, flooding bandwidth information wastes network resources. Assume that the bandwidth of a link is 100 Mbit/s and 100 TE tunnels are created along this link. Bandwidth information will be flooded 100 times.

If the flooding threshold is set to 10%, flooding bandwidth information is not performed after tunnels 1 to 9 have been created. If tunnel 10 has been created, information about the bandwidth of tunnels 1 to 10 will be flooded. Similarly, flooding bandwidth information is not performed after tunnel 11 to tunnel 18 have been created. If tunnel 19 has been created, information about the bandwidth tunnels 11 to 19 will be flooded, and so on. Configuring a bandwidth flooding threshold reduces the number of attempts to flood bandwidth information and ensures efficient use of network resources.

By default, an IGP will flood information about a link and CSPF will update TEDB information on the link if the ratio of the bandwidth used or released by an MPLS TE tunnel to the bandwidth remained in the TEDB is equal to or higher than 10%.

Pre-configuration Tasks

Before adjusting the threshold for flooding bandwidth, complete the following task:

- **Configuring an RSVP-TE Tunnel**

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The view of the interface on which the MPLS TE tunnel is established is displayed.

Step 3 Run:

```
mpls te bandwidth change thresholds { down | up } percent
```

The flooding threshold is configured.

The flooding threshold is set only on a physical interface.

Step 4 Run:

```
commit
```

The configurations are committed.

----End

2.9 Configuring MPLS TE Manual FRR

MPLS TE manual FRR is a local protection mechanism and protects traffic on a link or a node along a CR-LSP.

Applicable Environment

MPLS TE manual FRR is a local protection technique.

NOTE

FRR is applicable to RSVP-TE tunnels in the shared explicit (SE) reservation style.

FRR requires additional bandwidth because a bypass tunnel needs to be pre-established. If available bandwidth is insufficient, FRR protects only important nodes or links along a tunnel.

FRR does not take effect if multiple nodes fail simultaneously. After FRR switches traffic from a primary CR-LSP to a bypass CR-LSP, the bypass CR-LSP must be kept Up when transmitting traffic. If the bypass CR-LSP goes Down, the protected traffic is interrupted and FRR fails. Even though the bypass CR-LSP goes Up again, it cannot forward traffic. Traffic can be forwarded only after the primary CR-LSP is restored or re-established.

The link or node protected by a bypass CR-LSP needs to be determined before the bypass CR-LSP is established. This ensures that the bypass CR-LSP does not pass through the protected link or node; otherwise, the protection function fails.

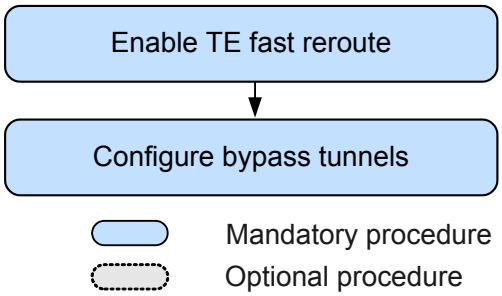
Pre-configuration Tasks

Before configuring MPLS TE manual FRR, complete the following tasks:

- Setting up a primary RSVP-TE tunnel
- Enabling MPLS TE and RSVP-TE in the MPLS and physical interface views on every node along a bypass tunnel (See **Enabling MPLS TE and RSVP TE**.)
- (Optional) Configuring the physical link bandwidth for the bypass tunnel (See **(Optional) Configuring TE Attributes**.)
- Enabling CSPF on a PLR
- (Optional) Configuring an explicit path for the bypass tunnel

Configuration Procedures

Figure 2-4 Flowchart for configuring MPLS TE manual FRR



2.9.1 Enabling TE FRR

TE FRR must be enabled on the ingress of a primary tunnel before TE manual FRR is configured.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The view of the primary MPLS TE tunnel interface is displayed.

Step 3 Run:

```
mpls te fast-reroute
```

TE FRR is enabled.

By default, TE manual FRR is disabled.

NOTE

After TE FRR is enabled by running the **mpls te fast-reroute** command, run the **mpls te bypass-attributes** command to set bypass tunnel attributes.

Step 4 Run:

```
commit
```

The configuration is committed.

----End

2.9.2 Configuring a Bypass Tunnel

A path and attributes need to be configured for a bypass tunnel after TE manual FRR is enabled on a PLR.

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Run:

interface tunnel *tunnel-number*

The view of the bypass tunnel interface is displayed.

Step 3 Run:

tunnel-protocol mpls te

MPLS TE is configured.

Step 4 Run:

destination *ip-address*

The LSR ID of an MP is configured as the destination address of the bypass tunnel.

Step 5 (Optional) Run:

mpls te path explicit-path *path-name* [**secondary**]

An explicit path is configured for the bypass tunnel.

NOTE

Physical links of a bypass tunnel cannot overlap protected physical links of the primary tunnel.

Step 6 (Optional) Run either of the following commands to set the bandwidth for the bypass tunnel:

- **mpls te bandwidth** { **ct0** | **ct1** } *bandwidth*
- **mpls te bandwidth** { { **ct0** *ct0-bw-value* | **ct1** *ct1-bw-value* | **ct2** *ct2-bw-value* | **ct3** *ct3-bw-value* | **ct4** *ct4-bw-value* | **ct5** *ct5-bw-value* | **ct6** *ct6-bw-value* | **ct7** *ct7-bw-value* } *

Step 7 Run:

mpls te bypass-tunnel

A bypass tunnel is configured.

NOTE

- The **mpls te bypass-tunnel** command and the **mpls te backup** command cannot be configured together.
- The **mpls te bypass-tunnel** command and the **mpls te fast-reroute** command cannot be configured together.

Step 8 Run:

mpls te protected-interface *interface-type interface-number*

The interface on which the bypass tunnel protects traffic is specified.

NOTE

- The **mpls te protected-interface** command and the **mpls te backup** command cannot be configured together.
- The **mpls te protected-interface** command and the **mpls te fast-reroute** command cannot be configured together.

Step 9 Run:

```
commit
```

The configurations are committed.

----End

Follow-up Procedure

Routes and labels are automatically recorded after a bypass tunnel is configured.

One bypass tunnel protects a maximum of 16 MPLS TE-enabled physical interfaces. A bypass tunnel is set up by configuring an explicit path on the PLR.

If a primary tunnel fails, traffic switches to a bypass tunnel. If the bypass tunnel also goes Down, the protected traffic is interrupted and FRR fails. Even though the bypass tunnel goes Up, traffic cannot be forwarded. Traffic will be forwarded only after the primary tunnel has been restored or re-established.

NOTE

- The **mpls te fast-reroute** command and the **mpls te bypass-tunnel** command cannot be configured on the same tunnel interface.
- After FRR switches traffic from a primary tunnel to a bypass tunnel, the bypass tunnel must be kept Up and its path must remain unchanged when transmitting traffic. If the bypass tunnel goes Down, the protected traffic is interrupted and FRR fails.

2.9.3 Checking the Configuration

After configuring MPLS TE manual FRR, you can view detailed information about the bypass tunnel.

Prerequisite

The configurations of the MPLS TE manual FRR function are complete.

Procedure

- Run the **display mpls lsp** [**lsp-id** *ingress-lsr-id session-id lsp-id*] [**verbose**] command to check information about the primary tunnel.
- Run the **display mpls lsp attribute** [**bypass-inuse** { **inuse** | **not-exists** | **exists-not-used** } | **bypass-tunnel** *tunnel-name*] command to check information about the bypass tunnel.
- Run the **display mpls te tunnel-interface** [**tunnel** *tunnel-number*] command to check information about the tunnel interface on the ingress of a primary or bypass tunnel.
- Run the **display mpls te tunnel path** [[*tunnel-name*] [**lsp-id** *ingress-lsr-id session-id lsp-id*] | **fast-reroute** { **local-protection-available** | **local-protection-inuse** }] command to check information about paths of a primary or bypass tunnel.

----End

Example

Run the following commands to check the previous configurations.

Run the **display mpls lsp** command, and you can view information about the primary tunnel. For example:

```
<HUAWEI> display mpls lsp

------------------------------------------------------------------------------
                LSP Information: RSVP LSP
------------------------------------------------------------------------------
  FEC                In/Out Label  In/Out IF                      Vrf Name
  4.4.4.4/32         NULL/11264    -/Pos1/0/1
```

Run the **display mpls te tunnel-interface** command, and you can see that the tunnel is Up. For example:

```
<HUAWEI> display mpls te tunnel-interface
    Tunnel Name       : Tunnel1
    Tunnel State Desc : CR-LSP is Up
    Tunnel Attributes   :
    Active LSP          : Primary LSP
    Traffic Switch      : Primary LSP -> Hot-Standby LSP
    Session ID          : 1
    Ingress LSR ID      : 1.1.1.1               Egress LSR ID: 4.4.4.4
    Admin State         : UP                    Oper State   : UP
    Signaling Protocol  : RSVP
    FTid                : 1
    Tie-Breaking Policy : None                  Metric Type  : None
    BypassBW Flag       : Not Supported
    BypassBW Type       : -                     Bypass BW    : -
    Bfd Cap             : None                  Retry Int    : -
    Reopt               : Disabled              Reopt Freq   : -
    Auto BW             : Disabled
    Current Collected BW: -                     Auto BW Freq : -
    Min BW              : -                     Max BW       : -
    Tunnel Group        : -
    Interfaces Protected: -
    Excluded IP Address : -
    Is On Radix-Tree    : -                     Referred LSP Count: -
    Primary Tunnel      : -                     Pri Tunn Sum : -
    Backup Tunnel       : -
    Group Status        : -                     Oam Status   : -
    IPTN InLabel        : -
    BackUp Type         : None                  BestEffort   : Disabled
    SRLG Disjoing       : NA
    Secondary HopLimit  : -
    BestEffort HopLimit : -
    Secondary Explicit Path Name: -
    Secondary Affinity Prop/Mask: -
    BestEffort Affinity Prop/Mask: 0x0/0x0
    IsConfigLspConstraint: -

    Primary LSP ID      : 1.1.1.1:116
    LSP State           : FRR INUSE             LSP Type     : Primary
    Setup Priority      : 7                     Hold Priority: 7
    IncludeAll          : 0x0
    IncludeAny          : 0x0
    ExcludeAny          : 0x0
    Affinity Prop/Mask  : 0x0/0x0               Resv Style   :  SE
    Configured Bandwidth Information:
    CT0 Bandwidth(Kbit/sec): 50000          CT1 Bandwidth(Kbit/sec): 0
    CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
    CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
    CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
    Actual Bandwidth Information:
    CT0 Bandwidth(Kbit/sec): 50000          CT1 Bandwidth(Kbit/sec): 0
    CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
```

```
    CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
    CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
    Explicit Path Name  : pri-path              Hop Limit           : -
    Record Route        : Enabled             Record Label : Enabled
    Route Pinning       : Disabled
    FRR Flag            : Enabled
    IdleTime Remain     : -
    BFD Status          : -
```

Run the **display mpls te tunnel path** command, and you can view path attributes of tunnels. For example:

```
<HUAWEI> display mpls te tunnel path
Tunnel Interface Name : Tunnel2
 Lsp ID : 1.1.1.1 :200:1
 Hop Information
  Hop 1   2.1.1.1 Local-Protection available | bandwidth | node
  Hop 2   2.1.1.2  Label 106497
  Hop 3   2.2.2.2
  Hop 4   3.1.1.1 Local-Protection available | bandwidth
  Hop 5   3.1.1.2  Label 3
  Hop 6   3.3.3.3
 Tunnel Interface Name : AutoTunnel2
 Lsp ID : 1.1.1.1 :2 :2
 Hop Information
  Hop 1   10.1.1.2
  Hop 2   10.1.1.1
  Hop 3   3.3.3.3

 Tunnel Interface Name : AutoTunnel33
 Lsp ID : 2.2.2.2 :33 :209
 Hop Information
  Hop 1   2.2.2.2
  Hop 2   2.1.1.2
  Hop 3   2.1.1.1
  Hop 4   1.1.1.1
  Hop 5   10.1.1.2
  Hop 6   10.1.1.1
  Hop 7   3.3.3.3
```

2.10 Configuring MPLS TE Auto FRR

MPLS TE Auto FRR is a local protection mechanism that protects traffic on a link or a node on a CR-LSP.

Applicable Environment

On a network that requires high reliability, FRR is configured to improve network reliability. If the network topology is complex and a large number of links must be configured, the configuration procedure is complex.

Auto FRR automatically sets up an eligible bypass tunnel, simplifying configurations.

MPLS TE Auto FRR, similar to MPLS TE manual FRR, can be performed in the RSVP GR process. For details about MPLS TE manual FRR, see **Configuring MPLS TE Manual FRR**.

NOTE

Only a primary CR-LSP supports MPLS TE Auto FRR.

On the NE5000E, assume that a bypass tunnel with a higher priority is available. MPLS TE Auto FRR automatically deletes a binding between a primary tunnel and a bypass tunnel with a lower priority and binds the primary tunnel to another bypass tunnel with a higher priority. A bypass tunnel has a higher priority than another based on the following conditions in descending order:

- SRLG

  In MPLS TE Auto FRR, if the shared risk link group (SRLG) attribute needs to be configured, ensure that the primary and bypass tunnels are in different SRLGs; otherwise, the bypass tunnel cannot be set up.
- Bandwidth protection takes precedence over non-bandwidth protection.
- Node protection takes precedence over link protection.
- Manual protection takes precedence over auto protection.

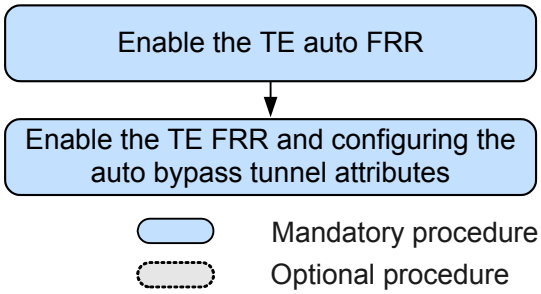
Pre-configuration Tasks

Before configuring MPLS TE Auto FRR, complete the following tasks:

- Setting up a primary RSVP-TE tunnel
- Enabling MPLS, MPLS TE, and RSVP-TE in the system view and the interface view on every node along a bypass tunnel (See **Enabling MPLS TE and RSVP-TE**.)
- (Optional) Configuring the physical bandwidth for a bypass tunnel if the primary tunnel bandwidth needs to be protected (See **(Optional) Configuring TE Attributes**.)
- Enabling CSPF on the ingress and transit nodes along a primary tunnel

Configuration Procedures

Figure 2-5 Flowchart for configuring MPLS TE Auto FRR



2.10.1 Enabling TE Auto FRR

MPLS TE Auto FRR must be enabled on the ingress or a transit node of a primary tunnel before MPLS TE Auto FRR is configured.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Step 3 Run:

```
mpls te auto-frr
```

MPLS TE Auto FRR is enabled globally.

By default, MPLS TE Auto FRR is disabled.

Step 4 Run:

```
quit
```

Return to the system view.

Step 5 Run:

```
interface interface-type interface-number
```

The view of the outbound interface of the primary tunnel is displayed.

Step 6 (Optional) Run:

```
mpls te auto-frr { link | node | default }
```

TE Auto FRR is enabled on the interface.

By default, all MPLS TE-enabled interfaces support TE Auto FRR after MPLS TE Auto FRR is enabled globally. To disable TE Auto FRR on interfaces, run the **undo mpls te auto-frr** command on these interfaces. The **undo mpls te auto-frr** command disables TE Auto FRR on interfaces, even if TE Auto FRR is enabled or re-enabled globally.

NOTE

- If the **mpls te auto-frr default** command is configured in the interface view, the Auto FRR capability on the interface is consistent with the global Auto FRR capability.
- After node protection is enabled, if an automatic bypass tunnel cannot be set up due to none available links, the penultimate hop (not other hops) on the primary tunnel attempts to set up an automatic bypass tunnel for link protection.

Step 7 Run:

```
commit
```

The configuration is committed.

----End

2.10.2 Enabling MPLS TE FRR and Configuring Attributes for an Automatic Bypass Tunnel

After MPLS TE FRR is enabled on the ingress of a primary tunnel, a bypass tunnel is set up automatically.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The view of the primary tunnel interface is displayed.

Step 3 Run:

```
mpls te fast-reroute [ bandwidth ]
```

TE FRR is enabled.

By default, the bandwidth of a specified tunnel is under protection.

Step 4 (Optional) Run:

```
mpls te bypass-attributes [ bandwidth bandwidth | priority setup-priority [ hold-priority ] ]
```

Attributes are set for the automatic bypass tunnel.

NOTE

- Bypass tunnel attributes can be configured only after MPLS TE FRR has been configured for a primary tunnel by running the **mpls te fast-reroute** [**bandwidth**]command.
- The bypass tunnel bandwidth cannot exceed the primary tunnel bandwidth.
- If no attributes are configured for an automatic bypass tunnel, by default, the automatic bypass tunnel uses the same bandwidth as that of the primary tunnel.
- The setup priority of a bypass tunnel must be equal to or lower than its holding priority. These priorities cannot be higher than the corresponding priorities of the primary tunnel.
- If the primary tunnel bandwidth is changed or FRR is disabled, the bypass tunnel attributes are automatically deleted.
- On one TE tunnel interface, the bypass tunnel bandwidth cannot be configured together with the multi-CT.

Step 5 Run:

```
commit
```

The configurations are committed.

----End

2.10.3 Checking the Configuration

After configuring MPLS TE Auto FRR, you can view detailed information about the bypass tunnel.

Prerequisite

The configurations of MPLS TE Auto FRR are complete.

Procedure

- Run the **display mpls te tunnel verbose** command to check the binding of a primary tunnel and an automatic bypass tunnel.
- Run the **display mpls te tunnel-interface** [**tunnel** *tunnel-number* | **auto-bypass-tunnel** *tunnel-name*] command to check detailed information about an automatic bypass tunnel.
- Run the **display mpls te tunnel path** [[*tunnel-name*] [**lsp-id** *ingress-lsr-id session-id lsp-id*] | **fast-reroute** { **local-protection-available** | **local-protection-inuse** }] command to check information about paths of a primary or bypass tunnel.

----End

Example

Run the following commands to check the previous configurations.

Run the **display mpls te tunnel verbose** command, and you can view detailed information about TE tunnels. For example:

```
<HUAWEI> display mpls te tunnel verbose

    No                      :  1
    Tunnel-Name             :  Tunnel2
    TunnelIndex             :  1           LSP Index         :  3072
    Session ID              :  200         LSP ID            :  1
    Lsr Role                :  Ingress
    Ingress LSR ID          :  1.1.1.1
    Egress LSR ID           :  3.3.3.3
    In-Interface            :  -
    Out-Interface           :  GE2/0/0
    Sign-Protocol           :  RSVP TE     Resv Style        :  SE
    IncludeAnyAff           :  0x0         ExcludeAnyAff     :  0x0
    IncludeAllAff           :  0x0
    ER-Hop Table Index      :  -           AR-Hop Table Index:  2
    C-Hop Table Index       :  -
    PrevTunnelIndexInSession:  -           NextTunnelIndexInSession:  -
    PSB Handle              :  65546
    Created Time            :  2009/03/30 09:52:03 DST
    --------------------------------
              DS-TE Information
    --------------------------------
    Bandwidth Reserved Flag :  Reserved
    CT0 Bandwidth(Kbit/sec) :  10000       CT1 Bandwidth(Kbit/sec):  0
    CT2 Bandwidth(Kbit/sec) :  0           CT3 Bandwidth(Kbit/sec):  0
    CT4 Bandwidth(Kbit/sec) :  0           CT5 Bandwidth(Kbit/sec):  0
    CT6 Bandwidth(Kbit/sec) :  0           CT7 Bandwidth(Kbit/sec):  0
    Setup-Priority          :  7           Hold-Priority     :  7
    --------------------------------
                FRR Information
    --------------------------------
    Primary LSP Info
    TE Attribute Flag       :  0x63        Protected Flag    :  0x1
    Bypass In Use           :  Not Used
    Bypass Tunnel Id        :  67141670
    BypassTunnel            :  Tunnel Index[AutoTunnel2], InnerLabel[3]
    Bypass Lsp ID           :  -           FrrNextHop        :  3.3.3.3
    ReferAutoBypassHandle   :  2049
    FrrPrevTunnelTableIndex :  -           FrrNextTunnelTableIndex:  -
    Bypass Attribute(Not configured)
    Setup Priority          :  -           Hold Priority     :  -
    HopLimit                :  -           Bandwidth         :  -
    IncludeAnyGroup         :  -           ExcludeAnyGroup   :  -
    IncludeAllGroup         :  -
    Bypass Unbound Bandwidth Info(Kbit/sec)
    CT0 Unbound Bandwidth   :  -         CT1 Unbound Bandwidth:  -
    CT2 Unbound Bandwidth   :  -         CT3 Unbound Bandwidth:  -
    CT4 Unbound Bandwidth   :  -         CT5 Unbound Bandwidth:  -
    CT6 Unbound Bandwidth   :  -         CT7 Unbound Bandwidth:  -
    --------------------------------
               BFD Information
    --------------------------------
    NextSessionTunnelIndex  :  -           PrevSessionTunnelIndex:  -
    NextLspId               :  -           PrevLspId         :  -
```

Run the **display mpls te tunnel-interface** command, and you can see that the tunnel is Up. For example:

```
<HUAWEI> display mpls te tunnel-interface
    Tunnel Name       : Tunnel1
    Tunnel State Desc : CR-LSP is Up
    Tunnel Attributes   :
    Active LSP          : Primary LSP
    Traffic Switch      : Primary LSP -> Hot-Standby LSP
    Session ID          : 1
    Ingress LSR ID      : 1.1.1.1              Egress LSR ID: 4.4.4.4
    Admin State         : UP                   Oper State   : UP
    Signaling Protocol  : RSVP
    FTid                : 1
    Tie-Breaking Policy : None                 Metric Type  : None
```

```
    BypassBW Flag       : Not Supported
    BypassBW Type       : -                     Bypass BW    : -
    Bfd Cap             : None                  Retry Int    : -
    Reopt               : Disabled              Reopt Freq   : -
    Auto BW             : Disabled
    Current Collected BW: -                     Auto BW Freq : -
    Min BW              : -                     Max BW       : -
    Tunnel Group        : -
    Interfaces Protected: -
    Excluded IP Address : -
    Is On Radix-Tree    : -                     Referred LSP Count: -
    Primary Tunnel      : -                     Pri Tunn Sum : -
    Backup Tunnel       : -
    Group Status        : -                     Oam Status   : -
    IPTN InLabel        : -
    BackUp Type         : None                  BestEffort   : Disabled
    SRLG Disjoing       : NA
    Secondary HopLimit  : -
    BestEffort HopLimit : -
    Secondary Explicit Path Name: -
    Secondary Affinity Prop/Mask: -
    BestEffort Affinity Prop/Mask: 0x0/0x0
    IsConfigLspConstraint: -

    Primary LSP ID      : 1.1.1.1:116
    LSP State           : FRR INUSE             LSP Type     : Primary
    Setup Priority      : 7                     Hold Priority: 7
    IncludeAll          : 0x0
    IncludeAny          : 0x0
    ExcludeAny          : 0x0
    Affinity Prop/Mask  : 0x0/0x0               Resv Style   :  SE
    Configured Bandwidth Information:
    CT0 Bandwidth(Kbit/sec): 50000          CT1 Bandwidth(Kbit/sec): 0
    CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
    CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
    CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
    Actual Bandwidth Information:
    CT0 Bandwidth(Kbit/sec): 50000          CT1 Bandwidth(Kbit/sec): 0
    CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
    CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
    CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
    Explicit Path Name  : pri-path              Hop Limit          : -
    Record Route        : Enabled               Record Label : Enabled
    Route Pinning       : Disabled
    FRR Flag            : Enabled
    IdleTime Remain     : -
    BFD Status          : -
```

Run the **display mpls te tunnel path** command, and you can view information about path attributes of tunnels. For example:

```
<HUAWEI> display mpls te tunnel path
Tunnel Interface Name : Tunnel2
 Lsp ID : 1.1.1.1 :200:1
 Hop Information
  Hop 1   2.1.1.1 Local-Protection available | bandwidth | node
  Hop 2   2.1.1.2  Label 106497
  Hop 3   2.2.2.2
  Hop 4   3.1.1.1 Local-Protection available | bandwidth
  Hop 5   3.1.1.2  Label 3
  Hop 6   3.3.3.3
 Tunnel Interface Name : AutoTunnel2
 Lsp ID : 1.1.1.1 :2 :2
 Hop Information
  Hop 1   10.1.1.2
  Hop 2   10.1.1.1
  Hop 3   3.3.3.3

 Tunnel Interface Name : AutoTunnel33
 Lsp ID : 2.2.2.2 :33 :209
```

```
Hop Information
  Hop 1   2.2.2.2
  Hop 2   2.1.1.2
  Hop 3   2.1.1.1
  Hop 4   1.1.1.1
  Hop 5   10.1.1.2
  Hop 6   10.1.1.1
  Hop 7   3.3.3.3
```

2.11 Configuring CR-LSP Backup

CR-LSP backup is configured to provide end-to-end protection for a CR-LSP.

Applicable Environment

CR-LSP backup provides an end-to-end path protection for an entire CR-LSP.

A backup CR-LSP is established in either of the following modes:

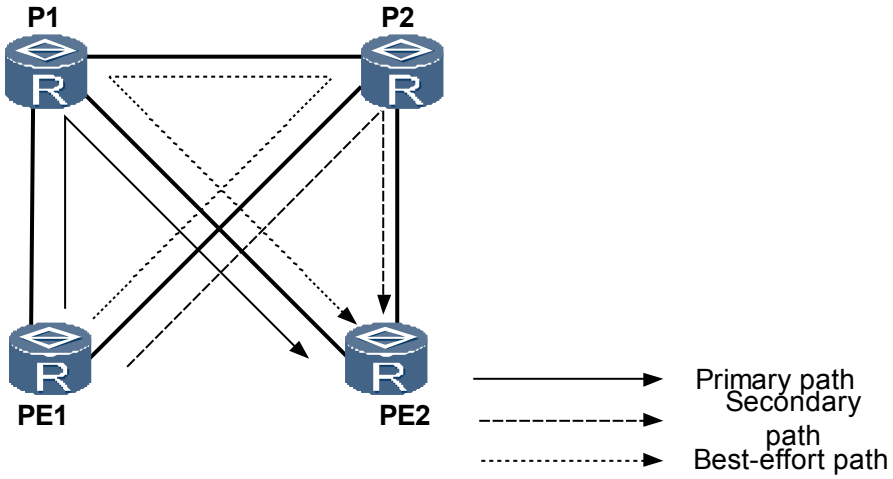
- Hot-standby mode: A backup CR-LSP and a primary CR-LSP are created together.
- Ordinary backup mode: A backup CR-LSP is created only after a primary CR-LSP fails.

The paths of backup CR-LSPs in the preceding modes are different:

- Hot standby mode: The path of a backup CR-LSP and the path of a primary CR-LSP overlap only if the backup CR-LSP is set up over an explicit path.
- Ordinary backup mode: The path of a backup CR-LSP and the path of a primary CR-LSP overlap in any cases.

Hot standby supports best-effort paths. If both the primary and backup CR-LSPs fail, a temporary path, called a best-effort path, is set up, and all traffic switches to this path. As shown in **Figure 2-6**, the path of the primary CR-LSP is PE1 -> P1 -> PE2 and the path of the backup CR-LSP is PE1 -> P2 -> PE2. If both the primary and backup CR-LSPs fail, the node triggers the setup of a best-effort path along the path PE1 -> P2 -> P1 -> PE2.

Figure 2-6 Schematic diagram for a best-effort path



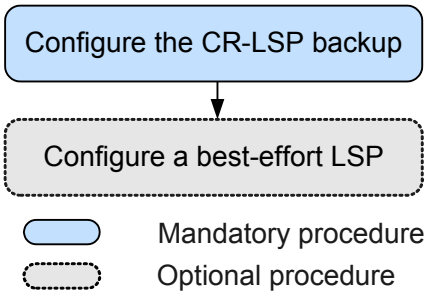
Pre-configuration Tasks

Before configuring CR-LSP backup, complete the following tasks:

- Setting up a primary RSVP-TE tunnel
- Enabling MPLS, MPLS TE, and RSVP-TE in the system view and the physical interface view on every node along a bypass tunnel (See **Enabling MPLS TE and RSVP-TE**.)
- (Optional) Configuring the link bandwidth for the backup CR-LSP (See **(Optional) Configuring TE Attributes**.)
- (Optional) Configuring an explicit path for the backup CR-LSP (See **(Optional) Configuring an Explicit Path**.)

Configuration Procedures

Figure 2-7 Flowchart for configuring CR-LSP backup



2.11.1 Configuring CR-LSP Backup

A backup CR-LSP is established in either hot standby or ordinary backup mode. A hot-standby CR-LSP and an ordinary backup CR-LSP cannot be established together.

Context

CR-LSP backup is disabled by default. After CR-LSP backup is configured on the ingress of a primary CR-LSP, the system automatically selects a path for a backup CR-LSP.

NOTE

CR-LSP backup and CR-LSP re-optimization cannot be configured together.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The view of the MPLS TE tunnel interface is displayed.

Step 3 Run:

```
mpls te backup { hot-standby | ordinary [ best-effort ] }
```

The mode of establishing a backup CR-LSP is configured.

NOTE

The bypass and backup tunnels cannot be configured on the same tunnel interface. The **mpls te bypass-tunnel** and **mpls te backup** commands cannot be configured on the same tunnel interface. Also, the **mpls te protected-interface** and **mpls te backup** commands cannot be configured on the same tunnel interface.

Step 4 (Optional) Run:

mpls te path explicit-path *path-name* **secondary**

An explicit path is specified for the backup CR-LSP.

NOTE

The **mpls te path explicit-path** *path-name* **secondary** and **mpls te backup** commands must be configured together.

Step 5 (Optional) Run:

mpls te affinity property *properties* [**mask** *mask-value*] **secondary**

The affinity property is configured for the backup CR-LSP.

The default affinity property used by the backup CR-LSP is 0x0.

Step 6 (Optional) Run:

mpls te hop-limit *hop-limit-value* **secondary**

The hop limit is set for the backup CR-LSP.

NOTE

mpls te hop-limit *hop-limit-value* **secondary** and **mpls te backup** commands must be configured together.

Step 7 Run:

commit

The configurations are committed.

----End

2.11.2 (Optional) Configuring a Best-effort Path

A best-effort path is configured to take over traffic if both the primary and backup CR-LSPs fail.

Context

In hot-standby mode, do as follows on the ingress of a TE tunnel:

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Run:

interface tunnel *tunnel-number*

The view of the MPLS TE tunnel interface is displayed.

Step 3 Run:

```
mpls te backup ordinary best-effort
```

A best-effort path is configured.

NOTE

The **mpls te backup ordinary best-effort** command and the **mpls te backup ordinary** command cannot be configured on the same tunnel interface.

Step 4 (Optional) Run:

```
mpls te affinity property properties [ mask mask-value ] best-effort
```

The affinity property of the best-effort path is configured.

The default affinity property used by a best-effort path is 0x0.

Step 5 (Optional) Run:

```
mpls te hop-limit hop-limit-value best-effort
```

The hop limit is set for the best-effort path.

Step 6 Run:

```
commit
```

The configuration is committed.

----End

2.11.3 Checking the Configuration

After configuring CR-LSP backup, you can view information about backup CR-LSPs.

Prerequisite

The configurations of CR-LSP backup are complete.

Procedure

- Run the **display mpls te tunnel-interface** [**tunnel** *tunnel-number*] command to check information about a tunnel interface on the ingress of a tunnel.
- Run the **display mpls te hot-standby state** { **all** [**verbose**] | **interface tunnel** *interface-number* } command to check information about the hot-standby status.

----End

Example

Run the following commands to check the previous configurations.

Run the **display mpls te tunnel-interface** command, and you can see that the tunnel is Up. For example:

```
<HUAWEI> display mpls te tunnel-interface
    Tunnel Name       : Tunnel1
    Tunnel State Desc : CR-LSP is Up
    Tunnel Attributes   :
    Active LSP          : Primary LSP
    Traffic Switch      : Primary LSP -> Hot-Standby LSP
    Session ID          : 1
    Ingress LSR ID      : 1.1.1.1              Egress LSR ID: 4.4.4.4
```

```
    Admin State         : UP                  Oper State   : UP
    Signaling Protocol  : RSVP
    FTid                : 1
    Tie-Breaking Policy : None                Metric Type  : None
    BypassBW Flag       : Not Supported
    BypassBW Type       : -                   Bypass BW    : -
    Bfd Cap             : None                Retry Int    : -
    Reopt               : Disabled            Reopt Freq   : -
    Auto BW             : Disabled
    Current Collected BW: -                   Auto BW Freq : -
    Min BW              : -                   Max BW       : -
    Tunnel Group        : -
    Interfaces Protected: -
    Excluded IP Address : -
    Is On Radix-Tree    : -                   Referred LSP Count: -
    Primary Tunnel      : -                   Pri Tunn Sum : -
    Backup Tunnel       : -
    Group Status        : -                   Oam Status   : -
    IPTN InLabel        : -
    BackUp Type         : None                BestEffort   : Disabled
    SRLG Disjoing       : NA
    Secondary HopLimit  : -
    BestEffort HopLimit : -
    Secondary Explicit Path Name: -
    Secondary Affinity Prop/Mask: -
    BestEffort Affinity Prop/Mask: 0x0/0x0
    IsConfigLspConstraint: -

    Primary LSP ID      : 1.1.1.1:116
    LSP State           : FRR INUSE           LSP Type     : Primary
    Setup Priority      : 7                   Hold Priority: 7
    IncludeAll          : 0x0
    IncludeAny          : 0x0
    ExcludeAny          : 0x0
    Affinity Prop/Mask  : 0x0/0x0             Resv Style   :  SE
    Configured Bandwidth Information:
    CT0 Bandwidth(Kbit/sec): 50000          CT1 Bandwidth(Kbit/sec): 0
    CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
    CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
    CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
    Actual Bandwidth Information:
    CT0 Bandwidth(Kbit/sec): 50000          CT1 Bandwidth(Kbit/sec): 0
    CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
    CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
    CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
    Explicit Path Name  : pri-path              Hop Limit           : -
    Record Route        : Enabled               Record Label : Enabled
    Route Pinning       : Disabled
    FRR Flag            : Enabled
    IdleTime Remain     : -
    BFD Status          : -
```

Run the **display mpls te hot-standby state interface tunnel** *interface-number* command, and you can view the hot-standby status of the tunnel interface. For example:

```
<HUAWEI> display mpls te hot-standby state interface Tunnel 1
------------------------------------------------------------------
Verbose information about the Tunnel1 hot-standby state
------------------------------------------------------------------
    Tunnel Name           : Tunnel1
    Session ID            : 502
    Main LSP index        : 503
    Hot-standby LSP index : 504
    HSB switch result     : main LSP
    WTR                   : -
```

2.12 Configuring an RSVP GR Helper

An RSVP GR Helper is configured to allow devices along an RSVP-TE tunnel to retain RSVP sessions during a master/slave switchover.

