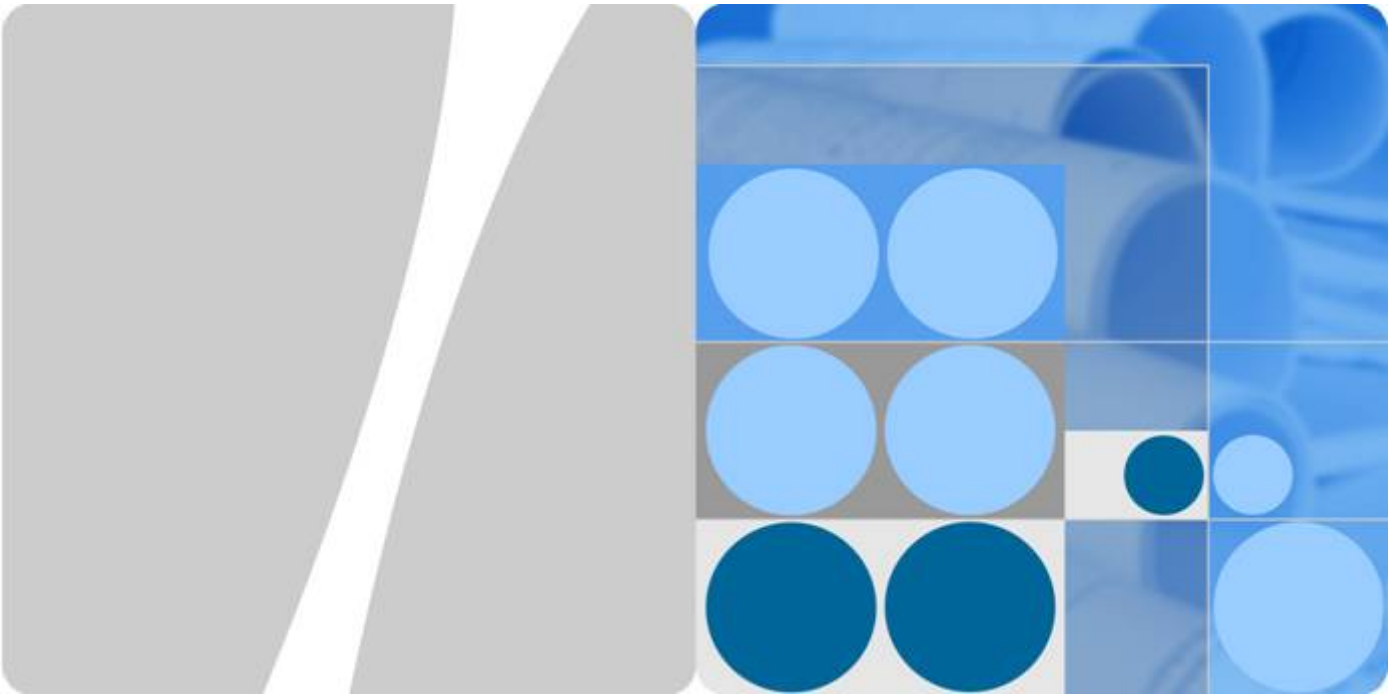


Quidway S9300 Terabit Routing Switch

V100R006C01

Configuration Guide - MPLS

Issue 01

Date 2011-10-26

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2011. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of 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.

This document describes how to configure the MPLS features.

NOTE

- The MPLS function of the S9300 is controlled by the license. By default, the MPLS function is disabled on the S9300. To use the MPLS function of the S9300,buy the license from the Huawei local office.
- The G24SA,G24CA and X12SA boards do not support the MPLS function.

This document is intended for:

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

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.
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.

Copyright © Huawei Technologies Co., Ltd.

Symbol	Description
NOTE	Provides additional information to emphasize or supplement important points of the main text.

Command Conventions

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 (2011-10-26)

Initial commercial release.

Copyright © Huawei Technologies Co., Ltd.

Contents

Copyright © Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd.

1 Static LSPs Configuration

About This Chapter

You can set up a static LSP by manually allocating labels to LSRs. The static LSP is applicable to stable and small-scale networks.

1.1 Overview of Static LSPs
The static LSP cannot be set up through a label distribution protocol but can be set up by an administrator. The static LSP is applicable to a stable and small-scaled network with the simple topology.

1.2 Static LSPs Features Supported by the S9300
Static LSPs features supported by the system include configuring Static LSPs and Static BFD for Static LSP.

1.3 Configuring Static LSPs
A static LSP can be set up only after each LSR is manually configured.

1.4 Configuring Static BFD for Static LSP
By configuring static BFD for static LSPs, you can detect connectivity of static LSPs.

1.5 Maintaining Static LSPs
The operations of static LSP maintenance include deleting MPLS statistics, detecting connectivity or reachability of an LSP, and configuring the trap function on an LDP LSP.

1.6 Configuration Examples
This section provides several configuration examples of static LSPs.

Copyright © Huawei Technologies Co., Ltd.

1.1 Overview of Static LSPs

The static LSP cannot be set up through a label distribution protocol but can be set up by an administrator. The static LSP is applicable to a stable and small-scaled network with the simple topology.

When configuring a static LSP, the administrator needs to manually allocate labels for each LSR by following the rule that the value of the outgoing label of the previous node is equal to the value of the incoming label of the next node. Each LSR on the static LSP cannot sense the changes of other LSRs on the LSP. Therefore, the static LSP is a local concept.

A static LSP is set up without using label distribution protocols, and does not need to exchange control packets. Thus, the static LSP consumes few resources and is applicable to small-scale networks with simple and stable topology. The static LSP cannot vary with the network topology dynamically. The administrator needs to adjust the static LSP according to the network topology.

1.2 Static LSPs Features Supported by the S9300

Static LSPs features supported by the system include configuring Static LSPs and Static BFD for Static LSP.

Static LSPs

Static LSPs need to be configured manually by the administrator. Each LSR on the static LSP cannot sense the status of the entire LSP, because the static LSP is a local concept. A static LSP cannot vary with the change of a route dynamically. The administrator then needs to adjust the static LSP.

Static BFD for Static LSPs

The S9300 supports static BFD for static LSPs. BFD is a bidirectional detection mechanism. When static BFD is applied to static LSPs which are unidirectional, the reverse links can be either IP links or static LSPs.

1.3 Configuring Static LSPs

A static LSP can be set up only after each LSR is manually configured.

1.3.1 Establishing the Configuration Task

Before configuring a static LSP, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you rapidly and correctly finish the configuration task.

Applicable Environment

A static LSP works normally only after all the LSRs along the LSP are configured.

The setup of static LSPs does not require the label distribution protocol or exchange any control packet. Thus, the static LSPs consume little resources and are applicable to small-scale networks

Copyright © Huawei Technologies Co., Ltd.

with simple and stable topology. The static LSPs cannot vary with the network topology dynamically. The administrator, therefore, needs to adjust the static LSPs according to the network topology.

Static LSPs and static CR-LSPs share the same label space (16 - 1023).

Static LSPs are used over the MPLS L2VPN.

For information about the MPLS L2VPN configuration, refer to the Quidway S9300 Terabit Routing Switch *Configuration Guide - VPN*.

Pre-configuration Tasks

Before configuring static LSPs, complete the following tasks:

- Configuring the static unicast route or an IGP to connect LSRs on the network layer

Data Preparation

To configure static LSPs, you need the following data.

No.	Data
1	Name of the static LSP
2	Destination address and mask
3	Value of incoming label or outgoing label on each LSR
4	Next hop address or outgoing interface on the ingress
5	Incoming interface, next hop address, or outgoing interface on the transit node
6	Incoming interface on the egress

1.3.2 Configuring the LSR ID

Before enabling MPLS, you must configure LSR ID.

Context

When configuring an LSR ID, note the following:

- The LSR ID must be configured before other MPLS commands are run.
- The LSR ID does not have a default value, and must be configured manually.
- It is recommended to use the address of the loopback interface of the LSR as the LSR ID.
- To modify the configured LSR ID, you must run the **undo mpls** command in the system view to delete all the MPLS configurations.

Do as follows on each LSR in an MPLS domain:

Copyright © Huawei Technologies Co., Ltd.

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.

lsr-id: It is in dotted decimal notation and identifies an LSR.

----End

1.3.3 Enabling MPLS

MPLS features can be configured only after MPLS is enabled.

Context

Do as follows on each LSR in an MPLS domain:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

MPLS is enabled globally and the MPLS view is displayed.

Step 3 Run:

```
quit
```

Return to the system view.

Step 4 Run:

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

The interface to participate in MPLS forwarding is specified.

The interface can be a VLANIF interface or a POS interface.

Step 5 Run:

```
mpls
```

MPLS is enabled on the interface.

----End

1.3.4 Configuring the Ingress for a Static LSP

To set up a static LSP, you need to configure the ingress node in manual mode.

Copyright © Huawei Technologies Co., Ltd.

Context

Do as follows on the LSR to be configured as the ingress:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
static-lsp ingress lsp-name destination ip-address { mask-length | mask }
{ nexthop next-hop-address | outgoing-interface interface-type interface-number }
out-label out-label
```

The interface can be a VLANIF interface or a POS interface.

The LSR is configured as the ingress on the specified LSP.

----End

1.3.5 Configuring the Transit for a Static LSP

To set up a static LSP, you need to configure the transit node in manual mode.

Context

Do as follows on the LSR to be configured as a transit node:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
static-lsp transit lsp-name incoming-interface interface-type interface-number in-
label in-label { nexthop next-hop-address | outgoing-interface interface-type
interface-number } out-label out-label
```

The interface can be a VLANIF interface or a POS interface.

The LSR is configured as the transit node on the specified LSP.

----End

1.3.6 Configuring the Egress for a Static LSP

To set up a static LSP, you need to configure the egress node in manual mode.

Context

Do as follows on the LSR to be configured as the egress:

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

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

The interface can be a VLANIF interface or a POS interface.

The LSR is configured as the egress on the specified LSP.

----End

1.3.7 Checking the Configuration

After a static LSP is set up, you can view that the static LSP is Up and the route status is Ready.

Prerequisite

The configurations of the static LSP function are complete.

Procedure

- Run the **display mpls static-lsp** [*lsp-name*] [{ **include** | **exclude** } *ip-address mask-length*] [**verbose**] command to check the static LSP.
- Run the **display mpls route-state** [**vpn-instance** *vpn-instance-name*] [{ **exclude** | **include** } { **idle** | **ready** | **settingup** } * | *destination-address mask-length*] [**verbose**] command to check the LSP route on the ingress.

----End

Example

If the configurations succeed, run the preceding commands, and you can view as follows:

- When the **display mpls static-lsp** command, information about the static LSP configuration is displayed, including the name of the static LSP, FEC, values of the incoming label and the outgoing label, and the incoming and outgoing interfaces. In addition, you can view that the status of the LSP is Up.

```
<Quidway> display mpls static-lsp
TOTAL          : 1       STATIC LSP(S)
UP             : 1       STATIC LSP(S)
DOWN           : 0       STATIC LSP(S)
Name       FEC               I/O Label  I/O If                Stat
lsp1       3.3.3.9/32        NULL/100   -/GE1/0/0             Up
```

- When the **display mpls route-state** command is run on the ingress, routing information about the LSP is displayed, including the destination address, next hop IP address, outgoing interface, and the status of MPLS routing information on the control plane. When the route is in Ready state, this indicates that the route triggers the establishment of the LSP.

```
<Quidway> disp mpls route-state
Codes: B(BGP), I(IGP), L(Public Label BGP), O(Original BGP), U(Unknow)
------------------------------------------------------------------------------
--
Dest/Mask          Next-Hop        Out-Interface              State LSP VRF
```


Copyright © Huawei Technologies Co., Ltd.

```
Type
------------------------------------------------------------------------------
--
220.1.1.0/24       20.1.13.3       Vlanif131                 READY 2   0
I
220.1.1.0/24       20.2.13.3       Vlanif132                 READY 2   0
I
220.1.2.0/24       20.1.13.3       Vlanif131                 READY 2   0
I
```

1.4 Configuring Static BFD for Static LSP

By configuring static BFD for static LSPs, you can detect connectivity of static LSPs.

1.4.1 Establishing the Configuration Task

Before configuring static BFD for static LSPs, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you rapidly and correctly finish the configuration task.

Applicable Environment

BFD is used to detect the connectivity of the static LSP that is established manually.

NOTE

When the static BFD works on the static LSP, the BFD session can be created for non-host routes.

BFD for LSP can function properly though the forward path is an LSP and the backward path is an IP link. The forward path and the backward path must be established over the same link; otherwise, if a fault occurs, BFD cannot identify the faulty path. Before deploying BFD, ensure that the forward and backward paths are over the same link so that BFD can correctly identify the faulty path.

Pre-configuration Tasks

Before configuring static BFD for static LSP, complete the following tasks:

- Configuring the static LSP

NOTE

For the static CR-LSP bound to an MPLS TE tunnel, the BFD is available after it is bound to the MPLS TE tunnel.

Data Preparations

Before configuring static BFD for a static LSP, you need the following data.

No.	Data
1	Name of static LSP
2	BFD configuration name

Copyright © Huawei Technologies Co., Ltd.

No.	Data
3	Parameters of reverse channel ● IP link: IP address of egress, outgoing interface (optional), and source IP address (optional) ● Dynamic LSP: IP address of egress, address of next hop in LSP, and egress (optional) ● Static LSP: LSP name ● MPLS TE: number of an MPLS TE tunnel
4	Local discriminator and remote discriminator of a BFD session

1.4.2 Enable Global BFD Capability

You can enable BFD globally on both ends of a link to be detected.