Applicable Environment

If an RSVP node undergoes master/slave switchover, its RSVP adjacency with its neighbor may be torn down due to a signaling protocol timeout. As a result, the CR-LSP is removed, and a temporary network interruption occurs. RSVP GR prevents the preceding problem. RSVP GR restores an RSVP adjacency without interrupting an RSVP session.

On the NE5000E, FRR can be performed during the RSVP GR process. FRR shortens fault duration when a master/slave switchover is performed on a PLR, the PLR' upstream node, an MP, or the MP's downstream node, and the outbound interface of a primary tunnel on the PLR fails.

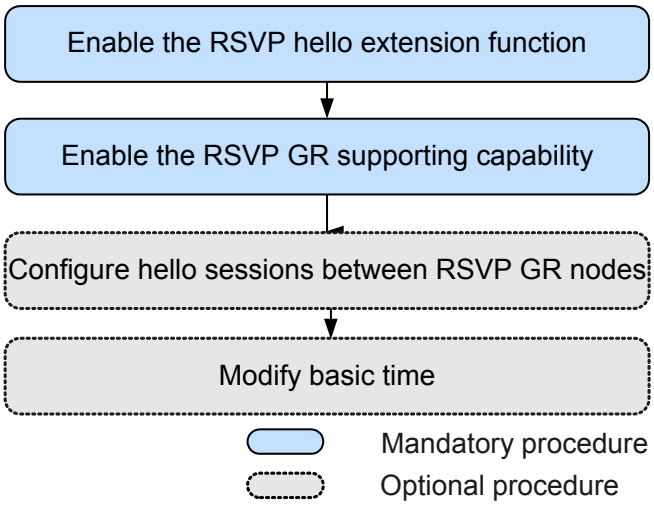
Pre-configuration Tasks

Before configuring an RSVP GR Helper, complete the following task:

- **Configuring an RSVP-TE Tunnel**

Configuration Procedures

Figure 2-8 Flowchart for configuring an RSVP GR Helper



2.12.1 Enabling the RSVP Hello Extension

The RSVP Hello extension is configured on a GR node and its neighbor, rapidly detecting reachability between these RSVP nodes.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Step 3 Run:

```
mpls rsvp-te hello
```

The RSVP Hello extension is enabled globally.

Step 4 Run:

```
quit
```

The system view is displayed.

Step 5 Run:

```
interface interface-type interface-number
```

The view of an RSVP-enabled interface is displayed.

Step 6 Run:

```
mpls rsvp-te hello
```

The RSVP Hello extension is enabled on an interface.

After RSVP Hello extension is enabled globally on a node, enable the RSVP Hello extension on each interface of the node.

Step 7 Run:

```
commit
```

The configuration is committed.

----End

2.12.2 Enabling the RSVP GR Support Capability

The RSVP GR support capability helps a node to support its neighbor's GR capabilities.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Step 3 Run:

```
mpls rsvp-te
```

RSVP-TE is enabled.

Step 4 Run:

```
mpls rsvp-te hello
```

The RSVP Hello extension is enabled on the local node.

Step 5 Run:

```
mpls rsvp-te hello support-peer-gr
```

The RSVP GR support function is enabled.

Step 6 Run:

```
commit
```

The configurations are committed.

----End

2.12.3 (Optional) Configuring a Hello Session Between RSVP GR Nodes

If TE FRR is deployed, a Hello session needs to be set up between a PLR and an MP. A Hello session must be manually set up if it cannot be automatically set up between RSVP neighboring nodes.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Step 3 Run:

```
mpls rsvp-te
```

RSVP-TE is enabled.

Step 4 Run:

```
mpls rsvp-te hello
```

The RSVP Hello extension is enabled on the local node.

Step 5 Run:

```
mpls rsvp-te hello nodeid-session ip-address
```

A Hello session is set up between two RSVP neighboring nodes.

ip-address specifies the LSR ID of an RSVP neighboring node.

Step 6 Run:

```
commit
```

The configurations are committed.

----End

2.12.4 (Optional) Changing the Basic Time

Changing the basic time and the number of ingress CR-LSPs affects the restart time.

Context

If a master/slave switchover starts, an RSVP GR node enters the RSVP smoothing phase, during which the forwarding plane continues forwarding data but the control plane is not restored. After RSVP smoothing is completed, a restart timer starts.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Step 3 Run:

```
mpls rsvp-te hello basic-restart-time basic-restart-time
```

The RSVP GR basic time is changed.

The default RSVP GR basic time is 90 seconds.

Step 4 Run:

```
commit
```

The configuration is committed.

----End

2.12.5 Checking the Configuration

After configuring RSVP GR, you can verify that the TE tunnel properly forwards data during the GR process.

Prerequisite

The configurations of RSVP GR are complete.

Procedure

- Run the **display mpls rsvp-te graceful-restart** command to check the RSVP-TE GR status.
- Run the **display mpls rsvp-te graceful-restart peer** [{ **interface** *interface-type interface-number* | **node-id** } [*ip-address*]] command to check information about the RSVP GR status on a neighbor.

----End

Example

Run the following commands to check the previous configurations.

Run the **display mpls rsvp-te graceful-restart** command, and you can view the RSVP GR status on the local node. For example:

```
<HUAWEI> display mpls rsvp-te graceful-restart
Display Mpls Rsvp te graceful restart information
 LSR ID: 3.3.3.3
 Graceful-Restart Capability:    GR-Support
 Restart Time:  90000 Milli Second
 Recovery Time: 0 Milli Second
 GR Status:  Gracefully Restart Not going on
 Number of Restarting neighbors: 0
 Number of LSPs recovered: 0
 Received Gr Path message count: 0
 Send Gr Path message count: 0
 Received RecoveryPath message count: 0
 Send RecoveryPath message count: 0
```

Run the **display mpls rsvp-te graceful-restart peer** command, and you can view the RSVP GR status on a neighbor. For example:

```
<HUAWEI> display mpls rsvp-te graceful-restart peer
 Remote Node id Neighbor
 Neighbor Addr: 1.1.1.1
 SrcInstance: 0x8A9CB904                    NbrSrcInstance: 0x8A96435C
 Neighbor Capability:
                     Can Do Self GR
                     Can Support GR
 Self Gr Capability with this Nbr:   GR-None
 GR Status:          Normal
 Restart Time:  90060 Milli Second
 Recovery Time: 0 Milli Second
 Stored GR message number: 0

 Neighbor on Interface GigabitEthernet1/0/0
 Neighbor Addr: 10.1.2.1             Last Attribute: Added Usually
 SrcInstance: 0x8A9CB904             NbrSrcInstance: 0x0
 Neighbor Capability:
                    No Gr capabilities
 Self Gr Capability with this Nbr:     GR-None
 GR Status:          Normal
 Restart Time:  0 Milli Second
 Recovery Time: 0 Milli Second
 Stored GR message number: 0
```

2.13 Configuring Static BFD for CR-LSP

By configuring static BFD for CR-LSP, you can detect a static CR-LSP or an RSVP CR-LSP.

Applicable Environment

BFD can detect CR-LSPs of the following types:

- Static CR-LSP
- RSVP CR-LSP

BFD for CR-LSP can be used to replace MPLS Operation Administration and Maintenance (OAM) to detect an MPLS TE protection group and trigger the primary/backup CR-LSP switchover of the protection group. BFD for CR-LSP can also detect the primary CR-LSP and the hot-standby CR-LSP, and trigger the traffic switchover between the primary CR-LSP and the hot-standby CR-LSP.

NOTE

For one CR-LSP, MPLS OAM and BFD cannot be configured together.

In the scenario where static BFD for CR-LSP is applied and the BFD status is Up, if the tunnel interface of the CR-LSP is shut down, the BFD status remains Up.

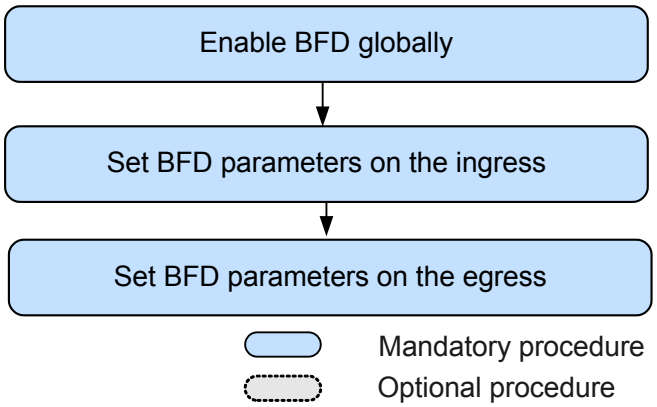
Pre-configuration Tasks

Before configuring static BFD for CR-LSP, complete the following task:

- Configuring a static CR-LSP or an RSVP-TE tunnel or configuring CR-LSP backup or an MPLS TE tunnel protection group

Configuration Procedures

Figure 2-9 Flowchart of configuring static BFD for CR-LSP



2.13.1 Enabling BFD Globally

BFD must be enabled globally before configurations relevant to BFD are performed.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bfd
```

BFD is enabled globally on the local node and the BFD view is displayed.

Configurations relevant to BFD can be performed only after the **bfd** command is run globally.

Step 3 Run:

```
commit
```

The configurations are committed.

----End

2.13.2 Setting BFD Parameters on the Ingress

This section describes how to set BFD parameters on the ingress to detect the CR-LSP through BFD sessions.

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Run:

bfd *session-name* **bind mpls-te interface tunnel** *interface-number* **te-lsp** [**backup**]

The BFD session is bound to the primary or backup CR-LSP of the specified tunnel.

If the parameter **backup** is specified, the BFD session is bound to the backup CR-LSP.

Step 3 Run:

discriminator local *discr-value*

The local discriminator of the BFD session is configured.

Step 4 Run:

discriminator remote *discr-value*

The remote discriminator of the BFD session is configured.

NOTE

The local discriminators and remote discriminators of the two ends on a BFD session must be correctly associated. That is, the local discriminator of the local device and the remote discriminator of the remote device are the same, and the remote discriminator of the local device and the local discriminator of the remote device are the same. Otherwise, the BFD session cannot be correctly set up. In addition, the local and remote discriminators cannot be modified after being successfully configured.

Step 5 (Optional) Run:

min-tx-interval *interval*

The minimum interval for sending BFD packets is configured.

By default, the minimum interval for sending BFD packets is 10 milliseconds (ms).

Actual local interval for receiving BFD packets = MAX { Local sending interval, Remote receiving interval }.

Actual local interval for receiving BFD packets = MAX { Remote sending interval, Local receiving interval }.

Local detection period = Local receiving interval x Remote BFD detection multiplier.

For example: assume that the locally-configured interval for sending BFD packets is 200 ms, the interval for receiving BFD packets is 300 ms, the detection multiplier is 4, and the remotely-configured interval for sending BFD packets is 100 ms, the interval for receiving BFD packets is 600 ms, the detection multiplier is 5.

- The actual local interval for sending BFD packets is 600 ms (MAX { 200 ms, 600 ms }), the actual local interval for receiving BFD packets is 300 ms (MAX { 100 ms, 300 ms }), and the detection interval is 1500 ms (300 ms x 5).

- The actual remote interval for sending BFD packets is 300 ms (MAX { 100 ms, 300 ms }), the actual remote interval for receiving BFD packets is 600 ms (MAX { 200 ms, 600 ms}), and the detection interval is 2400 ms (600 ms x 4).

Step 6 (Optional) Run:

min-rx-interval *interval*

The minimum interval for the local device to receive BFD packets is configured.

By default, the minimum interval for the local device to receive BFD packets is 10 ms.

Step 7 (Optional) Run:

detect-multiplier *multiplier*

The local BFD detection multiplier is configured.

By default, the local BFD detection multiplier is 3.

Step 8 Run:

commit

The configurations are committed.

----End

2.13.3 Setting BFD Parameters on the Egress

This section describes how to set BFD parameters on the egress to detect the CR-LSP through BFD sessions.

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 The IP link, LSP, or TE tunnel can be used as the reverse tunnel to inform the ingress of a fault. If there is a reverse LSP or a TE tunnel, you need to use the reverse LSP or the TE tunnel; otherwise, you can choose an IP link. If the configured reverse tunnel requires BFD detection, you can configure a pair of BFD sessions for it. Run the following commands as required:

- Run:

  bfd *session-name* **bind peer-ip** *ip-address* [**vpn-instance** *vpn-name*] [**source-ip** *ip-address*]

  A BFD session with the reverse tunnel being an IP link is established.

- Run:

  bfd *session-name* **bind ldp-lsp peer-ip** *ip-address* [**nexthop** *ip-address* [**interface** *interface-type interface-number*]]

  A BFD session with the reverse tunnel being an LDP LSP is established.

- Run:

  bfd *session-name* **bind mpls-te interface tunnel** *interface-number* **te-lsp** [**backup**]

  A BFD session with the reverse tunnel being a CR-LSP is established.

- Run:

  bfd *session-name* **bind mpls-te interface tunnel** *interface-number*

A BFD session with the reverse tunnel being a TE tunnel is established.

Step 3 Run:

```
discriminator local discr-value
```

The local discrimitor of the BFD session is configured.

Step 4 Run:

```
discriminator remote discr-value
```

The remote discriminator of the BFD session is configured.

NOTE

The local discriminators and remote discriminators of the two ends on a BFD session must be correctly associated. That is, the local discriminator of the local device and the remote discriminator of the remote device are the same, and the remote discriminator of the local device and the local discriminator of the remote device are the same. Otherwise, the BFD session cannot be correctly set up. In addition, the local and remote discriminators cannot be modified after being successfully configured.

Step 5 (Optional) Run:

```
min-tx-interval interval
```

The minimum interval for sending BFD packets is configured.

By default, the minimum interval for sending BFD packets is 10 milliseconds.

If the reverse tunnel is an IP link, this parameter is not applicable.

Actual local interval for receiving BFD packets = MAX { Local sending interval, Remote receiving interval }.

Actual local interval for receiving BFD packets = MAX { Remote sending interval, Local receiving interval }.

Local detection period = Local receiving interval x Remote BFD detection multiplier.

For example: assume that the locally-configured interval for sending BFD packets is 200 milliseconds, the interval for receiving BFD packets is 300 milliseconds, the detection multiplier is 4, and the remotely-configured interval for sending BFD packets is 100 milliseconds, the interval for receiving BFD packets is 600 milliseconds, the detection multiplier is 5.

- The actual local interval for sending BFD packets is 600 milliseconds (MAX { 200 milliseconds, 600 milliseconds }), the actual local interval for receiving BFD packets is 300 milliseconds (MAX { 100 milliseconds, 300 milliseconds }), and the detection interval is 1500 milliseconds (300 milliseconds x 5).
- The actual remote interval for sending BFD packets is 300 milliseconds (MAX { 100 milliseconds, 300 milliseconds }), the actual remote interval for receiving BFD packets is 600 milliseconds (MAX { 200 milliseconds, 600 milliseconds}), and the detection interval is 2400 milliseconds (600 milliseconds x 4).

Step 6 (Optional) Run:

```
min-rx-interval interval
```

The minimum interval for the local device to receive BFD packets is configured.

By default, the minimum interval for the local device to receive BFD packets is 10 milliseconds.

Step 7 (Optional) Run:

```
detect-multiplier multiplier
```

The BFD detection multiplier is configured.

Step 8 Run:

```
commit
```

The configurations are committed.

----End

2.13.4 Checking the Configuration

After the static BFD for CR-LSP is configured, you can view configurations, such as the status of the BFD sessions being Up.

Prerequisite

All configurations of the static BFD for CR-LSP are complete.

Procedure

- Run the **display bfd session mpls-te interface** *tunnel-name* **te-lsp** [**verbose**] command, and you can view information about the BFD session on the ingress.
- Run the following commands to view information about the BFD session on the egress.
  - Run the **display bfd session all** [**for-ip** | **for-lsp** | **for-te**] [**verbose**] command, and you can view information about all BFD sessions.
  - Run the **display bfd session static** [**for-ip** | **for-lsp** | **for-te**] [**verbose**] command, and you can view information about the static BFD session.
  - Run the **display bfd session peer-ip** *peer-ip* [**vpn-instance** *vpn-name*] [**verbose**] command, and you can view information about the BFD session with the reverse tunnel being the IP link.
  - Run the **display bfd session ldp-lsp peer-ip** *ip-address* [**interface** *interface-type interface-number*] [**verbose**] command, and you can view information about the BFD session with the reverse tunnel being the LDP LSP.
  - Run the **display bfd session mpls-te interface** *tunnel-name* **te-lsp** [**verbose**] command, and you can view information about the BFD session with the reverse tunnel being the CR-LSP.
  - Run the **display bfd session mpls-te interface** *tunnel-name* [**verbose**] command, and you can view information about the BFD session with the reverse tunnel being the TE tunnel.
- Run the following commands to view the statistics on the BFD session.
  - Run the **display bfd statistics session all** [**for-ip** | **for-lsp** | **for-te**] [**verbose**] command, and you can view the statistics on all BFD sessions.
  - Run the **display bfd statistics session static** [**discriminator** *local-discriminator* | **for-ip** | **for-lsp** | **for-te**] [**verbose**] command, and you can view the statistics on static BFD sessions.
  - Run the **display bfd statistics session peer-ip** *peer-ip* [**vpn-instance** *vpn-name*] command, and you can view the statistics on the BFD sessions with the reverse tunnel being the IP link.

- Run the **display bfd statistics session ldp-lsp peer-ip** *peer-ip* [**interface** *interface-type interface-number*] command, and you can view the statistics on the BFD sessions with the reverse tunnel being the LDP LSP.
- Run the **display bfd statistics session mpls-te interface tunnel** { *tunnel-id* | *tunnel-number* } **te-lsp** command, and you can view statistics on the BFD sessions with the reverse tunnel being the CR-LSP.

----End

Example

After the configuration is complete, run the **display bfd session all** command, and you can find that the BFD session status is Up, and the BFD session type is S_TE_LSP.

```
<HUAWEI> display bfd session discriminator 10
--------------------------------------------------------------------------------
Local  Remote PeerIpAddr        State     Type              InterfaceName
--------------------------------------------------------------------------------
10     20     3.3.3.3           Up        S_TE_LSP          Tunnel1/0/0
--------------------------------------------------------------------------------
```

Run the **display bfd statistics session all** command, and you can view statistics on all BFD sessions.

```
<HUAWEI> display bfd statistics session all
--------------------------------------------------------------------------------
  State : Up                     Name : atob
--------------------------------------------------------------------------------
  Session Type                        : Static
  Bind Type                           : TE_LSP
  Local/Remote Discriminator          : 10/20
  Received Packets                    : 1710577
  Sent Packets                        : 1710593
  Received Bad Packets                : 0
  Sent Failed Packets                 : 0
  Down Count                          : 0
  ShortBreak Count                    : 0
  Sent Lsp Ping Count                 : 0
  Create Time                         : 2009/09/27 07:20:06
  Last Down Time                      : 0000/00/00 00:00:00
  Total Time From Last DOWN           : -D:--H:--M:--S
  Total Time From Create              : 0D:09H:03M:47S
--------------------------------------------------------------------------------

     Total Session Number :  1
```

2.14 Configuring the Static BFD for TE

This section describes how to configure the static BFD for TE to detect faults on the TE tunnel.

Applicable Environment

Detecting the TE tunnel through BFD sessions triggers VPN FRR to quickly switch traffic when the primary TE tunnel is faulty, which reduces the adverse effect on services.

NOTE

You cannot configure both MPLS OAM and BFD detection on a TE tunnel.

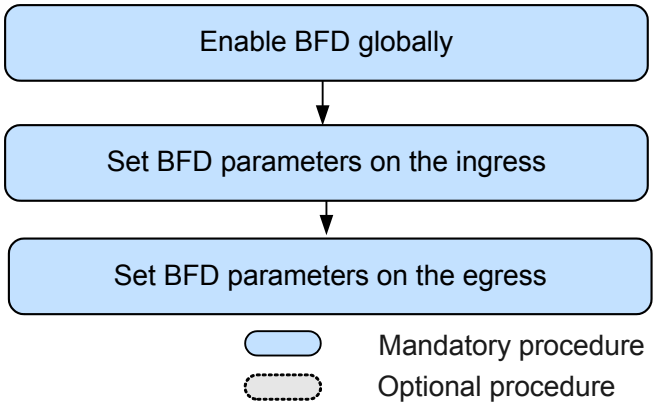
Pre-configuration Task

Before configuring the static BFD for TE, complete the following tasks:

- Configuring a static CR-LSP or an MPLS TE tunnel

Configuration Procedures

Figure 2-10 Networking diagram of the static BFD for TE



2.14.1 Enabling BFD Globally

BFD must be enabled globally before configurations relevant to BFD are performed.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bfd
```

BFD is enabled globally on the local device and the BFD view is displayed.

Configurations relevant to BFD can be performed only after the **bfd** command is run globally.

Step 3 Run:

```
commit
```

The configurations are committed.

----End

2.14.2 Setting BFD Parameters on the Ingress

After setting BFD parameters on the ingress, you can use BFD sessions to detect the TE tunnel.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bfd session-name bind mpls-te interface tunnel interface-number
```

The TE tunnel to be detected by BFD sessions is specified.

When the TE tunnel is in the Down state, a BFD session cannot be established.

Step 3 Run:

```
discriminator local discr-value
```

The local discriminator of the BFD session is configured.

Step 4 Run:

```
discriminator remote discr-value
```

The remote discriminator of the BFD session is configured.

NOTE

The local discriminators and remote discriminators of the two ends on a BFD session must be correctly associated. That is, the local discriminator of the local device and the remote discriminator of the remote device are the same, and the remote discriminator of the local device and the local discriminator of the remote device are the same. Otherwise, the BFD session cannot be correctly set up. In addition, the local and remote discriminators cannot be modified after being successfully configured.

Step 5 (Optional) Run:

```
min-tx-interval interval
```

The minimum interval for the local device to send BFD packets is configured.

By default, the minimum interval for the local device to send BFD packets is 10 ms.

Actual local interval for receiving BFD packets = MAX { Local sending interval, Remote receiving interval }.

Actual local interval for receiving BFD packets = MAX { Remote sending interval, Local receiving interval }.

Local detection period = Local receiving interval x Remote BFD detection multiplier.

For example: assume that the locally-configured interval for sending BFD packets is 200 ms, the interval for receiving BFD packets is 300 ms, the detection multiplier is 4, and the remotely-configured interval for sending BFD packets is 100 ms, the interval for receiving BFD packets is 600 ms, the detection multiplier is 5.

- The actual local interval for sending BFD packets is 600 ms (MAX { 200 ms, 600 ms }), the actual local interval for receiving BFD packets is 300 ms (MAX { 100 ms, 300 ms }), and the detection interval is 1500 ms (300 ms x 5).
- The actual remote interval for sending BFD packets is 300 ms (MAX { 100 ms, 300 ms }), the actual remote interval for receiving BFD packets is 600 ms (MAX { 200 ms, 600 ms}), and the detection interval is 2400 ms (600 ms x 4).

Step 6 (Optional) Run:

```
min-rx-interval interval
```

The minimum interval for the local device to receive BFD packets is configured.

By default, the minimum interval for the local device to receive BFD packets is 10 ms.

Step 7 (Optional) Run:

```
detect-multiplier multiplier
```

The BFD detection multiplier is configured.

Step 8 Run:

```
commit
```

The configurations are committed.

----End

2.14.3 Setting BFD Parameters on the Egress

This section describes how to set BFD parameters on the egress to detect the CR-LSP through BFD sessions.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 The IP link, LSP, or TE tunnel can be used as the reverse tunnel to inform the ingress of a fault. If there is a reverse LSP or a TE tunnel, you need to use the reverse LSP or the TE tunnel; otherwise, you can choose an IP link. If the configured reverse tunnel requires BFD detection, you can configure a pair of BFD sessions for it. Run the following commands as required:

- Run:

  ```
  bfd session-name bind peer-ip ip-address [ vpn-instance vpn-name ] [ source-ip ip-address ]
  ```

  A BFD session with the reverse tunnel being an IP link is established.

- Run:

  ```
  bfd session-name bind ldp-lsp peer-ip ip-address [ nexthop ip-address [ interface interface-type interface-number ] ]
  ```

  A BFD session with the reverse tunnel being an LDP LSP is established.

- Run:

  ```
  bfd session-name bind mpls-te interface tunnel interface-number te-lsp [ backup ]
  ```

  A BFD session with the reverse tunnel being a CR-LSP is established.

- Run:

  ```
  bfd session-name bind mpls-te interface tunnel interface-number
  ```

  A BFD session with the reverse tunnel being a TE tunnel is established.

Step 3 Run:

```
discriminator local discr-value
```

The local discrimitor of the BFD session is configured.

Step 4 Run:

```
discriminator remote discr-value
```

The remote discriminator of the BFD session is configured.

NOTE

The local discriminators and remote discriminators of the two ends on a BFD session must be correctly associated. That is, the local discriminator of the local device and the remote discriminator of the remote device are the same, and the remote discriminator of the local device and the local discriminator of the remote device are the same. Otherwise, the BFD session cannot be correctly set up. In addition, the local and remote discriminators cannot be modified after being successfully configured.

Step 5 (Optional) Run:

min-tx-interval *interval*

The minimum interval for sending BFD packets is configured.

By default, the minimum interval for sending BFD packets is 10 milliseconds.

If the reverse tunnel is an IP link, this parameter is not applicable.

Actual local interval for receiving BFD packets = MAX { Local sending interval, Remote receiving interval }.

Actual local interval for receiving BFD packets = MAX { Remote sending interval, Local receiving interval }.

Local detection period = Local receiving interval x Remote BFD detection multiplier.

For example: assume that the locally-configured interval for sending BFD packets is 200 milliseconds, the interval for receiving BFD packets is 300 milliseconds, the detection multiplier is 4, and the remotely-configured interval for sending BFD packets is 100 milliseconds, the interval for receiving BFD packets is 600 milliseconds, the detection multiplier is 5.

- The actual local interval for sending BFD packets is 600 milliseconds (MAX { 200 milliseconds, 600 milliseconds }), the actual local interval for receiving BFD packets is 300 milliseconds (MAX { 100 milliseconds, 300 milliseconds }), and the detection interval is 1500 milliseconds (300 milliseconds x 5).
- The actual remote interval for sending BFD packets is 300 milliseconds (MAX { 100 milliseconds, 300 milliseconds }), the actual remote interval for receiving BFD packets is 600 milliseconds (MAX { 200 milliseconds, 600 milliseconds}), and the detection interval is 2400 milliseconds (600 milliseconds x 4).

Step 6 (Optional) Run:

min-rx-interval *interval*

The minimum interval for the local device to receive BFD packets is configured.

By default, the minimum interval for the local device to receive BFD packets is 10 milliseconds.

Step 7 (Optional) Run:

detect-multiplier *multiplier*

The BFD detection multiplier is configured.

Step 8 Run:

commit

The configurations are committed.

----End

2.14.4 Checking the Configuration

After static BFD for TE is configured, you can view configurations, such as the status of the BFD sessions.

Prerequisite

All configurations of static BFD for TE are complete.

Procedure

- Run the **display bfd session mpls-te interface** *tunnel-name* [**verbose**] command to view information about the BFD sessions on the ingress.
- Run the following commands to view information about the BFD sessions on the egress.
  - Run the **display bfd session all** [**for-ip** | **for-lsp** | **for-te**] [**verbose**] command, and you can view information about all BFD sessions.
  - Run the **display bfd session static** [**for-ip** | **for-lsp** | **for-te**] [**verbose**] command, and you can view information about static BFD sessions.
  - Run the **display bfd session peer-ip** *peer-ip* [**vpn-instance** *vpn-name*] [**verbose**] command, and you can view information about BFD sessions with the reverse tunnel being the IP link.
  - Run the **display bfd session ldp-lsp peer-ip** *peer-ip* [**interface** *interface-type interface-number*] [**verbose**] command, and you can view information about BFD sessions with the reverse tunnel being the LDP LSP.
  - Run the **display bfd session mpls-te interface** *tunnel-name* **te-lsp** [**verbose**] command, and you can view information about BFD sessions with the reverse tunnel being the CR-LSP.
  - Run the **display bfd session mpls-te interface** *tunnel-name* [**verbose**] command, and you can view information about BFD sessions with the reverse tunnel being the TE tunnel.
- Run the following commands to view BFD statistics.
  - Run the **display bfd statistics session all** [**for-ip** | **for-lsp** | **for-te**] [**verbose**] command, and you can view the statistics on all BFD sessions.
  - Run the **display bfd statistics session static** [**discriminator** *local-discriminator* | **for-ip** | **for-lsp** | **for-te**] [**verbose**] command, and you can view the statistics on static BFD sessions.
  - Run the **display bfd statistics session peer-ip** *peer-ip* **[vpn-instance** *vpn-name*] command, and you can view the statistics on the BFD sessions with the reverse tunnel being an IP link.
  - Run the **display bfd statistics session ldp-lsp peer-ip** *peer-ip* [*interface-type interface-number*] command, and you can view the statistics on the BFD sessions with the reverse tunnel being an LDP LSP.
  - Run the **display bfd statistics session mpls-te interface tunnel** { *tunnel-id* | *tunnel-number* } **te-lsp** command, and you can view the statistics on the BFD sessions with the reverse tunnel being a CR-LSP.

----End

Example

After the configuration is complete, run the **display bfd session** command, and you can find that the BFD session status is Up, and the BFD session type is S_TE_TNL.

```
<HUAWEI> display bfd session discriminator 10
--------------------------------------------------------------------------------
Local  Remote PeerIpAddr        State     Type              InterfaceName
--------------------------------------------------------------------------------
10     20     3.3.3.3           Up        S_TE_TNL          Tunnel1/0/0
--------------------------------------------------------------------------------
```

Run the **display bfd statistics session all** command, and you can view statistics on all BFD sessions.

```
<HUAWEI> display bfd statistics session all
--------------------------------------------------------------------------------
  State : Up                      Name : atob
--------------------------------------------------------------------------------
  Session Type                          : Static
  Bind Type                             : TE_TUNNEL
  Local/Remote Discriminator            : 10/20
  Received Packets                      : 1710577
  Sent Packets                          : 1710593
  Received Bad Packets                  : 0
  Sent Failed Packets                   : 0
  Down Count                            : 0
  ShortBreak Count                      : 0
  Sent Lsp Ping Count                   : 0
  Create Time                           : 2009/09/27 07:20:06
  Last Down Time                        : 0000/00/00 00:00:00
  Total Time From Last DOWN             : -D:--H:--M:--S
  Total Time From Create                : 0D:09H:03M:47S
--------------------------------------------------------------------------------

     Total Session Number :  1
```

2.15 Maintaining MPLS TE

This section describes how to remove MPLS TE information and debug MPLS TE.

2.15.1 Checking Connectivity of a TE Tunnel

The connectivity of a TE tunnel between the ingress and egress is checked.

Context

After configuring an MPLS TE tunnel, you can run the **ping lsp** command on the ingress of the TE tunnel to verify that the ping from the ingress to the egress is successful. If the ping fails, run the **tracert lsp** command to locate the fault.

Procedure

- Run the **ping lsp** [**-a** *source-ip* | **-c** *count* | **-exp** *exp-value* | **-h** *ttl-value* | **-m** *interval* | **-r** *reply-mode* | **-s** *packet-size* | **-t** *time-out* | **-v**] * **te tunnel** *tunnel-number* [**hot-standby**] [**draft6**] command to check connectivity of a TE tunnel from the ingress to the egress.

If **draft6** is configured, the ping operation is implemented in compliance with draft-ietf-mpls-lsp-ping-06. By default, the ping operation is implemented in compliance with RFC 4379. If **hot-standby** is configured, a hot-standby CR-LSP is checked.

- Run the **tracert lsp** [**-a** *source-ip* | **-exp** *exp-value* | **-h** *ttl-value* | **-r** *reply-mode* | **-t** *time-out*] * **te tunnel** *tunnel-number* [**hot-standby**] [**draft6**] command to check the nodes through which data packets pass along a TE tunnel from the ingress to the egress.

  If **draft6** is configured, the tracert operation is implemented in compliance with draft-ietf-mpls-lsp-ping-06. By default, the command is implemented in compliance with RFC 4379. If **hot-standby** is configured, a hot-standby CR-LSP is checked.

----End

2.15.2 Checking a TE Tunnel Using NQA

After configuring MPLS TE, you can use Network Quality Analysis (NQA) to check the connectivity and jitter of a TE tunnel.

Context

For information about configurations for detecting a TE tunnel using NQA, see the chapter "NQA Configuration" in the *HUAWEI NetEngine5000E Core Router Configuration Guide - System Management*.

2.15.3 Checking Tunnel Error Information

If an RSVP-TE tunnel interface is Down, run display commands to view information about faults.

Context

Run the **display mpls te tunnel-interface last-error** command on the ingress to view error information. The following errors may occur:

- CSPF computation failures
- Errors that occur when the RSVP signaling is triggered
- Errors that are carried in the received RSVP PathErr messages

This command shows the last five recorded errors that occur on a TE tunnel.

Procedure

Step 1 Run the **display mpls te tunnel-interface last-error** [*tunnel-name*] command to check error information of a tunnel interface.

----End

2.15.4 Deleting RSVP-TE Statistics

A reset command is used to delete RSVP-TE statistics.

Context

CAUTION

RSVP-TE statistics are deleted if you reset RSVP-TE statistics with the reset command. Exercise caution when running the reset command.

To delete RSVP-TE statistics, run the **reset** command in the user view to delete RSVP-TE statistics.

Procedure

Step 1 Run the **reset mpls rsvp-te statistics** { **global** | **interface** [*interface-type interface-number*] } command in the user view to delete RSVP-TE statistics.

----End

2.15.5 Resetting a Tunnel Interface

Resetting a tunnel interface makes tunnel configurations take effect.

Procedure

Step 1 Run the **reset mpls te tunnel-interface tunnel** *interface-number* command to reset a specified tunnel interface.

----End

2.15.6 Resetting the RSVP Process

Resetting the RSVP process triggers a node to re-establish all RSVP CR-LSPs or verify the RSVP process.

Context

CAUTION

Resetting the RSVP process causes all RSVP CR-LSPs to be torn down and re-established.

Procedure

Step 1 Run the **reset mpls rsvp-te** command in the user view to reset the RSVP process.

----End

2.15.7 Deleting an Automatic Bypass Tunnel and Re-establishing a New One

If MPLS TE Auto FRR is enabled, a command is used to trigger a node to delete an automatic bypass tunnel and re-establish a new one.

Procedure

Step 1 Run the **reset mpls te auto-frr** { **lsp-id** *ingress-lsrid tunnel-id* | **name** *bypass-tunnel-name* } command to delete an automatic bypass tunnel and re-establish a new one.

----End

2.16 Configuration Examples

This section provides MPLS TE configuration examples.

2.16.1 Example for Configuring an RSVP-TE Tunnel

Networking Requirements

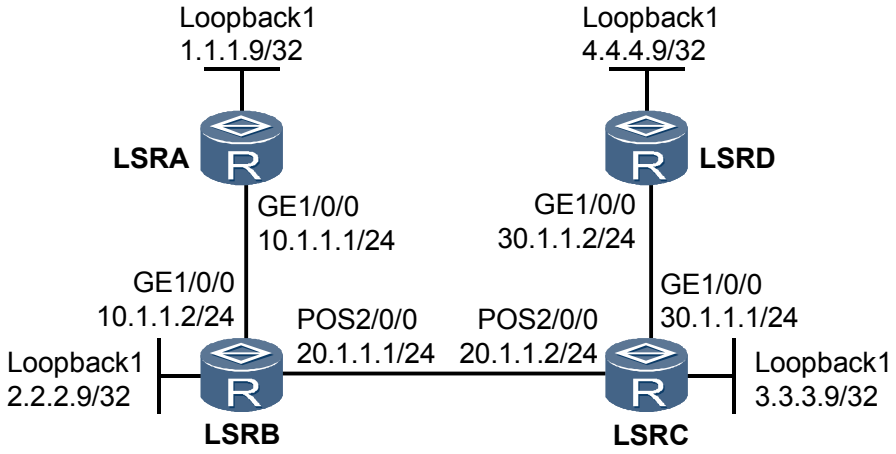
CAUTION

On a single NE5000E, an interface is numbered in the format: slot number/subcard number/interface number. On an NE5000E cluster, an interface is numbered in the format: chassis ID/slot number/subcard number/interface number. The slot number and chassis ID must be specified together.

On a network shown in **Figure 2-11**, IS-IS runs on LSR A, LSR B, LSR C, and LSR D. These nodes are level-2 routers.

RSVP-TE is used to set up a TE tunnel with the bandwidth of 20 Mbit/s from LSR A to LSR D. The maximum reservable bandwidth for every link along the TE tunnel is 100 Mbit/s. The default Russian Dolls Model (RDM) is used, and the BC0 bandwidth is 100 Mbit/s.

Figure 2-11 Networking diagram for an RSVP-TE tunnel



Configuration Notes

None.

Configuration Roadmap

The configuration roadmap is as follows:

1. Assign an IP address and its mask to every interface and configure a loopback interface address as an LSR ID on every node.
2. Enable IS-IS globally; configure network entity name; set the cost type of TE to enable IS-IS TE; enable IS-IS on every interface such as a loopback interface.
3. Set an MPLS LSR ID for every LSR, and enable MPLS, MPLS TE, RSVP-TE, and CSPF globally.
4. Enable MPLS, MPLS TE, and RSVP-TE on every interface.
5. Set the maximum reservable bandwidth and BC bandwidth on an outbound interface of every link along the TE tunnel.
6. Create a tunnel interface on the ingress and configure the source and destination IP addresses for the tunnel, tunnel protocol, destination address, RSVP-TE signaling protocol, and tunnel bandwidth.

Data Preparation

To complete the configuration, you need the following data:

- Origin AS number, and IS IS level and area ID of every LSR
- BC bandwidth and maximum reservable bandwidth on every link along the TE tunnel
- Tunnel interface number, source and destination addresses of, ID, RSVP-TE signaling protocol, and bandwidth of a tunnel

Procedure

Step 1 Assign an IP address and its mask to every interface.

Configure the IP address and its mask for every interface as shown in **Figure 2-11**. The configuration procedure is not provided.

Step 2 Configure IS-IS.

Configure LSR A.