Context

Do as follows on each LSR at both ends of the link to be detected:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bfd
```

This node is enabled with the global BFD function. The BFD global view is displayed.

----End

1.4.3 Configuring BFD with Specific Parameters on Ingress

To detect a static LSP through a static BFD session, you need to configure BFD parameters on the ingress node of the static LSP.

Context

Do as follows on the ingress of the static LSP:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bfd cfg-name bind static-lsp lsp-name
```


Copyright © Huawei Technologies Co., Ltd.

The BFD session is bound to the static LSP.

Step 3 Configure the discriminators.

- Run:

  discriminator local *discr-value*

  The local discriminator is configured.

- Or, run:

  discriminator remote *discr-value*

  The remote discriminator is configured.

Step 4 (Optional) Run the following commands to adjust the minimum interval for the local device to send BFD packets, the minimum interval for receiving BFD packets and the local BFD detection multiple:

1. Run the **quit** command to return to the system view.
2. Run the **mpls** command to globally enable MPLS and the enter the MPLS view.
3. Run the **mpls bfd min-tx-interval** *interval* command to adjust the minimum interval for the local device to send BFD packets.

   The minimum interval for the local device to send BFD packets is set.

   When the device is equipped with an FSU, by default, the value is 10 milliseconds; otherwise, by default, the value is 1000 milliseconds.

   If the backward link is an IP link, this parameter is not applicable.

   Actual interval for the local device to send BFD packets = MAX { Locally configured interval for sending BFD packets, Remotely configured interval for receiving BFD packets}; Actual interval for the local to receive BFD packets = MAX {Remotely configured interval for sending BFD packets, Locally configured interval for receiving BFD packets}; Local detection period = Actual interval for the local device to Receive BFD packets x Remotely configured BFD detection multiple.

   For example, assume that the values of parameters are as follows:

   - On the local device, the interval for sending BFD packets is set to 200 ms, the interval for receiving BFD packets is set to 300 ms, and the detection multiple is set to 4.
   - On the peer device, the interval for sending BFD packets is 100 ms, the interval for receiving BFD packets is 600 ms, and the detection multiple is 5.

   Then,

   - On the local device, the actual interval for sending BFD packets is 600 ms calculated by using the formula max {200 ms, 600 ms}, the interval for receiving BFD packets is 300 ms calculated by using the formula max {100 ms, 300 ms}, and the detection period is 1500 ms calculated by 300 ms multiplied by 5.
   - On the peer device, the actual interval for sending local BFD packets is 300 ms obtained by using the formula max {100 ms, 300 ms}, the interval for receiving BFD packets is 600 ms obtained by using the formula max {200 ms, 600 ms}, and the detection period is 2400 ms obtained by 600 ms multiplied by 4.
4. Run the **mpls bfd min-rx-interval** *interval* command to adjust the minimum interval for receiving BFD packets.

   The minimum interval for receiving BFD packets is adjusted on the local device.

Copyright © Huawei Technologies Co., Ltd.

When the device is equipped with an FSU, by default, the value is 10 milliseconds; otherwise, by default, the value is 1000 milliseconds.

If the backward link is an IP link, this parameter is not applicable.

5. Run the **mpls bfd detect-multiplier** *multiplier* command to adjust the local BFD detection multiple.

   The default value is 3.

6. Run the **quit** command to return to the system view.
7. Run the **bfd** *cfg-name* command to enter the BFD session view.

Step 5 Run:

```
commit
```

The configuration is committed.

When configuring the BFD session of the static LSP, note the following:

- When the static LSP status goes Up, a BFD session is renewed.
- When the static LSP status goes Down, the BFD session becomes Down too.
- When the static LSP is deleted, the session and configuration entries of BFD are deleted.

----End

1.4.4 Configuring BFD with Specific Parameters on Egress

To detect a static LSP through a static BFD session, you need to configure BFD parameters on the egress node of the static LSP.

Context

The IP link, LSP, or TE tunnel can be used as the reverse tunnel to inform the ingress of a fault. To avoid affecting BFD detection, an IP link is preferentially selected to inform the ingress of an LSP fault. If the configured reverse tunnel requires BFD detection, you can configure a pair of BFD sessions for it.

Do as follows on the egress of the LSP:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Configure BFD sessions:

- For the IP link, run:

  bfd *cfg-name* **bind peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] [**interface** *interface-type interface-number*] [**source-ip** *source-ip*]

- For the dynamic LSP, run:

  bfd *cfg-name* **bind ldp-lsp peer-ip** *ip-address* **nexthop** *ip-address* [**interface** *interface-type interface-number*]

- For the static LSP, run:

  bfd *cfg-name* **bind static-lsp** *lsp-name*

Copyright © Huawei Technologies Co., Ltd.

- For MPLS TE, run:

  bfd *cfg-name* **bind mpls-te interface tunnel** *tunnel-number* [**te-lsp**]

Step 3 Configure the discriminators.

- Run:

  discriminator local *discr-value*

  The local discriminator is configured.

- Run:

  discriminator remote *discr-value*

  The remote discriminator is configured.

Step 4 (Optional) Run the following commands to adjust the minimum interval for the local device to send BFD packets, the minimum interval for receiving BFD packets and the local BFD detection multiple:

1. Run the **quit** command to return to the system view.
2. Run the **mpls** command to globally enable MPLS and the enter the MPLS view.
3. Run the **mpls bfd min-tx-interval** *interval* command to adjust the minimum interval for the local device to send BFD packets.

   The minimum interval for the local device to send BFD packets is set.

   When the device is equipped with an FSU, by default, the value is 10 milliseconds; otherwise, by default, the value is 1000 milliseconds.

   If the backward link is an IP link, this parameter is not applicable.

   Actual interval for the local device to send BFD packets = MAX { Locally configured interval for sending BFD packets, Remotely configured interval for receiving BFD packets}; Actual interval for the local to receive BFD packets = MAX {Remotely configured interval for sending BFD packets, Locally configured interval for receiving BFD packets}; Local detection period = Actual interval for the local device to Receive BFD packets x Remotely configured BFD detection multiple.

   For example, assume that the values of parameters are as follows:

   - On the local device, the interval for sending BFD packets is set to 200 ms, the interval for receiving BFD packets is set to 300 ms, and the detection multiple is set to 4.
   - On the peer device, the interval for sending BFD packets is 100 ms, the interval for receiving BFD packets is 600 ms, and the detection multiple is 5.

   Then,

   - On the local device, the actual interval for sending BFD packets is 600 ms calculated by using the formula max {200 ms, 600 ms}, the interval for receiving BFD packets is 300 ms calculated by using the formula max {100 ms, 300 ms}, and the detection period is 1500 ms calculated by 300 ms multiplied by 5.
   - On the peer device, the actual interval for sending local BFD packets is 300 ms obtained by using the formula max {100 ms, 300 ms}, the interval for receiving BFD packets is 600 ms obtained by using the formula max {200 ms, 600 ms}, and the detection period is 2400 ms obtained by 600 ms multiplied by 4.
4. Run the **mpls bfd min-rx-interval** *interval* command to adjust the minimum interval for receiving BFD packets.

   The minimum interval for receiving BFD packets is adjusted on the local device.

Copyright © Huawei Technologies Co., Ltd.

When the device is equipped with an FSU, by default, the value is 10 milliseconds; otherwise, by default, the value is 1000 milliseconds.

If the backward link is an IP link, this parameter is not applicable.

5. Run the **mpls bfd detect-multiplier** *multiplier* command to adjust the local BFD detection multiple.

   The default value is 3.

6. Run the **quit** command to return to the system view.
7. Run the **bfd** *cfg-name* command to enter the BFD session view.

Step 5 Run:

```
commit
```

The configuration is committed.

----End

1.4.5 Checking the Configuration

After the configuration of detecting a static LSP through a static BFD session, you can view the BFD configuration, BFD session information, BFD statistics, and the status of the static LSP.

Prerequisite

The configurations of the static BFD for static LSP function are complete.

Procedure

- Run the **display bfd configuration** { **all** | **static** } command to check the BFD configuration.
- Run the **display bfd session** { **all** | **static** } command to check information about the BFD session.
- Run the **display bfd statistics session** { **all** | **static** } command to check information about BFD statistics.
- Run the **display mpls static-lsp** [*lsp-name*] [{ **include** | **exclude** } *ip-address mask-length*] [**verbose**] command to check the status of the static LSP.

----End

1.5 Maintaining Static LSPs

The operations of static LSP maintenance include deleting MPLS statistics, detecting connectivity or reachability of an LSP, and configuring the trap function on an LDP LSP.

1.5.1 Clearing MPLS Statistics

By running the **reset** command, you can delete MPLS statistics.

Copyright © Huawei Technologies Co., Ltd.

Context

CAUTION

MPLS statistics cannot be restored after being cleared. Therefore, confirm the action before you run the following commands.

Procedure

- Run the **reset mpls statistics interface** { *interface-type interface-number* | **all** } command in the user view to clear the statistics of the MPLS interface.
- Run the **reset mpls statistics lsp** { *lsp-name* | **all** } command in the user view to clear LSP statistics.

----End

1.5.2 Checking the LSP Connectivity and Reachability

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

Context

You can run the following commands in any view to perform MPLS ping and MPLS tracert.

Procedure

- Run:

  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*] [**nexthop** *nexthop-address* | **draft6**]

  MPLS ping is performed.

  If **draft6** is specified, the command is implemented according to draft-ietf-mpls-lsp-ping-06. By default, the command is implemented according to RFC 4379.

- Run:

  tracert lsp [**-a** *source-ip* | **-exp** *exp-value* | **-h** *ttl-value* | **-r** *reply-mode* | **-t** *time-out*] * **ip** *destination-address mask-length* [*ip-address*] [**nexthop** *nexthop-address* | **draft6**]

  MPLS tracert is performed.

  If **draft6** is specified, the command is implemented according to draft-ietf-mpls-lsp-ping-06. By default, the command is implemented according to RFC 4379.

----End

1.5.3 Enabling the Trap Function of LSP

By configuring the trap function on an LSP, you can notify the NMS of the changes of the LSP status.

Copyright © Huawei Technologies Co., Ltd.

Context

Run the following commands in the system view to notify the Network Management System (NMS) of the LSP status change.

By default, the trap function is disabled during the setup of the LDP LSP.

Procedure

- Run the **snmp-agent trap suppress feature-name lsp trap-name** { **mplsxcup** | **mplsxcdown** } **trap-interval** *trap-interval* [**max-trap-number** *max-trap-number*] command in the system view to enable the trap function for the LDP LSP and enable the debugging of excessive mplsxcup or mplsxcdown.

----End

1.6 Configuration Examples

This section provides several configuration examples of static LSPs.

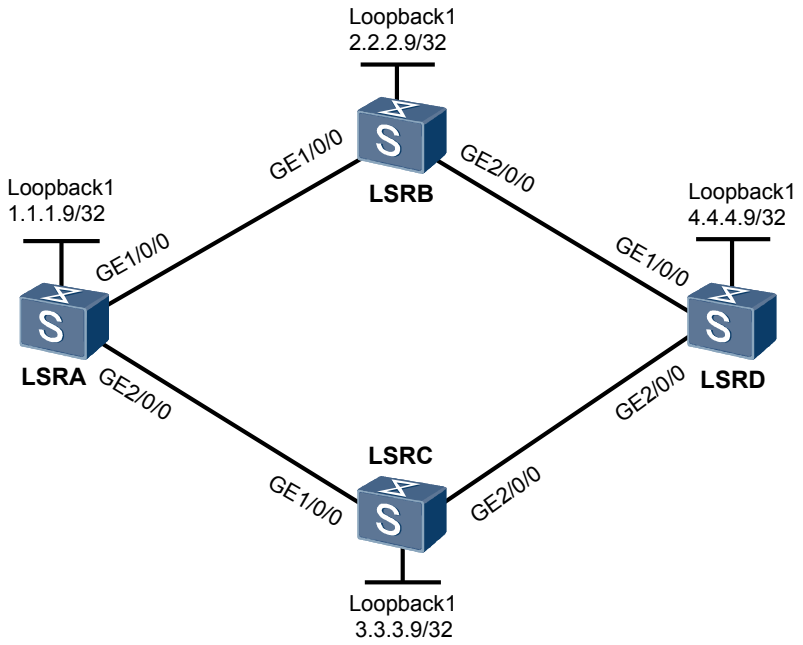
1.6.1 Example for Configuring Static LSPs

Networking Requirements

As shown in **Figure 1-1**, the nodes support MPLS and OSPF as an IGP is run on the MPLS backbone network.

Bidirectional static LSPs are set up between LSRA and LSRD. The LSP from LSRA to LSRD is LSRA->LSRB->LSRD;the LSP from LSRD to LSRA is LSRD->LSRC->LSRA.

Figure 1-1 Networking diagram for configuring static LSPs



Copyright © Huawei Technologies Co., Ltd.

switch	Interface	VLANIF interface	IP address
LSRA	GE1/0/0	VLANIF10	10.1.1.1/24
LSRA	GE2/0/0	VLANIF30	10.3.1.1/24
LSRB	GE1/0/0	VLANIF10	10.1.1.2/24
LSRB	GE2/0/0	VLANIF20	10.2.1.1/24
LSRC	GE1/0/0	VLANIF30	10.3.1.2/24
LSRC	GE2/0/0	VLANIF40	10.4.1.1/24
LSRD	GE1/0/0	VLANIF20	10.2.1.2/24
LSRD	GE2/0/0	VLANIF40	10.4.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs on the switch and add interfaces to the VLANs.
2. Assign an IP address to each VLANIF interface on each node and assign the loopback address used as the LSR ID, and configure OSPF to advertise the network segments that the interfaces are connected to and the host route of the LSR ID.
3. Enable MPLS globally on each node.
4. Enable MPLS on each VLANIF interface.
5. Configure the destination IP address, next hop, value of the outgoing label for the LSP on the ingress node.
6. Configure the incoming interface, value of the incoming label corresponding to the outgoing label of the last node, and next hop and value of the outgoing label of the LSP on the transit node.
7. Configure the incoming interface and value of the incoming label corresponding to the outgoing label of the last node of the LSP on the egress node.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each interface on each node shown in **Figure 1-1**, OSPF process ID, and OSPF area ID
- Name of the static LSP
- Value of the outgoing label on each interface

Procedure

Step 1 Create VLANs on the switch and add GE interfaces to the VLANs, create VLANIF interfaces, and assign IP addresses to the VLANIF interfaces.

Configure LSRA.

```
<Quidway> system-view
[Quidway] sysname LSRA
```


Copyright © Huawei Technologies Co., Ltd.

```
[LSRA] interface loopback1
[LSRA-LoopBack1] ip address 1.1.1.9 32
[LSRA-LoopBack1] quit
[LSRA] interface gigabitethernet1/0/0
[LSRA-GigabitEthernet1/0/0] port link-type access
[LSRA-GigabitEthernet1/0/0] quit
[LSRA] vlan 10
[LSRA-vlan10] port gigabitethernet1/0/0
[LSRA-vlan10] quit
[LSRA] interface vlanif 10
[LSRA-Vlanif10] ip address 10.1.1.1 24
[LSRA-Vlanif10] quit
[LSRA] interface gigabitethernet2/0/0
[LSRA-GigabitEthernet2/0/0] port link-type access
[LSRA-GigabitEthernet2/0/0] quit
[LSRA] vlan 30
[LSRA-vlan30] port gigabitethernet2/0/0
[LSRA-vlan30] quit
[LSRA] interface vlanif 30
[LSRA-Vlanif30] ip address 10.3.1.1 24
[LSRA-Vlanif30] quit
```

Configure LSRB.

```
<Quidway> system-view
[Quidway] sysname LSRB
[LSRB] interface loopback1
[LSRB-LoopBack1] ip address 2.2.2.9 32
[LSRB-LoopBack1] quit
[LSRB] interface gigabitethernet1/0/0
[LSRB-GigabitEthernet1/0/0] port link-type access
[LSRB-GigabitEthernet1/0/0] quit
[LSRB] vlan 10
[LSRB-vlan10] port gigabitethernet1/0/0
[LSRB-vlan10] quit
[LSRB] interface vlanif 10
[LSRB-Vlanif10] ip address 10.1.1.2 24
[LSRB-Vlanif10] quit
[LSRB] interface gigabitethernet2/0/0
[LSRB-GigabitEthernet2/0/0] port link-type access
[LSRB-GigabitEthernet2/0/0] quit
[LSRB] vlan 20
[LSRB-vlan20] port gigabitethernet2/0/0
[LSRB-vlan20] quit
[LSRB] interface vlanif 20
[LSRB-Vlanif20] ip address 10.2.1.1 24
[LSRB-Vlanif20] quit
```

Configure LSRC.

```
<Quidway> system-view
[Quidway] sysname LSRC
[LSRC] interface loopback1
[LSRC-LoopBack1] ip address 3.3.3.9 32
[LSRC-LoopBack1] quit
[LSRC] interface gigabitethernet1/0/0
[LSRC-GigabitEthernet1/0/0] port link-type access
[LSRC-GigabitEthernet1/0/0] quit
[LSRC] vlan 30
[LSRC-vlan30] port gigabitethernet1/0/0
[LSRC-vlan30] quit
[LSRC] interface vlanif 30
[LSRC-Vlanif30] ip address 10.3.1.2 24
[LSRC-Vlanif30] quit
[LSRC] interface gigabitethernet2/0/0
[LSRC-GigabitEthernet2/0/0] port link-type access
[LSRC-GigabitEthernet2/0/0] quit
[LSRC] vlan 40
[LSRC-vlan40] port gigabitethernet2/0/0
[LSRC-vlan40] quit
```


Copyright © Huawei Technologies Co., Ltd.

```
[LSRC] interface vlanif 40
[LSRC-Vlanif40] ip address 10.4.1.1 24
[LSRC-Vlanif40] quit
```

Configure LSRD.

```
<Quidway> system-view
[Quidway] sysname LSRD
[LSRD] interface loopback1
[LSRD-LoopBack1] ip address 4.4.4.9 32
[LSRD-LoopBack1] quit
[LSRD] interface gigabitethernet1/0/0
[LSRD-GigabitEthernet1/0/0] port link-type access
[LSRD-GigabitEthernet1/0/0] quit
[LSRD] vlan 20
[LSRD-vlan20] port gigabitethernet1/0/0
[LSRD-vlan20] quit
[LSRD] interface vlanif 20
[LSRD-Vlanif20] ip address 10.2.1.2 24
[LSRD-Vlanif20] quit
[LSRD] interface gigabitethernet2/0/0
[LSRD-GigabitEthernet2/0/0] port link-type access
[LSRD-GigabitEthernet2/0/0] quit
[LSRD] vlan 40
[LSRD-vlan40] port gigabitethernet2/0/0
[LSRD-vlan40] quit
[LSRD] interface vlanif 40
[LSRD-Vlanif40] ip address 10.4.1.2 24
[LSRD-Vlanif40] quit
```

Step 2 Configure OSPF to advertise the network segments that the interfaces are connected to and the host route of the LSR ID.

Configure LSRA.

```
[LSRA] ospf 1
[LSRA-ospf-1] area 0
[LSRA-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[LSRA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[LSRA-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[LSRA-ospf-1-area-0.0.0.0] quit
[LSRA-ospf-1] quit
```

Configure LSRB.

```
[LSRB] ospf 1
[LSRB-ospf-1] area 0
[LSRB-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[LSRB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[LSRB-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[LSRB-ospf-1-area-0.0.0.0] quit
[LSRB-ospf-1] quit
```

Configure LSRC.

```
[LSRC] ospf 1
[LSRC-ospf-1] area 0
[LSRC-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[LSRC-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[LSRC-ospf-1-area-0.0.0.0] network 10.4.1.0 0.0.0.255
[LSRC-ospf-1-area-0.0.0.0] quit
[LSRC-ospf-1] quit
```

Configure LSRD.

```
[LSRD] ospf 1
[LSRD-ospf-1] area 0
[LSRD-ospf-1-area-0.0.0.0] network 4.4.4.9 0.0.0.0
[LSRD-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[LSRD-ospf-1-area-0.0.0.0] network 10.4.1.0 0.0.0.255
```


Copyright © Huawei Technologies Co., Ltd.

```
[LSRD-ospf-1-area-0.0.0.0] quit
[LSRD-ospf-1] quit
```

After the configuration, run the **display ip routing-table** command on each node. You can view that the nodes learn the routes from each other.

Take the display on LSRA as an example.

```
[LSRA] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: 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       InLoopBack1
        2.2.2.9/32  OSPF   10   2           D  10.1.1.2        Vlanif10
        3.3.3.9/32  OSPF   10   2           D  10.3.1.2        Vlanif30
     4.4.4.9/32  OSPF   10   3           D  10.1.1.2        Vlanif10
                 OSPF   10   3           D  10.3.1.2        Vlanif30
       10.1.1.0/24  Direct 0    0           D  10.1.1.1        Vlanif10
       10.1.1.1/32  Direct 0    0           D  127.0.0.1       InLoopBack1
       10.1.1.2/32  Direct 0    0           D  10.1.1.2        Vlanif10
       10.2.1.0/24  OSPF   10   2           D  10.1.1.2        Vlanif10
       10.3.1.0/24  Direct 0    0           D  10.3.1.1        Vlanif30
       10.3.1.1/32  Direct 0    0           D  127.0.0.1       InLoopBack1
       10.3.1.2/32  Direct 0    0           D  10.3.1.2        Vlanif30
       10.4.1.0/24  OSPF   10   2           D  10.3.1.2        Vlanif30
      127.0.0.0/8   Direct 0    0           D  127.0.0.1       InLoopBack1
      127.0.0.1/32  Direct 0    0           D  127.0.0.1       InLoopBack1
```

The next hop of the static LSP on 4.4.4.9/32 from LSRA to LSRD is determined by the routing table. It is shown in boldface. In this example, the next hop IP address is 10.1.1.2/30.

Take the display on LSRD as an example.

```
[LSRD] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 14       Routes : 15
Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface
     1.1.1.9/32  OSPF   10   3           D  10.2.1.1         Vlanif20
                 OSPF   10   3           D  10.4.1.1         Vlanif40
        2.2.2.9/32  OSPF   10   2           D  10.2.1.1        Vlanif20
        3.3.3.9/32  OSPF   10   2           D  10.4.1.1        vlanif40
        4.4.4.9/32  Direct 0    0           D  127.0.0.1       InLoopBack1
       10.1.1.0/24  OSPF   10   2           D  10.2.1.1        Vlanif20
       10.2.1.0/24  Direct 0    0           D  10.2.1.2        Vlanif20
       10.2.1.1/32  Direct 0    0           D  10.2.1.1        Vlanif20
       10.2.1.2/32  Direct 0    0           D  127.0.0.1       InLoopBack1
       10.3.1.0/24  OSPF   10   2           D  10.4.1.1        vlanif40
       10.4.1.0/24  Direct 0    0           D  10.4.1.2        vlanif40
       10.4.1.1/32  Direct 0    0           D  10.4.1.1        vlanif40
       10.4.1.2/32  Direct 0    0           D  127.0.0.1       InLoopBack1
      127.0.0.0/8   Direct 0    0           D  127.0.0.1       InLoopBack1
      127.0.0.1/32  Direct 0    0           D  127.0.0.1       InLoopBack1
```

The next hop of the static LSP on 1.1.1.9/32 from LSRD to LSRA is determined by the routing table. It is shown in boldface. In this example, the next hop IP address is 10.4.1.1/24.

Step 3 Enable basic MPLS functions on each node.

Configure LSRA.

```
[LSRA] mpls lsr-id 1.1.1.9
[LSRA] mpls
[LSRA-mpls] quit
```

Configure LSRB.

Copyright © Huawei Technologies Co., Ltd.

```
[LSRB] mpls lsr-id 2.2.2.9
[LSRB] mpls
[LSRB-mpls] quit
```

Configure LSRC.

```
[LSRC] mpls lsr-id 3.3.3.9
[LSRC] mpls
[LSRC-mpls] quit
```

Configure LSRD.

```
[LSRD] mpls lsr-id 4.4.4.9
[LSRD] mpls
[LSRD-mpls] quit
```

Step 4 Enable MPLS on each interface.

Configure LSRA.

```
[LSRA] interface vlanif 10
[LSRA-Vlanif10] mpls
[LSRA-Vlanif10] quit
[LSRA] interface vlanif 30
[LSRA-Vlanif30] mpls
[LSRA-Vlanif30] quit
```

Configure LSRB.

```
[LSRB] interface vlanif 10
[LSRB-Vlanif10] mpls
[LSRB-Vlanif10] quit
[LSRB] interface vlanif 20
[LSRB-Vlanif20] mpls
[LSRB-Vlanif20] quit
```

Configure LSRC.

```
[LSRC] interface vlanif 30
[LSRC-Vlanif30] mpls
[LSRC-Vlanif30] quit
[LSRC] interface vlanif 40
[LSRC-Vlanif40] mpls
[LSRC-Vlanif40] quit
```

Configure LSRD.

```
[LSRD] interface vlanif 20
[LSRD-Vlanif20] mpls
[LSRD-Vlanif20] quit
[LSRD] interface vlanif 40
[LSRD-Vlanif40] mpls
[LSRD-Vlanif40] quit
```

Step 5 Create a static LSP from LSRA to LSRD.

Configure ingress node LSRA.

```
[LSRA] static-lsp ingress SAtoSD destination 4.4.4.9 32 nexthop 10.1.1.2 out-label
20
```

Configure transit node LSRB.

```
[LSRB] static-lsp transit SAtoSD incoming-interface vlanif 10 in-label 20 nexthop
10.2.1.2 out-label 40
```

Configure egress node LSRD.

```
[LSRD] static-lsp egress SAtoSD incoming-interface vlanif 20 in-label 40
```


Copyright © Huawei Technologies Co., Ltd.

After the configuration, run the **display mpls static-lsp** command on each node to view the status of the static LSP. Take the display on LSRA as an example.

```
[LSRA] display mpls static-lsp
TOTAL          : 1       STATIC LSP(S)
UP             : 1       STATIC LSP(S)
DOWN           : 0       STATIC LSP(S)
Name            FEC                I/O Label  I/O If                 Stat
SAtoSD          4.4.4.9/32         NULL/20    -/Vlanif10             Up
```

The LSP is unidirectional, you need to configure a static LSP from LSRD to LSRA.

Step 6 Create a static LSP from LSRD to LSRA.

Configure ingress node LSRD.

```
[LSRD] static-lsp ingress SDtoSA destination 1.1.1.9 32 nexthop 10.4.1.1 out-label
30
```

Configure transit node LSRC.

```
[LSRC] static-lsp transit SDtoSA incoming-interface vlanif 40 in-label 30 nexthop
10.3.1.1 out-label 60
```

Configure egress node LSRA.

```
[LSRA] static-lsp egress SDtoSA incoming-interface vlanif 30 in-label 60
```

Step 7 Verify the configuration.

After the configuration, run the **ping lsp ip 1.1.1.9 32** command on LSRD, and you can find that the LSP can be pinged.