```
[~LSRA] isis 1
[~LSRA-isis-1] network-entity 00.0005.0000.0000.0001.00
[~LSRA-isis-1] is-level level-2
[~LSRA-isis-1] quit
[~LSRA] interface gigabitethernet 1/0/0
[~LSRA-GigabitEthernet1/0/0] isis enable 1
[~LSRA-GigabitEthernet1/0/0] quit
[~LSRA] interface loopback 1
[~LSRA-LoopBack1] isis enable 1
[~LSRA-LoopBack1] commit
[~LSRA-LoopBack1] quit
```

Configure LSR B.

```
[~LSRB] isis 1
[~LSRB-isis-1] network-entity 00.0005.0000.0000.0002.00
[~LSRB-isis-1] is-level level-2
[~LSRB-isis-1] quit
[~LSRB] interface gigabitethernet 1/0/0
[~LSRB-GigabitEthernet1/0/0] isis enable 1
[~LSRB-GigabitEthernet1/0/0] quit
[~LSRB] interface pos 2/0/0
[~LSRB-Pos2/0/0] isis enable 1
[~LSRB-Pos2/0/0] quit
[~LSRB] interface loopback 1
[~LSRB-LoopBack1] isis enable 1
[~LSRB-LoopBack1] commit
[~LSRB-LoopBack1] quit
```

Configure LSR C.

```
[~LSRC] isis 1
[~LSRC-isis-1] network-entity 00.0005.0000.0000.0003.00
[~LSRC-isis-1] is-level level-2
[~LSRC-isis-1] quit
[~LSRC] interface gigabitethernet 1/0/0
[~LSRC-GigabitEthernet1/0/0] isis enable 1
[~LSRC-GigabitEthernet1/0/0] quit
[~LSRC] interface pos 2/0/0
[~LSRC-Pos2/0/0] isis enable 1
[~LSRC-Pos2/0/0] quit
[~LSRC] interface loopback 1
[~LSRC-LoopBack1] isis enable 1
[~LSRC-LoopBack1] commit
[~LSRC-LoopBack1] quit
```

Configure LSR D.

```
[~LSRD] isis 1
[~LSRD-isis-1] network-entity 00.0005.0000.0000.0004.00
[~LSRD-isis-1] is-level level-2
[~LSRD-isis-1] quit
[~LSRD] interface gigabitethernet 1/0/0
[~LSRD-GigabitEthernet1/0/0] isis enable 1
[~LSRD-GigabitEthernet1/0/0] quit
[~LSRD] interface loopback 1
[~LSRD-LoopBack1] isis enable 1
[~LSRD-LoopBack1] commit
[~LSRD-LoopBack1] quit
```

After completing the configurations, run the **display ip routing-table** command on every LSR. All LSRs have learned routes from each other. Use the display on LSR A as an example.

```
[~LSRA] display ip routing-table
Route Flags: R - relay, D - download for forwarding
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 10       Routes : 10
Destination/Mask  Proto  Pre  Cost  Flags   NextHop         Interface
      1.1.1.9/32  Direct 0    0         D   127.0.0.1       InLoopBack0
      2.2.2.9/32  ISIS   15   10        D    10.1.1.2        GigabitEthernet1/0/0
      3.3.3.9/32  ISIS   15   20        D    10.1.1.2        GigabitEthernet1/0/0
      4.4.4.9/32  ISIS   15   30        D    10.1.1.2        GigabitEthernet1/0/0
     10.1.1.0/24  Direct 0    0        D     10.1.1.1        GigabitEthernet1/0/0
     10.1.1.1/32  Direct 0    0        D     127.0.0.1       InLoopBack0
     20.1.1.0/24  ISIS   15   20       D     10.1.1.2        GigabitEthernet1/0/0
     30.1.1.0/24  ISIS   15   30       D     10.1.1.2        GigabitEthernet1/0/0
    127.0.0.0/8   Direct 0    0        D     127.0.0.1       InLoopBack0
    127.0.0.1/32  Direct 0    0        D     127.0.0.1       InLoopBack0
```

Step 3 Configure basic MPLS functions and enable MPLS TE, RSVP-TE, and CSPF.

Enable MPLS, MPLS TE, and RSVP-TE on every LSR and their interfaces along a tunnel, and enable CSPF in the system view of the ingress.

Configure LSR A.

```
[~LSRA] mpls lsr-id 1.1.1.9
[~LSRA] mpls
[~LSRA-mpls] mpls te
[~LSRA-mpls] mpls rsvp-te
[~LSRA-mpls] mpls te cspf
[~LSRA-mpls] quit
[~LSRA] interface gigabitethernet 1/0/0
[~LSRA-GigabitEthernet1/0/0] mpls
[~LSRA-GigabitEthernet1/0/0] mpls te
[~LSRA-GigabitEthernet1/0/0] mpls rsvp-te
[~LSRA-GigabitEthernet1/0/0] commit
[~LSRA-GigabitEthernet1/0/0] quit
```

Configure LSR B.

```
[~LSRB] mpls lsr-id 2.2.2.9
[~LSRB] mpls
[~LSRB-mpls] mpls te
[~LSRB-mpls] mpls rsvp-te
[~LSRB-mpls] quit
[~LSRB] interface gigabitethernet 1/0/0
[~LSRB-GigabitEthernet1/0/0] mpls
[~LSRB-GigabitEthernet1/0/0] mpls te
[~LSRB-GigabitEthernet1/0/0] mpls rsvp-te
[~LSRB-GigabitEthernet1/0/0] quit
[~LSRB] interface pos 2/0/0
[~LSRB-Pos2/0/0] mpls
[~LSRB-Pos2/0/0] mpls te
[~LSRB-Pos2/0/0] mpls rsvp-te
[~LSRB-Pos2/0/0] commit
[~LSRB-Pos2/0/0] quit
```

Configure LSR C.

```
[~LSRC] mpls lsr-id 3.3.3.9
[~LSRC] mpls
[~LSRC-mpls] mpls te
[~LSRC-mpls] mpls rsvp-te
[~LSRC-mpls] quit
[~LSRC] interface gigabitethernet 1/0/0
[~LSRC-GigabitEthernet1/0/0] mpls
[~LSRC-GigabitEthernet1/0/0] mpls te
[~LSRC-GigabitEthernet1/0/0] mpls rsvp-te
[~LSRC-GigabitEthernet1/0/0] quit
[~LSRC] interface pos 2/0/0
[~LSRC-Pos2/0/0] mpls
[~LSRC-Pos2/0/0] mpls te
[~LSRC-Pos2/0/0] mpls rsvp-te
[~LSRC-Pos2/0/0] commit
[~LSRC-Pos2/0/0] quit
```

Configure LSR D.

```
[~LSRD] mpls lsr-id 4.4.4.9
[~LSRD] mpls
[~LSRD-mpls] mpls te
[~LSRD-mpls] mpls rsvp-te
[~LSRD-mpls] quit
[~LSRD] interface gigabitethernet 1/0/0
[~LSRD-GigabitEthernet1/0/0] mpls
[~LSRD-GigabitEthernet1/0/0] mpls te
[~LSRD-GigabitEthernet1/0/0] mpls rsvp-te
[~LSRD-GigabitEthernet1/0/0] commit
[~LSRD-GigabitEthernet1/0/0] quit
```

Step 4 Configure IS-IS TE.

Configure LSR A.

```
[~LSRA] isis 1
[~LSRA-isis-1] cost-style wide
[~LSRA-isis-1] traffic-eng level-2
[~LSRA-isis-1] commit
[~LSRA-isis-1] quit
```

Configure LSR B.

```
[~LSRB] isis 1
[~LSRB-isis-1] cost-style wide
[~LSRB-isis-1] traffic-eng level-2
[~LSRB-isis-1] commit
[~LSRB-isis-1] quit
```

Configure LSR C.

```
[~LSRC] isis 1
[~LSRC-isis-1] cost-style wide
[~LSRC-isis-1] traffic-eng level-2
[~LSRC-isis-1] commit
[~LSRC-isis-1] quit
```

Configure LSR D.

```
[~LSRD] isis 1
[~LSRD-isis-1] cost-style wide
[~LSRD-isis-1] traffic-eng level-2
[~LSRD-isis-1] commit
[~LSRD-isis-1] quit
```

Step 5 Set MPLS TE bandwidth attributes for links.

Set the maximum reservable bandwidth and BC0 bandwidth for a link on every interface along the TE tunnel.

Configure LSR A.

```
[~LSRA] interface gigabitethernet 1/0/0
[~LSRA-GigabitEthernet1/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[~LSRA-GigabitEthernet1/0/0] mpls te bandwidth bc0 100000
[~LSRA-GigabitEthernet1/0/0] commit
[~LSRA-GigabitEthernet1/0/0] quit
```

Configure LSR B.

```
[~LSRB] interface pos 2/0/0
[~LSRB-Pos2/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[~LSRB-Pos2/0/0] mpls te bandwidth bc0 100000
[~LSRB-Pos2/0/0] commit
[~LSRB-Pos2/0/0] quit
```

Configure LSR C.

```
[~LSRC] interface gigabitethernet 1/0/0
[~LSRC-GigabitEthernet1/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[~LSRC-GigabitEthernet1/0/0] mpls te bandwidth bc0 100000
[~LSRC-GigabitEthernet1/0/0] commit
[~LSRC-GigabitEthernet1/0/0] quit
```

Step 6 Configure an MPLS TE tunnel interface.

Create a tunnel interface on the ingress; configure the source and destination IP addresses for the tunnel, tunnel protocol, tunnel ID, and RSVP-TE signaling protocol; run the **commit** command to make the configurations take effect.

Configure LSR A.

```
[~LSRA] interface tunnel 1
[~LSRA-Tunnel1] ip address unnumbered interface loopback 1
```

```
[~LSRA-Tunnel1] tunnel-protocol mpls te
[~LSRA-Tunnel1] destination 4.4.4.9
[~LSRA-Tunnel1] mpls te signal-protocol rsvp-te
[~LSRA-Tunnel1] mpls te bandwidth ct0 20000
[~LSRA-Tunnel1] commit
[~LSRA-Tunnel1] quit
```

Step 7 Verify the configuration.

After completing the preceding configurations, run the **display interface tunnel** command on LSR A. The tunnel interface is **Up**.

```
[~LSRA] display interface tunnel

Tunnel1 current state : Up
Line protocol current state : Up
Last line protocol up time : 2010-09-10 04:09:11
Description: HUAWEI, Tunnel1 Interface (ifindex: 20, vr: 0)
Route Port,The Maximum Transmit Unit is 1500
Internet Address is unnumbered, using address of LoopBack1(1.1.1.9/32)
Encapsulation is TUNNEL, loopback not set
Tunnel protocol is MPLS
Current system time: 2010-09-10 04:09:18
Tunnel destination 4.4.4.9
Tunnel up/down statistics 0

QoS max-bandwidth : 0 Kbps
Output queue : (Urgent queue : Size/Length/Discards)  0/0/0
Output queue : (Protocol queue : Size/Length/Discards) 0/0/0
Output queue : (FIFO queue : Size/Length/Discards)  0/0/0
    300 seconds output rate 0 bits/sec, 0 packets/sec
    48 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets output,  0 bytes
    0 output error
    0 output drop
    ct0:0 packets output,  0 bytes
        0 output error
    Last 300 seconds input utility rate:  0.00%
    Last 300 seconds output utility rate: 0.00%
```

Run the **display mpls te tunnel-interface** command on LSR A. Detailed information about the tunnel interface is displayed.

```
[~LSRA] display mpls te tunnel-interface tunnel1

    Tunnel Name       : Tunnel1
    Tunnel State Desc : CR-LSP is Up
    Tunnel Attributes   :
    Session ID          : 1
    Ingress LSR ID      : 1.1.1.9              Egress LSR ID: 4.4.4.9
    Admin State         : UP                   Oper State   : UP
    Signaling Protocol  : RSVP
    FTid                : 1
    Tie-Breaking Policy : None                 Metric Type  : None
    BypassBW Flag       : Not Supported
    BypassBW Type       : -                    Bypass BW    : -
    Bfd Cap             : None                 Retry Int    : -
    Reopt               : Disabled             Reopt Freq   : -
    Auto BW             : Disabled
    Current Collected BW: -                    Auto BW Freq : -
    Min BW              : -                    Max BW       : -
    Tunnel Group        : -
    Interfaces Protected: -
    Excluded IP Address : -
    Is On Radix-Tree    : -                    Referred LSP Count: -
    Primary Tunnel      : -                    Pri Tunn Sum : -
    Backup Tunnel       : -
    Group Status        : -                    Oam Status   : -
    IPTN InLabel        : -
```

```
BackUp Type         : None                  BestEffort   : Disabled
SRLG Disjoining       : NA
Secondary HopLimit  : -
BestEffort HopLimit : -
Secondary Explicit Path Name: -
Secondary Affinity Prop/Mask: -
BestEffort Affinity Prop/Mask: 0x0/0x0
IsConfigLspConstraint: -

Primary LSP ID      : 1.1.1.9:1
Setup Priority      : 7                     Hold Priority: 7
IncludeAll          : 0x0
IncludeAny          : 0x0
ExcludeAny          : 0x0
Affinity Prop/Mask  : 0x0/0x0               Resv Style   :  SE
Configured Bandwidth Information:
CT0 Bandwidth(Kbit/sec): 20000          CT1 Bandwidth(Kbit/sec): 0
CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
Actual Bandwidth Information:
CT0 Bandwidth(Kbit/sec): 20000          CT1 Bandwidth(Kbit/sec): 0
CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
Explicit Path Name  : -                    Hop Limit           : -
Record Route        : Disabled             Record Label : Disabled
Route Pinning       : Disabled
FRR Flag            : Disabled
IdleTime Remain     : -
BFD Status          : -
```

Run the **display mpls te cspf tedb all** command on LSR A. Link information in the TEDB is displayed.

```
[~LSRA] display mpls te cspf tedb all

Maximum Nodes Supported: 2000     Current Total Node Number: 4
Maximum Links Supported: 8000     Current Total Link Number: 6
Maximum SRLGs supported: 10000    Current Total SRLG Number: 0

Id      Router-Id       IGP       Process-Id      Area             Link-Count
1       1.1.1.9         ISIS      1               Level-2          1
2       2.2.2.9         ISIS      1               Level-2          2
3       3.3.3.9         ISIS      1               Level-2          2
4       4.4.4.9         ISIS      1               Level-2          1
```

----End

Configuration Files

- Configuration file of LSR A

```
#
sysname LSRA
#
mpls lsr-id 1.1.1.9
#
mpls
 mpls te
 mpls te cspf
 mpls rsvp-te
#
te-class-mapping
#
isis 1
 is-level level-2
 cost-style wide
 traffic-eng level-2
```

```
 network-entity 00.0005.0000.0000.0001.00
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
 isis enable 1
#
interface Tunnel1
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 4.4.4.9
 mpls te bandwidth ct0 20000
#
return
```

- Configuration file of LSR B

```
#
 sysname LSRB
#
 mpls lsr-id 2.2.2.9
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
#
isis 1
 is-level level-2
 cost-style wide
 traffic-eng level-2
 network-entity 00.0005.0000.0000.0002.00
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls te
 isis enable 1
 mpls rsvp-te
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 20.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of LSR C

```
#
 sysname LSRC
```

```
#
 mpls lsr-id 3.3.3.9
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
#
isis 1
 is-level level-2
 cost-style wide
 traffic-eng level-2
 network-entity 00.0005.0000.0000.0003.00
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 30.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 isis enable 1
 mpls rsvp-te
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 20.1.1.2 255.255.255.0
 mpls
 mpls te
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of LSR D

```
#
 sysname LSRD
#
 mpls lsr-id 4.4.4.9
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
#
isis 1
 is-level level-2
 cost-style wide
 traffic-eng level-2
 network-entity 00.0005.0000.0000.0004.00
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 30.1.1.2 255.255.255.0
 mpls
 mpls te
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 4.4.4.9 255.255.255.255
 isis enable 1
#
```

```
return
```

2.16.2 Example for Configuring RSVP Authentication

Networking Requirements

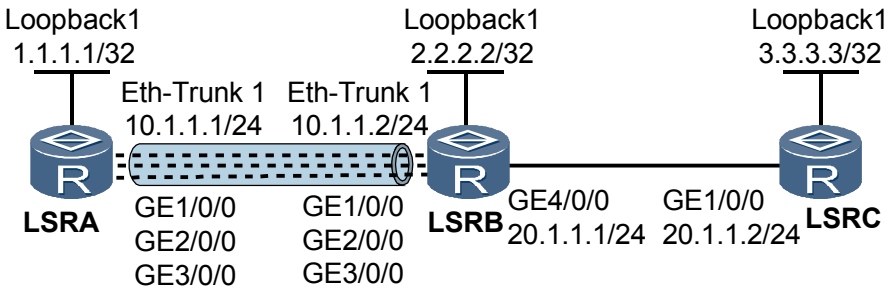
CAUTION

On a single NE5000E, an interface is numbered in the format: slot number/subcard number/interface number. On an NE5000E cluster, an interface is numbered in the format: chassis ID/slot number/subcard number/interface number. The slot number and chassis ID must be specified together.

On a network shown in **Figure 2-12**, GE 1/0/0, GE 2/0/0, and GE 3/0/0 on LSR A and LSR B join Eth-Trunk1. An MPLS TE tunnel is set up from LSR A to LSR C.

The handshake function, RSVP key authentication, and message window are configured for LSR A and LSR B. The handshake function allows LSR A and LSR B to perform RSVP key authentication. RSVP key authentication prevents forged packets from requesting network resource usage. The message window function prevents RSVP message mis-sequence.

Figure 2-12 Networking diagram for RSVP authentication



Configuration Notes

None.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure MPLS and establish an MPLS TE tunnel.
2. Configure RSVP authentication on the interfaces.
3. Configure the handshake function on the interfaces.
4. Set the size for the message window, allowing interfaces to store 32 sequence numbers.

NOTE

Setting the window size to 32 is recommended. If the window size is too small, received RSVP messages beyond the window are discarded, terminating RSVP neighbor relationships.

Data Preparation

To complete the configuration, you need the following data:

- OSPF process ID and area ID for every LSR
- Password and key for RSVP authentication
- RSVP message window size

Procedure

Step 1 Assign an IP address and its mask to every interface.

Assign an IP address and its mask to every interface as shown in **Figure 2-12**. Detailed configuration information is provided in the following configuration files.

Step 2 Configure OSPF.

Configure OSPF to advertise every network segment route and host route. Detailed configuration information is provided in the following configuration files.

After completing the configurations, run the **display ip routing-table** command on every node. All nodes have learned routes from each other.

Step 3 Configure basic MPLS functions, and enable MPLS TE, RSVP-TE, and CSPF.

Configure LSR A.

```
[~LSRA] mpls lsr-id 1.1.1.1
[~LSRA] mpls
[~LSRA-mpls] mpls te
[~LSRA-mpls] mpls rsvp-te
[~LSRA-mpls] mpls te cspf
[~LSRA-mpls] quit
[~LSRA] interface eth-trunk 1
[~LSRA-Eth-Trunk1] mpls
[~LSRA-Eth-Trunk1] mpls te
[~LSRA-Eth-Trunk1] mpls rsvp-te
[~LSRA-Eth-Trunk1] commit
[~LSRA-Eth-Trunk1] quit
```

NOTE

Configurations on LSR B and LSR C are similar to those on LSR A. The configuration procedure is not provided.

Step 4 Configure OSPF TE.

Configure LSR A.

```
[~LSRA] ospf 1
[~LSRA-ospf-1] opaque-capability enable
[~LSRA-ospf-1] area 0
[~LSRA-ospf-1-area-0.0.0.0] mpls-te enable
[~LSRA-ospf-1-area-0.0.0.0] commit
[~LSRA-ospf-1-area-0.0.0.0] quit
```

Configure LSR B.

```
[~LSRB] ospf 1
```

```
[~LSRB-ospf-1] opaque-capability enable
[~LSRB-ospf-1] area 0
[~LSRB-ospf-1-area-0.0.0.0] mpls-te enable
[~LSRB-ospf-1-area-0.0.0.0] commit
[~LSRB-ospf-1-area-0.0.0.0] quit
```

Configure LSR C.

```
[~LSRC] ospf 1
[~LSRC-ospf-1] opaque-capability enable
[~LSRC-ospf-1] area 0
[~LSRC-ospf-1-area-0.0.0.0] mpls-te enable
[~LSRC-ospf-1-area-0.0.0.0] commit
[~LSRC-ospf-1-area-0.0.0.0] quit
```

Step 5 Configure an MPLS RSVP-TE tunnel.

Configure the MPLS TE tunnel on LSR A.

```
[~LSRA] interface tunnel 1
[~LSRA-Tunnel1] ip address unnumbered interface loopback 1
[~LSRA-Tunnel1] tunnel-protocol mpls te
[~LSRA-Tunnel1] destination 3.3.3.3
[~LSRA-Tunnel1] mpls te signal-protocol rsvp-te
[~LSRA-Tunnel1] commit
[~LSRA-Tunnel1] quit
```

After completing the configuration, run the **display interface tunnel** command on LSR A. The tunnel interface is **Up**.

```
[~LSRA] display interface tunnel1

Tunnel1 current state : Up
Line protocol current state : Up
Last line protocol up time : 2010-10-13 07:21:27
Description: HUAWEI, Tunnel1 Interface (ifindex: 19, vr: 0)
Route Port,The Maximum Transmit Unit is 1500
Internet Address is unnumbered, using address of LoopBack1(1.1.1.1/32)
Encapsulation is TUNNEL, loopback not set
Tunnel protocol is MPLS
Current system time: 2010-10-15 02:01:51
Tunnel destination 3.3.3.3
Tunnel up/down statistics 0

QoS max-bandwidth : 0 Kbps
Output queue : (Urgent queue : Size/Length/Discards)  0/0/0
Output queue : (Protocol queue : Size/Length/Discards) 0/0/0
Output queue : (FIFO queue : Size/Length/Discards)  0/0/0
    300 seconds output rate 0 bits/sec, 0 packets/sec
    48 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets output,  0 bytes
    0 output error
    0 output drop
    ct0:0 packets output,  0 bytes
        0 output error
    Last 300 seconds input utility rate:  0.00%
    Last 300 seconds output utility rate: 0.00%
```

Step 6 Configure RSVP authentication on MPLS TE interfaces of LSR A and LSR B.

Configure LSR A.

```
[~LSRA] interface eth-trunk 1
[~LSRA-Eth-Trunk1] mpls rsvp-te authentication cipher 123456789
[~LSRA-Eth-Trunk1] mpls rsvp-te authentication handshake 12345678
[~LSRA-Eth-Trunk1] mpls rsvp-te authentication window-size 32
[~LSRA-Eth-Trunk1] commit
```

Configure LSR B.

```
[~LSRB] interface eth-trunk 1
[~LSRB-Eth-Trunk1] mpls rsvp-te authentication cipher  123456789
[~LSRB-Eth-Trunk1] mpls rsvp-te authentication handshake 12345678
[~LSRB-Eth-Trunk1] mpls rsvp-te authentication window-size 32
[~LSRB-Eth-Trunk1] commit
```

Step 7 Verify the configuration.

Run the **reset mpls rsvp-te** and **display interface tunnel** commands in sequence on LSR A. The tunnel interface is **Up**.

Run the **display mpls rsvp-te interface** command on LSR A or LSR B. RSVP authentication information is displayed.

```
[~LSRA] display mpls rsvp-te interface eth-trunk 1
Interface: Eth-Trunk1
 Interface Address: 10.1.1.1
 Interface state: Up                        Interface Index: 0x5
 Total-BW: 0                                Used-BW: 0
 Hello configured: NO                       Num of Neighbors: 1
 SRefresh feature: DISABLE                  SRefresh Interval: 30 sec
 Mpls Mtu: 1500                             Retransmit Interval: 500 msec
 Increment Value: 1                         Authentication: ENABLE
 Bfd Enabled: --                            Bfd Min-Tx: --
 Bfd Min-Rx: --                             Bfd Detect-Multi: --
 RSVP instance name: RSVP0
```

----End

Configuration Files

- Configuration file of LSR A

```
#
 sysname LSRA
#
 mpls lsr-id 1.1.1.1
#
 mpls
  mpls te
  mpls te cspf
  mpls rsvp-te
#
interface Eth-Trunk1
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
 mpls rsvp-te authentication cipher O'W3[_\M"`!./a!1$H@GYA!!
 mpls rsvp-te authentication handshake 12345678
 mpls rsvp-te authentication window-size 32
#
interface GigabitEthernet1/0/0
 undo shutdown
 eth-trunk 1
#
interface GigabitEthernet2/0/0
 undo shutdown
 eth-trunk 1
#
interface GigabitEthernet3/0/0
 undo shutdown
 eth-trunk 1
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
interface Tunnel1
 ip address unnumbered interface LoopBack1
```

```
 tunnel-protocol mpls te
 destination 3.3.3.3
#
te-class-mapping
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  mpls-te enable
  network 1.1.1.1 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
return
```

- Configuration file of LSR B

```
#
 sysname LSRB
#
 mpls lsr-id 2.2.2.2
#
 mpls
  mpls te
  mpls rsvp-te
#
interface Eth-Trunk1
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
 mpls rsvp-te authentication cipher O'W3[_\M"`!./a!1$H@GYA!!
 mpls rsvp-te authentication handshake 12345678
 mpls rsvp-te authentication window-size 32
#
interface GigabitEthernet1/0/0
 undo shutdown
 eth-trunk 1
#
interface GigabitEthernet2/0/0
 undo shutdown
 eth-trunk 1
#
interface GigabitEthernet3/0/0
 undo shutdown
 eth-trunk 1
#
interface GigabitEthernet4/0/0
 undo shutdown
 ip address 20.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
te-class-mapping
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  mpls-te enable
  network 2.2.2.2 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
#
return
```

- Configuration file of LSR C

```
#
 sysname LSRC
```

```
#
 mpls lsr-id 3.3.3.3
#
 mpls
  mpls te
  mpls rsvp-te
#
interface GigabiEthernet1/0/0
 undo shutdown
 ip address 20.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
te-class-mapping
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  mpls-te enable
  network 3.3.3.3 0.0.0.0
  network 20.1.1.0 0.0.0.255
#
return
```

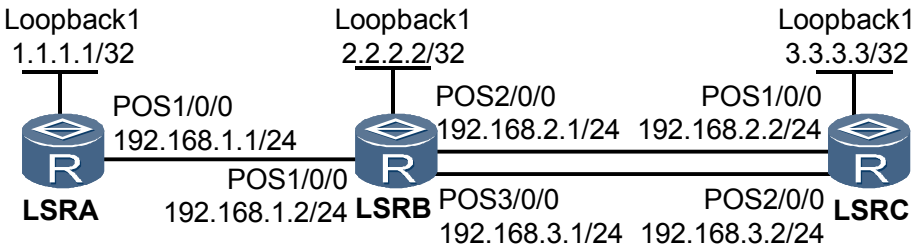
2.16.3 Example for Configuring the Affinity Property of an MPLS TE Tunnel

Networking Requirements

CAUTION

On a single NE5000E, an interface is numbered in the format: slot number/subcard number/interface number. On an NE5000E cluster, an interface is numbered in the format: chassis ID/slot number/subcard number/interface number. The slot number and chassis ID must be specified together.

Figure 2-13 Networking diagram for an MPLS TE tunnel with the affinity property



On the network shown in **Figure 2-13**, the maximum reservable bandwidth for every link is 100 Mbit/s, the RDM is used, and the BC0 bandwidth is 100 Mbit/s.

Two tunnels named Tunnel1 and Tunnel2 from LSR A to LSR C are established on LSR A. Both tunnels require 40 Mbit/s of bandwidth. The combined bandwidth of these two tunnels is 80 Mbit/s, larger than the bandwidth of 50 Mbit/s provided by the shared link from LSR A to LSR B. In addition, Tunnel2 has a higher priority than Tunnel1, and preemption is enabled.

In this example, SRLG attributes, affinity properties and masks for links are used to allow Tunnel1 and Tunnel2 on LSR A to use separate links from LSR B to LSR C.

Configuration Notes

None.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an RSVP-TE tunnel. See "Configuration Roadmap" in **Example for Configuring an RSVP-TE Tunnel**.
2. Configure an SRLG attribute on an outbound interface of every LSR along each RSVP TE tunnel.
3. Configure the affinity property and mask for each tunnel based on the administrative group attributes of links and networking requirements.
4. Set a priority value for each tunnel.

Data Preparation

To complete the configuration, you need the following data:

- OSPF process ID and area ID for every LSR
- Maximum reservable bandwidth and BFD bandwidth for every link along each tunnel
- Administrative group attributes for links from LSR A to LSR B and from LSR B to LSR C
- Affinity property and mask for each tunnel
- Tunnel interface number, source and destination IP addresses, bandwidth, priority values, and RSVP-TE signaling protocol of the tunnel

Procedure

Step 1 Assign an IP address and its mask to every interface.

Assign an IP address and its mask to every physical interface and configure a loopback interface address as an LSR ID on every node shown in **Figure 2-13**.

The configuration procedure is not provided.

Step 2 Configure an IGP.

Configure OSPF on every LSR to advertise every network segment route and host route.

The configuration procedure is not provided.

Step 3 Configure basic MPLS functions, enable MPLS TE, RSVP-TE, and OSPF TE on every LSR, and enable CSPF on the ingress.

Configure basic MPLS functions and enable MPLS TE and RSVP-TE on every LSR.

The configurations on LSR A are as follows:

```
[~LSRA] mpls lsr-id 1.1.1.1
[~LSRA] mpls
[~LSRA-mpls] mpls te
[~LSRA-mpls] mpls rsvp-te
[~LSRA-mpls] quit
[~LSRA] interface pos 1/0/0
[~LSRA-Pos1/0/0] mpls
[~LSRA-Pos1/0/0] mpls te
[~LSRA-Pos1/0/0] mpls rsvp-te
[~LSRA-Pos1/0/0] quit
```

Enable OSPF TE on every LSR. The configurations on LSR A are as follows:

```
[~LSRA] ospf
[~LSRA-ospf-1] opaque-capability enable
[~LSRA-ospf-1] area 0
[~LSRA-ospf-1-area-0.0.0.0] mpls-te enable
[~LSRA-ospf-1-area-0.0.0.0] quit
[~LSRA-ospf-1]  quit
```

The configurations on LSR B and LSR C are similar to those on LSR A. The configuration procedure is not provided.

Enable CSPF on the ingress LSR A.

```
[~LSRA]  mpls
[~LSRA-mpls] mpls te cspf
[~LSRA-mpls] commit
[~LSRA-mpls] quit
```

Step 4 Configure MPLS TE attributes on the outbound interface of every LSR.

Set the maximum reservable link bandwidth and BC0 bandwidth to 100 Mbit/s on LSR A.

```
[~LSRA] interface pos 1/0/0
[~LSRA-Pos1/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[~LSRA-Pos1/0/0] mpls te bandwidth bc0 100000
```

Se the administrative group attribute to 0x10001 on LSR A.

```
[~LSRA-Pos1/0/0] mpls te link administrative group 10001
[~LSRA-Pos1/0/0] commit
[~LSRA-Pos1/0/0] quit
```

Configure MPLS TE attributes on LSR B.

```
[~LSRB] interface pos 2/0/0
[~LSRB-Pos2/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[~LSRB-Pos2/0/0] mpls te bandwidth bc0 100000
[~LSRB-Pos2/0/0] mpls te link administrative group 10101
[~LSRB-Pos2/0/0] quit
[~LSRB] interface pos 3/0/0
[~LSRB-Pos3/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[~LSRB-Pos3/0/0] mpls te bandwidth bc0 100000
[~LSRB-Pos3/0/0] mpls te link administrative group 10011
[~LSRB-Pos3/0/0] commit
[~LSRB-Pos3/0/0] quit
```

After completing the configurations, run the **display mpls te cspf tedb node** command on LSR A. TEDB information displays maximum available and reservable bandwidth for every link, and the administrative group attribute in the **Color** field.