Run the **display mpls static-lsp** or **display mpls static-lsp verbose** command on each node to check the status and detailed information about the static LSP. Take the display on LSRD as an example.

```
[LSRD] display mpls static-lsp
TOTAL          : 2       STATIC LSP(S)
UP             : 2       STATIC LSP(S)
DOWN           : 0       STATIC LSP(S)
Name            FEC                I/O Label  I/O If                       Stat
SAtoSD            -/-                40/NULL    Vlanif20/-                 Up
SDtoSA          1.1.1.9/32         NULL/30    -/Vlanif40                   Up
[LSRD] display mpls static-lsp verbose
No             : 1
LSP-Name       : SAtoSD
LSR-Type       : Egress
FEC            : -/-
In-Label       : 40
Out-Label      : NULL
In-Interface   : Vlanif20
Out-Interface  : -
NextHop        : -
Static-Lsp Type: Normal
Lsp Status     : Up

No             : 2
LSP-Name       : SDtoSA
LSR-Type       : Ingress
FEC            : 1.1.1.9/32
In-Label       : NULL
Out-Label      : 30
In-Interface   : -
Out-Interface  : Vlanif40
NextHop        : 10.4.1.1
```


Copyright © Huawei Technologies Co., Ltd.

```
Static-Lsp Type: Normal
Lsp Status     : Up
```

----End

Configuration Files

- Configuration file of LSRA

```
#
 sysname LSRA
#
 vlan batch 10 30
#
 mpls lsr-id 1.1.1.9
 mpls
#
interface Vlanif 10
 ip address 10.1.1.1 255.255.255.0
 mpls
#
interface Vlanif 30
 ip address 10.3.1.1 255.255.255.0
 mpls
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 30
#
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 10.3.1.0 0.0.0.255
#
 static-lsp ingress SAtoSD destination 4.4.4.9 32 nexthop 10.1.1.2 out-labe
20
 static-lsp egress SDtoSA incoming-interface Vlanif30 in-label 60
#
return
```

- Configuration file of LSRB

```
#
 sysname LSRB
#
 vlan batch 10 20
#
 mpls lsr-id 2.2.2.9
 mpls
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 mpls
#
interface Vlanif20
 ip address 10.2.1.1 255.255.255.0
 mpls
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
```


Copyright © Huawei Technologies Co., Ltd.

```
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
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 10.2.1.0 0.0.0.255
#
static-lsp transit SAtoSD incoming-interface Vlanif 10 in-label 20 nexthop
10.2
.1.2 out-label 40
#
return
```

- Configuration file of LSRC

```
#
 sysname LSRC
#
 vlan batch 30 40
#
 mpls lsr-id 3.3.3.9
 mpls
#
interface Vlanif30
 ip address 10.3.1.2 255.255.255.0
 mpls
#
interface Vlanif40
 ip address 10.4.1.1 255.255.255.0
 mpls
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 30
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 40
#
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 0.0.0.255
  network 10.4.1.0 0.0.0.255
#
static-lsp transit SDtoSA incoming-interface vlanif 40 in-label 30 nexthop
10.3.1.1 out-label 60
#
return
```

- Configuration file of LSRD

```
#
 sysname LSRD
#
 vlan batch 20 40
#
 mpls lsr-id 4.4.4.9
 mpls
#
interface Vlanif20
 ip address 10.2.1.2 255.255.255.0
 mpls
```


Copyright © Huawei Technologies Co., Ltd.

```
#
interface Vlanif40
 ip address 10.4.1.2 255.255.255.0
 mpls
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 20
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 40
#
interface LoopBack1
 ip address 4.4.4.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 4.4.4.9 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.4.1.0 0.0.0.255
#
 static-lsp egress SAtoSD incoming-interface vlanif 20 in-label 40
 static-lsp ingress SDtoSA destination 1.1.1.9 32 nexthop 10.4.1.1 out-label
30
#
return
```

1.6.2 Example for Configuring Static BFD for Static LSPs

Networking Requirements

As shown in **Figure 1-2**:

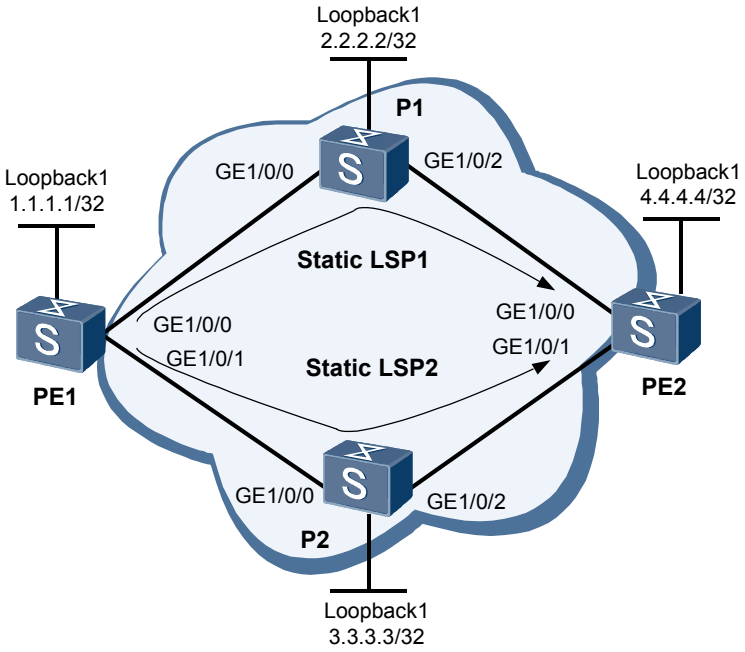
- PE1, PE2, P1, and P2 are in an MPLS domain.
- Two static LSPs are set up between PE1 and PE2; P1 functions as the transit node of **LSP1** and P2 functions as the transit node of **LSP2**.

P and PE devices are switches.

It is required that the connectivity of **LSP1** be detected when MPLS OAM is not used. When the static LSP fails, PE1 can receive the defect notification within 50 ms.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-2 Networking diagram for setting up a static LSP



Switch	Interface	VLANIF interface	IP address
PE1	GE1/0/0	VLANIF10	10.1.1.1/24
PE1	GE1/0/1	VLANIF30	10.3.1.1/24
P1	GE1/0/0	VLANIF10	10.1.1.2/24
P1	GE1/0/2	VLANIF20	10.2.1.1/24
P2	GE1/0/0	VLANIF30	10.3.1.2/24
P2	GE1/0/2	VLANIF40	10.4.1.1/24
PE2	GE1/0/0	VLANIF20	10.2.1.2/24
PE2	GE1/0/1	VLANIF40	10.4.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure VLANIF interfaces.
2. Configure OSPF in the MPLS domain to ensure the connectivity between nodes.
3. On PE1, create a BFD session to detect the static LSP.
4. On PE2, create a BFD session to notify PE1 of defects on the static LSP.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each interface on each node

Copyright © Huawei Technologies Co., Ltd.

- OSPF process ID
- BFD session parameters including the configuration name and minimum intervals for sending and receiving packets

Procedure

Step 1 Create VLANs on PE and P devices and add GE interfaces to the VLANs, create VLANIF interfaces, and assign IP addresses to the VLANIF interfaces.

Configure PE1.

```
<Quidway> system-view
[Quidway] sysname PE1
[PE1] interface loopback1
[PE1-LoopBack1] ip address 1.1.1.1 32
[PE1-LoopBack1] quit
[PE1] interface gigabitethernet1/0/0
[PE1-GigabitEthernet1/0/0] port link-type access
[PE1-GigabitEthernet1/0/0] quit
[PE1] vlan 10
[PE1-vlan10] port gigabitethernet1/0/0
[PE1-vlan10] quit
[PE1] interface vlanif 10
[PE1-Vlanif10] ip address 10.1.1.1 24
[PE1-Vlanif10] quit
[PE1] interface gigabitethernet1/0/1
[PE1-GigabitEthernet1/0/1] port link-type access
[PE1-GigabitEthernet1/0/1] quit
[PE1] vlan 30
[PE1-vlan30] port gigabitethernet1/0/1
[PE1-vlan30] quit
[PE1] interface vlanif 30
[PE1-Vlanif30] ip address 10.3.1.1 24
[PE1-Vlanif30] quit
```

Configure P1.

```
<Quidway> system-view
[Quidway] sysname P1
[P1] interface loopback1
[P1-LoopBack1] ip address 2.2.2.2 32
[P1-LoopBack1] quit
[P1] interface gigabitethernet1/0/0
[P1-GigabitEthernet1/0/0] port link-type access
[P1-GigabitEthernet1/0/0] quit
[P1] vlan 10
[P1-vlan10] port gigabitethernet1/0/0
[P1-vlan10] quit
[P1] interface vlanif 10
[P1-Vlanif10] ip address 10.1.1.2 24
[P1-Vlanif10] quit
[P1] interface gigabitethernet1/0/2
[P1-GigabitEthernet1/0/2] port link-type access
[P1-GigabitEthernet1/0/2] quit
[P1] vlan 20
[P1-vlan20] port gigabitethernet1/0/2
[P1-vlan20] quit
[P1] interface vlanif 20
[P1-Vlanif20] ip address 10.2.1.1 24
[P1-Vlanif20] quit
```

Configure P2.

```
<Quidway> system-view
[Quidway] sysname P2
[P2] interface loopback1
[P2-LoopBack1] ip address 3.3.3.3 32
```


Copyright © Huawei Technologies Co., Ltd.

```
[P2-LoopBack1] quit
[P2] interface gigabitethernet1/0/0
[P2-GigabitEthernet1/0/0] port link-type access
[P2-GigabitEthernet1/0/0] quit
[P2] vlan 30
[P2-vlan30] port gigabitethernet1/0/0
[P2-vlan30] quit
[P2] interface vlanif 30
[P2-Vlanif30] ip address 10.3.1.2 24
[P2-Vlanif30] quit
[P2] interface gigabitethernet1/0/2
[P2-GigabitEthernet1/0/2] port link-type access
[P2-GigabitEthernet1/0/2] quit
[P2] vlan 40
[P2-vlan40] port gigabitethernet1/0/2
[P2-vlan40] quit
[P2] interface vlanif 40
[P2-Vlanif40] ip address 10.4.1.1 24
[P2-Vlanif40] quit
```

Configure PE2.

```
<Quidway> system-view
[Quidway] sysname PE2
[PE2] interface loopback1
[PE2-LoopBack1] ip address 4.4.4.4 32
[PE2-LoopBack1] quit
[PE2] interface gigabitethernet1/0/0
[PE2-GigabitEthernet1/0/0] port link-type access
[PE2-GigabitEthernet1/0/0] quit
[PE2] vlan 20
[PE2-vlan20] port gigabitethernet1/0/0
[PE2-vlan20] quit
[PE2] interface vlanif 20
[PE2-Vlanif20] ip address 10.2.1.2 24
[PE2-Vlanif20] quit
[PE2] interface gigabitethernet1/0/1
[PE2-GigabitEthernet1/0/1] port link-type access
[PE2-GigabitEthernet1/0/1] quit
[PE2] vlan 40
[PE2-vlan40] port gigabitethernet1/0/1
[PE2-vlan40] quit
[PE2] interface vlanif 40
[PE2-Vlanif40] ip address 10.4.1.2 24
[PE2-Vlanif40] quit
```

Step 2 Configure OSPF to advertise the network segments that the interfaces are connected to and the host route of the LSR ID.

Configure PE1.

```
[PE1] ospf 1
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

Configure P1.

```
[P1] ospf 1
[P1-ospf-1] area 0
[P1-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[P1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0] quit
[P1-ospf-1] quit
```

Configure P2.

Copyright © Huawei Technologies Co., Ltd.

```
[P2] ospf 1
[P2-ospf-1] area 0
[P2-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[P2-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[P2-ospf-1-area-0.0.0.0] network 10.4.1.0 0.0.0.255
[P2-ospf-1-area-0.0.0.0] quit
[P2-ospf-1] quit
```

Configure PE2.

```
[PE2] ospf 1
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 10.4.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

Step 3 Enable basic MPLS functions on each node.

Configure PE1.

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls
[PE1-mpls]
```

Configure P1.

```
[P1] mpls lsr-id 2.2.2.2
[P1] mpls
[P1-mpls]
```

Configure P2.

```
[P2] mpls lsr-id 3.3.3.3
[P2] mpls
[P2-mpls]
```

Configure PE2.

```
[PE2] mpls lsr-id 4.4.4.4
[PE2] mpls
[PE2-mpls]
```

Step 4 Enable MPLS on each interface.

Configure PE1.

```
[PE1] interface Vlanif 10
[PE1-Vlanif10] mpls
[PE1-Vlanif10] quit
[PE1] interface Vlanif 30
[PE1-Vlanif30] mpls
[PE1-Vlanif30] quit
```

Configure P1.

```
[P1] interface Vlanif 10
[P1-Vlanif10] mpls
[P1-Vlanif10] quit
[P1] interface Vlanif 20
[P1-Vlanif20] mpls
[P1-Vlanif20] quit
```

Configure P2.

```
[P2] interface Vlanif 30
[P2-Vlanif30] mpls
[P2-Vlanif30] quit
[P2] interface Vlanif 40
```


Copyright © Huawei Technologies Co., Ltd.

```
[P2-Vlanif40] mpls
[P2-Vlanif40] quit
```

Configure PE2.

```
[PE2] interface Vlanif 20
[PE2-Vlanif20] mpls
[PE2-Vlanif20] quit
[PE2] interface Vlanif 40
[PE2-Vlanif40] mpls
[PE2-Vlanif40] quit
```

Step 5 Create a static LSP named **LSP1** with PE1 being the ingress node, P1 being the transit node, and PE2 being the egress node.

Configure ingress node PE1.

```
[PE1] static-lsp ingress LSP1 destination 4.4.4.4 32 nexthop 10.1.1.2 out-label 20
```

Configure transit node P1.

```
[P1] static-lsp transit LSP1 incoming-interface vlanif 10 in-label 20 nexthop
10.2.1.2 out-label 40
```

Configure egress node PE2.

```
[PE2] static-lsp egress LSP1 incoming-interface vlanif 20 in-label 40
```

Step 6 Create a static LSP named **LSP2** with PE2 being the ingress node, P2 being the transit node, and PE1 being the egress node.

Configure ingress node PE1.

```
[PE1] static-lsp ingress LSP2 destination 4.4.4.4 32 nexthop 10.3.1.2 out-label 30
```

Configure transit node P2.

```
[P2] static-lsp transit LSP2 incoming-interface vlanif 30 in-label 30 nexthop
10.4.1.2 out-label 60
```

Configure egress node PE1.

```
[PE2] static-lsp egress LSP2 incoming-interface vlanif 40 in-label 60
```

After the configuration, run the **ping lsp ip 4.4.4.4 32** command on PE1, and you can find that the LSP can be pinged.

Run the **display mpls static-lsp** or **display mpls static-lsp verbose** command on each node to check the status and detailed information about the static LSP. Take the display on PE1 as an example:

```
[PE1] display mpls static-lsp
TOTAL          : 2       STATIC LSP(S)
UP             : 2       STATIC LSP(S)
DOWN           : 0       STATIC LSP(S)
Name            FEC                I/O Label  I/O If                      Stat
LSP1          4.4.4.4/32           NULL/20     Vlanif10/-                 Up
LSP2          4.4.4.4/32           NULL/30     Vlanif30/-                  Up
[PE1] display mpls static-lsp verbose
No             : 1
LSP-Name       : LSP1
LSR-Type       : Ingress
FEC            : 4.4.4.4/32
In-Label       : -
Out-Label      : 20
In-Interface   : -
Out-Interface  : Vlanif10
NextHop        : 10.1.1.2
```


Copyright © Huawei Technologies Co., Ltd.

```
Static-Lsp Type: Normal
Lsp Status     : Up

No             : 2
LSP-Name       : LSP2
LSR-Type       : Ingress
FEC            : 4.4.4.4/32
In-Label       : NULL
Out-Label      : 30
In-Interface   : -
Out-Interface  : Vlanif30
NextHop        : 10.3.1.2
Static-Lsp Type: Normal
Lsp Status     : Up
```

Step 7 Configure the BFD session to detect static LSP **LSP1**.

On ingress node PE1, configure a BFD session, with the local discriminator as 1, the remote discriminator as 2, and the minimal intervals for sending and receiving packets as 500 ms. The PST can be modified.

```
[PE1] bfd
[PE1-bfd] quit
[PE1] bfd PE1toPE2 bind static-lsp LSP1
[PE1-bfd-lsp-session-PE1toPE2] discriminator local 1
[PE1-bfd-lsp-session-PE1toPE2] discriminator remote 2
[PE1-bfd-lsp-session-PE1toPE2] min-tx-interval 500
[PE1-bfd-lsp-session-PE1toPE2] min-rx-interval 500
[PE1-bfd-lsp-session-PE1toPE2] process-pst
[PE1-bfd-lsp-session-PE1toPE2] commit
[PE1-bfd-lsp-session-PE1toPE2] quit
```

On egress node PE2, configure a BFD session to notify PE1 of defects about the static LSP.

```
[PE2] bfd
[PE2-bfd] quit
[PE2] bfd PE2toPE1 bind peer-ip 1.1.1.1
[PE2-bfd-session-PE2toPE1] discriminator local 2
[PE2-bfd-session-PE2toPE1] discriminator remote 1
[PE2-bfd-session-PE2toPE1] min-tx-interval 500
[PE2-bfd-session-PE2toPE1] min-rx-interval 500
[PE2-bfd-session-PE2toPE1] commit
[PE2-bfd-session-PE2toPE1] quit
```

Run the **display bfd session all verbose** command on PE1, and you can view that the BFD session is on PE1 Up.

```
[PE1] display bfd session all verbose
-------------------------------------------------------------------------------
Session MIndex : 4096       State : Up        Name : PE1toPE2
-------------------------------------------------------------------------------
  Local   Discriminator     : 1               Remote Discriminator   : 2
  Session Detect Mode       : Asynchronous Mode Without Echo Function
  BFD Bind Type             : STATIC_LSP Bind
  Bind Session Type         : Static
  Bind Peer IP Address      : 4.4.4.4
  NextHop Ip Address        : 10.1.1.2
  Bind Interface            : -
  Static LSP name           : LSP1
  LSP Token                 : 0x10002
  FSM Board Id              : 0               TOS-EXP                : 7
  Min Tx Interval (ms)      : 500             Min Rx Interval (ms)   : 500
  Actual Tx Interval (ms)   : 500             Actual Rx Interval (ms): 500
  Local Detect Multi        : 3               Detect Interval (ms)   : 3000
  Echo Passive              : Disable         Acl Number             : -
  Proc Interface Status     : Disable         Process PST            : Disable
  WTR Interval (ms)         : -               Local Demand Mode      :
Disable
  Active Multi              : 3
```


Copyright © Huawei Technologies Co., Ltd.

```
  Last Local Diagnostic     : No Diagnostic
  Bind Application          : LSPM | L2VPN | OAM_MANAGER
  Session TX TmrID          : 16407
  Session Detect TmrID      : 16408
  Session Init TmrID        : -                Session WTR TmrID          : -
  Session Echo Tx TmrID     : -
  PDT Index                 : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description       : -
--------------------------------------------------------------------------------
     Total UP/DOWN Session Number : 1/0
```

Run the **display bfd session all verbose** command on PE2 to check the configuration.

```
[PE2] display bfd session all verbose
--------------------------------------------------------------------------------
Session MIndex : 4096       State : Up        Name : PE2toPE1
--------------------------------------------------------------------------------
  Local   Discriminator     : 2                Remote Discriminator   : 1
  Session Detect Mode       : Asynchronous Mode Without Echo Function
  BFD Bind Type             : STATIC_LSP Bind
  Bind Session Type         : Static
  Bind Peer IP Address      : 1.1.1.1
  NextHop Ip Address        : 10.2.1.1
  Bind Interface            : -
  Static LSP name           : LSP1
  LSP Token                 : 0x10002
  FSM Board Id              : 0                TOS-EXP                    : 7
  Min Tx Interval (ms)      : 500              Min Rx Interval (ms)       : 500
  Actual Tx Interval (ms)   : 500              Actual Rx Interval (ms)    : 500
  Local Detect Multi        : 3                Detect Interval (ms)      : 3000
  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          : LSPM | L2VPN | OAM_MANAGER
  Session TX TmrID          : 16407
  Session Detect TmrID      : 16408
  Session Init TmrID        : -                Session WTR TmrID          : -
  Session Echo Tx TmrID     : -
  PDT Index                 : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description       : -
--------------------------------------------------------------------------------
     Total UP/DOWN Session Number : 1/0
```

Step 8 Verify the configuration.

Run the **shutdown** command on VLANIF 20 of P1 to simulate a defect on a static LSP.

```
[P1] interface vlanif 20
[P1-Vlanif20] shutdown
```

Run the **display bfd session all verbose** command to check the status of the BFD session.

```
[PE2] display bfd session all verbose
--------------------------------------------------------------------------------
Session MIndex : 4096       State : Down        Name : PE2toPE1
--------------------------------------------------------------------------------
  Local   Discriminator     : 2                Remote Discriminator   : 1
  Session Detect Mode       : Asynchronous Mode Without Echo Function
  BFD Bind Type             : STATIC_LSP Bind
  Bind Session Type         : Static
  Bind Peer IP Address      : 1.1.1.1
  NextHop Ip Address        : 10.2.1.1
  Bind Interface            : -
  Static LSP name           : LSP1
  LSP Token                 : 0x10002
  FSM Board Id              : 0                TOS-EXP                    : 7
```


Copyright © Huawei Technologies Co., Ltd.

```
  Min Tx Interval (ms)      : 500             Min Rx Interval (ms)      : 500
  Actual Tx Interval (ms)   : 500             Actual Rx Interval (ms)   : 500
  Local Detect Multi        : 3               Detect Interval (ms)      : 3000
  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     :  Control Detection Time Expired
  Bind Application          : LSPM | L2VPN | OAM_MANAGER
  Session TX TmrID          : 16407
  Session Detect TmrID      : 16408
  Session Init TmrID        : -               Session WTR TmrID         : -
  Session Echo Tx TmrID     : -
  PDT Index                 : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description       : -
--------------------------------------------------------------------------------
     Total UP/DOWN Session Number : 1/0
[PE1] display bfd session all verbose
--------------------------------------------------------------------------------
Session MIndex : 4096       State : Init        Name : PE1toPE2
--------------------------------------------------------------------------------
  Local   Discriminator     : 1               Remote Discriminator   : 2
  Session Detect Mode       : Asynchronous Mode Without Echo Function
  BFD Bind Type             : STATIC_LSP Bind
  Bind Session Type         : Static
  Bind Peer IP Address      : 4.4.4.4
  NextHop Ip Address        : 10.1.1.2
  Bind Interface            : -
  Static LSP name           : LSP1
  LSP Token                 : 0x10002
  FSM Board Id              : 0               TOS-EXP                   : 7
  Min Tx Interval (ms)      : 500             Min Rx Interval (ms)      : 500
  Actual Tx Interval (ms)   : 500             Actual Rx Interval (ms)   : 500
  Local Detect Multi        : 3               Detect Interval (ms)     : 3000
  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     : Neighbor Signaled Session Down
  Bind Application          : LSPM | L2VPN | OAM_MANAGER
  Session TX TmrID          : 16407
  Session Detect TmrID      : 16408
  Session Init TmrID        : -               Session WTR TmrID         : -
  Session Echo Tx TmrID     : -
  PDT Index                 : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description       : -
--------------------------------------------------------------------------------
     Total UP/DOWN Session Number : 1/0
```

----End

Configuration Files

- Configuration file of PE1

```
#
 sysname PE1
#
 vlan batch 10 30
#
 bfd
#
 mpls lsr-id 1.1.1.1
 mpls
#
```


Copyright © Huawei Technologies Co., Ltd.

```
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 mpls
#
interface Vlanif30
 ip address 10.3.1.1 255.255.255.0
 mpls
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet1/0/1
 port link-type access
 port default vlan 30
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
bfd PE1toPE2 bind static-lsp LSP1
 discriminator local 1
 discriminator remote 2
 min-tx-interval 500
 min-rx-interval 500
 commit
#
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
  network 10.3.1.0 0.0.0.255
#
 static-lsp ingress LSP1 destination 4.4.4.4 32 nexthop 10.1.1.2 out-labe 20
 static-lsp ingress LSP2 destination 4.4.4.4 32 nexthop 10.3.1.2 out-labe 30
#
return
```

- Configuration file of P1

```
#
 sysname P1
#
 vlan batch 10 20
#
 mpls lsr-id 2.2.2.2
 mpls
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 mpls
#
interface Vlanif20
 ip address 10.2.1.1 255.255.255.0
 mpls
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet1/0/2
 port link-type access
 port default vlan 20
#
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 10.1.1.0 0.0.0.255
  network 10.2.1.0 0.0.0.255
```


Copyright © Huawei Technologies Co., Ltd.

```
#
static-lsp transit LSP1 incoming-interface Vlanif 10 in-label 20 nexthop 10.2
.1.2 out-label 40
#
return
```

- Configuration file of P2

```
#
 sysname P2
#
 vlan batch 30 40
#
 mpls lsr-id 3.3.3.3
 mpls
#
interface Vlanif30
 ip address 10.3.1.2 255.255.255.0
 mpls
#
interface Vlanif40
 ip address 10.4.1.1 255.255.255.0
 mpls
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 30
#
interface GigabitEthernet1/0/2
 port link-type access
 port default vlan 40
#
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 10.3.1.0 0.0.0.255
  network 10.4.1.0 0.0.0.255
#
static-lsp transit LSP2 incoming-interface vlanif 30 in-label 30 nexthop
10.4.1.2 out-label 60
#
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
 vlan batch 20 40
#
 bfd
#
 mpls lsr-id 4.4.4.4
 mpls
#
interface Vlanif20
 ip address 10.2.1.2 255.255.255.0
 mpls
#
interface Vlanif40
 ip address 10.4.1.2 255.255.255.0
 mpls
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 20
#
interface GigabitEthernet1/0/1
  port default vlan 40
```


Copyright © Huawei Technologies Co., Ltd.