```
[~LSRA] display mpls te cspf tedb node

Router ID:  1.1.1.1
  IGP Type:  OSPF       Process Id:  1       IGP Area: 0
  MPLS-TE Link Count:  1
```

```
  Link[1]:
   OSPF Router Id:  1.1.1.1      Opaque LSA ID: 1.0.0.1
   Interface IP Address:  192.168.1.1
   DR Address:  192.168.1.1
   IGP Area:  0
   Link Type:  Multi-access   Link Status:  Active
   IGP Metric:  -     TE Metric:  1    Color:  0x10001
   Bandwidth Allocation Model :  Russian Dolls Model
   Maximum Link-Bandwidth:  100000  (kbps)
   Maximum Reservable Bandwidth:  100000  (kbps)
   Operational Mode of Router :  TE
   Bandwidth Constraints:          Local Overbooking Multiplier:
       BC[0]:     100000     (kbps)           LOM[0]:          1
   BW  Unreserved :
         Class  Id:
         [0]:     100000     (kbps),  [1]:      100000     (kbps)
         [2]:     100000     (kbps),  [3]:      100000     (kbps)
         [4]:     100000     (kbps),  [5]:      100000     (kbps)
         [6]:     100000     (kbps),  [7]:      100000     (kbps)
Router ID:  2.2.2.2
  IGP Type:  OSPF       Process Id:  1       IGP Area: 0
  MPLS-TE Link Count:  3
  Link[1]:
   OSPF Router Id:  2.2.2.2      Opaque LSA ID: 1.0.0.1
   Interface IP Address:  192.168.1.2
   DR Address:  192.168.1.1
   IGP Area:  0
   Link Type:  Multi-access   Link Status:  Active
   IGP Metric:  -     TE Metric:  1    Color:  0x0
   Bandwidth Allocation Model :  Russian Dolls Model
   Maximum Link-Bandwidth:  0  (kbps)
   Maximum Reservable Bandwidth:  0  (kbps)
   Operational Mode of Router :  TE
   Bandwidth Constraints:          Local Overbooking Multiplier:
       BC[0]:     0          (kbps)           LOM[0]:          1
   BW  Unreserved :
         Class  Id:
         [0]:     0          (kbps),  [1]:      0          (kbps)
         [2]:     0          (kbps),  [3]:      0          (kbps)
         [4]:     0          (kbps),  [5]:      0          (kbps)
         [6]:     0          (kbps),  [7]:      0          (kbps)
  Link[2]:
   OSPF Router Id:  2.2.2.2      Opaque LSA ID: 1.0.0.2
   Interface IP Address:  192.168.2.1
   DR Address:  192.168.2.1
   IGP Area:  0
   Link Type:  Multi-access   Link Status:  Active
   IGP Metric:  -     TE Metric:  1    Color:  0x10101
   Bandwidth Allocation Model :  Russian Dolls Model
   Maximum Link-Bandwidth:  100000  (kbps)
   Maximum Reservable Bandwidth:  100000  (kbps)
   Operational Mode of Router :  TE
   Bandwidth Constraints:          Local Overbooking Multiplier:
       BC[0]:     100000     (kbps)           LOM[0]:          1
   BW  Unreserved :
         Class  Id:
         [0]:     100000     (kbps),  [1]:      100000     (kbps)
         [2]:     100000     (kbps),  [3]:      100000     (kbps)
         [4]:     100000     (kbps),  [5]:      100000     (kbps)
         [6]:     100000     (kbps),  [7]:      100000     (kbps)
  Link[3]:
    OSPF Router ID:  2.2.2.2      Opaque LSA ID:  1.0.0.3
    Interface IP Address:  192.168.3.1
    DR Address:  192.168.3.1
    IGP Area:  0
    Link Type:  Multi-access   Link Status:  Active
    IGP Metric:  1     TE Metric:  1    Color:  0x10011
    Bandwidth Allocation Model :  Russian Dolls Model
    Maximum Link-Bandwidth:  100000  (kbps)
```

```
    Maximum Reservable Bandwidth:  100000  (kbps)
    Operational Mode of Router :  TE
    Bandwidth Constraints:          Local Overbooking Multiplier:
       BC[0]:     100000     (kbps)           LOM[0]:          1
    BW  Unreserved :
         Class  Id:
         [0]:     100000     (kbps),  [1]:      100000     (kbps)
         [2]:     100000     (kbps),  [3]:      100000     (kbps)
         [4]:     100000     (kbps),  [5]:      100000     (kbps)
         [6]:     100000     (kbps),  [7]:      100000     (kbps)
Router ID:  3.3.3.3
  IGP Type:  OSPF       Process Id:  1       IGP Area: 0
  MPLS-TE Link Count:  2
  Link[1]:
   OSPF Router Id:  3.3.3.3       Opaque LSA ID: 1.0.0.1
   Interface IP Address:  192.168.2.2
   DR Address:  192.168.2.1
   IGP Area:  0
   Link Type:  Multi-access   Link Status:  Active
   IGP Metric:  -     TE Metric:  1    Color:  0x0
   Bandwidth Allocation Model :  Russian Dolls Model
   Maximum Link-Bandwidth:  0  (kbps)
   Maximum Reservable Bandwidth:  0  (kbps)
   Operational Mode of Router :  TE
   Bandwidth Constraints:          Local Overbooking Multiplier:
       BC[0]:     0          (kbps)           LOM[0]:          1
   BW  Unreserved :
         Class  Id:
         [0]:     0          (kbps),  [1]:      0          (kbps)
         [2]:     0          (kbps),  [3]:      0          (kbps)
         [4]:     0          (kbps),  [5]:      0          (kbps)
         [6]:     0          (kbps),  [7]:      0          (kbps)
  Link[2]:
    OSPF Router ID:  3.3.3.3       Opaque LSA ID:  1.0.0.2
    Interface IP Address:  192.168.3.2
    DR Address:  192.168.3.1
    IGP Area:  0
    Link Type:  Multi-access   Link Status:  Active
    IGP Metric:  1     TE Metric:  1    Color:  0x0
    Bandwidth Allocation Model :  Russian Dolls Model
    Maximum Link-Bandwidth:  0  (kbps)
    Maximum Reservable Bandwidth:  0  (kbps)
    Operational Mode of Router :  TE
    Bandwidth Constraints:          Local Overbooking Multiplier:
       BC[0]:     0          (kbps)           LOM[0]:          1
    BW  Unreserved :
         Class  Id:
         [0]:     0          (kbps),  [1]:      0          (kbps)
         [2]:     0          (kbps),  [3]:      0          (kbps)
         [4]:     0          (kbps),  [5]:      0          (kbps)
         [6]:     0          (kbps),  [7]:      0          (kbps)
```

Step 5 Configure an MPLS TE tunnel.

Configure a tunnel named **Tunnel1** on LSR A.

```
[~LSRA] interface tunnel 1
[~LSRA-Tunnel1] ip address unnumbered interface loopback 1
[~LSRA-Tunnel1] tunnel-protocol mpls te
[~LSRA-Tunnel1] destination 3.3.3.3
[~LSRA-Tunnel1] mpls te bandwidth ct0 40000
[~LSRA-Tunnel1] mpls te affinity property 10101 mask 11011
[~LSRA-Tunnel1] commit
[~LSRA-Tunnel1] quit
```

The default setup and holding priorities with the lowest priority value of 7 are used.

The affinity property is set to 0x10101 and the mask is set to 0x11011. The affinity property matches the administrative group attribute of every link.

After completing the configurations, run the **display mpls te tunnel-interface** command on LSR A. The tunnel status is displayed.

```
[~LSRA] display mpls te tunnel-interface

    Tunnel Name       : Tunnel1
    Tunnel State Desc : CR-LSP is Up
    Tunnel Attributes   :
    Session ID          : 1
    Ingress LSR ID      : 1.1.1.1              Egress LSR ID: 3.3.3.3
    Admin State         : UP                   Oper State   : UP
    Signaling Protocol  : RSVP
    FTid                : 1
    Tie-Breaking Policy : None                 Metric Type  : None
    BypassBW Flag       : Not Supported
    BypassBW Type       : -                    Bypass BW    : -
    Bfd Cap             : None                 Retry Int    : -
    Reopt               : Disabled             Reopt Freq   : -
    Auto BW             : Disabled
    Current Collected BW: -                    Auto BW Freq : -
    Min BW              : -                    Max BW       : -
    Tunnel Group        : -
    Interfaces Protected: -
    Excluded IP Address : -
    Is On Radix-Tree    : -                    Referred LSP Count: -
    Primary Tunnel      : -                    Pri Tunn Sum : -
    Backup Tunnel       : -
    Group Status        : -                    Oam Status   : -
    IPTN InLabel        : -
    BackUp Type         : None                 BestEffort   : Disabled
    SRLG Disjoining       : NA
    Secondary HopLimit  : -
    BestEffort HopLimit : -
    Secondary Explicit Path Name: -
    Secondary Affinity Prop/Mask: -
    BestEffort Affinity Prop/Mask: 0x0/0x0
    IsConfigLspConstraint: -

    Primary LSP ID      : 1.1.1.1:3
    Setup Priority      : 7                    Hold Priority: 7
    IncludeAll          : 0x0
    IncludeAny          : 0x10001
    ExcludeAny          : 0x1010
    Affinity Prop/Mask  : 0x0/0x0              Resv Style   :  SE
    Configured Bandwidth Information:
    CT0 Bandwidth(Kbit/sec): 40000          CT1 Bandwidth(Kbit/sec): 0
    CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
    CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
    CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
    Actual Bandwidth Information:
    CT0 Bandwidth(Kbit/sec): 40000          CT1 Bandwidth(Kbit/sec): 0
    CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
    CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
    CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
    Explicit Path Name  : main                 Hop Limit           : -
    Record Route        : Disabled             Record Label : Disabled
    Route Pinning       : Disabled
    FRR Flag            : Disabled
    IdleTime Remain     : -
    BFD Status          : -
```

Run the **display mpls te cspf tedb node** command on LSR A. TEDB information shows bandwidth for every link.

```
[~LSRA] display mpls te cspf tedb node

Router ID:  1.1.1.1
  IGP Type:  OSPF       Process Id:  1       IGP Area: 0
  MPLS-TE Link Count:  1
```

```
  Link[1]:
   OSPF Router Id:  30.1.1.1      Opaque LSA ID: 1.0.0.1
   Interface IP Address:  192.168.1.1
   DR Address:  192.168.1.1
   IGP Area:  0
   Link Type:  Multi-access   Link Status:  Active
   IGP Metric:  1     TE Metric:  1    Color:  0x10001
   Bandwidth Allocation Model :  Russian Dolls Model
   Maximum Link-Bandwidth:  100000  (kbps)
   Maximum Reservable Bandwidth:  100000  (kbps)
   Operational Mode of Router :  TE
   Bandwidth Constraints:          Local Overbooking Multiplier:
       BC[0]:     100000     (kbps)           LOM[0]:          1
   BW  Unreserved :
         Class  Id:
         [0]:     100000     (kbps),  [1]:      100000     (kbps)
         [2]:     100000     (kbps),  [3]:      100000     (kbps)
         [4]:     100000     (kbps),  [5]:      100000     (kbps)
         [6]:     100000     (kbps),  [7]:      60000      (kbps)
Router ID:  2.2.2.2
  IGP Type:  OSPF       Process Id:  1       IGP Area: 0
  MPLS-TE Link Count:  3
  Link[1]:
   OSPF Router Id:  50.1.1.1      Opaque LSA ID: 1.0.0.1
   Interface IP Address:  192.168.1.2
   DR Address:  192.168.1.1
   IGP Area:  0
   Link Type:  Multi-access   Link Status:  Active
   IGP Metric:  1     TE Metric:  1    Color:  0x0
   Bandwidth Allocation Model :  Russian Dolls Model
   Maximum Link-Bandwidth:  0  (kbps)
   Maximum Reservable Bandwidth:  0  (kbps)
   Operational Mode of Router :  TE
   Bandwidth Constraints:          Local Overbooking Multiplier:
       BC[0]:     0          (kbps)           LOM[0]:          1
   BW  Unreserved :
         Class  Id:
         [0]:     0          (kbps),  [1]:      0          (kbps)
         [2]:     0          (kbps),  [3]:      0          (kbps)
         [4]:     0          (kbps),  [5]:      0          (kbps)
         [6]:     0          (kbps),  [7]:      0          (kbps)
  Link[2]:
   OSPF Router Id:  50.1.1.1      Opaque LSA ID: 1.0.0.2
   Interface IP Address:  192.168.2.1
   DR Address:  192.168.2.1
   IGP Area:  0
   Link Type:  Multi-access   Link Status:  Active
   IGP Metric:  1     TE Metric:  1    Color:  0x10101
   Bandwidth Allocation Model :  Russian Dolls Model
   Maximum Link-Bandwidth:  100000  (kbps)
   Maximum Reservable Bandwidth:  100000  (kbps)
   Operational Mode of Router :  TE
   Bandwidth Constraints:          Local Overbooking Multiplier:
       BC[0]:     100000     (kbps)           LOM[0]:          1
   BW  Unreserved :
         Class  Id:
         [0]:     100000     (kbps),  [1]:      100000     (kbps)
         [2]:     100000     (kbps),  [3]:      100000     (kbps)
         [4]:     100000     (kbps),  [5]:      100000     (kbps)
         [6]:     100000     (kbps),  [7]:      60000      (kbps)
  Link[3]:
   OSPF Router Id:  50.1.1.1      Opaque LSA ID: 1.0.0.3
   Interface IP Address:  192.168.3.1
   DR Address:  192.168.3.1
   IGP Area:  0
   Link Type:  Multi-access   Link Status:  Active
   IGP Metric:  1     TE Metric:  1    Color:  0x10011
   Bandwidth Allocation Model :  Russian Dolls Model
   Maximum Link-Bandwidth:  100000  (kbps)
```

```
    Maximum Reservable Bandwidth:  100000  (kbps)
    Operational Mode of Router :  TE
    Bandwidth Constraints:          Local Overbooking Multiplier:
        BC[0]:     100000     (kbps)           LOM[0]:          1
    BW  Unreserved :
          Class  Id:
          [0]:     100000     (kbps),  [1]:      100000     (kbps)
          [2]:     100000     (kbps),  [3]:      100000     (kbps)
          [4]:     100000     (kbps),  [5]:      100000     (kbps)
          [6]:     100000     (kbps),  [7]:      100000     (kbps)
Router ID:  3.3.3.3
  IGP Type:  OSPF       Process Id:  1       IGP Area: 0
  MPLS-TE Link Count:  2
  Link[1]:
    OSPF Router Id:  3.3.3.3      Opaque LSA ID: 1.0.0.1
    Interface IP Address:  192.168.2.2
    DR Address:  192.168.2.1
    IGP Area:  0
    Link Type:  Multi-access   Link Status:  Active
    IGP Metric:  1     TE Metric:  1    Color:  0x0
    Bandwidth Allocation Model :  Russian Dolls Model
    Maximum Link-Bandwidth:  0  (kbps)
    Maximum Reservable Bandwidth:  0  (kbps)
    Operational Mode of Router :  TE
    Bandwidth Constraints:          Local Overbooking Multiplier:
        BC[0]:     0          (kbps)           LOM[0]:          1
    BW  Unreserved :
          Class  Id:
          [0]:     0          (kbps),  [1]:      0          (kbps)
          [2]:     0          (kbps),  [3]:      0          (kbps)
          [4]:     0          (kbps),  [5]:      0          (kbps)
          [6]:     0          (kbps),  [7]:      0          (kbps)
  Link[2]:
    OSPF Router Id:  3.3.3.3      Opaque LSA ID: 1.0.0.2
    Interface IP Address:  192.168.3.2
    DR Address:  192.168.3.1
    IGP Area:  0
    Link Type:  Multi-access   Link Status:  Active
    IGP Metric:  1     TE Metric:  1    Color:  0x0
    Bandwidth Allocation Model :  Russian Dolls Model
    Maximum Link-Bandwidth:  0  (kbps)
    Maximum Reservable Bandwidth:  0  (kbps)
    Operational Mode of Router :  TE
    Bandwidth Constraints:          Local Overbooking Multiplier:
        BC[0]:     0          (kbps)           LOM[0]:          1
    BW  Unreserved :
          Class  Id:
          [0]:     0          (kbps),  [1]:      0          (kbps)
          [2]:     0          (kbps),  [3]:      0          (kbps)
          [4]:     0          (kbps),  [5]:      0          (kbps)
          [6]:     0          (kbps),  [7]:      0          (kbps)
```

The **BW Unreserved for Class type 0** field indicates the remaining bandwidth reserved for tunnel links with various priorities. **[7]** indicates that bandwidth of 40 Mbit/s has been successfully reserved for a tunnel. The bandwidth information also matches the path of a tunnel. This proves that the affinity property and mask match the administrative group attribute of every link.

Alternatively, run the **display mpls te tunnel** command to check the outbound interfaces of links along the tunnel on LSR B.

```
[~LSRB] display mpls te tunnel
--------------------------------------------------------------------------------
LSP-Id                        Destination      In/Out-If
--------------------------------------------------------------------------------
1.1.1.1:1:3                   3.3.3.3          Pos1/0/0/Pos2/0/0
--------------------------------------------------------------------------------
```

Configure a tunnel named **Tunnel2** on LSR A.

```
[~LSRA] interface tunnel 2
[~LSRA-Tunnel2] ip address unnumbered interface loopback 1
[~LSRA-Tunnel2] tunnel-protocol mpls te
[~LSRA-Tunnel2] destination 3.3.3.3
[~LSRA-Tunnel2] mpls te tunnel-id 101
[~LSRA-Tunnel2] mpls te bandwidth ct0 40000
[~LSRA-Tunnel2] mpls te affinity property 10011 mask 11101
[~LSRA-Tunnel2] mpls te priority 6
[~LSRA-Tunnel2] commit
[~LSRA-Tunnel2] quit
```

Step 6 Verify the configuration.

After completing the configurations, run the **display interface tunnel** or **display mpls te tunnel-interface** command on LSR A. The status of Tunnel1 is **Down**. This is because since the maximum reservable bandwidth is insufficient, Tunnel2 is of a higher priority and has preempted the bandwidth reserved for Tunnel1.

Run the **display mpls te cspf tedb node** command. TEDB information shows the bandwidth for every link, which proves that Tunnel2 does pass through POS 3/0/0 of LSR B.

Alternatively, run the **display mpls te tunnel** command to check outbound interfaces of links along the tunnel on LSR B.

```
[~LSRB] display mpls te tunnel
------------------------------------------------------------------------------
LSP-Id                          Destination      In/Out-If
------------------------------------------------------------------------------
1.1.1.1:1:4                     3.3.3.3          Pos1/0/0/Pos3/0/0
------------------------------------------------------------------------------
```

----End

Configuration Files

- Configuration file of LSR A

```
#
 sysname LSRA
#
 mpls lsr-id 1.1.1.1
#
 mpls
  mpls te
  mpls te cspf
  mpls rsvp-te
#
te-class-mapping
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  mpls-te enable
  network 1.1.1.1 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 192.168.1.1 255.255.255.0
 mpls
 mpls te
 mpls te link administrative group 10001
 mpls te bandwidth max-reservable-bandwidth 100000
```

```
 mpls te bandwidth bc0 100000
 mpls rsvp-te
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
interface Tunnel1
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te affinity property 10101 mask 11011
 mpls te bandwidth ct0 40000
#
interface Tunnel2
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te priority 6
 mpls te affinity property 10011 mask 11101
 mpls te bandwidth ct0 40000
#
return
```

- Configuration file of LSR B

```
#
 sysname LSRB
#
 mpls lsr-id 2.2.2.2
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  mpls-te enable
  network 2.2.2.2 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 192.168.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 192.168.2.1 255.255.255.0
 mpls
 mpls te
 mpls te link administrative group 10101
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
#
interface Pos3/0/0
 undo shutdown
 link-protocol ppp
 ip address 192.168.3.1 255.255.255.0
 mpls
 mpls te
 mpls te link administrative group 10011
```

```
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
return
```

- Configuration file of LSR C

```
#
 sysname LSRC
#
 mpls lsr-id 3.3.3.3
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  mpls-te enable
  network 3.3.3.3 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 192.168.2.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 192.168.3.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
return
```

2.16.4 Example for Configuring SRLGs in TE FRR

Networking Requirements

CAUTION

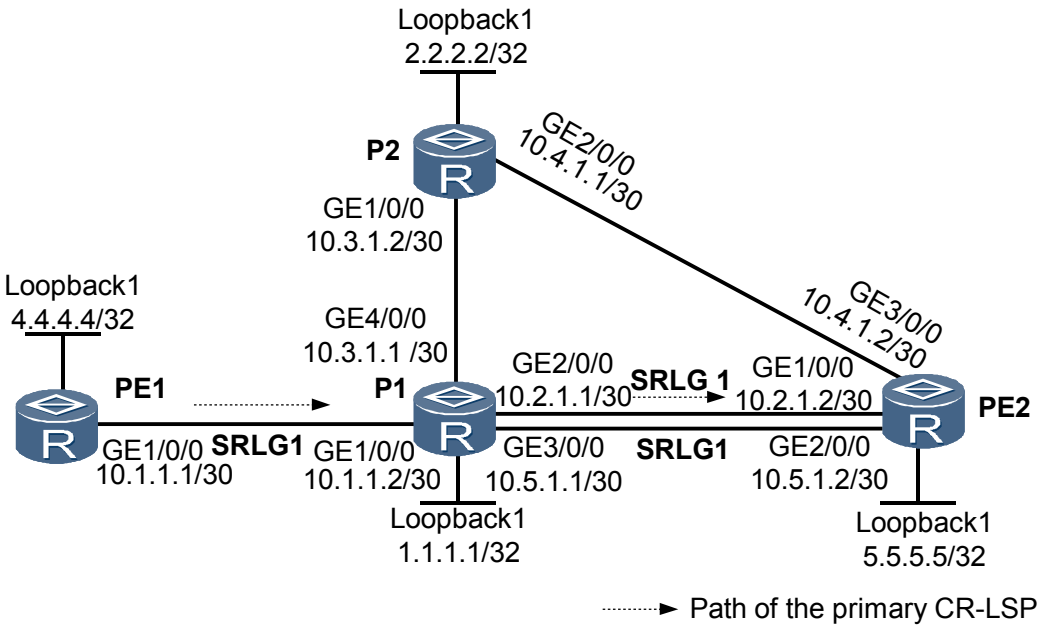
On a single NE5000E, an interface is numbered in the format: slot number/subcard number/interface number. On an NE5000E cluster, an interface is numbered in the format: chassis ID/slot number/subcard number/interface number. The slot number and chassis ID must be specified together.

Figure 2-14 shows an MPLS network. An RSVP-TE tunnel is established along the path PE1 -> P1 -> PE2 between PE1 and PE2. The outbound interface of the primary tunnel on P1 is GE 2/0/0.

The links on network segments of 10.2.1.0/30 and 10.5.1.0/30 are in SRLG1.

TE Auto FRR is required on P1 to improve reliability. The automatic bypass tunnel uses links in an SRLG different from those used by the primary tunnel.

Figure 2-14 Networking diagram for SRLGs in TE FRR



Configuration Notes

None.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure IP addresses and an IGP on all LSRs, ensuring connectivity on the network.
2. Enable MPLS, MPLS TE, and RSVP-TE on all LSRs and their interfaces.
3. Configure IS-IS TE on all LSRs and enable CSPF on PE1 and P1.
4. Set SRLG numbers for SRLG member interfaces.
5. Configure an SRLG mode in the system view on the PLR.
6. Establish an RSVP-TE tunnel between PE1 and PE2 over an explicit path PE1 -> P1 -> PE2.
7. Enable TE FRR in the tunnel interface view and TE Auto FRR on the outbound interface of the primary tunnel on the PLR.

Data Preparation

To complete the configuration, you need the following data:

- SRLG number

Configuration Procedure

1. Assign an IP address and its mask to every interface.

   Assign an IP address and its mask to every physical interface and configure a loopback interface address as an LSR ID on every LSR shown in **Figure 2-14**.

   Detailed configuration information is provided in the following configuration files.

2. Configure an IGP.

   Configure OSPF or IS-IS on every node, ensuring connectivity between them. IS-IS is used in this example.

   Detailed configuration information is provided in the following configuration files.

3. Configure basic MPLS functions.

   Set an LSR ID for every node and enable MPLS in the system and interface views.

   Detailed configuration information is provided in the following configuration files.

4. Configure MPLS TE and RSVP-TE.

   Enable MPLS TE and RSVP-TE in the system and interface views of every node. Set the maximum reservable bandwidth and BD bandwidth for every outbound interface.

   Detailed configuration information is provided in the following configuration files.

5. Configure IS-IS TE and CSPF.

   Configure IS-IS TE on all LSRs and enable CSPF on PE1 and P1.

   Detailed configuration information is provided in the following configuration files.

6. Configure an SRLG.

   # Add links with network segment addresses 10.2.1.0/30 and 10.5.1.0/30 to SRLG1 on P1.

   ```
   [~P1] interface gigabitethernet 2/0/0
   [~P1-GigabitEthernet2/0/0] mpls te srlg 1
   [~P1-GigabitEthernet2/0/0] quit
   [~P1] interface gigabitethernet 3/0/0
   [~P1-GigabitEthernet3/0/0] mpls te srlg 1
   [~P1-GigabitEthernet3/0/0] commit
   [~P1-GigabitEthernet3/0/0] quit
   ```

   # Run the **display mpls te srlg** command on P1. Information about the SRLG and SRLG member interfaces is displayed. Use the display on P1 as an example.

   ```
   [~P1] display mpls te srlg 1
    SRLG    1:               GE2/0/0             GE3/0/0
   ```

   # Run the **display mpls te link-administration srlg-information** command on P1. Mappings between interfaces and SRLGs are displayed.

   ```
   [~P1] display mpls te link-administration srlg-information

     SRLGs on GigabitEthernet2/0/0:
                 1

     SRLGs on GigabitEthernet3/0/0:
                 1
   ```

   # Run the **display mpls te cspf tedb srlg** command on P1. Information about the SRLG TEDB is displayed.

```
[~P1] display mpls te cspf tedb srlg 1
Interface-Address   IGP-Type            Area
10.2.1.1            ISIS                1
10.5.1.1            ISIS                1
10.2.1.1            ISIS                2
10.5.1.1            ISIS                2
```

7. Configure an explicit path for a primary tunnel.

   # Configure the explicit path for the primary tunnel on PE1.

```
<PE1> system-view
[~PE1] explicit-path main
[~PE1-explicit-path-main] next hop 10.1.1.2
[~PE1-explicit-path-main] next hop 10.2.1.2
[~PE1-explicit-path-main] next hop 5.5.5.5
[~PE1-explicit-path-main] commit
[~PE1-explicit-path-main] quit
```

   # Run the **display explicit-path main** command on PE1. Information about the explicit path for the primary tunnel is displayed.

```
[~PE1] display explicit-path main
Path Name : main        Path Status : Enabled
 1      10.1.1.2          Strict      Include
 2      10.2.1.2          Strict      Include
 3      5.5.5.5           Strict      Include
```

8. Configure the tunnel interface for the primary CR-LSP.

   # Create a tunnel interface on PE1, and specify the explicit path and tunnel bandwidth.

```
[~PE1] interface tunnel 1
[~PE1-Tunnel1] ip address unnumbered interface loopback 1
[~PE1-Tunnel1] tunnel-protocol mpls te
[~PE1-Tunnel1] destination 5.5.5.5
[~PE1-Tunnel1] mpls te path explicit-path main
[~PE1-Tunnel1] mpls te bandwidth ct0 10000
[~PE1-Tunnel1] commit
```

   Run the **display interface tunnel1** command on PE1. The tunnel is **Up**.

```
[~PE1] display interface tunnel1
Tunnel1 current state : UP
Line protocol current state : UP
...
```

   NOTE

   The preceding command output only shows a part of the information.

9. Configure TE Auto FRR.

   # Enable TE Auto FRR on GE 2/0/0 on P1.

```
[~P1] interface gigabitethernet 2/0/0
[~P1-GigabitEthernet2/0/0] mpls te auto-frr link
[~P1-GigabitEthernet2/0/0] commit
[~P1-GigabitEthernet2/0/0] quit
```

   # Enable TE FRR on the tunnel interface of PE1.

```
[~PE1] interface tunnel 1
[~PE1-Tunnel1] mpls te fast-reroute
[~PE1-Tunnel1] commit
```

   Run the **display mpls te tunnel path tunnel1** command on PE1. The outbound interface (10.2.1.1) on P1 along the primary tunnel is enabled with **Local-Protection**.

```
[~PE1] display mpls te tunnel path Tunnel1
 Tunnel Interface Name : Tunnel1
 Lsp ID : 5.5.5.5 :1
 Hop Information
  Hop 0   10.1.1.1
  Hop 1   10.1.1.2  Label 65536
  Hop 2   1.1.1.1  Label 65536
  Hop 3   10.2.1.1 Local-Protection available
```

```
  Hop 4   10.2.1.2  Label 3
  Hop 5   5.5.5.5  Label 3
```

10. Verify the configuration.

    # Run the **display mpls te tunnel name Tunnel1 verbose** command on P1. The primary tunnel is bound to a bypass tunnel named **Tunnel0/0/2048**, and the **FrrNextHop** field displays **5.5.5.5**.

```
[~P1] display mpls te tunnel name Tunnel1 verbose
    No                      :  1
    Tunnel-Name             :  Tunnel1
    TunnelIndex             :  1           LSP Index         :  3072
    Session ID              :  100         LSP ID            :  1
    Lsr Role                :  Transit
    Ingress LSR ID          :  4.4.4.4
    Egress LSR ID           :  5.5.5.5
    In-Interface            :  GE1/0/0
    Out-Interface           :  GE2/0/0
    Sign-Protocol           :  RSVP TE     Resv Style        :  SE
    IncludeAnyAff           :  0x0         ExcludeAnyAff     :  0x0
    IncludeAllAff           :  0x0
    ER-Hop Table Index      :  -           AR-Hop Table Index:  2
    C-Hop Table Index       :  -
    PrevTunnelIndexInSession:  -           NextTunnelIndexInSession:  -
    PSB Handle              :  65546
    Created Time            :  2010/10/15 09:52:03
    --------------------------------
              DS-TE Information
    --------------------------------
    Bandwidth Reserved Flag :  Reserved
    CT0 Bandwidth(Kbit/sec) :  10000       CT1 Bandwidth(Kbit/sec):  0
    CT2 Bandwidth(Kbit/sec) :  0           CT3 Bandwidth(Kbit/sec):  0
    CT4 Bandwidth(Kbit/sec) :  0           CT5 Bandwidth(Kbit/sec):  0
    CT6 Bandwidth(Kbit/sec) :  0           CT7 Bandwidth(Kbit/sec):  0
    Setup-Priority          :  7           Hold-Priority     :  7
    --------------------------------
                FRR Information
    --------------------------------
    Primary LSP Info
    TE Attribute Flag       :  0x63        Protected Flag    :  0x1
    Bypass In Use           :  Not Used
    Bypass Tunnel Id        :  67141670
    BypassTunnel            :  Tunnel Index[Tunnel0/0/2048], InnerLabel[3]
    Bypass Lsp ID           :  -           FrrNextHop        :  5.5.5.5
    ReferAutoBypassHandle   :  2049
    FrrPrevTunnelTableIndex :  -           FrrNextTunnelTableIndex:  -
    Bypass Attribute(Not configured)
    Setup Priority          :  -           Hold Priority     :  -
    HopLimit                :  -           Bandwidth         :  -
    IncludeAnyGroup         :  -           ExcludeAnyGroup   :  -
    IncludeAllGroup         :  -
    Bypass Unbound Bandwidth Info(Kbit/sec)
    CT0 Unbound Bandwidth   :  -         CT1 Unbound Bandwidth:  -
    CT2 Unbound Bandwidth   :  -         CT3 Unbound Bandwidth:  -
    CT4 Unbound Bandwidth   :  -         CT5 Unbound Bandwidth:  -
    CT6 Unbound Bandwidth   :  -         CT7 Unbound Bandwidth:  -
    --------------------------------
               BFD Information
    --------------------------------
    NextSessionTunnelIndex  :  -           PrevSessionTunnelIndex:  -
    NextLspId               :  -           PrevLspId         :  -
```

    # Run the **display mpls te tunnel path Tunnel0/0/2048** command on P1. The automatic bypass tunnel is along the path P1 -> P2 -> PE2.

```
[~P1] display mpls te tunnel path Tunnel0/0/2048
 Tunnel Interface Name : Tunnel0/0/2048
 Lsp ID : 1.1.1.1 :2049 :1
 Hop Information
  Hop 0   10.3.1.1
```

```
  Hop 1   10.3.1.2
  Hop 2   2.2.2.2
  Hop 3   10.4.1.1
  Hop 4   10.4.1.2
  Hop 5   5.5.5.5
```

Configuration Files

- Configuration file of PE1

```
#
 sysname PE1
#
 mpls lsr-id 4.4.4.4
#
 mpls
  mpls te
  mpls te cspf
  mpls rsvp-te
#
 explicit-path main
  next hop 10.1.1.2
  next hop 10.2.1.2
  next hop 5.5.5.5
#
te-class-mapping
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0004.00
 traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 isis enable 1
#
interface Tunnel1
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 5.5.5.5
 mpls te record-route
 mpls te bandwidth ct0 10000
 mpls te path explicit-path main
 mpls te fast-reroute
#
return
```

- Configuration file of P1

```
#
 sysname P1
#
 mpls lsr-id 1.1.1.1
#
 mpls
  mpls te
  mpls te cspf
  mpls rsvp-te
  mpls te srlg path-calculation preferred
#
```

```
te-class-mapping
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0001.00
 traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.2 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.2.1.1 255.255.255.252
 mpls
 mpls te
 mpls te auto-frr link
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 mpls te srlg 1
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 10.5.1.1 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 mpls te srlg 1
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet4/0/0
 undo shutdown
 ip address 10.3.1.1 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of P2

```
#
 sysname P2
#
 mpls lsr-id 2.2.2.2
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
#
isis 1
 cost-style wide
```

```
 network-entity 10.0000.0000.0002.00
 traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.3.1.2 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.4.1.1 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
 mpls lsr-id 5.5.5.5
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0006.00
 traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.2.1.2 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.5.1.2 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 10.4.1.2 255.255.255.252
 mpls
```

```
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 5.5.5.5 255.255.255.255
 isis enable 1
#
return
```

2.16.5 Example for Configuring SRLGs in Hot Standby

Networking Requirements

CAUTION

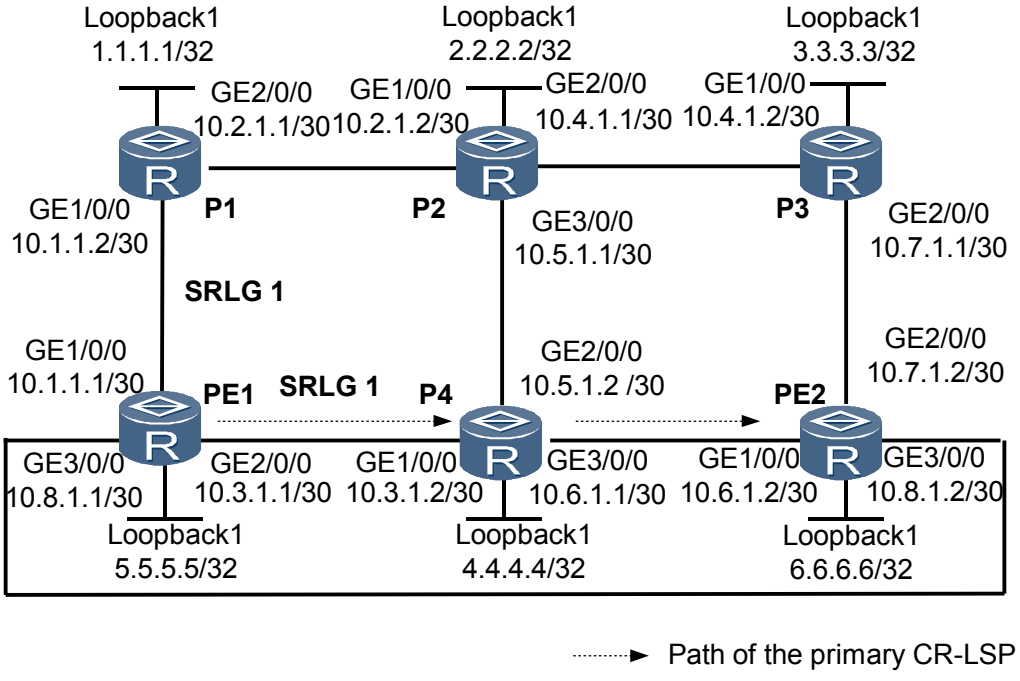
On a single NE5000E, an interface is numbered in the format: slot number/subcard number/interface number. On an NE5000E cluster, an interface is numbered in the format: chassis ID/slot number/subcard number/interface number. The slot number and chassis ID must be specified together.