```
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
#
bfd PE2toPE1 bind peer-ip 1.1.1.1
 discriminator local 1
 discriminator remote 2
 min-tx-interval 500
 min-rx-interval 500
 commit
#
ospf 1
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.4.1.0 0.0.0.255
#
 static-lsp egress LSP1 incoming-interface vlanif 20 in-label 40
 static-lsp egress LSP2 incoming-interface vlanif 40 in-label 60
#
return
```


Copyright © Huawei Technologies Co., Ltd.

2 MPLS LDP Configuration

About This Chapter

MPLS LDP defines the messages during label distribution and the processing of the messages that are used to negotiate parameters between LSRs and allocate labels to set up an LSP.

Copyright © Huawei Technologies Co., Ltd.

By configuring LDP and IGP synchronization, you can delay the route switchback by suppressing the setup of IGP neighbor relationship till an LDP session is established.

2.10 Configuring LDP GTSM
By configuring LDP GTSM, you can detect TTLs to prevent attacks.

2.11 Configuring LDP GR
By configuring LDP GR, you can realize the uninterrupted forwarding during the master/slave switchover or the protocol restart, which can limit the protocol flapping on the control plane.

2.12 Setting MPLS TTL Processing Modes
This section describes how to set the MPLS TTL processing modes.

2.13 Setting the Mapping of the Precedence in the MPLS Tunnel Label
This section describes how to set the mapping of the precedence in the MPLS tunnel label.

2.14 Setting the DiffServ Mode Supported by MPLS VPNs
This section describes how to set the DiffServ mode supported by the MPLS L3VPN and the MPLS L2VPN.

2.15 Maintaining MPLS LDP
The operations of MPLS LDP maintenance include deleting MPLS statistics, detecting connectivity and reachability of an LSP, and configuring the trap function on an LDP LSP.

2.16 Configuration Examples
This section provides several configuration examples of MPLS LDP.

Copyright © Huawei Technologies Co., Ltd.

2.1 MPLS LDP Overview

Through LDP, LSRs (Label Switched Router) can map the route information at the network layer to the switched paths at the data link layer to set up network layer LSPs.

With the prevalence of the Internet early in the 1990s, the IP technology that adopts the longest match for search becomes a bottleneck in forwarding over networks due to limitation of the hardware technology. The ATM (Asynchronous Transfer Mode) technology uses labels with fixed lengths and maintains a label table with a size much smaller than the size of the routing table. Therefore, compared with IP technology, the ATM technology supports better forwarding performance.

The traditional IP technology is simple to implement but limited in performance. The ATM technology has better performance but is difficult to popularize because of its complex signaling and high cost in deployment. The MPLS (Multiprotocol Label Switching) technology thus emerges to combine the advantages of IP and ATM technologies.

Initially, MPLS emerges to speed up the forwarding of the device. With the development of the ASIC (Application Specific Integrated Circuit) technology, the speed of routing is not the bottleneck to the network development. MPLS, however, does not feature in high-speed forwarding. As MPLS supports multi-layer labels, the connection-oriented forwarding plane, and the connectionless-oriented control plane, MPLS is widely used in VPN (Virtual Private Network), TE (Traffic Engineering), and QoS (Quality of Service).

2.2 MPLS LDP Features Supported by the S9300

MPLS LDP features supported by the system include LDP sessions, LDP LSPs , BFD for LDP LSPs, LDP FRR, LDP GR, LDP and IGP synchronization, and LDP GTSM.

LDP Sessions

Label Distribution Protocol (LDP) sessions are used between LSRs to swap labels.

- Local LDP session: can be set up only between adjacent LSRs.
- Remote LDP session: can be set between adjacent LSRs or non-adjacent LSRs.

LDP LSP

The LDP protocol is used to create dynamic LSPs. If you need not to strictly control the setup process of LSPs or to deploy traffic engineering (TE) on an MPLS network, you are recommended to use LDP to set up LSPs.

BFD for LDP LSP

BFD can detect faults on the data plane of the LDP LSP forwarding path. At the same time, the format of BFD packets is constant, adaptive to implementation in hardware and traversal through the firewall. The advantages of BFD for the data plane of LDP LSP are as follows:

- Quick detection
- Wide range of failure detection for LSPs

At present, in the S9300, BFD can detect LSPs of the following types:

Copyright © Huawei Technologies Co., Ltd.

- Static LSP
- LDP LSP
- TE tunnel

BFD for LSP is dedicated to public bear layer of VPN/PW and provides reliability to applications based on MPLS network, such as VPN FRR, TE FRR, and VLL FRR, to protect services.

When BFD works in unidirectional links, such as LSP and TE, only the IP route along the backward link needs to be reachable. Therefore, the backward link can be IP tunnels, LSPs, or TE tunnels.

LDP FRR

The traditional IP Fast Reroute (FRR) cannot effectively protect the traffic on an MPLS network. The S9300 provides the LDP FRR function as a solution to port protection.

When the network works normally, packets are forwarded through the primary LSP. When the outgoing interface of the primary LSP is Down, packets are forwarded through the bypass LSP. This ensures continuous traffic for a short time before network convergence completes. The S9300 supports the LDP FRR in primary/bypass LSP mode rather than in load balancing mode.

LDP FRR supports BFD to implement quick fault detection. For details of BFD, refer to the Quidway S9300 Terabit Routing Switch *Configuration Guide - Reliability*.

LDP and IGP Synchronization

On a network consisting of active and standby links, when an active link fails, traffic is switched from the active link to the standby link and the traffic interruption takes about hundreds of milliseconds. When the active link recovers from the fault, the traffic is switched back to the active link from the standby link and the traffic interruption takes about 5 seconds.

When LDP is synchronized with an IGP, the interruption duration when traffic is switched back to the active link is shortened to milliseconds.

The basic principle of LDP and IGP synchronization is to delay the switchback of the route by holding back the IGP neighbor establishment, and the latency depends on when the LDP convergence completes. That is, before LSPs of the active link are established, traffic is forwarded through the standby link. After the active link is established, the standby link can be deleted.

LDP GTSM

The Generalized TTL Security Mechanism (GTSM) protects the service above the IP layer by checking whether the TTL value in the IP packet header is within a pre-set range. In applications, GTSM is designed to protect the TCP/IP-based control plane (like routing protocols) from CPU-usage attacks, such as CPU overload attacks.

LDP GR

Graceful Restart (GR) is a key technology to HA implementation. At present, GR is widely applied to switchover and system upgrade.

The S9300 supports LDP GR. When the system performs the switchover, the interface board is not reset and the LDP LSP information on the data plane is stored. In this manner, the LSP forwarding continues and the impact on forwarding the MPLS packets is minimized.

Copyright © Huawei Technologies Co., Ltd.

2.3 Configuring LDP Sessions

An MPLS LDP session can be set up only after a device is configured with an LSR ID and enabled with MPLS LDP.

2.3.1 Establishing the Configuration Task

Before configuring an MPLS LDP session, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you rapidly and correctly finish the configuration task.

Applicable Environment

LDP sessions are classified into local LDP sessions and remote LDP sessions. These sessions are applicable to the following scenarios:

- Setting up an LDP LSP through local LDP sessions

  Before setting up an LDP LSP, you must set up LDP sessions between all directly connected LSRs on the LSP to be set up. For details of LDP LSPs, see **Configuring LDP LSP**.
- Allocating inner labels for L2VPN

  If a VLL or VPLS needs to be created in Martini mode between two LSRs, an LDP session must be set up between the two LSRs before they assign inner labels for each other. For details of L2VPN configuration, refer to the Quidway S9300 Terabit Routing Switch *Configuration Guide - VPN*.

In addition, the S9300 also supports the following attributes:

- LDP transport addresses

  LDP sessions are created on the basis of TCP connection. Before setting up an LDP session, two LSRs need to confirm the LDP transport address of each other, and then set up the TCP connection.

  Generally, it is not recommended to change the LDP transport address.
- LDP timers
  - Hello hold timer
  - Hello send timer

    It is used together with the Hello hold timer to maintain LDP Hello adjacencies.
  - Keepalive hold timer
  - Keepalive send timer

    It is used together with the Keepalive hold timer to maintain LDP sessions.
  - Exponential backoff timer

    It is used to control the interval for the active role to retry setting up an LDP session.
- MD5 authentication

  It is used to improve the security of LDP sessions. A session is set up between two LSRs successfully only when passwords on both ends are consistent.

Pre-configuration Tasks

Before configuring MPLS LDP sessions, complete the following tasks:

Copyright © Huawei Technologies Co., Ltd.

- Configuring a static route or IGP to connect LSRs on the network layer

Data Preparation

To configure MPLS LDP sessions, you need the following data.

No.	Data
1	LSR ID of each node
2	Name and number of the interface on which an LDP session is to be set up
3	Name and IP address of the remote peer on which a remote LDP session is to be set up
4	(Optional) LDP transport address
5	● (Optional) Value of the Hello Hold timer ● (Optional) Value of the Hello send timer ● (Optional) Value of the Keepalive Hold timer ● (Optional) Value of the Keepalive send timer ● (Optional) Value of the Exponential backoff timer
6	● (Optional) Peer IP address of MD5 authentication ● (Optional) Password of MD5 authentication

2.3.2 Configuring the LSR ID

Before enabling MPLS, you must configure LSR ID.

Context

When configuring an LSR ID, note the following:

- The LSR ID must be configured before other MPLS commands are run.
- The LSR ID does not have a default value, and must be configured manually.
- It is recommended to use the address of the loopback interface of the LSR as the LSR ID.
- To modify the configured LSR ID, you must run the **undo mpls** command in the system view to delete all the MPLS configurations.

Do as follows on each LSR in an MPLS domain:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

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


Copyright © Huawei Technologies Co., Ltd.

The LSR ID of the local node is configured.

lsr-id: It is in dotted decimal notation and identifies an LSR.

----End

2.3.3 Enabling MPLS

MPLS features can be configured only after MPLS is enabled.

Context

Do as follows on each LSR in an MPLS domain:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

MPLS is enabled globally and the MPLS view is displayed.

Step 3 Run:

```
quit
```

Return to the system view.

Step 4 Run:

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

The interface to participate in MPLS forwarding is specified.

The interface can be a VLANIF interface or a POS interface.

Step 5 Run:

```
mpls
```

MPLS is enabled on the interface.

----End

2.3.4 Enable Global MPLS LDP

An MPLS LDP session can be set up only after MPLS LDP is enabled.

Context

NOTE

Before enabling the global LDP functions, you must enable global MPLS functions.

Do as follows on each LSR at both ends of an LDP session:

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls ldp
```

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

By default, the global LDP functions are prohibited.

Step 3 (Optional) Run:

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

The LSR ID for LDP instance is configured.

By default, the LSR ID of the LDP instance is the same as that set in **Configuring an LSR ID**. You are recommended to use the default value.

Generally, LDP instances adopt default LSR IDs. In a certain networking solution where VPN instances are adopted, such as BGP/MPLS VPN network, if the VPN address space and the public network address space overlap, you need to configure LSR IDs for LDP instances to ensure successful setup of TCP connections.

----End

2.3.5 Configuring LDP Sessions

MPLS LDP sessions are classified into the locate LDP session and the remote LDP session.

Context

The MPLS LDP session is classified into the local LDP session and the remote LDP session. You can choose one of the following configurations according to your demands:

- **Configure local LDP session**
- **Configure remote LDP session**

  The remote LDP session is set up between two indirectly connected LSRs. The remote LDP session is applied in the following situations:

  - Configuring a VLL or VPLS in Martini mode

Procedure

- Configuring a local LDP session

  Do as follows on two directly connected LSRs. If an LDP session is set up between two directly-connected LSRs, an LDP LSP is set up between these two LSRs. For details of LDP LSPs, see **Configuring LDP LSP**.

  1. Run:

     ```
     system-view
     ```

     The system view is displayed.

Copyright © Huawei Technologies Co., Ltd.

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

   The view of the interface on which LDP session is to be set up is displayed.

   The interface can be a VLANIF interface or a POS interface.

   NOTE

   Before enabling the LDP function, you must enable the MPLS function on the interface.
3. Run:
   mpls ldp

   MPLS LDP is enabled on the interface.

   By default, MPLS LDP is disabled.

   NOTE

   Disabling LDP on the interface may interrupt all LDP sessions on the interface. In addition, all the LSPs based on these sessions are deleted accordingly.

- Configuring a remote MPLS LDP session

  Do as follows on the LSRs on both ends of a remote LDP session. The remote LDP session is set up between two indirectly-connected LSRs or directly-connected LSRs.

  1. Run:
     system-view

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

     The remote peer is created and the remote peer view is displayed.
  3. Run:
     remote-ip *ip-address*

     The IP address of the remote MPLS LDP peer is configured.

     The LSR ID configured in **Configuring an LSR ID** is recommended to be the IP address of the remote MPLS LDP peer.

     NOTE

     Modifying or deleting the configured address of a remote peer leads to the deletion of the related remote LDP session.

----End

2.3.6 (Optional) Configuring LDP Transport Addresses

LSRs need to confirm the transport address of the neighbor before an LDP session is set up between LSRs. By default, a transport address of an LSR is the LSR ID.

Context

LDP sessions are created on the basis of TCP connections. Before two LSRs set up an LDP session, they need to confirm the LDP transport address of each other, and then set up a TCP connection.

Copyright © Huawei Technologies Co., Ltd.

Generally, you are not recommended to modify LDP transport addresses.