Figure 2-15 shows an MPLS network. An RSVP-TE tunnel is established between PE1 and PE2 over an explicit path PE1 -> P4 -> PE2.

The path PE1 -> P1 -> P2 -> P4 and the path from PE1 to P4 are in SRLG1.

Hot standby is enabled. The primary and hot-standby CR-LSP must be in different SRLG.

Figure 2-15 Networking diagram for SRLGs in hot standby



Configuration Notes

None.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure IP addresses and an IGP on all LSRs, ensuring connectivity on the network.
2. Enable MPLS, MPLS TE, and RSVP-TE on all LSRs and their interfaces.
3. Establish an RSVP-TE tunnel between PE1 and PE2 over an explicit path PE1 -> P1 -> PE2.
4. Set SRLG numbers for SRLG member interfaces.
5. Configure an SRLG mode in the system view on the ingress.
6. Configure hot standby.

Data Preparation

To complete the configuration, you need the following data:

- SRLG number
- Either preferred or strict SRLG mode

Configuration Procedure

1. Assign an IP address and its mask to every interface.

   Assign an IP address and its mask to every physical interface and configure a loopback interface address as an LSR ID on every LSR shown in **Figure 2-15**.

   Detailed configuration information is provided in the following configuration files.
2. Configure an IGP.

   Configure OSPF or IS-IS on every node, ensuring connectivity between them. IS-IS is used in this example.

   Detailed configuration information is provided in the following configuration files.
3. Configure basic MPLS functions.

   Set an LSR ID for every node and enable MPLS in the system and interface views.

   Detailed configuration information is provided in the following configuration files.
4. Configure MPLS TE and RSVP-TE.

   Enable MPLS TE and RSVP-TE in the system and interface views on every node. Set the maximum reservable bandwidth and BD bandwidth for every outbound interface.

   Detailed configuration information is provided in the following configuration files.
5. Configure IS-IS TE and CSPF.

   Configure IS-IS TE on all LSRs and enable CSPF on PE1.

   Detailed configuration information is provided in the following configuration files.
6. Configure an explicit path for the primary CR-LSP.

   # Configure the explicit path for the primary CR-LSP on PE1.

```
<PE1> system-view
[~PE1] explicit-path main
[~PE1-explicit-path-main] next hop 10.3.1.2
[~PE1-explicit-path-main] next hop 10.6.1.2
[~PE1-explicit-path-main] next hop 6.6.6.6
[~PE1-explicit-path-main] commit
[~PE1-explicit-path-main] quit
```

Run the **display explicit-path main** command on PE1. Information about the explicit path for the primary CR-LSP is displayed.

```
[~PE1] display explicit-path main
Path Name : main        Path Status : Enabled
 1      10.3.1.2          Strict      Include
 2      10.6.1.2          Strict      Include
 3      6.6.6.6           Strict      Include
```

7. Configure the tunnel interface for the primary CR-LSP.

   # Create a tunnel interface on PE1, and specify the explicit path and tunnel bandwidth.

```
[~PE1] interface tunnel 1
[~PE1-Tunnel1] ip address unnumbered interface loopback 1
[~PE1-Tunnel1] tunnel-protocol mpls te
[~PE1-Tunnel1] destination 6.6.6.6
[~PE1-Tunnel1] mpls te path explicit-path main
[~PE1-Tunnel1] mpls te bandwidth ct0 10000
[~PE1-Tunnel1] commit
[~PE1-Tunnel1] quit
```

   Run the **display interface tunnel 1** command on PE1. The tunnel is **Up**.

```
[~PE1] display interface tunnel 1
Tunnel1 current state : UP
Line protocol current state : UP
...
```

   The preceding command output only shows a part of the information.

8. Configure an SRLG.

   # Add links from PE1 to P1 and from PE1 to P4 to SRLG1.

```
[~PE1] interface gigabitethernet 1/0/0
[~PE1-GigabitEthernet1/0/0] mpls te srlg 1
[~PE1-GigabitEthernet1/0/0] quit
[~PE1] interface gigabitethernet 2/0/0
[~PE1-GigabitEthernet2/0/0] mpls te srlg 1
[~PE1-GigabitEthernet2/0/0] commit
[~PE1-GigabitEthernet2/0/0] quit
```

   # Configure an SRLG mode on PE1.

```
[~PE1] mpls
[~PE1-mpls] mpls te srlg path-calculation strict
[~PE1-mpls] commit
[~PE1-mpls] quit
```

   # Run the **display mpls te srlg** command on P1. Information about the SRLG and SRLG member interfaces is displayed. Use the display on P1 as an example.

```
[~P1] display mpls te srlg all
Total SRLG supported : 512
Total SRLG configured : 1


 SRLG    1:               GE1/0/0            GE2/0/0
```

   # Run the **display mpls te link-administration srlg-information** command on PE1. Mappings between interfaces and SRLGs are displayed.

```
[~PE1] display mpls te link-administration srlg-information

  SRLGs on GigabitEthernet1/0/0:
              1
```

```
  SRLGs on GigabitEthernet2/0/0:
                1
```

Run the **display mpls te cspf tedb srlg** command. Information about the SRLG TEDB is displayed. The command output on PE1 is as follows:

```
[~PE1] display mpls te cspf tedb srlg 1
Interface-Address   IGP-Type            Area
10.1.1.1            ISIS                1
10.1.1.1            ISIS                2
10.3.1.1            ISIS                1
10.3.1.1            ISIS                2
```

9. Configure hot standby on the ingress PE1.

   # Configure PE1.

```
[~PE1] interface tunnel 1
[~PE1-Tunnel1] mpls te backup hot-standby
[~PE1-Tunnel1] commit
[~PE1-Tunnel1] quit
```

   # Run the **display mpls te hot-standby state interface tunnel 1** command. Information about hot standby is displayed.

```
[~PE1] display mpls te hot-standby state interface tunnel 1
------------------------------------------------------------------
Verbose information about the Tunnel1 hot-standby state
------------------------------------------------------------------
tunnel name                              : Tunnel1
session id                               : 100
main LSP index                           : 33
hot-standby LSP index                    : 161
HSB switch result                        : main LSP
WTR                                      : 10s
```

10. Verify the configuration.

    # Run the **shutdown** command on GE 3/0/0 on PE1.

```
[~PE1] interface gigabitethernet 3/0/0
[~PE1-GigabitEthernet 3/0/0] shutdown
[~PE1-GigabitEthernet 3/0/0] commit
[~PE1-GigabitEthernet 3/0/0] quit
```

    # Run the **display mpls te hot-standby state interface tunnel 1** command on PE1. The hot-standby CR-LSP **index** is **33**. The command output shows that no hot-standby CR-LSP is established, preventing the hot-standby CR-LSP from sharing the same SRLG with the primary CR-LSP.

```
[~PE1] display mpls te hot-standby state interface tunnel 1
------------------------------------------------------------------
Verbose information about the Tunnel1 hot-standby state
------------------------------------------------------------------
tunnel name                              : Tunnel1
session id                               : 100
main LSP index                           : 33
hot-standby LSP index                    : 161
HSB switch result                        : main LSP
WTR                                      : 10s
```

Configuration Files

- Configuration file of PE1

```
#
 sysname PE1
#
 mpls lsr-id 5.5.5.5
#
 mpls
  mpls te
  mpls te srlg path-calculation strict
```

```
  mpls te cspf
  mpls rsvp-te
#
 explicit-path main
  next hop 10.3.1.2
  next hop 10.6.1.2
  next hop 6.6.6.6
#
te-class-mapping
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0005.00
 traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 mpls te srlg 1
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.2.1.1 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 mpls te srlg 1
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 10.8.1.1 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 5.5.5.5 255.255.255.255
 isis enable 1
#
interface Tunnel
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 6.6.6.6
 mpls te record-route
 mpls te bandwidth ct0 10000
 mpls te backup hot-standby
 mpls te path explicit-path main
#
return
```

- Configuration file of P1

```
#
 sysname P1
#
 mpls lsr-id 1.1.1.1
#
 mpls
  mpls te
```

```
  mpls rsvp-te
#
te-class-mapping
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0001.00
 traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.2 255.255.255.252
  mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.2.1.1 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of P2

```
#
 sysname P2
#
 mpls lsr-id 2.2.2.2
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0002.00
 traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.2.1.2 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.4.1.1 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
```

```
 mpls rsvp-te
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 10.5.1.1 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of P3

```
#
 sysname P3
#
 mpls lsr-id 3.3.3.3
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0003.00
 traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.4.1.2 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.7.1.1 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of P4

```
#
 sysname P4
#
 mpls lsr-id 4.4.4.4
#
 mpls
  mpls te
  mpls rsvp-te
```

```
#
te-class-mapping
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0004.00
 traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.3.1.2 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.5.1.2 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 10.6.1.1 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
 mpls lsr-id 6.6.6.6
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0006.00
 traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.6.1.2 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
```

```
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.7.1.2 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 10.8.1.2 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 6.6.6.6 255.255.255.255
 isis enable 1
#
Return
```

2.16.6 Example for Configuring an Inter-area Tunnel

Networking Requirements

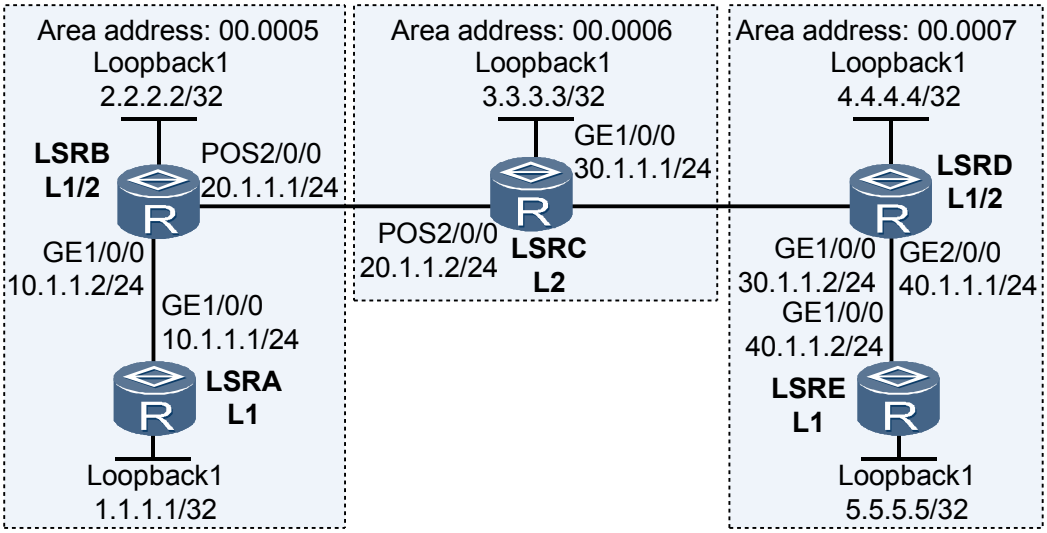
CAUTION

On a single NE5000E, an interface is numbered in the format: slot number/subcard number/interface number. On an NE5000E cluster, an interface is numbered in the format: chassis ID/slot number/subcard number/interface number. The slot number and chassis ID must be specified together.

Figure 2-16 shows a network:

- IS-IS runs on LSR A, LSR B, LSR C, LSR D, and LSR E.
  - LSR A and LSR E are level-1 routers.
  - LSR B and LSR D are level-1-2 routers.
  - LSR C is a level-2 router.
- RSVP-TE is used to establish a TE tunnel from LSR A to LSR E over IS-IS areas. The bandwidth for the TE tunnel is 20 Mbit/s.
- Both the maximum reservable bandwidth and BC0 bandwidth for every link along the TE tunnel are 100 Mbit/s.

Figure 2-16 Networking diagram for an inter-area tunnel



Configuration Notes

None.

Configuration Roadmap

The configuration roadmap is as follows:

1. Assign an IP address and its mask to every interface and configure a loopback address that is used as an LSR ID on every LSR.
2. Enable IS-IS globally and enable IS-IS TE.
3. Configure a loose explicit path on which LSR B, LSR C, and LSR D functioning as Area Border Routers (ABRs) are located.
4. Configure MPLS RSVP-TE.
5. Set bandwidth attributes for every outbound interface on every LSR along the TE tunnel.
6. Create a tunnel interface on the ingress and configure the source and destination IP addresses, protocol, RSVP-TE signaling protocol, and bandwidth for the tunnel.

Data Preparation

To complete the configuration, you need the following data:

- Origin AS number, and IS-IS level and area ID of every LSR
- Maximum reservable bandwidth and BC bandwidth for every link along the TE tunnel
- Tunnel interface number, source and destination addresses, ID, RSVP-TE signaling protocol, and bandwidth of the tunnel

Procedure

Step 1 Assign an IP address and its mask every interface.

Assign an IP address and its mask to every interface and configure a loopback address that is used as an LSR ID on every LSR shown in **Figure 2-16**.

Step 2 Configure IS-IS.

Configure LSR A.

```
[~LSRA] isis 1
[~LSRA-isis-1] network-entity 00.0005.0000.0000.0001.00
[~LSRA-isis-1] is-level level-1
[~LSRA-isis-1] quit
[~LSRA] interface gigabitethernet 1/0/0
[~LSRA-GigabitEthernet1/0/0] isis enable 1
[~LSRA-GigabitEthernet1/0/0] quit
[~LSRA] interface loopback 1
[~LSRA-LoopBack1] isis enable 1
[~LSRA-LoopBack1] commit
[~LSRA-LoopBack1] quit
```

Configure LSR B.

```
[~LSRB] isis 1
[~LSRB-isis-1] network-entity 00.0005.0000.0000.0002.00
[~LSRB-isis-1] is-level level-1-2
[~LSRB-isis-1] import-route isis level-2 into level-1
[~LSRB-isis-1] quit
[~LSRB] interface gigabitethernet 1/0/0
[~LSRB-GigabitEthernet1/0/0] isis enable 1
[~LSRB-GigabitEthernet1/0/0] quit
[~LSRB] interface pos 2/0/0
[~LSRB-Pos2/0/0] isis enable 1
[~LSRB-Pos2/0/0] quit
[~LSRB] interface loopback 1
[~LSRB-LoopBack1] isis enable 1
[~LSRB-LoopBack1] commit
[~LSRB-LoopBack1] quit
```

Configure LSR C.

```
[~LSRC] isis 1
[~LSRC-isis-1] network-entity 00.0006.0000.0000.0003.00
[~LSRC-isis-1] is-level level-2
[~LSRC-isis-1] quit
[~LSRC] interface gigabitethernet 1/0/0
[~LSRC-GigabitEthernet1/0/0] isis enable 1
[~LSRC-GigabitEthernet1/0/0] quit
[~LSRC] interface pos 2/0/0
[~LSRC-Pos2/0/0] isis enable 1
[~LSRC-Pos2/0/0] quit
[~LSRC] interface loopback 1
[~LSRC-LoopBack1] isis enable 1
[~LSRC-LoopBack1] commit
[~LSRC-LoopBack1] quit
```

Configure LSR D.

```
[~LSRD] isis 1
[~LSRD-isis-1] network-entity 00.0007.0000.0000.0004.00
[~LSRD-isis-1] is-level level-1-2
[~LSRD-isis-1] import-route isis level-2 into level-1
[~LSRD-isis-1] quit
[~LSRD] interface gigabitethernet 1/0/0
[~LSRD-GigabitEthernet1/0/0] isis enable 1
[~LSRD-GigabitEthernet1/0/0] quit
[~LSRD] interface gigabitethernet 2/0/0
[~LSRD-GigabitEthernet2/0/0] isis enable 1
[~LSRD-GigabitEthernet2/0/0] quit
[~LSRD] interface loopback 1
[~LSRD-LoopBack1] isis enable 1
```

```
[~LSRD-LoopBack1] commit
[~LSRD-LoopBack1] quit
```

Configure LSR E.

```
[~LSRE] isis 1
[~LSRE-isis-1] network-entity 00.0007.0000.0000.0005.00
[~LSRE-isis-1] is-level level-1
[~LSRE-isis-1] quit
[~LSRE] interface gigabitethernet 1/0/0
[~LSRE-GigabitEthernet1/0/0] isis enable 1
[~LSRE-GigabitEthernet1/0/0] quit
[~LSRE] interface loopback 1
[~LSRE-LoopBack1] isis enable 1
[~LSRE-LoopBack1] commit
[~LSRE-LoopBack1] quit
```

After completing the configurations, run the **display ip routing-table** command on every node. All nodes have learned routes from each other. In this example, the IP routing table on LSR A is displayed.

```
[~LSRA] display ip routing-table
Route Flags: R - relay, D - download for forwarding
------------------------------------------------------------------------------
Routing Table : _public_
         Destinations : 15       Routes : 15
Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface
        1.1.1.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
        2.2.2.2/32  ISIS   15   10          D  10.1.1.2        GigabitEthernet1/0/0
        3.3.3.3/32  ISIS   15   20          D  10.1.1.2        GigabitEthernet1/0/0
        4.4.4.4/32  ISIS   15   30          D  10.1.1.2        GigabitEthernet1/0/0
        5.5.5.5/32  ISIS   15   40          D  10.1.1.2        GigabitEthernet1/0/0
       10.1.1.0/24  Direct 0    0           D   10.1.1.1        GigabitEthernet1/0/0
       10.1.1.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
     10.1.1.255/32  Direct 0    0           D  127.0.0.1       InLoopBack0
       20.1.1.0/24  ISIS   15   20          D  10.1.1.2        GigabitEthernet1/0/0
       30.1.1.0/24  ISIS   15   30          D  10.1.1.2        GigabitEthernet1/0/0
       40.1.1.0/24  ISIS   15   40          D  10.1.1.2        GigabitEthernet1/0/0
      127.0.0.0/8   Direct 0    0           D  127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0           D  127.0.0.1       InLoopBack0
127.255.255.255/32  Direct 0    0           D  127.0.0.1       InLoopBack0
255.255.255.255/32  Direct 0    0           D  127.0.0.1       InLoopBack0
```

Step 3 Configure basic MPLS functions, and enable MPLS TE, RSVP-TE, and CSPF on the ingress of the TE tunnel.

Configure LSR A.

```
[~LSRA] mpls lsr-id 1.1.1.1
[~LSRA] mpls
[~LSRA-mpls] mpls te
[~LSRA-mpls] mpls rsvp-te
[~LSRA-mpls] mpls te cspf
[~LSRA-mpls] quit
[~LSRA] interface gigabitethernet 1/0/0
[~LSRA-GigabitEthernet1/0/0] mpls
[~LSRA-GigabitEthernet1/0/0] mpls te
[~LSRA-GigabitEthernet1/0/0] mpls rsvp-te
[~LSRA-GigabitEthernet1/0/0] commit
[~LSRA-GigabitEthernet1/0/0] quit
```

Configure LSR B.

```
[~LSRB] mpls lsr-id 2.2.2.2
[~LSRB] mpls
[~LSRB-mpls] mpls te
[~LSRB-mpls] mpls rsvp-te
[~LSRB-mpls] quit
[~LSRB] interface gigabitethernet 1/0/0
```

```
[~LSRB-GigabitEthernet1/0/0] mpls
[~LSRB-GigabitEthernet1/0/0] mpls te
[~LSRB-GigabitEthernet1/0/0] mpls rsvp-te
[~LSRB-GigabitEthernet1/0/0] quit
[~LSRB] interface pos 2/0/0
[~LSRB-Pos2/0/0] mpls
[~LSRB-Pos2/0/0] mpls te
[~LSRB-Pos2/0/0] mpls rsvp-te
[~LSRB-Pos2/0/0] commit
[~LSRB-Pos2/0/0] quit
```

Configure LSR C.

```
[~LSRC] mpls lsr-id 3.3.3.3
[~LSRC] mpls
[~LSRC-mpls] mpls te
[~LSRC-mpls] mpls rsvp-te
[~LSRC-mpls] quit
[~LSRC] interface gigabitethernet 1/0/0
[~LSRC-GigabitEthernet1/0/0] mpls
[~LSRC-GigabitEthernet1/0/0] mpls te
[~LSRC-GigabitEthernet1/0/0] mpls rsvp-te
[~LSRC-GigabitEthernet1/0/0] quit
[~LSRC] interface pos 2/0/0
[~LSRC-Pos2/0/0] mpls
[~LSRC-Pos2/0/0] mpls te
[~LSRC-Pos2/0/0] mpls rsvp-te
[~LSRC-Pos2/0/0] commit
[~LSRC-Pos2/0/0] quit
```

Configure LSR D.

```
[~LSRD] mpls lsr-id 4.4.4.4
[~LSRD] mpls
[~LSRD-mpls] mpls te
[~LSRD-mpls] mpls rsvp-te
[~LSRD-mpls] quit
[~LSRD] interface gigabitethernet 1/0/0
[~LSRD-GigabitEthernet1/0/0] mpls
[~LSRD-GigabitEthernet1/0/0] mpls te
[~LSRD-GigabitEthernet1/0/0] mpls rsvp-te
[~LSRD-GigabitEthernet1/0/0] quit
[~LSRD] interface gigabitethernet 2/0/0
[~LSRD-GigabitEthernet2/0/0] mpls
[~LSRD-GigabitEthernet2/0/0] mpls te
[~LSRD-GigabitEthernet2/0/0] mpls rsvp-te
[~LSRD-GigabitEthernet2/0/0] commit
[~LSRD-GigabitEthernet2/0/0] quit
```

Configure LSR E.

```
[~LSRE] mpls lsr-id 5.5.5.5
[~LSRE] mpls
[~LSRE-mpls] mpls te
[~LSRE-mpls] mpls rsvp-te
[~LSRE-mpls] quit
[~LSRE] interface gigabitethernet 1/0/0
[~LSRE-GigabitEthernet1/0/0] mpls
[~LSRE-GigabitEthernet1/0/0] mpls te
[~LSRE-GigabitEthernet1/0/0] mpls rsvp-te
[~LSRE-GigabitEthernet1/0/0] commit
[~LSRE-GigabitEthernet1/0/0] quit
```

Step 4 Configure IS-IS TE.

Configure LSR A.

```
[~LSRA] isis 1
[~LSRA-isis-1] cost-style wide
[~LSRA-isis-1] traffic-eng level-1
```

```
[~LSRA-isis-1] commit
[~LSRA-isis-1] quit
```

Configure LSR B.

```
[~LSRB] isis 1
[~LSRB-isis-1] cost-style wide
[~LSRB-isis-1] traffic-eng level-1-2
[~LSRB-isis-1] commit
[~LSRB-isis-1] quit
```

Configure LSR C.

```
[~LSRC] isis 1
[~LSRC-isis-1] cost-style wide
[~LSRC-isis-1] traffic-eng level-2
[~LSRC-isis-1] commit
[~LSRC-isis-1] quit
```

Configure LSR D.

```
[~LSRD] isis 1
[~LSRD-isis-1] cost-style wide
[~LSRD-isis-1] traffic-eng level-1-2
[~LSRD-isis-1] commit
[~LSRD-isis-1] quit
```

Configure LSR E.

```
[~LSRE] isis 1
[~LSRE-isis-1] cost-style wide
[~LSRE-isis-1] traffic-eng level-1
[~LSRE-isis-1] commit
[~LSRE-isis-1] quit
```

Step 5 Configure a loose explicit path.

```
[~LSRA] explicit-path atoe enable
[~LSRA-explicit-path-atoe] next hop 10.1.1.2 include loose
[~LSRA-explicit-path-atoe] next hop 20.1.1.2 include loose
[~LSRA-explicit-path-atoe] next hop 30.1.1.2 include loose
[~LSRA-explicit-path-atoe] next hop 40.1.1.2 include loose
[~LSRA-explicit-path-atoe] commit
[~LSRE-isis-1] quit
```

Step 6 Configure MPLS TE attributes for links.

Set the maximum reservable bandwidth and BC0 bandwidth for links on LSR A.

```
[~LSRA] interface gigabitethernet 1/0/0
[~LSRA-GigabitEthernet1/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[~LSRA-GigabitEthernet1/0/0] mpls te bandwidth bc0 100000
[~LSRA-GigabitEthernet1/0/0] commit
[~LSRA-GigabitEthernet1/0/0] quit
```

Set the maximum bandwidth and reservable bandwidth for links on LSR B.

```
[~LSRB] interface pos 2/0/0
[~LSRB-Pos2/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[~LSRB-Pos2/0/0] mpls te bandwidth bc0 100000
[~LSRB-Pos2/0/0] commit
[~LSRB-Pos2/0/0] quit
```

Set the maximum bandwidth and reservable bandwidth for links on LSR C.

```
[~LSRC] interface gigabitethernet 1/0/0
[~LSRC-GigabitEthernet1/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[~LSRC-GigabitEthernet1/0/0] mpls te bandwidth bc0 100000
[~LSRC-GigabitEthernet1/0/0] commit
[~LSRC-GigabitEthernet1/0/0] quit
```

Set the maximum bandwidth and reservable bandwidth for links on LSR D.

```
[~LSRD] interface gigabitethernet 2/0/0
[~LSRD-GigabitEthernet2/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[~LSRD-GigabitEthernet2/0/0] mpls te bandwidth bc0 100000
[~LSRD-GigabitEthernet2/0/0] commit
[~LSRD-GigabitEthernet2/0/0] quit
```

Step 7 Configure an MPLS RSVP-TE tunnel.

Configure the MPLS TE tunnel on LSR A.

```
[~LSRA] interface tunnel 1
[~LSRA-Tunnel1] ip address unnumbered interface loopback 1
[~LSRA-Tunnel1] tunnel-protocol mpls te
[~LSRA-Tunnel1] destination 5.5.5.5
[~LSRA-Tunnel1] mpls te signal-protocol rsvp-te
[~LSRA-Tunnel1] mpls te bandwidth ct0 20000
[~LSRA-Tunnel1] mpls te path explicit-path atoe
[~LSRA-Tunnel1] commit
[~LSRA-Tunnel1] quit
```

Step 8 Verify the configuration.

After completing the configuration, run the **display interface tunnel** command on LSR A. The tunnel interface is **Up**.

```
[~LSRA] display interface Tunnel

Tunnel1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2010-10-13 07:21:27
Description: HUAWEI,Tunnel1 Interface (ifindex: 19, vr: 0)
Route Port,The Maximum Transmit Unit is 1500
Internet Address is unnumbered, using address of LoopBack1(1.1.1.9/32)
Encapsulation is TUNNEL, loopback not set
Tunnel protocol is MPLS
Current system time: 2010-10-15 01:51:11
Tunnel destination 5.5.5.5
Tunnel up/down statistics 0

QoS max-bandwidth : 0 Kbps
Output queue : (Urgent queue : Size/Length/Discards)  0/0/0
Output queue : (Protocol queue : Size/Length/Discards) 0/0/0
Output queue : (FIFO queue : Size/Length/Discards)  0/0/0
    300 seconds output rate 0 bits/sec, 0 packets/sec
    48 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets output,  0 bytes
    0 output error
    0 output drop
    ct0:0 packets output,  0 bytes
        0 output error
    Last 300 seconds input utility rate:  0.00%
    Last 300 seconds output utility rate: 0.00%
```

Run the **display mpls te tunnel-interface** command on LSR A. Detailed information about the TE tunnel interface is displayed.

```
[~LSRA] display mpls te tunnel-interface tunnel1
  Tunnel Name          :  Tunnel1
  Tunnel State Desc    :  CR-LSP is Up
  Tunnel Attributes    :
    Ingress LSR ID     :  1.1.1.1              Egress LSR ID:  4.4.4.4
    Admin State        :  UP                   Oper State    :  UP
    Signaling Protocol :  RSVP
    FTid               :  289
    Tie-Breaking Policy :  None                Metric Type   :  None
    BypassBW Flag      :  Not Supported
    BypassBW Type      :  -                    Bypass BW     :  -
```

```
Bfd Cap      :  None                          Retry Int    :  2 sec
Reopt              :  Disabled                Reopt Freq   :  -
Auto BW            :  Disabled
Current Collected BW:  -                      Auto BW Freq :  -
Min BW             :  -                       Max BW       :  -
Tunnel  Group      :  Primary
Interfaces Protected:  -
Excluded IP Address :  -
Is On Radix-Tree   :  Yes                     Referred LSP Count:  0
Primary Tunnel     :  -                       Pri Tunn Sum :  -
Backup Tunnel      :  -
Group Status       :  Up                      Oam Status   :  Up
IPTN InLabel       :  -
BackUp Type        :  None                    BestEffort   :  Disabled
SRLG Disjoining: NA
Secondary HopLimit  :  -
BestEffort HopLimit :  -
Secondary Explicit Path Name:  -
Secondary Affinity Prop/Mask:  0x0/0x0
BestEffort Affinity Prop/Mask:  0x0/0x0
IsConfigLspConstraint: -

Primary LSP ID     :  1.1.1.1:1
Setup Priority     :  7                       Hold Priority:  7
IncludeAll         :  0x0
IncludeAny         :  0x0
ExcludeAny         :  0x0
Affinity Prop/Mask  : 0x0/0x0                Resv Style   :  SE
Configured Bandwidth Information:
CT0 Bandwidth(Kbit/sec): 20000          CT1 Bandwidth(Kbit/sec): 0
CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
Actual Bandwidth Information:
CT0 Bandwidth(Kbit/sec): 20000          CT1 Bandwidth(Kbit/sec): 0
CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
Explicit Path Name  :  -                    Hop Limit           : -
Record Route       :  Disabled              Record Label :  Disabled
Route Pinning      :  Disabled
FRR Flag           :  -
IdleTime Remain    :  -
BFD Status         :  -
```

----End

Configuration Files

- Configuration file of LSR A

```
#
 sysname LSRA
#
 mpls lsr-id 1.1.1.1
#
 mpls
  mpls te
  mpls te cspf
  mpls rsvp-te
#
 explicit-path atoe
  next hop 10.1.1.2 include loose
  next hop 20.1.1.2 include loose
  next hop 30.1.1.2 include loose
  next hop 40.1.1.2 include loose
#
te-class-mapping
isis 1
```

```
 is-level level-1
 cost-style wide
 traffic-eng level-1
 network-entity 00.0005.0000.0000.0001.00
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 isis enable 1
#
interface Tunnel1
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 5.5.5.5
 mpls te bandwidth ct0 20000
mpls te path explicit-path atoe
#
return
```

- Configuration file of LSR B

```
#
 sysname LSRB
#
 mpls lsr-id 2.2.2.2
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
isis 1
 is-level level-1-2
 cost-style wide
 traffic-eng level-1-2
 import-route isis level-2 into level-1
 network-entity 00.0005.0000.0000.0002.00
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls te
 isis enable 1
 mpls rsvp-te
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 20.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
#
```

```
return
```

- Configuration file of LSR C

```
#
 sysname LSRC
#
 mpls lsr-id 3.3.3.3
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
isis 1
 is-level level-2
 cost-style wide
 traffic-eng level-2
 network-entity 00.0006.0000.0000.0003.00
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 30.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 isis enable 1
 mpls rsvp-te
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 20.1.1.2 255.255.255.0
 mpls
 mpls te
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of LSR D

```
#
 sysname LSRD
#
 mpls lsr-id 4.4.4.4
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
isis 1
 is-level level-1-2
 cost-style wide
 traffic-eng level-1-2
 network-entity 00.0007.0000.0000.0004.00
 import-route isis level-2 into level-1
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 30.1.1.2 255.255.255.0
 mpls
 mpls te
 isis enable 1
 mpls rsvp-te
#
```

```
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 40.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of LSR E

```
#
 sysname LSRE
#
 mpls lsr-id 5.5.5.5
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
isis 1
 is-level level-1
 cost-style wide
 traffic-eng level-1
 network-entity 00.0007.0000.0000.0005.00
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 40.1.1.2 255.255.255.0
 mpls
 mpls te
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 5.5.5.5 255.255.255.255
 isis enable 1
#
return
```

2.16.7 Example for Configuring the Threshold for Flooding Bandwidth Information

Networking Requirements

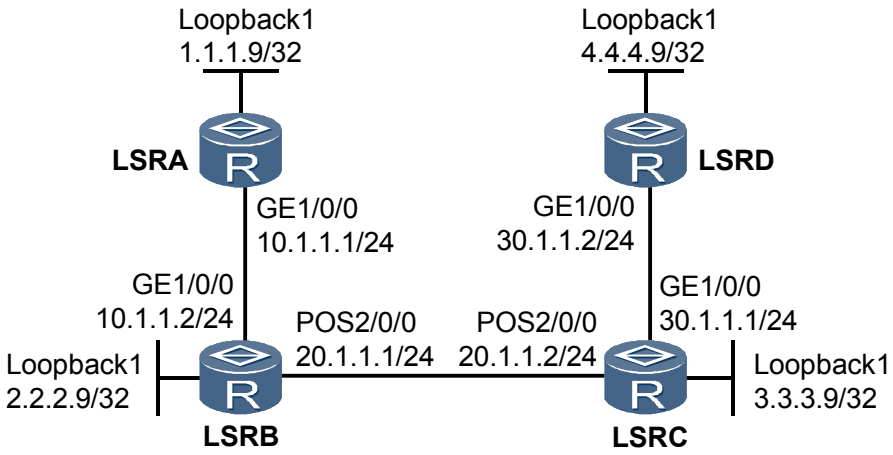
CAUTION

On a single NE5000E, an interface is numbered in the format: slot number/subcard number/interface number. On an NE5000E cluster, an interface is numbered in the format: chassis ID/slot number/subcard number/interface number. The slot number and chassis ID must be specified together.

On the network shown in **Figure 2-17**. An RSVP-TE tunnel is established from LSR A to LSR D. The bandwidth is 50 Mbit/s. The maximum reservable bandwidth and BC0 bandwidth for every link are 100 Mbit/s. The RDM is used.

The threshold for flooding bandwidth information is set to 20%. This reduces the number of attempts to flood bandwidth information and saves network resources. If the proportion of the bandwidth used or released by an MPLS TE tunnel to the available bandwidth in the TEDB is equal to or larger than 20%, an IGP floods the bandwidth information and CSPF updates TEDB information accordingly.

Figure 2-17 Networking diagram for configuring the threshold for flooding bandwidth information



Configuration Notes

None.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an RSVP-TE tunnel. See "Configuration Roadmap" in **Example for Configuring an RSVP-TE Tunnel**.
2. Configure bandwidth and the threshold for flooding bandwidth information

Data Preparation

To complete the configuration, you need the following data:

- OSPF process ID and area ID for every LSR
- Maximum reservable bandwidth and BC bandwidth for every link along the TE tunnel
- Tunnel interface type and number, source and destination addresses, ID, and RSVP-TE signaling protocol of the tunnel
- Threshold for flooding bandwidth information

Procedure

Step 1 Assign an IP address and its mask to every interface.

Assign an IP address and its mask to every physical interface and configure a loopback interface address as an LSR ID on every node shown in **Figure 2-17**.

Detailed configuration information is provided in the following configuration files.

Step 2 Configure an IGP.

Configure OSPF or IS-IS on every node, ensuring connectivity between them. IS-IS is used in this example.

Detailed configuration information is provided in the following configuration files.

Step 3 Configure basic MPLS functions and enable MPLS TE, RSVP-TE, and CSPF.

Enable MPLS, MPLS TE, and RSVP-TE on every LSR and their interfaces along a tunnel, and enable CSPF in the system view of the ingress.

Detailed configuration information is provided in the following configuration files.

Step 4 Set MPLS TE bandwidth for links.

Set the maximum reservable bandwidth and BC0 bandwidth for a link on every interface along the TE tunnel.

Detailed configuration information is provided in the following configuration files.

Step 5 Configure the threshold for flooding bandwidth information.

Set the threshold for flooding bandwidth information to 20% on a physical interface on LSR A. If the proportion of the bandwidth used or released by an MPLS TE tunnel to the available bandwidth in the TEDB is equal to or larger than 20%, an IGP floods the bandwidth information and CSPF updates TEDB information accordingly.

```
[~LSRA] interface gigabitethernet 1/0/0
[~LSRA-GigabitEthernet1/0/0] mpls te bandwidth change thresholds up 20
[~LSRA-GigabitEthernet1/0/0] mpls te bandwidth change thresholds down 20
[~LSRA-GigabitEthernet1/0/0] commit
[~LSRA-GigabitEthernet1/0/0] quit
```

Run the **display mpls te cspf tedb** command on LSR A. TEDB information is displayed.

```
[~LSRA] display mpls te cspf tedb interface 10.1.1.1

Router ID:  1.1.1.9
  IGP Type:  ISIS       Process Id:  1
  Link[1]:
    ISIS System ID:  0000.0000.0001.00     Opaque LSA ID:  0000.0000.0001.00:00
    Interface IP Address:  10.1.1.1
    Peer  IP Address:  10.1.1.2
    Peer  Router  Id:  2.2.2.9
    Peer  ISIS System ID:  0000.0000.0001.00
    IGP Area:  Level-2
    Link Type:  P2P   Link Status:  Active
    IGP Metric:  10     TE Metric:  10    Color:  0x0
    Bandwidth Allocation Model :  Russian Dolls Model
    Maximum Link-Bandwidth:  100000  (kbps)
    Maximum Reservable Bandwidth:  100000  (kbps)
    Operational Mode of Router :  TE
    Bandwidth Constraints:          Local Overbooking Multiplier:
       BC[0]:     100000     (kbps)           LOM[0]:          1
    BW  Unreserved :
```

```
Class  Id:
[0]:     100000     (kbps),  [1]:      100000     (kbps)
[2]:     100000     (kbps),  [3]:      100000     (kbps)
[4]:     100000     (kbps),  [5]:      100000     (kbps)
[6]:     100000     (kbps),  [7]:      100000     (kbps)
```

Step 6 Configure an MPLS TE tunnel.

Configure a tunnel named **Tunnel1** on LSR A.

```
[~LSRA]interface tunnel 1
[~LSRA-Tunnel1] ip address unnumbered interface loopback 1
[~LSRA-Tunnel1] destination 4.4.4.9
[~LSRA-Tunnel1] tunnel-protocol mpls te
[~LSRA-Tunnel1] mpls te bandwidth ct0 10000
[~LSRA-Tunnel1] commit
[~LSRA-Tunnel1] quit
```

After the configuration, run the **display mpls te tunnel-interface** command on LSR A. The tunnel interface is **Up**.

```
[~LSRA] display mpls te tunnel-interface tunnel1

    Tunnel Name       : Tunnel1
    Tunnel State Desc : CR-LSP is Up
    Tunnel Attributes   :
    Session ID          : 1
    Ingress LSR ID      : 1.1.1.9              Egress LSR ID: 4.4.4.9
    Admin State         : UP                   Oper State   : UP
    Signaling Protocol  : RSVP
    FTid                : 1
    Tie-Breaking Policy : RANDOM               Metric Type : None
    BypassBW Flag       : Not Supported
    BypassBW Type       : -                    Bypass BW    : -
    Bfd Cap      : None                        Retry Int    : -
    Reopt               : Disabled             Reopt Freq   : -
    Auto BW             : Disabled
    Current Collected BW: -                    Auto BW Freq : -
    Min BW              : -                    Max BW       : -
    Tunnel Group       : -
    Interfaces Protected: -
    Excluded IP Address : -
    Is On Radix-Tree    : -                    Referred LSP Count: -
    Primary Tunnel      : -                    Pri Tunn Sum : -
    Backup Tunnel       : -
    Group Status        : -                    Oam Status   : -
    IPTN InLabel        : -
    BackUp Type         : None                 BestEffort  : Disabled
    SRLG Disjoining: NA
    Secondary HopLimit : -
    BestEffort HopLimit : -
    Secondary Explicit Path Name: -
    Secondary Affinity Prop/Mask: -
    BestEffort Affinity Prop/Mask: 0x0/0x0
    IsConfigLspConstraint: -

    Primary LSP ID      :  1.1.1.9:1
    Setup Priority      :  7                    Hold Priority:  7
    IncludeAll          :  0x0
    IncludeAny          :  0x0
    ExcludeAny          :  0x0
    Affinity Prop/Mask  : 0x0/0x0              Resv Style   :  SE
    Configured Bandwidth Information:
    CT0 Bandwidth(Kbit/sec): 10000          CT1 Bandwidth(Kbit/sec): 0
    CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
    CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
    CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
    Actual Bandwidth Information:
    CT0 Bandwidth(Kbit/sec): 10000          CT1 Bandwidth(Kbit/sec): 0
    CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
```

```
    CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
    CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
   Explicit Path Name   : main                 Hop Limit           : -
    Record Route        :  Disabled              Record Label :  Disabled
    Route Pinning       :  Disabled
    FRR Flag            :  Disabled
    IdleTime Remain     :  -
    BFD Status          :  -
```

Run the **display mpls te cspf tedb** command on LSR A. Bandwidth information is unchanged.

```
[~LSRA] display mpls te cspf tedb interface 10.1.1.1

Router ID:  1.1.1.9
  IGP Type:  ISIS       Process Id:  1
  Link[1]:
    ISIS System ID:  0000.0000.0001.00     Opaque LSA ID:  0000.0000.0001.00:00
    Interface IP Address:  10.1.1.1
    Peer  IP Address:  10.1.1.2
    Peer  Router  Id:  2.2.2.9
    Peer  ISIS System ID:  0000.0000.0001.00
    IGP Area:  Level-2
    Link Type:  P2P   Link Status:  Active
    IGP Metric:  10     TE Metric:  10    Color:  0x0
    Bandwidth Allocation Model :  Russian Dolls Model
    Maximum Link-Bandwidth:  100000  (kbps)
    Maximum Reservable Bandwidth:  100000  (kbps)
    Operational Mode of Router :  TE
    Bandwidth Constraints:          Local Overbooking Multiplier:
       BC[0]:     100000     (kbps)           LOM[0]:          1
    BW  Unreserved :
         Class  Id:
         [0]:     100000     (kbps),  [1]:      100000     (kbps)
         [2]:     100000     (kbps),  [3]:      100000     (kbps)
         [4]:     100000     (kbps),  [5]:      100000     (kbps)
         [6]:     100000     (kbps),  [7]:      100000     (kbps)
```

Step 7 Verify the configuration.

After the configurations are complete, the bandwidth has been changed to 20 kbit/s.

```
[~LSRA] interface tunnel 1
[~LSRA-Tunnel1] mpls te bandwidth ct0 20000
[~LSRA-Tunnel1] commit
[~LSRA-Tunnel1] quit
```

Run the **display mpls te cspf tedb interface 10.1.1.1** command on LSR A. TEDB information shows that the TE tunnel named Tunnel1 has been re-established successfully. Its bandwidth is 20 kbit/s, reaching 20%, the threshold for flooding bandwidth information. Therefore, CSPF TEDB information has been updated.

```
[~LSRA]  display mpls te cspf tedb interface 10.1.1.1

Router ID:  1.1.1.9
  IGP Type:  ISIS       Process Id:  1
  Link[1]:
    ISIS System ID:  0000.0000.0001.00     Opaque LSA ID:  0000.0000.0001.00:00
    Interface IP Address:  10.1.1.1
    Peer  IP Address:  10.1.1.2
    Peer  Router  Id:  2.2.2.9
    Peer  ISIS System ID:  0000.0000.0001.00
    IGP Area:  Level-2
    Link Type:  P2P   Link Status:  Active
    IGP Metric:  10     TE Metric:  10    Color:  0x0
    Bandwidth Allocation Model :  Russian Dolls Model
    Maximum Link-Bandwidth:  100000  (kbps)
    Maximum Reservable Bandwidth:  100000  (kbps)
    Operational Mode of Router :  TE
    Bandwidth Constraints:          Local Overbooking Multiplier:
```

```
   BC[0]:     100000     (kbps)           LOM[0]:          1
BW  Unreserved :
     Class  Id:
     [0]:     100000     (kbps),  [1]:      100000     (kbps)
     [2]:     100000     (kbps),  [3]:      100000     (kbps)
     [4]:     100000     (kbps),  [5]:      100000     (kbps)
     [6]:     100000     (kbps),  [7]:      80000      (kbps)
```

----End

Configuration Files

- Configuration file of LSR A

```
#
 sysname LSRA
#
 mpls lsr-id 1.1.1.9
#
 mpls
  mpls te
  mpls te cspf
  mpls rsvp-te
#
te-class-mapping
isis 1
 is-level level-2
 cost-style wide
 traffic-eng level-2
 network-entity 00.0005.0000.0000.0001.00
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls te bandwidth change thresholds up 20
 mpls te bandwidth change thresholds down 20
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
 isis enable 1
#
interface Tunnel1
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 4.4.4.9
 mpls te bandwidth ct0 20000
#
return
```

- Configuration file of LSR B

```
#
 sysname LSRB
#
 mpls lsr-id 2.2.2.9
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
isis 1
 is-level level-2
 cost-style wide
```

```
 traffic-eng level-2
 network-entity 00.0005.0000.0000.0002.00
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls te
 isis enable 1
 mpls rsvp-te
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 20.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls te bandwidth change thresholds up 20
 mpls te bandwidth change thresholds down 20
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of LSR C

```
#
 sysname LSRC
#
 mpls lsr-id 3.3.3.9
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
isis 1
 is-level level-2
 cost-style wide
 traffic-eng level-2
 network-entity 00.0005.0000.0000.0003.00
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 30.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 isis enable 1
 mpls rsvp-te
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 20.1.1.2 255.255.255.0
 mpls
 mpls te
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
 isis enable 1
#
```

```
return
```

- Configuration file of LSR D

```
#
 sysname LSRD
#
 mpls lsr-id 4.4.4.9
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
isis 1
 is-level level-2
 cost-style wide
 traffic-eng level-2
 network-entity 00.0005.0000.0000.0004.00
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 30.1.1.2 255.255.255.0
 mpls
 mpls te
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 4.4.4.9 255.255.255.255
 isis enable 1
#
return
```

2.16.8 Example for Configuring MPLS TE Manual FRR

Networking Requirements

CAUTION

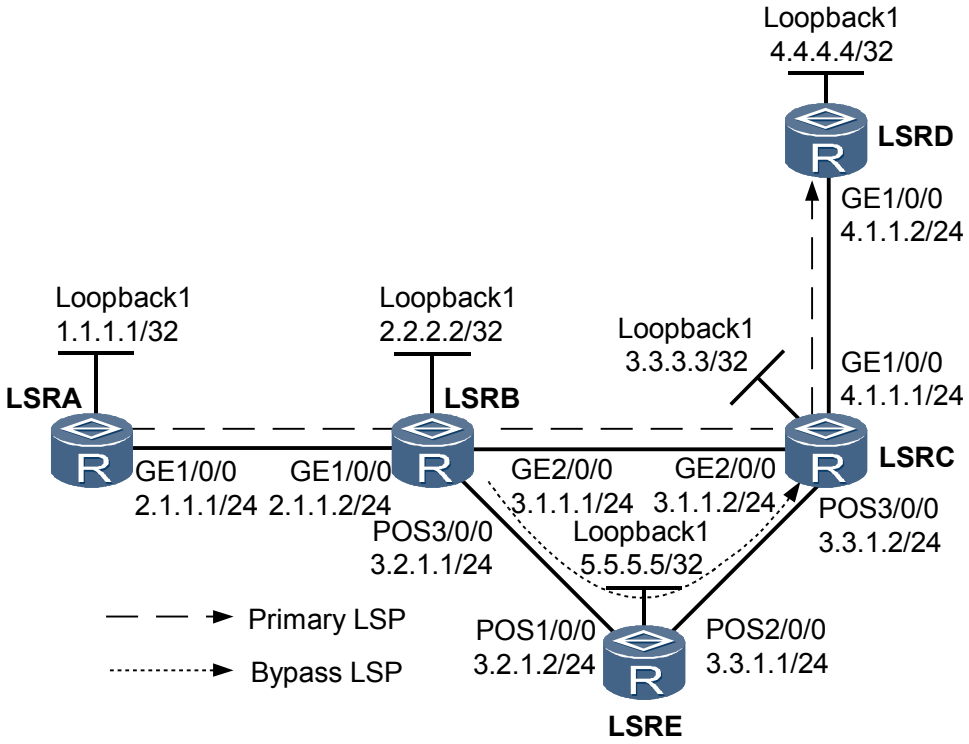
On a single NE5000E, an interface is numbered in the format: slot number/subcard number/interface number. On an NE5000E cluster, an interface is numbered in the format: chassis ID/slot number/subcard number/interface number. The slot number and chassis ID must be specified together.

On the network shown in **Figure 2-18**, a primary tunnel is along the path LSR A -> LSR B -> LSR C -> LSR D. FRR is enabled on LSR B to protect traffic on the link from LSR B to LSR C.

A bypass CR-LSP is established over the path LSR B -> LSR E -> LSR C. LSR B is a PLR and LSR C is an MP.

Explicit paths are used to establish the primary and bypass CR-LSPs. RSVP-TE is used as a signaling protocol.

Figure 2-18 Networking diagram for MPLS TE manual FRR



Configuration Notes

None.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a primary CR-LSP and enable TE FRR on the tunnel interface of the primary CR-LSP.
2. Configure a bypass CR-LSP on the PLR (ingress) and specify the protected bandwidth and the interface of the protected link.

Data Preparation

To complete the configuration, you need the following data:

- Origin AS number, and IS IS level and area ID of every LSR
- Maximum reservable bandwidth and BC bandwidth for every link along the TE tunnel
- Explicit paths for the primary and bypass CR-LSPs
- Tunnel interface number, source and destination IP addresses, ID, and RSVP-TE signaling protocol for each of the primary and bypass CR-LSPs
- Protected bandwidth and type and number of the interface on the protected link

Procedure

Step 1 Assign an IP address and its mask to every interface.

Assign an IP address and its mask to every physical interface and configure a loopback interface address as an LSR ID on every node shown in **Figure 2-18**. The configuration procedure is not provided.

Step 2 Configure an IGP.

Enable IS-IS on all nodes to advertise host routes. The configuration procedure is not provided.

After completing the configurations, run the **display ip routing-table** command on every node. All nodes have learned routes from each other.

Step 3 Configure basic MPLS functions and enable MPLS TE, CSPF, RSVP-TE, and IS-IS TE.

Configure LSR A.

```
[~LSRA] mpls lsr-id 1.1.1.1
[~LSRA] mpls
[~LSRA-mpls] mpls te
[~LSRA-mpls] mpls rsvp-te
[~LSRA-mpls] mpls te cspf
[~LSRA-mpls] quit
[~LSRA] interface gigabitethernet 1/0/0
[~LSRA-GigabitEthernet1/0/0] mpls
[~LSRA-GigabitEthernet1/0/0] mpls te
[~LSRA-GigabitEthernet1/0/0] mpls rsvp-te
[~LSRA-GigabitEthernet1/0/0] quit
[~LSRA] isis
[~LSRA-isis-1] cost-style wide
[~LSRA-isis-1] traffic-eng level-2
[~LSRA-isis-1] commit
```

NOTE

The configurations on LSR B, LSR C, LSR D, and LSR E are similar to those on LSR A. The configuration procedure is not provided. CSPF is enabled only on LSR A and LSR B, which are ingress nodes of the primary and bypass CR-LSPs respectively.

Step 4 Set MPLS TE bandwidth attributes for links.

Set both the maximum reservable bandwidth and BC0 bandwidth to 100 Mbit/s for links on every LSR.

Configure LSR A.

```
[~LSRA] interface gigabitethernet 1/0/0
[~LSRA-GigabitEthernet1/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[~LSRA-GigabitEthernet1/0/0] mpls te bandwidth bc0 100000
[~LSRA-GigabitEthernet1/0/0] commit
[~LSRA-GigabitEthernet1/0/0] quit
```

Configure LSR B.

```
[~LSRB] interface gigabitethernet 2/0/0
[~LSRB-GigabitEthernet2/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[~LSRB-GigabitEthernet2/0/0] mpls te bandwidth bc0 100000
[~LSRB-GigabitEthernet2/0/0] quit
[~LSRB] interface pos 3/0/0
[~LSRB-Pos3/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[~LSRB-Pos3/0/0] mpls te bandwidth bc0 100000
[~LSRB-Pos3/0/0] commit
[~LSRB-Pos3/0/0] quit
```

Configure LSR C.

```
[~LSRC] interface gigabitethernet 1/0/0
[~LSRC-GigabitEthernet1/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[~LSRC-GigabitEthernet1/0/0] mpls te bandwidth bc0 100000
[~LSRC-GigabitEthernet1/0/0] commit
[~LSRC-GigabitEthernet1/0/0] quit
```

Configure LSR E.

```
[~LSRE] interface pos 2/0/0
[~LSRE-Pos2/0/0] mpls te bandwidth max-reservable-bandwidth 100000
[~LSRE-Pos2/0/0] mpls te bandwidth bc0 100000
[~LSRE-Pos2/0/0] commit
[~LSRE-Pos2/0/0] quit
```

Step 5 Configure an MPLS TE tunnel on LSR A.

Configure an explicit path for the primary CR-LSP.

```
[~LSRA] explicit-path pri-path
[~LSRA-explicit-path-pri-path] next hop 2.1.1.2
[~LSRA-explicit-path-pri-path] next hop 3.1.1.2
[~LSRA-explicit-path-pri-path] next hop 4.1.1.2
[~LSRA-explicit-path-pri-path] next hop 4.4.4.4
[~LSRA-explicit-path-pri-path] quit
```

Configure the MPLS TE tunnel for the primary CR-LSP.

```
[~LSRA] interface tunnel 1
[~LSRA-Tunnel1] ip address unnumbered interface loopback 1
[~LSRA-Tunnel1] tunnel-protocol mpls te
[~LSRA-Tunnel1] destination 4.4.4.4
[~LSRA-Tunnel1] mpls te signal-protocol rsvp-te
[~LSRA-Tunnel1] mpls te bandwidth ct0 50000
[~LSRA-Tunnel1] mpls te path explicit-path pri-path
```

Enable FRR.

```
[~LSRA-Tunnel1] mpls te fast-reroute
[~LSRA-Tunnel1] commit
[~LSRA-Tunnel1] quit
```

After completing the configurations, run the **display interface tunnel** command on LSR A. **Tunnel1** is **Up**.

```
[~LSRA] display interface tunnel

Tunnel1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2011-05-31 06:30:58
Description: HUAWEI, Quidway Series, Tunnel1 Interface (ifindex: 20, vr: 0)
Route Port,The Maximum Transmit Unit is 1500
Internet Address is unnumbered, using address of LoopBack0(1.1.1.1/32)
Encapsulation is TUNNEL, loopback not set
Tunnel destination 4.4.4.4
Tunnel up/down statistics 1
Tunnel protocol/transport MPLS/MPLS, ILM is available,
primary tunnel id is 0x321, secondary tunnel id is 0x0
Current system time: 2011-05-31 07:32:31
    0 seconds output rate 0 bits/sec, 0 packets/sec
    0 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets output,  0 bytes
    0 output error
    0 output drop
    Last 300 seconds input utility rate:  0.00%
    Last 300 seconds output utility rate: 0.00%
```

Run the **display mpls te tunnel-interface** command on LSR A. Detailed information about the TE tunnel interface is displayed.

```
[~LSRA] display mpls te tunnel-interface
```

```
Tunnel Name       : Tunnel1
Tunnel State Desc : CR-LSP is Up
Tunnel Attributes   :
Session ID          : 1
Ingress LSR ID      : 1.1.1.1              Egress LSR ID: 4.4.4.4
Admin State         : UP                   Oper State   : UP
Signaling Protocol  : RSVP
FTid                : 1
Tie-Breaking Policy : None                 Metric Type  : None
BypassBW Flag       : Not Supported
BypassBW Type       : -                    Bypass BW    : -
Bfd Cap             : None                 Retry Int    : -
Reopt               : Disabled             Reopt Freq   : -
Auto BW             : Disabled
Current Collected BW: -                    Auto BW Freq : -
Min BW              : -                    Max BW       : -
Tunnel Group        : -
Interfaces Protected: -
Excluded IP Address : -
Is On Radix-Tree    : -                    Referred LSP Count: -
Primary Tunnel      : -                    Pri Tunn Sum : -
Backup Tunnel       : -
Group Status        : -                    Oam Status   : -
IPTN InLabel        : -
BackUp Type         : None                 BestEffort   : Disabled
SRLG Disjoining       : NA
Secondary HopLimit  : -
BestEffort HopLimit : -
Secondary Explicit Path Name: -
Secondary Affinity Prop/Mask: -
BestEffort Affinity Prop/Mask: 0x0/0x0
IsConfigLspConstraint: -

Primary LSP ID      : 1.1.1.1:3
Setup Priority      : 7                    Hold Priority: 7
IncludeAll          : 0x0
IncludeAny          : 0x0
ExcludeAny          : 0x0
Affinity Prop/Mask  : 0x0/0x0              Resv Style   :  SE
Configured Bandwidth Information:
CT0 Bandwidth(Kbit/sec): 50000          CT1 Bandwidth(Kbit/sec): 0
CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
Actual Bandwidth Information:
CT0 Bandwidth(Kbit/sec): 50000          CT1 Bandwidth(Kbit/sec): 0
CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
Explicit Path Name  : pri-path              Hop Limit           : -
Record Route        : Enabled              Record Label : Enabled
Route Pinning       : Disabled
FRR Flag            : Enabled
IdleTime Remain     : -
BFD Status          : -
```

Step 6 Configure a bypass CR-LSP on LSR B.

Configure an explicit path for the bypass CR-LSP.

```
[~LSRB] explicit-path by-path
[~LSRB-explicit-path-by-path] next hop 3.2.1.2
[~LSRB-explicit-path-by-path] next hop 3.3.1.2
[~LSRB-explicit-path-by-path] next hop 3.3.3.3
[~LSRB-explicit-path-by-path] quit
```

Configure the bypass CR-LSP.

```
[~LSRB] interface tunnel 3
[~LSRB-Tunnel3] ip address unnumbered interface loopback 1
```

```
[~LSRB-Tunnel3] tunnel-protocol mpls te
[~LSRB-Tunnel3] destination 3.3.3.3
[~LSRB-Tunnel3] mpls te signal-protocol rsvp-te
[~LSRB-Tunnel3] mpls te path explicit-path by-path
[~LSRB-Tunnel3] mpls te bandwidth ct0 100000
```

Configure the bandwidth protected by the bypass CR-LSP.

```
[~LSRB-Tunnel3] mpls te bypass-tunnel
```

Bind the bypass CR-LSP to the interface of the protected link.

```
[~LSRB-Tunnel3] mpls te protected-interface gigabitethernet 2/0/0
[~LSRB-Tunnel3] commit
[~LSRB-Tunnel3] quit
```

After completing the configuration, run the **display interface tunnel** command on LSR B. The tunnel named **Tunnel3** is **Up**.

Run the **display mpls te tunnel name tunnel1 verbose** command on LSR B. The bypass tunnel is bound to the outbound interface GE 2/0/0 and is not in use.

```
[~LSRB] display mpls te tunnel name Tunnel1 verbose

    No                      :  1
    Tunnel-Name             :  Tunnel1
    TunnelIndex             :  -
    Session ID              :  1           LSP ID            :  4
    Lsr Role                :  Transit
    Ingress LSR ID          :  1.1.1.1
    Egress LSR ID           :  4.4.4.4
    In-Interface            :  GE1/0/0
    Out-Interface           :  GE2/0/0
    Sign-Protocol           :  RSVP TE     Resv Style        :  SE
    IncludeAnyAff           :  0x0         ExcludeAnyAff     :  0x0
    IncludeAllAff           :  0x0
    ER-Hop Table Index      :  -           AR-Hop Table Index:  -
    C-Hop Table Index       :  -
    PrevTunnelIndexInSession:  -           NextTunnelIndexInSession:  -
    PSB Handle              :  -
    Created Time            :  2011/05/31 06:32:22
    --------------------------------
              DS-TE Information
    --------------------------------
    Bandwidth Reserved Flag :  Reserved
    CT0 Bandwidth(Kbit/sec) :  50000       CT1 Bandwidth(Kbit/sec):  0
    CT2 Bandwidth(Kbit/sec) :  0           CT3 Bandwidth(Kbit/sec):  0
    CT4 Bandwidth(Kbit/sec) :  0           CT5 Bandwidth(Kbit/sec):  0
    CT6 Bandwidth(Kbit/sec) :  0           CT7 Bandwidth(Kbit/sec):  0
    Setup-Priority          :  7           Hold-Priority          :  7
    --------------------------------
                FRR Information
    --------------------------------
    Primary LSP Info
    TE Attribute Flag       :  -           Protected Flag    : -
    Bypass In Use           :  Not Used
    Bypass Tunnel Id        :  1
    BypassTunnel          :  Tunnel Index[Tunnel3], InnerLabel[98956]
    Bypass Lsp ID           :  3           FrrNextHop        :  3.3.1.1
    ReferAutoBypassHandle   :  -
    FrrPrevTunnelTableIndex :  -           FrrNextTunnelTableIndex:  -
    Bypass Attribute
    Setup Priority          :  7           Hold Priority     :  7
    HopLimit                :  32          Bandwidth         :  0
    IncludeAnyGroup         :  0           ExcludeAnyGroup   :  0
    IncludeAllGroup         :  0
    Bypass Unbound Bandwidth Info(Kbit/sec)
    CT0 Unbound Bandwidth   :  -         CT1 Unbound Bandwidth:  -
    CT2 Unbound Bandwidth   :  -         CT3 Unbound Bandwidth:  -
```

```
    CT4 Unbound Bandwidth   :  -         CT5 Unbound Bandwidth:  -
    CT6 Unbound Bandwidth   :  -         CT7 Unbound Bandwidth:  -
    ------------------------------
              BFD Information
    ------------------------------
    NextSessionTunnelIndex  :  -           PrevSessionTunnelIndex:  -
    NextLspId               :  -           PrevLspId         :  -
```

Step 7 Verify the configuration.

Shut down the outbound interface of the protected link on the PLR.

```
[~LSRB] interface gigabitethernet 2/0/0
[~LSRB-GigabitEthernet2/0/0] shutdown
[~LSRB-GigabitEthernet2/0/0] commit
```

Run the **display interface tunnel 1** command on LSR A. The tunnel interface of the primary CR-LSP is still **Up**.

Run the **tracert lsp te tunnel1** command on LSR A. The path through which the primary CR-LSP passes is displayed.

```
[~LSRA] tracert lsp te tunnel1
  LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel1 , press CTRL_C to break.
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   2.1.1.2/
  1     2.1.1.2            7       Transit   3.1.1.2/
  2     Request time out
  3     3.3.1.2            4    Transit   4.1.1.2/
  4     4.4.4.4            4    Egress
```

The preceding command output shows that traffic has switched to the bypass CR-LSP.

NOTE

If the **display mpls te tunnel-interface** command is run immediately after FRR switching has been performed, two CR-LSPs are both Up. This is because FRR uses the make-before-break mechanism to establish a bypass CR-LSP. The original CR-LSP will be deleted a period time after a new CR-LSP has been established.

Run the **display mpls te tunnel name Tunnel1 verbose** command on LSR B. The bypass CR-LSP is being used.

```
[~LSRB] display mpls te tunnel name Tunnel1 verbose

    No                      :  1
    Tunnel-Name             :  Tunnel1
    TunnelIndex             :  -
    Session ID              :  1           LSP ID            :  4
    Lsr Role                :  Transit
    Ingress LSR ID          :  1.1.1.1
    Egress LSR ID           :  4.4.4.4
    In-Interface            :  GE1/0/0
    Out-Interface           :  GE2/0/0
    Sign-Protocol           :  RSVP TE     Resv Style        :  SE
    IncludeAnyAff           :  0x0         ExcludeAnyAff     :  0x0
    IncludeAllAff           :  0x0
    ER-Hop Table Index      :  -           AR-Hop Table Index:  -
    C-Hop Table Index       :  -
    PrevTunnelIndexInSession:  -           NextTunnelIndexInSession:  -
    PSB Handle              :  -
    Created Time            :  2011/05/31 06:32:22
    ------------------------------
              DS-TE Information
    ------------------------------
    Bandwidth Reserved Flag :  Reserved
    CT0 Bandwidth(Kbit/sec) :  50000       CT1 Bandwidth(Kbit/sec):  0
    CT2 Bandwidth(Kbit/sec) :  0           CT3 Bandwidth(Kbit/sec):  0
```

```
CT4 Bandwidth(Kbit/sec) :  0           CT5 Bandwidth(Kbit/sec):  0
CT6 Bandwidth(Kbit/sec) :  0           CT7 Bandwidth(Kbit/sec):  0
Setup-Priority          :  7           Hold-Priority          :  7
--------------------------------
            FRR Information
--------------------------------
Primary LSP Info
TE Attribute Flag       :  -           Protected Flag    : -
Bypass In Use           :  In Use
Bypass Tunnel Id        :  1
BypassTunnel            :  Tunnel Index[Tunnel3], InnerLabel[98956]
Bypass Lsp ID           :  3           FrrNextHop        :  3.3.1.1
ReferAutoBypassHandle   :  -
FrrPrevTunnelTableIndex :  -           FrrNextTunnelTableIndex:  -
Bypass Attribute
Setup Priority          :  7           Hold Priority     :  7
HopLimit                :  32          Bandwidth         :  0
IncludeAnyGroup         :  0           ExcludeAnyGroup   :  0
IncludeAllGroup         :  0
Bypass Unbound Bandwidth Info(Kbit/sec)
CT0 Unbound Bandwidth   :  -         CT1 Unbound Bandwidth:  -
CT2 Unbound Bandwidth   :  -         CT3 Unbound Bandwidth:  -
CT4 Unbound Bandwidth   :  -         CT5 Unbound Bandwidth:  -
CT6 Unbound Bandwidth   :  -         CT7 Unbound Bandwidth:  -
--------------------------------
            BFD Information
--------------------------------
NextSessionTunnelIndex  :  -           PrevSessionTunnelIndex:  -
NextLspId               :  -           PrevLspId         :  -
```

Start the outbound interface of the protected link on the PLR.

```
[~LSRB] intrface gigabitethernet 2/0/0
[~LSRB-GigabitEthernet2/0/0] undo shutdown
[~LSRB-GigabitEthernet2/0/0] commit
```

Run the **display interface tunnel 1** command on LSR A. The tunnel interface of the primary CR-LSP is **Up**.

After a period of time, run the **display mpls te tunnel name tunnel1 verbose** command on LSR B. Tunnel1's **Bypass In Use** status is **Not Used**, indicating that traffic has switched back to GE 2/0/0.

----End

Configuration Files

- Configuration file of LSR A

```
#
 sysname LSRA
#
 mpls lsr-id 1.1.1.1
#
 mpls
  mpls te
  mpls te cspf
  mpls rsvp-te
#
 explicit-path pri-path
  next hop 2.1.1.2
  next hop 3.1.1.2
  next hop 4.1.1.2
  next hop 4.4.4.4
#
te-class-mapping
isis 1
 is-level level-2
```

```
 cost-style wide
 traffic-eng level-2
 network-entity 00.0005.0000.0000.0001.00
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 2.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 isis enable 1
#
interface Tunnel1
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 4.4.4.4
mpls te record-route label
 mpls te bandwidth ct0 50000
 mpls te path explicit-path pri-path
mpls te fast-reroute
#
return
```

- Configuration file of LSR B

```
#
 sysname LSRB
#
 mpls lsr-id 2.2.2.2
#
 mpls
  mpls te
  mpls te cspf
  mpls rsvp-te
#
 explicit-path by-path
  next hop 3.2.1.2
  next hop 3.3.1.2
  next hop 3.3.3.3
#
te-class-mapping
isis 1
 is-level level-2
 cost-style wide
 traffic-eng level-2
 network-entity 00.0005.0000.0000.0002.00
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 2.1.1.2 255.255.255.0
 mpls
 mpls te
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 3.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 isis enable 1
 mpls rsvp-te
#
```

```
interface Pos3/0/0
 undo shutdown
 link-protocol ppp
 ip address 3.2.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
#
interface Tunnel3
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te record-route
  mpls te path explicit-path by-path
  mpls te bandwidth ct0 100000
  mpls te bypass-tunnel
 mpls te protected-interface GigabitEthernet 2/0/0
#
return
```

- Configuration file of LSR C

```
#
 sysname LSRC
#
 mpls lsr-id 3.3.3.3
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
isis 1
 is-level level-2
 cost-style wide
 traffic-eng level-2
 network-entity 00.0005.0000.0000.0003.00
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 4.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 3.1.1.2 255.255.255.0
 mpls
 mpls te
 isis enable 1
 mpls rsvp-te
#
interface Pos3/0/0
 undo shutdown
 link-protocol ppp
 ip address 3.3.1.2 255.255.255.0
 mpls
 mpls te
 isis enable 1
 mpls rsvp-te
```

```
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of LSR D

```
#
 sysname LSRD
#
 mpls lsr-id 4.4.4.4
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
isis 1
 is-level level-2
 cost-style wide
 traffic-eng level-2
 network-entity 00.0005.0000.0000.0004.00
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 4.1.1.2 255.255.255.0
 mpls
 mpls te
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of LSR E

```
#
 sysname LSRE
#
 mpls lsr-id 5.5.5.5
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
isis 1
 is-level level-2
 cost-style wide
 traffic-eng level-2
 network-entity 00.0005.0000.0000.0005.00
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 3.2.1.2 255.255.255.0
 mpls
 mpls te
 isis enable 1
 mpls rsvp-te
#
interface Pos2/0/0
 undo shutdown
 link-protocol ppp
 ip address 3.3.1.1 255.255.255.0
 mpls
 mpls te
```

```
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 5.5.5.5 255.255.255.255
 isis enable 1
#
return
```

2.16.9 Example for Configuring MPLS TE Auto FRR

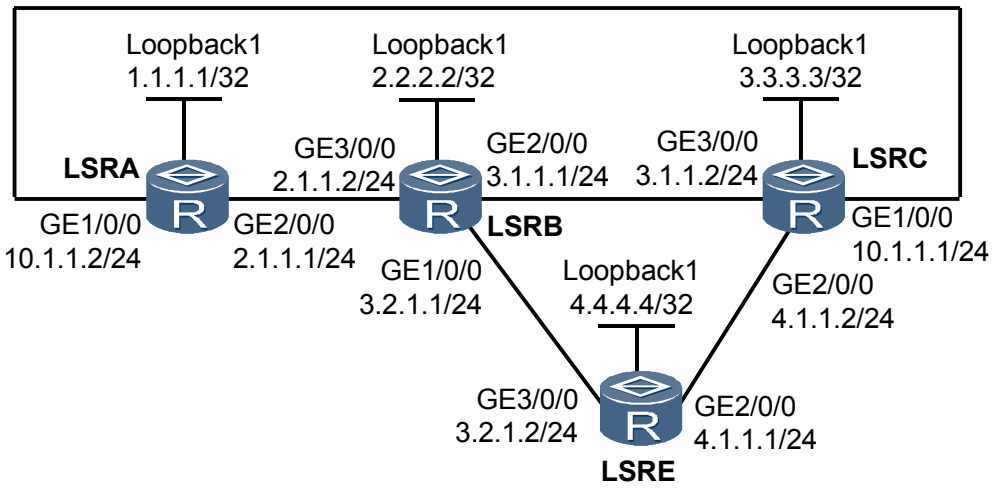
Networking Requirements

CAUTION

On a single NE5000E, an interface is numbered in the format: slot number/subcard number/interface number. On an NE5000E cluster, an interface is numbered in the format: chassis ID/slot number/subcard number/interface number. The slot number and chassis ID must be specified together.

On the network shown in **Figure 2-19**, a primary CR-LSP is established over an explicit path LSR A -> LSR B -> LSR C. Bypass CR-LSPs need to be established on the ingress LSR A and the transit node LSR B respectively. These bypass CR-LSPs are required to provide bandwidth protection.

Figure 2-19 Networking diagram for MPLS TE Auto FRR



Configuration Notes

None.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a primary CR-LSP, and enable MPLS Auto FRR in the MPLS and tunnel interface views.
2. Set the protected bandwidth and priorities for the bypass CR-LSP in the tunnel interface view.

Data Preparation

To complete the configuration, you need the following data:

- OSPF process ID and OSFP area ID for every node
- Maximum reservable bandwidth and BC bandwidth for every link along the TE tunnel
- Path for the primary CR-LSP
- Tunnel interface number, source and destination addresses of the primary tunnel, tunnel ID, RSVP-TE signaling protocol, and tunnel bandwidth

Procedure

Step 1 Assign an IP address and its mask to every interface.

Assign an IP address and its mask to every physical interface and configure a loopback interface address as an LSR ID on every node shown in **Figure 2-19**. The configuration procedure is not provided.

Step 2 Configure OSPF to advertise every network segment route and host route.

Configure OSPF on all nodes to advertise host routes. The configuration procedure is not provided.

After completing the configurations, run the **display ip routing-table** command on every node. All nodes have learned routes from each other.

Step 3 Configure basic MPLS functions and enable MPLS TE, RSVP-TE, and CSPF.

Configure LSR A.

```
[~LSRA] mpls lsr-id 1.1.1.1
[~LSRA] mpls
[~LSRA-mpls] mpls te
[~LSRA-mpls] mpls rsvp-te
[~LSRA-mpls] mpls te cspf
[~LSRA-mpls] quit
[~LSRA] interface gigabitethernet 2/0/0
[~LSRA-GigabitEthernet2/0/0] mpls
[~LSRA-GigabitEthernet2/0/0] mpls te
[~LSRA-GigabitEthernet2/0/0] mpls rsvp-te
[~LSRA-GigabitEthernet2/0/0] quit
[~LSRA] interface gigabitethernet 1/0/0
[~LSRA-GigabitEthernet1/0/0] mpls
[~LSRA-GigabitEthernet1/0/0] mpls te
[~LSRA-GigabitEthernet1/0/0] mpls rsvp-te
[~LSRA-GigabitEthernet1/0/0] commit
[~LSRA-GigabitEthernet1/0/0] quit
```

NOTE

The configurations on LSR B, LSR C, and LSR D are similar to those on LSR A. The configuration procedure is not provided.

Step 4 Configure OSPF TE.

Configure LSR A.

```
[~LSRA] ospf
[~LSRA-ospf-1] opaque-capability enable
[~LSRA-ospf-1] area 0
[~LSRA-ospf-1-area-0.0.0.0] mpls-te enable
[~LSRA-ospf-1-area-0.0.0.0] commit
[~LSRA-ospf-1-area-0.0.0.0] quit
[~LSRA-ospf-1] quit
```

Configure LSR B.

```
[~LSRB] ospf
[~LSRB-ospf-1] opaque-capability enable
[~LSRB-ospf-1] area 0
[~LSRB-ospf-1-area-0.0.0.0] mpls-te enable
[~LSRB-ospf-1-area-0.0.0.0] commit
[~LSRB-ospf-1-area-0.0.0.0] quit
[~LSRB-ospf-1] quit
```

Configure LSR C.

```
[~LSRC] ospf
[~LSRC-ospf-1] opaque-capability enable
[~LSRC-ospf-1] area 0
[~LSRC-ospf-1-area-0.0.0.0] mpls-te enable
[~LSRC-ospf-1-area-0.0.0.0] commit
[~LSRC-ospf-1-area-0.0.0.0] quit
[~LSRC-ospf-1] quit
```

Configure LSR D.

```
[~LSRD] ospf
[~LSRD-ospf-1] opaque-capability enable
[~LSRD-ospf-1] area 0
[~LSRD-ospf-1-area-0.0.0.0] mpls-te enable
[~LSRD-ospf-1-area-0.0.0.0] commit
[~LSRD-ospf-1-area-0.0.0.0] quit
[~LSRD-ospf-1] quit
```

Step 5 Configure MPLS TE attributes for links.

Set the maximum reservable bandwidth and BC0 bandwidth both to 10 Mbit/s and the BC1 bandwidth to 3 Mbit/s.

Configure LSR A.

```
[~LSRA] interface gigabitethernet 2/0/0
[~LSRA-GigabitEthernet2/0/0] mpls te bandwidth max-reservable-bandwidth 10000
[~LSRA-GigabitEthernet2/0/0] mpls te bandwidth bc0 10000 bc1 3000
[~LSRA-GigabitEthernet2/0/0] commit
[~LSRA-GigabitEthernet2/0/0] quit
```

The configurations on LSR B, LSR C, and LSR D are similar to those on LSR A. The configuration procedure is not provided.

Step 6 Configure an explicit path for the primary CR-LSP.

```
[~LSRA] explicit-path master
[~LSRA-explicit-path-master] next hop 2.1.1.2
[~LSRA-explicit-path-master] next hop 3.1.1.2
[~LSRA-explicit-path-master] commit
```

```
[~LSRA-explicit-path-master] quit
```

Step 7 Configure TE Auto FRR.

Configure LSR A.

```
[~LSRA] mpls
[~LSRA-mpls] mpls te auto-frr
[~LSRA-mpls] commit
[~LSRA-mpls] quit
```

Configure LSR B.

```
[~LSRB] mpls
[~LSRB-mpls] mpls te auto-frr
[~LSRB-mpls] commit
[~LSRB-mpls] quit
```

Step 8 Configure a primary tunnel.

```
[~LSRA] interface tunnel2
[~LSRA-Tunnel2] ip address unnumbered interface loopback1
[~LSRA-Tunnel2] tunnel-protocol mpls te
[~LSRA-Tunnel2] destination 3.3.3.3
[~LSRA-Tunnel2] mpls te record-route label
[~LSRA-Tunnel2] mpls te path explicit-path master
[~LSRA-Tunnel2] mpls te bandwidth ct0 400
[~LSRA-Tunnel2] mpls te priority 4 3
[~LSRA-Tunnel2] mpls te fast-reroute bandwidth
[~LSRA-Tunnel2] mpls te bypass-attributes bandwidth 200 priority 5 4
[~LSRA-Tunnel2] commit
[~LSRA-Tunnel2] quit
```

Step 9 Verify the configuration.

Run the **display mpls te tunnel name tunnel2 verbose** command on LSR A. Information about the primary and bypass CR-LSPs is displayed.

```
[~LSRA] display mpls te tunnel name Tunnel2 verbose
    No                      :  1
    Tunnel-Name             :  Tunnel2
    TunnelIndex             :  1           LSP Index         :  3072
    Session ID              :  200         LSP ID            :  1
    Lsr Role                :  Ingress
    Ingress LSR ID          :  1.1.1.1
    Egress LSR ID           :  3.3.3.3
    In-Interface            :  -
    Out-Interface           :  GE2/0/0
    Sign-Protocol           :  RSVP TE     Resv Style        :  SE
    IncludeAnyAff           :  0x0         ExcludeAnyAff     :  0x0
    IncludeAllAff           :  0x0
    ER-Hop Table Index      :  -           AR-Hop Table Index:  2
    C-Hop Table Index       :  -
    PrevTunnelIndexInSession:  -           NextTunnelIndexInSession:  -
    PSB Handle              :  65546
    Created Time            :  2009/03/30 09:52:03
    --------------------------------
              DS-TE Information
    --------------------------------
    Bandwidth Reserved Flag :  Reserved
    CT0 Bandwidth(Kbit/sec) :  10000       CT1 Bandwidth(Kbit/sec):  0
    CT2 Bandwidth(Kbit/sec) :  0           CT3 Bandwidth(Kbit/sec):  0
    CT4 Bandwidth(Kbit/sec) :  0           CT5 Bandwidth(Kbit/sec):  0
    CT6 Bandwidth(Kbit/sec) :  0           CT7 Bandwidth(Kbit/sec):  0
    Setup-Priority          :  7           Hold-Priority     :  7
    --------------------------------
                FRR Information
    --------------------------------
    Primary LSP Info
    TE Attribute Flag       :  0x63        Protected Flag    :  0x1
```

```
    Bypass In Use           :  Not Used
    Bypass Tunnel Id        :  67141670
    BypassTunnel            :  Tunnel Index[AutoTunnel2], InnerLabel[3]
    Bypass Lsp ID           :  -           FrrNextHop        :  3.3.3.3
    ReferAutoBypassHandle   :  2049
    FrrPrevTunnelTableIndex :  -           FrrNextTunnelTableIndex:  -
    Bypass Attribute(Not configured)
    Setup Priority          :  -           Hold Priority     :  -
    HopLimit                :  -           Bandwidth         :  -
    IncludeAnyGroup         :  -           ExcludeAnyGroup   :  -
    IncludeAllGroup         :  -
    Bypass Unbound Bandwidth Info(Kbit/sec)
    CT0 Unbound Bandwidth   :  -         CT1 Unbound Bandwidth:  -
    CT2 Unbound Bandwidth   :  -         CT3 Unbound Bandwidth:  -
    CT4 Unbound Bandwidth   :  -         CT5 Unbound Bandwidth:  -
    CT6 Unbound Bandwidth   :  -         CT7 Unbound Bandwidth:  -
    --------------------------------
              BFD Information
    --------------------------------
    NextSessionTunnelIndex  :  -           PrevSessionTunnelIndex:  -
    NextLspId               :  -           PrevLspId         :  -
```

The primary CR-LSP has been bound to a bypass CR-LSP named **AutoTunnel2**.

Run the **display mpls te tunnel-interface auto-bypass-tunnel** command. Detailed information about the automatic bypass CR-LSP is displayed. Its bandwidth, and setup and holding priorities are the same as bypass attributes displayed in the primary CR-LSP information.

```
[~LSRA] display mpls te tunnel-interface auto-bypass-tunnel AutoTunnel2
    Tunnel Name          :  AutoTunnel2
    Tunnel State Desc    :  CR-LSP is Up
    Tunnel Attributes    :
    Session ID           :2049
    Ingress LSR ID       :  1.1.1.1              Egress LSR ID:  3.3.3.3
    Admin State          :  UP                   Oper State   :  UP
    Signaling Protocol   :  RSVP
    FTid                 : 2
    Tie-Breaking Policy  :  None                 Metric Type  :  None
    BypassBW Flag        :  Not Supported
    BypassBW Type        :  -                    Bypass BW    :
    Bfd Cap      : None                          Retry Int    : -
    Reopt                : Disabled              Reopt Freq   : -
    Auto BW              : Disabled
    Current Collected BW: -                      Auto BW Freq : -
    Min BW               : -                     Max BW       : -
    Tunnel Group         : -
    Interfaces Protected: -:  GE2/0/0
    Excluded IP Address :
                           2.1.1.1
                           2.2.2.2
                           3.1.1.2
    Is On Radix-Tree     :  Yes                  Referred LSP Count:  1
    Primary Tunnel       :  -                    Pri Tunn Sum :  -
    Backup Tunnel        :  -
    Group Status         :  Up                   Oam Status   :  Up
    IPTN InLabel         :  -
    BackUp Type          :  None                 BestEffort   :  Disabled
    SRLG Disjoining: NA
    Secondary HopLimit   :  -
    BestEffort HopLimit  :  -
    Secondary Explicit Path Name:  -
    Secondary Affinity Prop/Mask:  0x0/0x0
    BestEffort Affinity Prop/Mask:  0x0/0x0
    IsConfigLspConstraint: -

    Primary LSP ID       :  1.1.1.1:3
    Setup Priority       :  5                    Hold Priority:  4
    IncludeAll           :  0x0
    IncludeAny           :  0x0
```

```
  ExcludeAny          :  0x0
  Affinity Prop/Mask  : 0x0/0x0              Resv Style   :  SE
  Configured Bandwidth Information:
  CT0 Bandwidth(Kbit/sec): 200          CT1 Bandwidth(Kbit/sec): 0
  CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
  CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
  CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
  Actual Bandwidth Information:
  CT0 Bandwidth(Kbit/sec): 200           CT1 Bandwidth(Kbit/sec): 0
  CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
  CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
  CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
  Explicit Path Name  :  -                    Hop Limit    : -
  Record Route        :  Enabled              Record Label :  Disabled
  Route Pinning       :  Disabled
  FRR Flag            :  -
  IdleTime Remain     :  -
  BFD Status          :  -
```

The automatic bypass CR-LSP protects traffic on GE 2/0/0, the outbound interface of the primary CR-LSP, not other three interfaces. The bandwidth is 200 kbit/s, and the setup and holding priority values are 5 and 4 respectively.

Run the **display mpls te tunnel path** command on LSR A. The bypass CR-LSP is providing node and bandwidth protection for the primary CR-LSP.

```
[~LSRA] display mpls te tunnel path
Tunnel Interface Name : Tunnel2
 Lsp ID : 1.1.1.1 :200:1
 Hop Information
  Hop 1   2.1.1.1 Local-Protection available | bandwidth | node
  Hop 2   2.1.1.2  Label 106497
  Hop 3   2.2.2.2
  Hop 4   3.1.1.1 Local-Protection available | bandwidth
  Hop 5   3.1.1.2  Label 3
  Hop 6   3.3.3.3
 Tunnel Interface Name : AutoTunnel2
 Lsp ID : 1.1.1.1 :2 :2
 Hop Information
  Hop 1   10.1.1.2
  Hop 2   10.1.1.1
  Hop 3   3.3.3.3

 Tunnel Interface Name : AutoTunnel33
 Lsp ID : 2.2.2.2 :33 :209
 Hop Information
  Hop 1   2.2.2.2
  Hop 2   2.1.1.2
  Hop 3   2.1.1.1
  Hop 4   1.1.1.1
  Hop 5   10.1.1.2
  Hop 6   10.1.1.1
  Hop 7   3.3.3.3
```

----End

Configuration Files

- Configuration file of LSR A

```
#
 sysname LSR A
#
 mpls lsr-id 1.1.1.1
#
 mpls
  mpls te
  mpls te auto-frr
```

```
  mpls te cspf
  mpls rsvp-te
#
 explicit-path master
  next hop 2.1.1.2
  next hop 3.1.1.2
#
te-class-mapping
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  mpls-te enable
  network 10.1.1.0 0.0.0.255
  network 2.1.1.0 0.0.0.255
  network 1.1.1.1 0.0.0.0
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 10000
 mpls te bandwidth bc0 10000 bc1 3000
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 2.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 10000
 mpls te bandwidth bc0 10000 bc1 3000
 mpls rsvp-te
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
interface Tunnel2
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te record-route label
 mpls te priority 4 3
 mpls te bandwidth ct0 400
 mpls te path explicit-path master
 mpls te fast-reroute bandwidth
 mpls te bypass-attributes bandwidth 200 priority 5 4
#
return
```

- Configuration file of LSR B

```
#
 sysname LSRB
#
 mpls lsr-id 2.2.2.2
#
 mpls
  mpls te
  mpls te auto-frr
  mpls te cspf
  mpls rsvp-te
#
te-class-mapping
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  mpls-te enable
  network 3.1.1.0 0.0.0.255
```

```
  network 3.2.1.0 0.0.0.255
  network 2.1.1.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 3.2.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 10000
 mpls te bandwidth bc0 10000 bc1 3000
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 3.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 10000
 mpls te bandwidth bc0 10000 bc1 3000
 mpls rsvp-te
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 2.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
return
```

- Configuration file of LSR C

```
#
 sysname LSRC
#
 mpls lsr-id 3.3.3.3
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  mpls-te enable
  network 10.1.1.0 0.0.0.255
  network 3.1.1.0 0.0.0.255
  network 4.1.1.0 0.0.0.255
  network 3.3.3.3 0.0.0.0
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 4.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet3/0/0
```

```
 undo shutdown
 ip address 3.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
return
```

- Configuration file of LSR D

```
#
 sysname LSRD
#
 mpls lsr-id 4.4.4.4
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  mpls-te enable
  network 3.2.1.0 0.0.0.255
  network 4.1.1.0 0.0.0.255
  network 4.4.4.4 0.0.0.0
#
interface GigabitEthernet2/0/0
 undo shutdown
 mpls
 ip address 4.1.1.1 255.255.255.0
 mpls te
 mpls te bandwidth max-reservable-bandwidth 10000
 mpls te bandwidth bc0 10000 bc1 3000
 mpls rsvp-te
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 3.2.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
#
Return
```

2.16.10 Example for Configure a Hot-standby CR-LSP

Networking Requirements

CAUTION

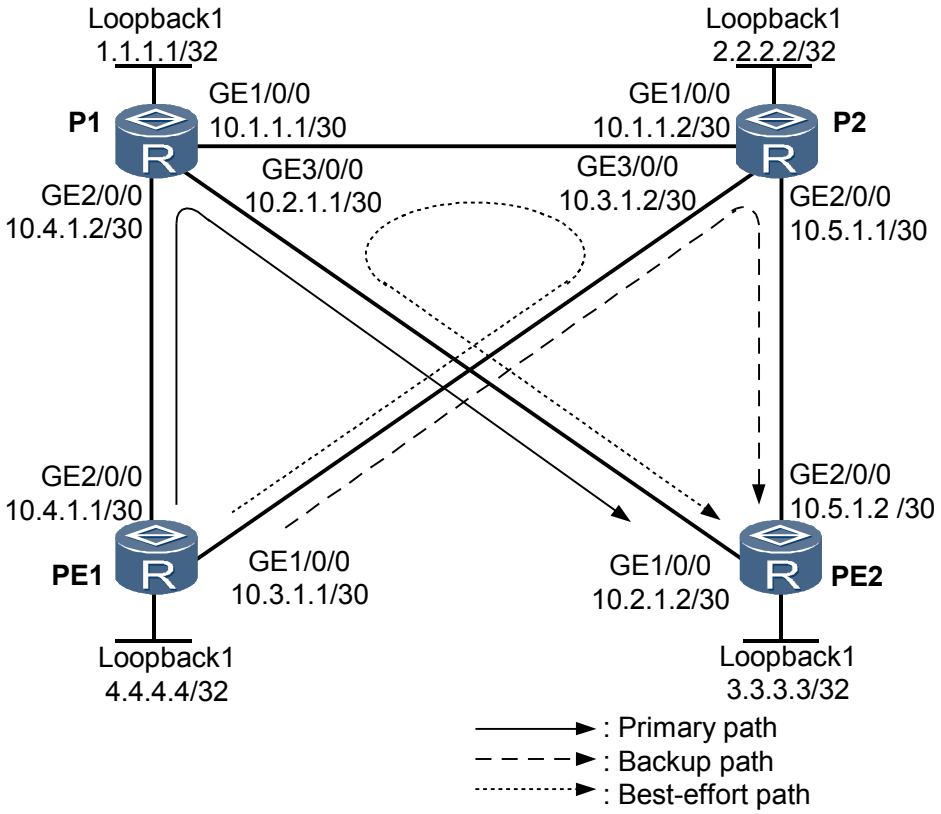
On a single NE5000E, an interface is numbered in the format: slot number/subcard number/interface number. On an NE5000E cluster, an interface is numbered in the format: chassis ID/slot number/subcard number/interface number. The slot number and chassis ID must be specified together.

Figure 2-20 shows an MPLS VPN network. A TE tunnel is established from PE1 to PE2. A hot-standby CR-LSP and a best-effort path are configured. The networking is as follows:

- The primary CR-LSP is along the path PE1 -> P1 -> PE2.
- The hot-standby CR-LSP is along the path PE1 -> P2 -> PE2.
- The best-effort path PE1 -> P2 -> P1 -> PE2 is set up.

If the primary CR-LSP fails, traffic switches to the hot-standby CR-LSP. If the primary CR-LSP recovers, traffic will switch back to the primary CR-LSP 15 seconds later. If both the primary and hot-standby CR-LSPs fail, a best-effort path is established and takes over traffic.

Figure 2-20 Networking diagram of a hot-standby CR-LSP



Configuration Notes

None.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an IP address to every interface and an IGP, ensuring connectivity.
2. Configure basic MPLS and MPLS TE functions.
3. Configure explicit paths on PE1 for the primary and hot-standby CR-LSPs.

4. Create a tunnel destined for PE2; specify explicit paths; enable hot standby; configure a best-effort path; set the switchback delay time to 15 seconds on PE1.

Data Preparation

To complete the configuration, you need the following data:

- IGP type and data
- MPLS LSR IDs
- Bandwidth attributes
- Tunnel interface number and bandwidth
- Explicit paths for the primary and hot-standby CR-LSPs

Procedure

Step 1 Assign an IP address and its mask to every interface.

Assign an IP address and its mask every interface and configure a loopback interface address as an LSR ID on every node. Detailed configuration information is provided in the following configuration files.

Step 2 Configure an IGP.

Configure OSPF or IS-IS on every node, ensuring connectivity between the nodes. IS-IS is used in this example. Detailed configuration information is provided in the following configuration files.

Step 3 Configure basic MPLS functions.

Set an LSR ID in the system view, and enable MPLS in the system and interface views on every node. Detailed configuration information is provided in the following configuration files.

Step 4 Configure basic MPLS functions.

Enable MPLS TE and RSVP-TE in the MPLS and interface views on every node. Set the maximum reservable bandwidth and BC0 bandwidth both to 100 Mbit/s and BC1 bandwidth to 50 Mbit/s. Detailed configuration information is provided in the following configuration files.

Step 5 Configure IS-IS TE and CSPF.

Configure IS-IS TE on all nodes and enable CSPF on PE1. For information about the configuration procedure, see **Configuring an RSVP-TE Tunnel**.

Step 6 Configure explicit paths for the primary and hot-standby CR-LSPs.

Configure an explicit path for the primary CR-LSP on PE1.

```
<PE1> system-view
[~PE1] explicit-path main
[~PE1-explicit-path-main] next hop 10.4.1.2
[~PE1-explicit-path-main] next hop 10.2.1.2
[~PE1-explicit-path-main] next hop 3.3.3.3
[~PE1-explicit-path-main] quit
```

Configure an explicit path for the hot-standby CR-LSP on PE1.

```
[~PE1] explicit-path backup
[~PE1-explicit-path-backup] next hop 10.3.1.2
[~PE1-explicit-path-backup] next hop 10.5.1.2
[~PE1-explicit-path-backup] next hop 3.3.3.3
```

```
[~PE1-explicit-path-backup] commit
[~PE1-explicit-path-backup] quit
```

After completing the configurations, run the **display explicit-path main** command on PE1. Information about the explicit paths for the primary and hot-standby CR-LSPs is displayed.

```
[~PE1] display explicit-path main
Path Name : main        Path Status : Enabled
 1      10.4.1.2          Strict      Include
 2      10.2.1.2          Strict      Include
 3      3.3.3.3           Strict      Include
[~PE1] display explicit-path backup
Path Name : backup      Path Status : Enabled
 1      10.3.1.2          Strict      Include
 2      10.5.1.2          Strict      Include
 3      3.3.3.3           Strict      Include
```

Step 7 Configure tunnel interfaces.

Create a tunnel interface; specify an explicit path; set the tunnel bandwidth to 10 Mbit/s on PE1.

```
[~PE1] interface tunnel 1
[~PE1-Tunnel1] ip address unnumbered interface loopback 1
[~PE1-Tunnel1] tunnel-protocol mpls te
[~PE1-Tunnel1] destination 3.3.3.3
[~PE1-Tunnel1] mpls te path explicit-path main
[~PE1-Tunnel1] mpls te bandwidth ct0 10000
```

Configure hot standby on the tunnel interface; set the switchback delay time to 15 seconds; specify an explicit path; configure a best-effort path.

```
[~PE1-Tunnel1] mpls te backup hot-standby wtr 15
[~PE1-Tunnel1] mpls te path explicit-path backup secondary
[~PE1-Tunnel1] mpls te backup ordinary best-effort
[~PE1-Tunnel1] commit
[~PE1-Tunnel1] quit
```

After completing the configurations, run the **display mpls te tunnel-interface tunnel1** command on PE1. Both the primary and hot-standby CR-LSPs have been established.

```
[~PE1] display mpls te tunnel-interface tunnel1

    Tunnel Name       : Tunnel1
    Tunnel State Desc : Primary CR-LSP Up and HotBackup CR-LSP Up
    Tunnel Attributes   :
    Session ID          : 502
    Ingress LSR ID      : 4.4.4.4               Egress LSR ID: 3.3.3.3
    Admin State         : UP                    Oper State   : UP
    Signaling Protocol  : RSVP
    FTid                : 502
    Tie-Breaking Policy : RANDOM                Metric Type : None
    BypassBW Flag       : Not Supported
    BypassBW Type       : -                     Bypass BW    : -
    Bfd Cap      : None                         Retry Int    :
-
    Reopt               : Disabled              Reopt Freq   : -
    Auto BW             : Disabled
    Current Collected BW: -                     Auto BW Freq : -
    Min BW              : -                     Max BW       : -
    Tunnel Group       : -
    Interfaces Protected: -
    Excluded IP Address : -
    Is On Radix-Tree    : -                     Referred LSP Count: -
    Primary Tunnel      : -                     Pri Tunn Sum : -
    Backup Tunnel       : -
    Group Status        : -                     Oam Status   : -
    IPTN InLabel        : -
    BackUp Type         : HotStandby            BestEffort  : Enabled
```

```
    SRLG Disjoining: NA
    Secondary HopLimit : -
    BestEffort HopLimit : -
    Secondary Explicit Path Name: -
    Secondary Affinity Prop/Mask: -
    BestEffort Affinity Prop/Mask: 0x0/0x0
    IsConfigLspConstraint: -

    Primary LSP ID      :  4.4.4.4:503
    Setup Priority      :  7                    Hold Priority:  7
    IncludeAll          :  0x0
    IncludeAny          :  0x0
    ExcludeAny          :  0x0
    Affinity Prop/Mask  : 0x0/0x0              Resv Style   :  SE
    Configured Bandwidth Information:
    CT0 Bandwidth(Kbit/sec): 10000          CT1 Bandwidth(Kbit/sec): 0
    CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
    CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
    CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
    Actual Bandwidth Information:
    CT0 Bandwidth(Kbit/sec): 10000          CT1 Bandwidth(Kbit/sec): 0
    CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
    CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
    CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
    Explicit Path Name  : main                 Hop Limit    : -
    Record Route        :  Enabled             Record Label :  Disabled
    Route Pinning       :  Disabled
    FRR Flag            :  Disabled
    IdleTime Remain     :  -
    BFD Status          :  -

    Backup LSP ID       :  4.4.4.4:504
    IsBestEffortPath       : No
    Setup Priority      :  7                    Hold Priority:  7
    IncludeAll          :  0x0
    IncludeAny          :  0x0
    ExcludeAny          :  0x0
    Affinity Prop/Mask  : 0x0/0x0              Resv Style   :  SE
    Configured Bandwidth Information:
    CT0 Bandwidth(Kbit/sec): 10000          CT1 Bandwidth(Kbit/sec): 0
    CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
    CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
    CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
    Actual Bandwidth Information:
    CT0 Bandwidth(Kbit/sec): 10000          CT1 Bandwidth(Kbit/sec): 0
    CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
    CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
    CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
    Explicit Path Name  : backup               Hop Limit           : -
    Record Route        :  Enabled             Record Label :  Disabled
    Route Pinning       :  Disabled
    FRR Flag            :  Disabled
    IdleTime Remain     :  -
    BFD Status          :  -
```

Run the **display mpls te hot-standby state** command on PE1. Hot standby information is displayed.

```
[~PE1] display mpls te hot-standby state interface tunnel1
------------------------------------------------------------------
Verbose information about the Tunnel1 hot-standby state
------------------------------------------------------------------
    Tunnel Name           : Tunnel1
    Session ID            : 502
    Main LSP token        : 503
    Hot-standby LSP token : 504
    HSB switch result     : main LSP
    WTR                   : -
```

Run the **ping lsp te** command. The hot-standby CR-LSP is reachable.

```
[~PE1] ping lsp te tunnel1 hot-standby
  LSP PING FEC: RSVP IPV4 SESSION QUERY Tunnel1 : 100  data bytes, press CTR
L_C to break
  Reply from 3.3.3.3: bytes=100 Sequence=1 time = 4 ms
  Reply from 3.3.3.3: bytes=100 Sequence=2 time = 3 ms
  Reply from 3.3.3.3: bytes=100 Sequence=3 time = 3 ms
  Reply from 3.3.3.3: bytes=100 Sequence=4 time = 3 ms
  Reply from 3.3.3.3: bytes=100 Sequence=5 time = 6 ms
  --- FEC: RSVP IPV4 SESSION QUERY Tunnel1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/6 ms
```

Run the **tracert lsp te** command on PE1. The path for the hot-standby CR-LSP is reachable.

```
[~PE1] tracert lsp te tunnel1 hot-standby
  LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel1 , press CTRL_C to
break.
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   10.3.1.2/[13313 ]
  1     10.3.1.2           90 ms   Transit   10.5.1.2/[3 ]
  2     3.3.3.3            130 ms  Egress
```

Step 8 Verify the configuration.

Connect Port1 and Port2 on a tester to PE1 and PE2 respectively; set correct labels; send MPLS traffic from Port1 to Port2. If the cable is removed from GE 2/0/0 on PE1 or P1, traffic is restored in milliseconds. Run the **display mpls te hot-standby state interface tunnel1** command on PE1. Traffic has switched to the hot-standby CR-LSP.

```
[~PE1] display mpls te hot-standby state interface tunnel1
------------------------------------------------------------------
Verbose information about the Tunnel1 hot-standby state
------------------------------------------------------------------
tunnel name                              : Tunnel1
session id                               : 100
main LSP token                           : 0x0
hot-standby LSP token                    : 0x100201b
HSB switch result                        : hot-standby LSP
WTR                                      : 15s
```

Insert the cable into GE 2/0/0 and wait 15 seconds. Traffic switches back to the primary CR-LSP.

If the cables to GE 2/0/0 on PE1 (or P1) and PE2 (or P2) are removed, the tunnel interface goes Down and then Up. A best-effort path is established and takes over traffic.

```
[~PE1] display mpls te tunnel-interface tunnel1
    Tunnel Name       : Tunnel1
    Tunnel State Desc : Backup CR-LSP In use and Primary CR-LSP setting Up
    Tunnel Attributes   :
    Session ID          : 502
    Ingress LSR ID      : 4.4.4.4              Egress LSR ID: 3.3.3.3
    Admin State         : UP                   Oper State   : UP
    Signaling Protocol  : RSVP
    FTid                : 502
    Tie-Breaking Policy : RANDOM               Metric Type : None
     BypassBW Flag       : Not Supported
    BypassBW Type       : -                    Bypass BW    : -
    Bfd Cap      : None                        Retry Int    :
-
    Reopt               : Disabled             Reopt Freq   : -
    Auto BW             : Disabled
    Current Collected BW: -                    Auto BW Freq : -
    Min BW              : -                    Max BW       : -
    Tunnel Group       : -
    Interfaces Protected: -
    Excluded IP Address : -
```

```
    Is On Radix-Tree    : -                     Referred LSP Count: -
    Primary Tunnel      : -                     Pri Tunn Sum : -
    Backup Tunnel       : -
    Group Status        : -                     Oam Status   : -
    IPTN InLabel        : -
    BackUp Type         : HotStandby            BestEffort  : Enabled
    SRLG Disjoining: NA
    Secondary HopLimit : -
    BestEffort HopLimit : -
    Secondary Explicit Path Name: -
    Secondary Affinity Prop/Mask: -
    BestEffort Affinity Prop/Mask: 0x0/0x0
    IsConfigLspConstraint: -

    Primary LSP ID      :  4.4.4.4:503
    Setup Priority      :  7                     Hold Priority:  7
    IncludeAll          :  0x0
    IncludeAny          :  0x0
    ExcludeAny          :  0x0
    Affinity Prop/Mask  : 0x0/0x0               Resv Style   :  SE
    Configured Bandwidth Information:
    CT0 Bandwidth(Kbit/sec): 10000          CT1 Bandwidth(Kbit/sec): 0
    CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
    CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
    CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
    Actual Bandwidth Information:
    CT0 Bandwidth(Kbit/sec): 10000          CT1 Bandwidth(Kbit/sec): 0
    CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
    CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
    CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
    Explicit Path Name  : main                 Hop Limit    : -
    Record Route        :  Enabled             Record Label :  Disabled
    Route Pinning       :  Disabled
    FRR Flag            :  Disabled
    IdleTime Remain     :  -
    BFD Status          :  -

    Backup LSP ID       :  4.4.4.4:504
    IsBestEffortPath    : No
    Setup Priority      :  7                     Hold Priority:  7
    IncludeAll          :  0x0
    IncludeAny          :  0x0
    ExcludeAny          :  0x0
    Affinity Prop/Mask  : 0x0/0x0               Resv Style   :  SE
    Configured Bandwidth Information:
    CT0 Bandwidth(Kbit/sec): 10000          CT1 Bandwidth(Kbit/sec): 0
    CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
    CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
    CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
    Actual Bandwidth Information:
    CT0 Bandwidth(Kbit/sec): 10000          CT1 Bandwidth(Kbit/sec): 0
    CT2 Bandwidth(Kbit/sec): 0              CT3 Bandwidth(Kbit/sec): 0
    CT4 Bandwidth(Kbit/sec): 0              CT5 Bandwidth(Kbit/sec): 0
    CT6 Bandwidth(Kbit/sec): 0              CT7 Bandwidth(Kbit/sec): 0
    Explicit Path Name  : backup                Hop Limit    : -
    Record Route        :  Enabled             Record Label :  Disabled
    Route Pinning       :  Disabled
    FRR Flag            :  Disabled
    IdleTime Remain     :  -
    BFD Status          :  -
[~PE1] display mpls te tunnel path
 Tunnel Interface Name : Tunnel1
 Lsp ID : 4.4.4.4 :100 :32776
 Hop Information
  Hop 0   10.3.1.1
  Hop 1   10.3.1.2
  Hop 2   2.2.2.2
  Hop 3   10.1.1.2
  Hop 4   10.1.1.1
```

```
Hop 5   1.1.1.1
Hop 6   10.2.1.1
Hop 7   10.2.1.2
Hop 8   3.3.3.3
```

----End

Configuration Files

- Configuration file of PE1

```
#
 sysname PE1
#
 mpls lsr-id 4.4.4.4
#
 mpls
  mpls te
  mpls te cspf
  mpls rsvp-te
#
 explicit-path backup
  next hop 10.3.1.2
  next hop 10.5.1.2
  next hop 3.3.3.3
#
 explicit-path main
  next hop 10.4.1.2
  next hop 10.2.1.2
  next hop 3.3.3.3
#
te-class-mapping
isis 1
 cost-style wide
 traffic-eng level-1-2
 network-entity 10.0000.0000.0004.00
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.3.1.1 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.4.1.1 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 isis enable 1
#
interface Tunnel1
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls
te
 destination
3.3.3.3
 mpls te record-
route
```

```
 mpls te bandwidth ct0
10000
 mpls te backup hot-
standby
 mpls te backup ordinary best-
effort
 mpls te path explicit-path
main
 mpls te path explicit-path backup
secondary
#
return
```

- Configuration file of P1

```
#
 sysname P1
#
 mpls lsr-id 1.1.1.1
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
isis 1
 cost-style wide
 traffic-eng level-1-2
 network-entity 10.0000.0000.0001.00
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.1 255.255.255.252
 mpls
 mpls te
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.4.1.2 255.255.255.252
 mpls
 mpls te
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 10.2.1.1 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 isis enable 1
 ip address 1.1.1.1 255.255.255.255
#
return
```

- Configuration file of P2

```
#
 sysname P2
#
 mpls lsr-id 2.2.2.2
#
 mpls
  mpls te
  mpls rsvp-te
```

```
#
te-class-mapping
isis 1
 cost-style wide
 traffic-eng level-1-2
 network-entity 10.0000.0000.0002.00
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.1.2 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.5.1.1 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet3/0/0
 undo shutdown
 ip address 10.3.1.2 255.255.255.252
 mpls
 mpls te
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
 mpls lsr-id 3.3.3.3
#
 mpls
  mpls te
  mpls rsvp-te
#
te-class-mapping
isis 1
 cost-style wide
 traffic-eng level-1-2
 network-entity 10.0000.0000.0003.00
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.2.1.2 255.255.255.252
 mpls
 mpls te
 isis enable 1
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 10.5.1.2 255.255.255.252
 mpls
 mpls te
```

```
 isis enable 1
 mpls rsvp-te
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 isis enable 1
#
return
```

2.16.11 Example for Configuring Static BFD for CR-LSP

By configuring static BFD for CR-LSP, you can switch traffic to the backup CR-LSP in the case of the primary CR-LSP failure. When the primary CR-LSP recovers, the traffic can be switched back from the backup CR-LSP to the primary CR-LSP.

Networking Requirements

CAUTION

On a single NE5000E, an interface is numbered in the format of slot number/card number/interface number. On an NE5000E cluster, the interface is numbered in the format of chassis ID/slot number/card number/interface number. This requires the chassis ID to be specified along with the slot number.

Figure 2-21 is a networking diagram of CR-LSP hot standby. A TE tunnel is established from PE1 to PE2. The tunnel is enabled with hot standby and configured with the best-effort path. Where,

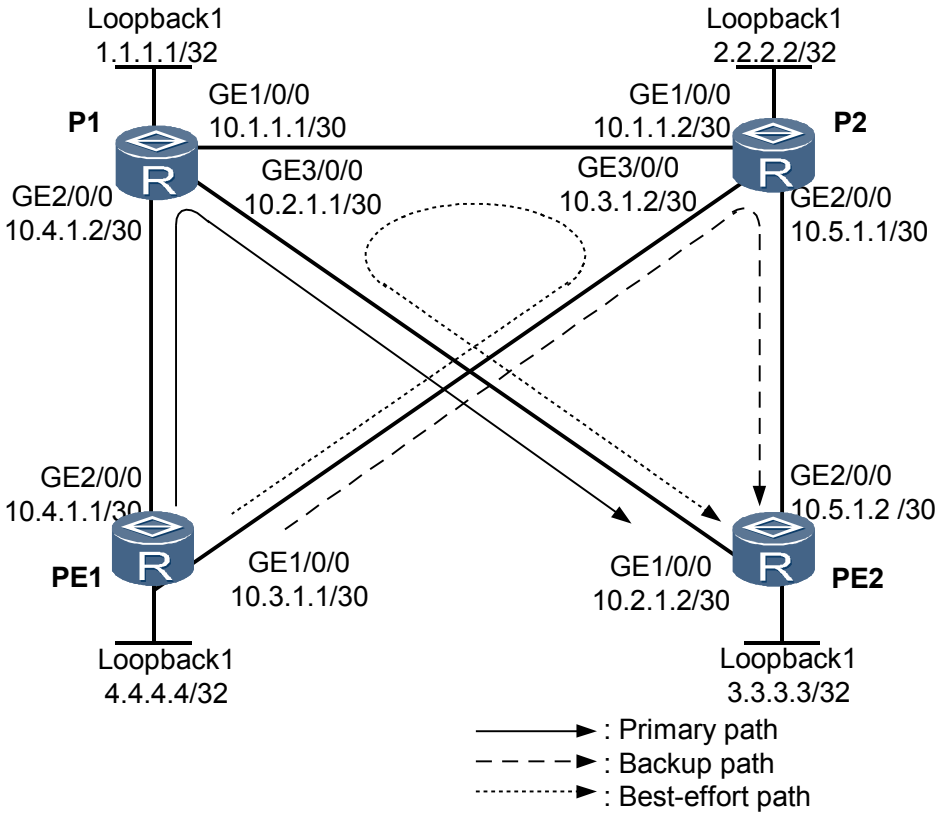
- The primary CR-LSP is PE1 → P1 → PE2.
- The backup CR-LSP is PE1 → P2 → PE2.
- The best-effort path is PE1 → P2 → P1 → PE2.

If the primary CR-LSP fails, traffic can be switched to the backup CR-LSP. After the primary CR-LSP recovers, the traffic can be switched back to the primary CR-LSP in 15 seconds. If both the primary and backup CR-LSPs fail, traffic can be switched to the best-effort path.

Two static BFD sessions are required to detect the primary and backup CR-LSPs. After the configuration, the following objects should be achieved:

- When the primary CR-LSP fails, traffic is switched to the backup CR-LSP.
- If the primary CR-LSP recovers and the backup CR-LSP fails during the switchover time (15s), traffic is switched back to the primary CR-LSP.

Figure 2-21 Networking diagram of CR-LSP hot standby



Configuration Notes

None.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure CR-LSP hot standby.
2. On PE1, establish two BFD sessions and bind the two sessions to the primary CR-LSP and the backup CR-LSP respectively; on PE2, establish two BFD sessions and bind the two sessions to the IP link (PE2 → PE1).

Data Preparation

To complete the configuration, you need the following data:

- Name of a BFD session
- Local and remote discriminators of BFD sessions
- Minimum interval for receiving and sending BFD packets
- Other data as described in the section "Example for Configuring CR-LSP Hot Standby" in the *HUAWEI NetEngine5000E Core Router Configuration Guide - MPLS.*

Procedure

Step 1 Configure CR-LSP hot standby.

NOTE

For configuration details, refer to the section "Example for Configuring CR-LSP Hot Standby" in the *HUAWEI NetEngine5000E Core Router Configuration Guide - MPLS.*

Step 2 Configuring BFD for CR-LSP.

Establish BFD sessions between PE1 and PE2 to detect the primary and backup CR-LSPs. Bind the BFD sessions on PE1 to the primary and backup CR-LSP and the BFD session on PE2 to the IP link. Set the minimum interval for sending and receiving BFD packets to 100 milliseconds and the local BFD detection multiplier to 3.

Configure PE1.

```
<HUAWEI> system-view
[~HUAWEI] sysname PE1
[~HUAWEI] commit
[~PE1] bfd
[~PE1-bfd] quit
[~PE1] bfd mainlsptope2 bind mpls-te interface tunnel 1 te-lsp
[~PE1-bfd-lsp-session-mainlsptope2] discriminator local 413
[~PE1-bfd-lsp-session-mainlsptope2] discriminator remote 314
[~PE1-bfd-lsp-session-mainlsptope2] min-tx-interval 100
[~PE1-bfd-lsp-session-mainlsptope2] min-rx-interval 100
[~PE1-bfd-lsp-session-mainlsptope2] process-pst
[~PE1-bfd-lsp-session-mainlsptope2] quit
[~PE1] bfd backuplsptope2 bind mpls-te interface tunnel 1 te-lsp backup
[~PE1-bfd-lsp-session-backuplsptope2] discriminator local 423
[~PE1-bfd-lsp-session-backuplsptope2] discriminator remote 324
[~PE1-bfd-lsp-session-backuplsptope2] min-tx-interval 100
[~PE1-bfd-lsp-session-backuplsptope2] min-rx-interval 100
[~PE1-bfd-lsp-session-backuplsptope2] process-pst
[~PE1-bfd-lsp-session-backuplsptope2] commit
[~PE1-bfd-lsp-session-backuplsptope2] quit
```

Configure PE2.

```
<HUAWEI> system-view
[~HUAWEI] sysname PE2
[~HUAWEI] commit
[~PE2] bfd
[~PE2-bfd] quit
[~PE2] bfd mainlsptope2 bind peer-ip 4.4.4.4
[~PE2-bfd-lsp-session-mainlsptope2] discriminator local 314
[~PE2-bfd-lsp-session-mainlsptope2] discriminator remote 413
[~PE2-bfd-lsp-session-mainlsptope2] min-tx-interval 100
[~PE2-bfd-lsp-session-mainlsptope2] min-rx-interval 100
[~PE2-bfd-lsp-session-mainlsptope2] quit
[~PE2] bfd backuplsptope2 bind peer-ip 4.4.4.4
[~PE2-bfd-lsp-session-backuplsptope2] discriminator local 324
[~PE2-bfd-lsp-session-backuplsptope2] discriminator remote 423
[~PE2-bfd-lsp-session-backuplsptope2] min-tx-interval 100
[~PE2-bfd-lsp-session-backuplsptope2] min-rx-interval 100
[~PE2-bfd-lsp-session-backuplsptope2] commit
[~PE2-bfd-lsp-session-backuplsptope2] quit
```

After the preceding operation, run the **display bfd session discriminator** *local-discriminator-value* command on PE1 and PE2. You can find that the status of BFD sessions is Up.

Take the display on PE1 as an example.

```
[~PE1] display bfd session discriminator 413
Local  Remote PeerIpAddr        State     Type             InterfaceName
------------------------------------------------------------------------------
```

```
413    314    3.3.3.3           Up       S_TE_LSP         Tunnel1
------------------------------------------------------------------------------
[~PE1] display bfd session discriminator 423
------------------------------------------------------------------------------
Local  Remote PeerIpAddr        State     Type              InterfaceName
------------------------------------------------------------------------------
423    324    3.3.3.3           Up       S_TE_LSP         Tunnel1
------------------------------------------------------------------------------
```

Step 3 Verify the configuration.

Connect two interfaces on a tester, namely, Port 1 and Port 2, to PE1 and PE2 respectively. Inject MPLS traffic from Port 1 to Port 2. Note the label setting of the MPLS packet. After the cable of GE 2/0/0 on PE1 or P1 is pulled out, the fault recovers at the millisecond level.

After inserting the cable into GE 2/0/0 and then pulling out the cable from GE 1/0/0 on PE1 within 15 seconds, you can find that the fault recovers at the millisecond level.

----End

Configuration File

- Configuration file of PE1

```
#
 sysname PE1
#
 bfd
#
 mpls lsr-id 4.4.4.4
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
 explicit-path backup
  next hop 10.3.1.2
  next hop 10.5.1.2
  next hop 3.3.3.3
#
 explicit-path main
  next hop 10.4.1.2
  next hop 10.2.1.2
  next hop 3.3.3.3
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0004.00
 traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
 ip address 10.3.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 ip address 10.4.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
#
```

```
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 isis enable 1
#
interface Tunnel1
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te tunnel-id 100
 mpls te record-route
 mpls te bandwidth ct0 10000
 mpls te path explicit-path main
 mpls te path explicit-path backup secondary
 mpls te backup hot-standby wtr 15
 mpls te backup ordinary best-effort
 mpls te commit
#
bfd backuplsptope2 bind mpls-te interface Tunnel1 te-lsp backup
 discriminator local 423
 discriminator remote 324
 min-tx-interval 100
 min-rx-interval 100
 process-pst
#
bfd mainlsptope2 bind mpls-te interface Tunnel1 te-lsp
 discriminator local 413
 discriminator remote 314
 min-tx-interval 100
 min-rx-interval 100
 process-pst
return
```

- Configuration file of P1

```
#
 sysname P1
#
 mpls lsr-id 1.1.1.1
 mpls
  mpls te
  mpls rsvp-te
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0001.00
 traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 ip address 10.4.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet3/0/0
 ip address 10.2.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
#
interface LoopBack1
```

```
 ip address 1.1.1.1 255.255.255.255
 isis enable 1
return
```

- Configuration file of P2

```
#
 sysname P2
#
 mpls lsr-id 2.2.2.2
 mpls
  mpls te
  mpls rsvp-te
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0002.00
 traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 ip address 10.5.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 50000
 mpls rsvp-te
#
interface GigabitEthernet3/0/0
 ip address 10.3.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
 bfd
#
 mpls lsr-id 3.3.3.3
 mpls
  mpls te
  mpls rsvp-te
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0003.00
 traffic-eng level-1-2
#
interface GigabitEthernet1/0/0
 ip address 10.2.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
```

```
#
interface GigabitEthernet2/0/0
 ip address 10.5.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 isis enable 1
#
bfd backuplsptope2 bind peer-ip 4.4.4.4
 discriminator local 324
 discriminator remote 423
 min-tx-interval 100
 min-rx-interval 100
#
bfd mainlsptope2 bind peer-ip 4.4.4.4
 discriminator local 314
 discriminator remote 413
 min-tx-interval 100
 min-rx-interval 100
return
```

2.16.12 Example for Configuring Static BFD for TE

After static BFD for TE is configured, the VPN is enabled to fast sense tunnel faults and perform traffic switchover.

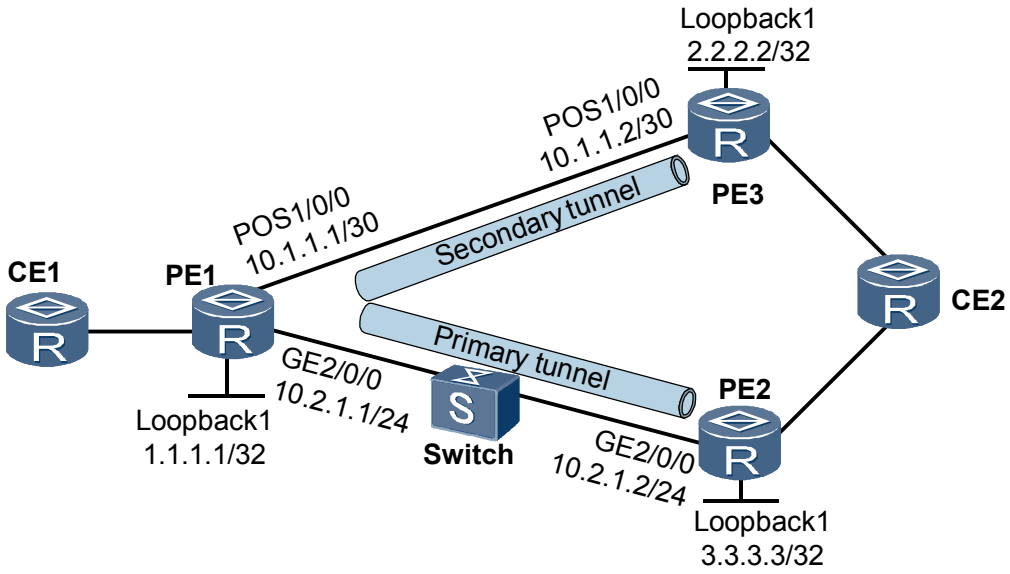
Networking Requirements

CAUTION

On a single NE5000E, an interface is numbered in the format of slot number/card number/interface number. On an NE5000E cluster, the interface is numbered in the format of chassis ID/slot number/card number/interface number. This requires the chassis ID to be specified along with the slot number.

Figure 2-22 shows an MPLS network where a switch (a Layer 2 device) exists between PE1 and PE2. PE1 is configured with VPN FRR and the MPLS TE tunnel. The primary path of VPN FRR is PE1 → Switch → PE2; the backup path of VPN FRR is PE1 → PE3. In a normal situation, VPN traffic is transmitted over the primary path. If the primary path fails, VPN traffic is switched to the backup path. BFD for TE is required to detect the TE tunnel over the primary path and enable VPN to rapidly sense tunnel faults. Thus, traffic can be rapidly switched between the primary path and backup path in the case of faults, and fault recovery is shortened.

Figure 2-22 Networking diagram of static BFD for TE



NOTE

For simplicity, the IP addresses of the interfaces connected the PEs and the CEs are not shown in the diagram.

Configuration Notes

None.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an MPLS network, and establish bi-directional TE tunnels between PE1 and PE2, and between PE1 and PE3.
2. Configure VPN FRR on PE1.
3. Enable global BFD on PE1, PE2, and PE3.
4. Establish a BFD session on PE1 to detect the TE tunnel over the primary path.
5. Establish a BFD session on PE2 and PE3, and specify the TE tunnel as the BFD reverse tunnel.

Data Preparation

To complete the configuration, you need the following data:

- An IGP and its parameters
- BGP AS number and interfaces of BGP sessions
- MPLS LSR ID
- Maximum BC bandwidth and maximum reservable bandwidth on the outgoing interface of the link along the tunnel

- Tunnel interface number, bandwidth occupied by the tunnel, and explicit paths
- VPN instance name, RD, and route target (RT)
- Name of the tunnel policy
- Data required for configuring VPN FRR on PE1, such as IP prefix name and routing policy name
- Name of a BFD session
- Local and remote discriminators of BFD sessions

Procedure

Step 1 Assign an IP address to each interface.

Assign an IP address to each interface as shown in networking diagram, create loopback interfaces on routers, and then configure the IP addresses of the loopback interfaces to MPLS LSR IDs. The configuration details are not mentioned here.

Step 2 Configure an IGP.

Configure OSPF or IS-IS on each router to ensure interworking between PE1 and PE2, and between PE1 and PE3. OSPF is adopted in the example. The configuration details are not mentioned here.

Step 3 Enable the basic MPLS functions.

On each router, configure an LSR ID and enable MPLS in the system view and then enable MPLS in the interface view. The configuration details are not mentioned here.

Step 4 Configure the basic MPLS TE functions.

On each router, enable MPLS-TE and MPLS RSVP-TE in the view of MPLS and the physical interface. Configure the maximum bandwidth for the MPLS TE reserved on each outgoing interface of the link along the tunnel to 100 Mbit/s and the BC bandwidth to 100 Mbit/s. The configuration details are not mentioned here.

Step 5 Enable OSPF TE and configure the CSPF.

Enable OSPF TE on each router and configure the CSPF on PE1 and PE2. The configuration details are not mentioned here.

Step 6 Configure tunnel interfaces.

Specify explicit paths on PE1, PE2, and PE3. For PE1, two explicit paths must be specified.

Configure the explicit paths from PE1 to PE2 and PE3 respectively.

```
[~PE1] explicit-path tope2
[~PE1-explicit-path-tope2] next hop 10.2.1.2
[~PE1-explicit-path-tope2] next hop 3.3.3.3
[~PE1-explicit-path-tope2] quit
[~PE1] explicit-path tope3
[~PE1-explicit-path-tope3] next hop 10.1.1.2
[~PE1-explicit-path-tope3] next hop 2.2.2.2
[~PE1-explicit-path-tope3] commit
[~PE1-explicit-path-tope3] quit
```

Configure an explicit path from PE2 to PE1.

```
[~PE2] explicit-path tope1
[~PE2-explicit-path-tope1] next hop 10.2.1.1
[~PE2-explicit-path-tope1] next hop 1.1.1.1
```

```
[~PE2-explicit-path-tope1] commit
[~PE2-explicit-path-tope1] quit
```

Configure an explicit path from PE3 to PE1.

```
[~PE3] explicit-path tope1
[~PE3-explicit-path-tope1] next hop 10.1.1.1
[~PE3-explicit-path-tope1] next hop 1.1.1.1
[~PE3-explicit-path-tope1] commit
[~PE3-explicit-path-tope1] quit
```

Create tunnel interfaces on PE1, PE2, and PE3, specify explicit paths, and configure the tunnel bandwidth to 10 Mbit/s. Bind the tunnel to the specified VPN. For PE1, two tunnel interfaces must be created.

Configure PE1.

```
[~PE1] interface tunnel 2
[~PE1-Tunnel2] ip address unnumbered interface loopback 1
[~PE1-Tunnel2] tunnel-protocol mpls te
[~PE1-Tunnel2] destination 3.3.3.3
[~PE1-Tunnel2] mpls te path explicit-path tope2
[~PE1-Tunnel2] mpls te bandwidth ct0 10000
[~PE1-Tunnel2] mpls te reserved-for-binding
[~PE1-Tunnel2] commit
[~PE1-Tunnel2] quit
[~PE1] interface tunnel 1
[~PE1-Tunnel1] ip address unnumbered interface loopback 1
[~PE1-Tunnel1] tunnel-protocol mpls te
[~PE1-Tunnel1] destination 2.2.2.2
[~PE1-Tunnel1] mpls te path explicit-path tope3
[~PE1-Tunnel1] mpls te bandwidth ct0 10000
[~PE1-Tunnel1] mpls te reserved-for-binding
[~PE1-Tunnel1] commit
[~PE1-Tunnel1] quit
```

Configure PE2.

```
[~PE2] interface tunnel 2
[~PE2-Tunnel2] ip address unnumbered interface loopback 1
[~PE2-Tunnel2] tunnel-protocol mpls te
[~PE2-Tunnel2] destination 1.1.1.1
[~PE2-Tunnel2] mpls te path explicit-path tope1
[~PE2-Tunnel2] mpls te bandwidth ct0 10000
[~PE2-Tunnel2] mpls te reserved-for-binding
[~PE2-Tunnel2] commit
[~PE2-Tunnel2] quit
```

Configure PE3.

```
[~PE3] interface tunnel 1
[~PE3-Tunnel1] ip address unnumbered interface loopback 1
[~PE3-Tunnel1] tunnel-protocol mpls te
[~PE3-Tunnel1] destination 1.1.1.1
[~PE3-Tunnel1] mpls te path explicit-path tope1
[~PE3-Tunnel1] mpls te bandwidth ct0 10000
[~PE3-Tunnel1] mpls te reserved-for-binding
[~PE3-Tunnel1] commit
[~PE3-Tunnel1] quit
```

After the preceding operation, run the **display mpls te tunnel-interface tunnel** *interface-number* command on the PEs. You can find that the status of tunnel 1 and tunnel 2 on PE1, tunnel 2 on PE2, and tunnel 1 on PE3 shows "CR-LSP is Up."

Step 7 Configure VPN FRR.

Configure VPN instances on PE1, PE2, and PE3. Configure all VPN instance names to vpn1, RDs to 100:1, 100:2, and 100:3 respectively, and all RTs to 100:1. Configure the CEs to access the PEs. The configuration details are not mentioned here.

Establish MP IBGP peer relationship between PE1 and PE2, and between PE1 and PE3. The BGP AS number of PE1, PE2, and PE3 are 100. The loopback interface Loopback1 on PE1, PE2, and PE3 is used as the interface to set up BGP sessions. The configuration details are not mentioned here.

Configure tunnel policies for PE1, PE2, and PE3 and apply the policies to the VPN instances.

Configure PE1.

```
[~PE1] tunnel-policy policy1
[~PE1-tunnel-policy-policy1] tunnel binding destination 3.3.3.3 te tunnel 2
[~PE1-tunnel-policy-policy1] tunnel binding destination 2.2.2.2 te tunnel 1
[~PE1-tunnel-policy-policy1] quit
[~PE1] ip vpn-instance vpn1
[~PE1-ip-vpn-instance-vpn1] tnl-policy policy1
[~PE1-ip-vpn-instance-vpn1] commit
[~PE1-ip-vpn-instance-vpn1] quit
```

Configure PE2.

```
[~PE2] tunnel-policy policy1
[~PE2-tunnel-policy-policy1] tunnel binding destination 1.1.1.1 te tunnel 2
[~PE2-tunnel-policy-policy1] quit
[~PE2] ip vpn-instance vpn1
[~PE2-ip-vpn-instance-vpn1] tnl-policy policy1
[~PE2-ip-vpn-instance-vpn1] commit
[~PE2-ip-vpn-instance-vpn1] quit
```

Configure PE3.

```
[~PE3] tunnel-policy policy1
[~PE3-tunnel-policy-policy1] tunnel binding destination 1.1.1.1 te tunnel 1
[~PE3-tunnel-policy-policy1] quit
[~PE3] ip vpn-instance vpn1
[~PE3-ip-vpn-instance-vpn1] tnl-policy policy1
[~PE3-ip-vpn-instance-vpn1] commit
[~PE3-ip-vpn-instance-vpn1] quit
```

Configure VPN on PE1. FRR.

```
[~PE1] ip ip-prefix vpn_frr_list permit 3.3.3.3 32
[~PE1] route-policy vpn_frr_rp permit node 10
[~PE1-route-policy] if-match ip next-hop ip-prefix vpn_frr_list
[~PE1-route-policy] apply backup-nexthop 2.2.2.2
[~PE1-route-policy] quit
[~PE1] ip vpn-instance vpn1
[~PE1-vpn-instance-vpn1] vpn frr route-policy vpn_frr_rp
[~PE1-vpn-instance-vpn1] commit
[~PE1-vpn-instance-vpn1] quit
```

After the configuration, CEs can communicate with eath other, and traffic flows through PE1, Switch, and PE2. After the cable of any interface connecting PE1 to PE2 is pulled out, or Switch fails, or PE2 fails, VPN traffic is switched to the backup path PE1 → PE3. Time taken in fault recovery is near to the IGP convergence time.

Step 8 Configure BFD for TE.

Configure a BFD session on PE1 to detect the TE tunnel of the primary path. Set the minimum interval for sending and receiving BFD packets.

```
[~PE1] bfd
[~PE1-bfd] quit
```

```
[~PE1] bfd pe1tope2 bind mpls-te interface tunnel2
[~PE1-bfd-lsp-session-pe1tope2] discriminator local 12
[~PE1-bfd-lsp-session-pe1tope2] discriminator remote 21
[~PE1-bfd-lsp-session-pe1tope2] min-tx-interval 100
[~PE1-bfd-lsp-session-pe1tope2] min-rx-interval 100
[~PE1-bfd-lsp-session-pe1tope2] process-pst
[~PE1-bfd-lsp-session-pe1tope2] commit
```

Establish a BFD session on PE2 and specify the TE tunnel as the reverse BFD tunnel. Set the minimum interval for sending and receiving BFD packets.

```
[~PE2] bfd
[~PE2-bfd] quit
[~PE2] bfd pe2tope1 bind mpls-te interface tunnel2
[~PE2-bfd-lsp-session-pe2tope1] discriminator local 21
[~PE2-bfd-lsp-session-pe2tope1] discriminator remote 12
[~PE2-bfd-lsp-session-pe2tope1] min-tx-interval 100
[~PE2-bfd-lsp-session-pe2tope1] min-rx-interval 100
[~PE2-bfd-lsp-session-pe2tope1] commit
```

After the configuration, run the **display bfd session** { **all** | **discriminator** *discr-value* | **mpls-te interface** *interface-type interface-number* } [**verbose**] command on PE1 and PE2. You can find that the status of the BFD session is Up.

Step 9 Verify the configuration.

Connect two interfaces on a tester, namely, Port 1 and Port 2, to CE1 and CE2 respectively. Inject traffic from Port 1 to Port 2, and you can find that a fault can be recovered at the millisecond level.

----End

Configuration File

NOTE

Configuration files of CE1, CE2 and the switch are omitted and the configuration of PE accessing CE is not mentioned here.

- Configuration file of PE1

```
#
 sysname PE1
#
ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn frr route-policy vpn_frr_rp
 tnl-policy policy1
 vpn-target 100:1 export-extcommunity
 vpn-target 100:1 import-extcommunity
#
 bfd
#
 mpls lsr-id 1.1.1.1
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
 explicit-path tope2
  next hop 10.2.1.2
  next hop 3.3.3.3
#
 explicit-path tope3
  next hop 10.1.1.2
  next hop 2.2.2.2
#
interface gigabitethernet2/0/0
```

```
 undo shutdown
 ip address 10.2.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.1.1.1 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
interface Tunnel1
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 2.2.2.2
 mpls te bandwidth ct0 10000
 mpls te path explicit-path tope3
 mpls te reserved-for-binding
 commit
#
interface Tunnel2
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te bandwidth ct0 10000
 mpls te path explicit-path tope2
 mpls te reserved-for-binding
 commit
#
bgp 100
 peer 2.2.2.2 as-number 100
 peer 2.2.2.2 connect-interface LoopBack1
 peer 3.3.3.3 as-number 100
 peer 3.3.3.3 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 2.2.2.2 enable
  peer 3.3.3.3 enable
#
 ipv4-family vpnv4
  policy vpn-target
  peer 2.2.2.2 enable
  peer 3.3.3.3 enable
#
 ipv4-family vpn-instance vpn1
  import-route direct
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 10.1.1.0 0.0.0.3
  network 10.2.1.0 0.0.0.255
  network 1.1.1.1 0.0.0.0
  mpls-te enable
#
route-policy vpn_frr_rp permit node 10
 if-match ip next-hop ip-prefix vpn_frr_list
 apply backup-nexthop 2.2.2.2
```

```
#
ip ip-prefix vpn_frr_list permit 3.3.3.3 32
#
tunnel-policy  policy1
 tunnel binding destination 3.3.3.3 te Tunnel2
 tunnel binding destination 2.2.2.2 te Tunnel1
#
bfd pe1tope2 bind mpls-te interface Tunnel2
 discriminator local 12
 discriminator remote 21
 min-tx-interval 100
 min-rx-interval 100
 process-pst
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
ip vpn-instance vpn1
 route-distinguisher 100:2
 tnl-policy policy1
 vpn-target 100:1 export-extcommunity
 vpn-target 100:1 import-extcommunity
#
 bfd
#
 mpls lsr-id 3.3.3.3
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
 explicit-path tope1
  next hop 10.2.1.1
  next hop 1.1.1.1
#
interface gigabitethernet2/0/0
 undo shutdown
 ip address 10.2.1.2 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
interface Tunnel2
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 1.1.1.1
 mpls te bandwidth ct0 10000
 mpls te path explicit-path tope1
 mpls te reserved-for-binding
 commit
#
bgp 100
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 1.1.1.1 enable
#
 ipv4-family vpnv4
  policy vpn-target
  peer 1.1.1.1 enable
#
```

```
 ipv4-family vpn-instance vpn1
  import-route direct
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 3.3.3.3 0.0.0.0
  mpls-te enable
#
tunnel-policy  policy1
 tunnel binding destination 1.1.1.1 te Tunnel2
#
bfd pe2tope1 bind mpls-te interface Tunnel2
 discriminator local 21
 discriminator remote 12
 min-tx-interval 100
 min-rx-interval 100
return
```

- Configuration file of PE3

```
#
 sysname PE3
#
ip vpn-instance vpn1
 route-distinguisher 100:3
 tnl-policy policy1
 vpn-target 100:1 export-extcommunity
 vpn-target 100:1 import-extcommunity
#
 mpls lsr-id 2.2.2.2
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
 explicit-path tope1
  next hop 10.1.1.1
  next hop 1.1.1.1
#
interface Pos1/0/0
 undo shutdown
 link-protocol ppp
 ip address 10.1.1.2 255.255.255.252
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls te bandwidth bc0 100000
 mpls rsvp-te
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
interface Tunnel1
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 1.1.1.1
 mpls te bandwidth ct0 10000
 mpls te path explicit-path tope1
 mpls te reserved-for-binding
 commit
#
bgp 100
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 1.1.1.1 enable
#
```

```
 ipv4-family vpnv4
  policy vpn-target
  peer 1.1.1.1 enable
#
 ipv4-family vpn-instance vpn1
  import-route direct
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 10.1.1.0 0.0.0.3
  network 2.2.2.2 0.0.0.0
  mpls-te enable
#
tunnel-policy  policy1
 tunnel binding destination 1.1.1.1 te Tunnel1
return
```