To modify LDP transport addresses, do as follows on the two LSRs at both ends of an LDP session:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface vlanif vlan-id
```

The view of the VLANIF interface on which the LDP session is set up is displayed.

Step 3 Run:

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

An LDP transport address is specified as the IP address of a specified interface.

By default, the LDP transport address in the public network is the LSR ID set in **Configuring an LSR ID**.

If multiple links exist between two LSRs and you intend to establish an LDP session on these links, the interfaces on the same side of the session must adopt the default transport address or be configured with the same transport address; otherwise, the LDP session is established only on one link.

There are two methods of configuring LDP sessions on multiple links:

- Use LSR IDs to set up LDP sessions for each link.
- Each link adopts the LDP transport address specified through the **mpls ldp transport-address** command for the same interface.

----End

2.3.7 (Optional) Configuring LDP Timers

LDP timers are classified into Hello hold timer, Hello send timer, Keepalive hold timer, Keepalive send timer, and the Exponential backoff timer, which can be configured as required.

Context

CAUTION

You are recommended to set the value of a timer equal to or greater than the default value. When many LDP sessions are set up between LSRs or the CPU usage is high, the status of LDP sessions may frequently switch between Up and Down if the value of the timer is smaller than the default value. Increasing the values of timers can improve the stability of LDP sessions.

LDP timers are classified into Hello hold timer, Hello send timer, Keepalive hold timer, Keepalive send timer, and the Exponential backoff timer.

Copyright © Huawei Technologies Co., Ltd.

- Hello hold timers are classified into the following timers:
  - Link-Hello hold timer
  - Targeted-Hello hold timer
- Hello send timers are classified into the following timers:
  - Link-Hello send timer
  - Targeted-Hello send timer
- Keepalive hold timers are classified into the following timers:
  - Keepalive hold timers of local LDP session
  - Keepalive hold timers of remote LDP session
- Keepalive send timers are classified into the following timers:
  - Keepalive send timer of local LDP session
  - Keepalive send timer of remote LDP session

You can select the timers and configure them as required.

Procedure

- Configure a link-Hello hold timer.

  Do as follows on the LSRs at both ends of the 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 the LDP session is set up is displayed.

     The interface can be a VLANIF interface or a POS interface.
  3. Run:
     mpls ldp timer hello-hold *interval*

     The link-Hello hold timer is configured.

     By default, the value of the link-Hello hold timer is 45 seconds.

     The value of the link-Hello hold timer configured on the LSR may be not equal to the value of the timer that takes effect. The value of the timer that takes effect is equal to the smaller value of two values of the timers configured on both ends. When an interface is connected to multiple LSRs, the value of the effective timer is equal to the smallest value of the timers configured on all the interfaces.
- Configure a link-Hello send timer.

  Do as follows on each LSR on both ends of a local LDP session:

  1. Run:
     system-view

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

Copyright © Huawei Technologies Co., Ltd.

The view of the interface on which the LDP session is to be set up is displayed.

The interface can be a VLANIF interface or a POS interface.

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 the link-Hello hold timer.

   If the value of the link-Hello send timer is set greater than one third the value of the link-Hello hold timer, the value of the link-Hello send timer that is equal to one third the value of the link-Hello hold timer will take effect.

- Configure a targeted-Hello hold timer.

  Do as follows on the each LSR of both ends of 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 hello-hold *interval*

     The targeted-Hello hold timer is configured.

     By default, the value of the targeted-Hello hold timer is 45 seconds.

     The value of the target-Hello hold timer configured on the LSR may be not equal to the value of the timer that takes effect. The value of the timer that takes effect is equal to the smaller value of two values of the timers configured on both ends.

- Configure a targeted-Hello send timer.

  Do as follows on each LSR on both ends of 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 hello-send *interval*

     A targeted-Hello send timer is configured.

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

Copyright © Huawei Technologies Co., Ltd.

If the value of the targeted-Hello send timer is set greater than one third the value of the targeted-Hello hold timer, the value of the targeted-Hello send timer that is equal to one third the value of the targeted-Hello hold timer will take effect.

- Configure a Keepalive hold timer for the local LDP session.

  Do as follows on the LSRs on both ends of the 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 the LDP session is set up is displayed.

     The interface can be a VLANIF interface or a POS interface.
  3. Run:
     mpls ldp timer keepalive-hold *interval*

     The Keepalive timer is configured for the local LDP session.

     By default, the value of the Keepalive timer of the local LDP session is 45 seconds.

     The value of the Keepalive timer configured on the LSR may be not equal to the value of the timer that takes effect. The value of the timer that takes effect is equal to the smaller value of two values of the timers configured on both ends.

     NOTE

     Modifying the value of KeepAlive hold timer leads to reestablish of LDP sessions and all LSPs based on the LDP sessions.

- Configure a Keepalive send timer for setting up a local LDP session.

  Do as follows on each LSR on both ends of 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 the LDP session is to be set up is displayed.

     The interface can be a VLANIF interface or a POS interface.
  3. Run:
     mpls ldp timer keepalive-send *interval*

     A Keepalive send timer for setting up a local LDP session is configured.

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

     If the value of the Keepalive send timer is set greater than one third the value of the Keepalive hold timer, the value of the Keepalive send time that is equal to one third the value of the Keepalive hold timer will take effect.

- Configuring a Keepalive hold timer for the remote LDP session

Copyright © Huawei Technologies Co., Ltd.

Do as follows on the LSRs at both ends of the 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*

   The Keepalive timer is configured for the remote LDP session.

   By default, the value of the Keepalive timer of the remote LDP session is 45 seconds.

   The value of the Keepalive timer configured on the LSR may be not equal to the value of the timer that takes effect. The value of the timer that takes effect is equal to the smaller value of two values of the timers configured on both ends.

   NOTE

   Modifying the value of KeepAlive hold timer leads to reestablish of LDP sessions and all LSPs based on the LDP sessions.

- Configure a Keepalive send timer for setting up a remote LDP session.

  Do as follows on each LSR on both ends of 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 setting up a remote LDP session is configured.

     By default, for setting up a remote LDP session, the value of a Keepalive send timer is one third the value of the Keepalive hold timer.

     If the value of the Keepalive send timer is set greater than one third the value of the Keepalive hold timer, the value of the Keepalive send time that is equal to one third the value of the Keepalive hold timer will take effect.
- Configure an Exponential backoff timer.

  Do as follows on each LSR on both ends of an LDP session:

  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     mpls

Copyright © Huawei Technologies Co., Ltd.

The MPLS view is displayed.

3. Run:
   quit

   Return to the system view.
4. Run:
   mpls ldp

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

   An Exponential backoff timer is configured.

   By default, the initial value is 15 and the 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.

----End

2.3.8 (Optional) Configuring LDP MD5 Authentication

You can configure LDP MD5 authentication to improve security of the LDP session connection.

Context

To enhance the security of LDP sessions, MD5 authentication is used to set up TCP connections used by LDP.

Both peers of the LDP session can be configured with different authentication modes, but must be with the same password.

Do as follows on each LSR of both ends 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:
md5-password { **plain** | **cipher** } *peer-lsr-id password*

The LDP MD5 authentication is configured.

By default, the MD5 authentication is disabled.

Copyright © Huawei Technologies Co., Ltd.

NOTE

The MD5 authentication password that starts and ends with $@$@ is invalid, because $@$@ is used to distinguish old and new passwords.

----End

2.3.9 Checking the Configuration

After an MPLS LDP session is successfully set up, you can view information about the interface enabled with MPLS and MPLS LDP, LDP, the LDP session status, the LDP session peers, and the remote peer of the LDP session.

Prerequisite

The configurations of the MPLS LDP sessions function are complete.

Procedure

- Run **display mpls interface** [*interface-type interface-number*] [**verbose**]command to check information about an interface enabled with MPLS.
- Run **display mpls ldp** [**all**] [**verbose**] command to check information about LDP.
- Check information about the interface enabled with LDP.
  - Run **display mpls ldp interface** [*interface-type interface-number* | **verbose**] command to check information about the specified interface which is enabled with LDP.
  - Run **display mpls ldp interface** [**all**] [**verbose**] command to check information of all interfaces enabled with LDP.
- Check information about the LDP session status.
  - Run **display mpls ldp session** [**verbose** | *peer-id*] command to check information about the specified LDP session.
  - Run **display mpls ldp session** [**all**] [**verbose**] to check information of all LDP sessions.
- Check information about the LDP peer.
  - Run **display mpls ldp peer** *peer-id* command to check information about the specified LDP peer.
  - Run **display mpls ldp peer** [**all**] [**verbose**] command to check information of all LDP peers.
- Run **display mpls ldp remote-peer** [*remote-peer-name*] command to check information about the LDP remote peer.

----End

Example

Run the **display mpls interface** command, and you can view information about all the interfaces enabled with MPLS.

```
<Quidway> display mpls interface
Interface             Status    TE Attr   LSP Count  CRLSP Count Effective MTU
Vlanif10                 Up         Dis        0           0             1500
```

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

```
<Quidway> display mpls ldp
```


Copyright © Huawei Technologies Co., Ltd.

```
                          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   : On
 DU Explicit Request     : Off          Request Retry Flag     : On
 Label Distribution Mode : Ordered      Label Retention Mode   : Liberal
 Instance Deleting State : No           Instance Reseting State : No
------------------------------------------------------------------------------
```

Run the **display mpls ldp interface** [**verbose**] command, and you can view information about an LDP interface, including the transport address and all timers.

```
<Quidway> 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
 ------------------------------------------------------------------------------
 Vlanif10       Active       DU    172.17.1.1         2495/2514
  ------------------------------------------------------------------------------
<Quidway> display mpls ldp interface verbose

 LDP Interface Information in Public Network
 ------------------------------------------------------------------------------
 Interface Name : Vlanif10
 LDP ID         : 1.1.1.1:0             Transport Address : 1.1.1.1
 Entity Status  : Active                Effective MTU : 1500

 Configured Hello Hold Timer     : 15 Sec
 Negotiated Hello Hold Timer     : 15 Sec
 Configured Hello Send Timer     : 2 Sec
 Configured Keepalive Hold Timer : 45 Sec
 Configured Keepalive Send Timer : 3 Sec
 Configured Delay Timer          : 0 Sec
 Label Advertisement Mode        : Downstream Unsolicited
 Hello Message Sent/Rcvd         : 29913/29878 (Message Count)
 Entity Deletion Status          : No

 ------------------------------------------------------------------------------
```

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

```
<Quidway> display mpls ldp session
 LDP Session(s) in Public Network
 Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
 A '*' before a session means the session is being deleted.
 ------------------------------------------------------------------------------
 PeerID             Status      LAM  SsnRole  SsnAge      KASent/Rcv
 ------------------------------------------------------------------------------
 2.2.2.2:0          Operational DU   Passive  0000:01:36  387/386
 3.3.3.3:0          Operational DU   Passive  0000:01:30  361/361
 ------------------------------------------------------------------------------
 TOTAL: 2 session(s) Found.
<Quidway> 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
```


Copyright © Huawei Technologies Co., Ltd.

```
 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       : 1/1 (Message Count)
 Label Advertisement Mode          : Downstream Unsolicited
 Label Resource Status(Peer/Local) : Available/Available
 Session Age                       : 0000:00:00 (DDDD:HH:MM)
 Session Deletion Status           : No

 Addresses received from peer: (Count: 3)
 10.1.1.2           10.2.1.1            2.2.2.9

 ------------------------------------------------------------------------------
```

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

```
<Quidway> display mpls ldp peer
 LDP Peer Information in Public network
 ------------------------------------------------------------------------------
 PeerID               TransportAddress   DiscoverySource
 ------------------------------------------------------------------------------
 2.2.2.2:0            2.2.2.2            Vlanif20
                                         Vlanif10
 3.3.3.3:0            3.3.3.3            Vlanif40
 ------------------------------------------------------------------------------
 TOTAL: 2 Peer(s) Found.
<Quidway> 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 : ---
 Configured Hello Hold Timer     : 45 Sec
 Negotiated Hello Hold Timer     : 45 Sec
 Configured Hello Send Timer     : ---
 Configured Delay Timer          : 0 Sec
 Hello Packet sent/received      : 61/59
 Remote Peer Deletion Status     : No
 ------------------------------------------------------------------------------
 TOTAL: 1 Peer(s) Found.
```

2.4 Configuring LDP LSP

LDP is a label distribution protocol in an MPLS domain to distribute labels during the setup of an LSP.

2.4.1 Establishing the Configuration Task

Before configuring an LDP LSP, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you rapidly and correctly finish the configuration task.

Applicable Environment

If you need not to strictly control the setup process of LSPs or deploy TE on an MPLS network, you can set up LSPs by using LDP as the label distribution protocol in an MPLS domain.

Copyright © Huawei Technologies Co., Ltd.

The number of LSPs that can be set up on an LSR depends on the capacity and performance of the LSR. Excessive LSPs, however, may lead to unstability of the LSR.

The setup of LSPs requires that proper routes exist on the LSRs and trigger policies be set on the LSRs. Only routes that meet the trigger policy can trigger the setup of LSPs. In this manner, you can control the number of LSPs.

The S9300 provides the following types of policies for controlling the number of LSPs:

- The policies for setting up LSPs on the egress or ingress are as follows:
  - All static routes and IGP routes trigger the setup of LSPs.
  - Labeled BGP routes with 32-bit addresses of the public network trigger the setup of LSPs. For more information, refer to the chapter "BGP/MPLS IP VPN Configuration" in the Quidway S9300 Terabit Routing Switch *Configuration Guide - VPN*.
  - Host routes trigger the setup of LSPs.
  - The setup of LSPs is triggered on the basis of the IP prefix list.
  - All routes trigger the setup of LSPs with LDP being disabled.
- When an LSR is a transit LSR, the IP prefix list can be used to filter routes to prevent the generation of excessive transit LSPs. Only the routes that match the filtering policy can be used to set up the transit LSP.

As defined in RFC 5036, the label advertisement mode of LDP is classified into two modes:

- Downstream Unsolicited (DU)
- Downstream on Demand (DoD)

As defined in RFC 5036, the label distribution control mode of LDP is classified into two modes:

- Independent
- Ordered

As defined in RFC 5036, the label retention mode of LDP is classified into two modes:

- Liberal
- Conservative

The S9300 recommends combination of DU mode + Ordered mode + Liberal mode.

To correctly implement path Maximum Transmission Unit (MTU) detection, an LSR needs to know the MTU of each link to which the LSR is connected. Then, LDP MTU signaling is required.

Pre-configuration Tasks

Before configuring an LDP LSP, complete the following task:

- **Configure local LDP sessions**

Data Preparation

To configure an LDP LSP, you need the following data.

No.	Data
1	(Optional) Configuring Label Distribution and Retention Modes

Copyright © Huawei Technologies Co., Ltd.

No.	Data
2	(Optional) Maximum hops in loop detection

2.4.2 Configuring LDP LSP

An LDP LSP can be set up only after an LDP session is set up.

Prerequisite

Configuring LDP Sessions

Context

The MPLS LDP session is created on neighboring LSRs along the LSP. After the MPLS LDP session is created, the LDP LSP starts to be set up automatically.

2.4.3 (Optional) Configuring Loop Detection

You need to configure the LDP loop detection on each node to avoid loops.

Context

The S9300 does not support loop detection. However, in the scenario where its neighbor supports the loop detection function and requires that the notification about whether the loop detection function be consistent on the two ends, to ensure that the S9300 sets up an LDP session with such a neighbor, do as follows:

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:

```
loop-detect
```

The device is enabled to advertise that the device has the capable of loop detection during the initialization of an LDP session.

NOTE

After the device is configured with the **loop-detect** command, the device still does not support the loop detection function but only has the loop detection negotiation capability.

----End

Copyright © Huawei Technologies Co., Ltd.

2.4.4 (Optional) Configuring LDP MTU Signaling

By configuring the LDP MTU signaling, you can determine the size of MPLS packets to be forwarded according to an MTU.

Context

LDP automatically computes the minimum MTU value of all interfaces on each LSP. Based on the minimum MTU value, MPLS determines the size of packets to be forwarded on the ingress. This prevents the forwarding failure that is caused by large packets on the transit.

Do as follows on each LSR along an LSP:

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 system is enabled to send the MTU TLV.

By default, the system sends the private MTU TLV.

NOTE

Enabling or disabling the sending of the MTU TLV may cause the original LDP session to be re-created.

----End

2.4.5 (Optional) Configuring split horizon

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

Context

By default, an LSR allocates labels to both upstream and downstream devices, which speeds up the convergence of the LDP LSP. In the networking where the DSLAM is deployed, to save memory, it is recommended to configure the **outbound peer** { *peer-id* | **all** } **split-horizon** command on LSRs to enable split horizon. After that, the LSRs allocate labels only to their upstream LDP peers.

Procedure

Step 1 Run:

```
system-view
```


Copyright © Huawei Technologies Co., Ltd.

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
```

The split horizon is enabled on the LSR, that is, the LSR allocates labels only to its upstream LDP peers.

By default, split horizon is disabled on the LDP peer, that is, an LSR allocates labels to both upstream and downstream devices.

----End

2.4.6 (Optional) Configuring the Policy of Triggering to Establish LSPs

By configuring the trigger policy of establishing LSPs, you can use eligible routes to trigger LDP to set up LSPs.

Context

To set up an LSP according to LDP, you need to set the FEC.

NOTE

- The establishment of an LSP requires precisely matched routes on the LSR. If a loopback interface with a 32-bit mask is used, the precisely matched host route is required to trigger the establishment of LSPs.
- Changing LSP triggering policies during the LDP graceful restart (GR) does not take effect.

Do as follows on all the LSRs along the LSP:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Step 3 Run the following commands as required.

- To configure the policy of triggering static routes and IGP routes to establish LSPs, run:

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

- To configure the policy of triggering labeled BGP routes of the public network to establish LSPs, run:

  ```
  lsp-trigger bgp-label-route [ ip-prefix ip-prefix-name ]
  ```

By default, the triggering policy is **host**, namely, the route of host IP with the 32-bit address triggering to establish an LSP.

Copyright © Huawei Technologies Co., Ltd.

- If the triggering policy is **all**, all static route entries and IGP route entries trigger to establish an LSP. BGP public routes cannot trigger to establish LSPs.
- If the triggering policy is **ip-prefix**, only the FEC entry filtered in the IP address prefix list can trigger to establish an LSP.
- If the triggering policy is **none**, the LSP is not established.
- If the triggering policy is **bgp-label-route**, the labeled BGP routes of the public network trigger to establish an LSP.

----End

2.4.7 (Optional) Configuring the Policy of Establishing Transit LSPs

By configuring the trigger policy of establishing transit LSPs, you can use eligible routes to trigger LDP to set up transit LSPs.

Context

Do as follows on the transit node:

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
```

The policy of establishing transit LSPs is configured.

By default, LDP does not filter the received routing information while establishing transit LSPs.

NOTE

Modifying the policy for setting up transit LSPs does not take effect during LDP GR.

----End

2.4.8 Checking the Configuration

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

Prerequisite

The configurations of the LDP LSP function are complete.

Copyright © Huawei Technologies Co., Ltd.

Procedure

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

----End

Example

If the configurations succeed, you can view the following information:

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

```
<Quidway> 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               : 1.1.1.9
 Hop Count Limit         : 32           Path Vector Limit    : 32
 Loop Detection          : Off
 DU Re-advertise Timer   : 10 Sec       DU Re-advertise Flag : On
 DU Explicit Request     : Off          Request Retry Flag   : On
 Label Distribution Mode : Ordered      Label Retention Mode : Liberal
 Instance Deleting State : No           Instance Reseting State : No

 ------------------------------------------------------------------------------
```

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

```
<Quidway> display mpls ldp lsp

 LDP LSP Information
 ------------------------------------------------------------------------------
 DestAddress/Mask  In/OutLabel   UpstreamPeer   NextHop      OutInterface
 ------------------------------------------------------------------------------
 3.3.3.9/32        NULL/1025     -              10.1.1.2     Vlanif10
 ------------------------------------------------------------------------------
 TOTAL: 1 Normal LSP(s) Found.
 TOTAL: 0 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
<Quidway> display mpls lsp
------------------------------------------------------------------------
                LSP Information: LDP LSP
------------------------------------------------------------------------
FEC                In/Out Label  In/Out IF                     Vrf Name
1.1.1.1/32         NULL/3        -/Vlanif10
```


Copyright © Huawei Technologies Co., Ltd.

2.5 Configuring Static BFD for LDP LSP

By configuring a static BFD session to detect an LDP LSP, you can detect LSP connectivity according to specified parameters.

2.5.1 Establishing the Configuration Task

Before configuring a static BFD session to detect an LDP LSP, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you rapidly and correctly finish the configuration task.

Applicable Environment

When the static BFD works in an LDP LSP, note that:

- BFD can be bound only on the ingress of LDP LSP.
- One LSP can be bound to only one BFD session.
- The detection only supports the LDP LSP that is triggered to establish by the host route.

NOTE

BFD for LSP can function properly though the forward path is an LSP and the backward path is an IP link. The forward path and the backward path must be established over the same link; otherwise, if a fault occurs, BFD cannot identify the faulty path. Before deploying BFD, ensure that the forward and backward paths are over the same link so that BFD can correctly identify the faulty path.

Pre-configuration Tasks

Before configuring the static BFD for LDP LSP, complete the following tasks:

- Configuring parameters of the network layer to make the network accessible
- Enabling MPLS LDPs on all nodes and establishing an LDP session
- Configuring an LDP LSP

Data Preparations

Before configuring the static BFD for LDP LSP, you need the following data.

No.	Data
1	BFD configuration name
2	LDP LSP parameters: ● Next hop address of an LSP ● (Optional) Type and number of interfaces
3	Local discriminator and remote discriminator of a BFD session

2.5.2 Enabling Global BFD Capability

You need to only enable BFD on both ends of the link to be detected.

Copyright © Huawei Technologies Co., Ltd.

Context

Do as follows on each LSR on both ends of a link that to be detected:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bfd
```

This node is enabled with the global BFD function. The BFD global view is displayed.

----End

2.5.3 Configuring BFD with Specific Parameters on Ingress

You need to configure BFD parameters on the ingress node before configuring a static BFD session to detect an LDP LSP.

Context

Do as follows on the ingress of an LSP:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

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

The BFD session is bound to a dynamic LSP.

When the IP address of the egress on the LSP to be detected is borrowed or lent, an interface must be specified.

Step 3 Configure the discriminators.

- Run:

  ```
  discriminator local discr-value
  ```

  The local discriminator is configured.

- Or, run:

  ```
  discriminator remote discr-value
  ```

  The remote discriminator is configured.

Copyright © Huawei Technologies Co., Ltd.

NOTE

The local identifier and remote identifier on both ends of a BFD session must accord with each other. Otherwise, the session cannot be established correctly. In addition, the local identifier and remote identifier cannot be modified after configuration.

Step 4 (Optional) Run the following commands to adjust the minimum interval for the local device to send BFD packets, the minimum interval for receiving BFD packets and the local BFD detection multiple:

1. Run the **quit** command to return to the system view.
2. Run the **mpls** command to globally enable MPLS and the enter the MPLS view.
3. Run the **mpls bfd min-tx-interval** *interval* command to adjust the minimum interval for the local device to send BFD packets.

   The minimum interval for the local device to send BFD packets is set.

   When the device is equipped with an FSU, by default, the value is 10 milliseconds; otherwise, by default, the value is 1000 milliseconds.

   If the backward link is an IP link, this parameter is not applicable.

   Actual interval for the local device to send BFD packets = MAX { Locally configured interval for sending BFD packets, Remotely configured interval for receiving BFD packets}; Actual interval for the local to receive BFD packets = MAX {Remotely configured interval for sending BFD packets, Locally configured interval for receiving BFD packets}; Local detection period = Actual interval for the local device to Receive BFD packets x Remotely configured BFD detection multiple.

   For example, assume that the values of parameters are as follows:

   - On the local device, the interval for sending BFD packets is set to 200 ms, the interval for receiving BFD packets is set to 300 ms, and the detection multiple is set to 4.
   - On the peer device, the interval for sending BFD packets is 100 ms, the interval for receiving BFD packets is 600 ms, and the detection multiple is 5.

   Then,

   - On the local device, the actual interval for sending BFD packets is 600 ms calculated by using the formula max {200 ms, 600 ms}, the interval for receiving BFD packets is 300 ms calculated by using the formula max {100 ms, 300 ms}, and the detection period is 1500 ms calculated by 300 ms multiplied by 5.
   - On the peer device, the actual interval for sending local BFD packets is 300 ms obtained by using the formula max {100 ms, 300 ms}, the interval for receiving BFD packets is 600 ms obtained by using the formula max {200 ms, 600 ms}, and the detection period is 2400 ms obtained by 600 ms multiplied by 4.
4. Run the **mpls bfd min-rx-interval** *interval* command to adjust the minimum interval for receiving BFD packets.

   The minimum interval for receiving BFD packets is adjusted on the local device.

   When the device is equipped with an FSU, by default, the value is 10 milliseconds; otherwise, by default, the value is 1000 milliseconds.

   If the backward link is an IP link, this parameter is not applicable.
5. Run the **mpls bfd detect-multiplier** *multiplier* command to adjust the local BFD detection multiple.

Copyright © Huawei Technologies Co., Ltd.

The default value is 3.

6. Run the **quit** command to return to the system view.
7. Run the **bfd** *cfg-name* command to enter the BFD session view.

Step 5 Run:

```
commit
```

The configuration is committed.

----End

Follow-up Procedure

When the BFD session is established and its status is Up, the BFD starts to detect failure in an LDP LSP.

When the LDP LSP is deleted, the BFD status turns Down.

The system does not delete BFD configuration entries and session entries until the LDP session is deleted.

2.5.4 Configuring BFD with Specific Parameters on Egress

You need to configure BFD parameters on the egress node before configuring a static BFD session to detect an LDP LSP.

Context

The IP link, LSP, or TE tunnel can be used as the reverse tunnel to inform the ingress of a fault. To avoid affecting BFD detection, an IP link is preferentially selected to inform the ingress of an LSP fault. If the configured reverse tunnel requires BFD detection, you can configure a pair of BFD sessions for it.

Do as follows on the egress of the LSP:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Configure BFD session:

- For the IP link, run:

  bfd *cfg-name* **bind peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] [**interface** *interface-type interface-number*] [**source-ip** *source-ip*]

- For the dynamic LSP, run:

  bfd *cfg-name* **bind ldp-lsp peer-ip** *ip-address* **nexthop** *ip-address* [**interface** *interface-type interface-number*]

- For the static LSP, run:

  bfd *cfg-name* **bind static-lsp** *lsp-name*

- For MPLS TE, run:

  bfd *cfg-name* **bind mpls-te interface tunnel** *tunnel-number* [**te-lsp**]

Copyright © Huawei Technologies Co., Ltd.

Step 3 Configure the discriminators.

- Run:

  discriminator local *discr-value*

  The local discriminator is configured.

- Run:

  discriminator remote *discr-value*

  The remote discriminator is configured.

NOTE

The local identifier and remote identifier on both ends of a BFD session must accord with each other. The session cannot be established correctly otherwise. In addition, the local identifier and remote identifier cannot be modified after configuration.

Step 4 (Optional) Run the following commands to adjust the minimum interval for the local device to send BFD packets, the minimum interval for receiving BFD packets and the local BFD detection multiple:

1. Run the **quit** command to return to the system view.
2. Run the **mpls** command to globally enable MPLS and the enter the MPLS view.
3. Run the **mpls bfd min-tx-interval** *interval* command to adjust the minimum interval for the local device to send BFD packets.

   The minimum interval for the local device to send BFD packets is set.

   When the device is equipped with an FSU, by default, the value is 10 milliseconds; otherwise, by default, the value is 1000 milliseconds.

   If the backward link is an IP link, this parameter is not applicable.

   Actual interval for the local device to send BFD packets = MAX { Locally configured interval for sending BFD packets, Remotely configured interval for receiving BFD packets}; Actual interval for the local to receive BFD packets = MAX {Remotely configured interval for sending BFD packets, Locally configured interval for receiving BFD packets}; Local detection period = Actual interval for the local device to Receive BFD packets x Remotely configured BFD detection multiple.

   For example, assume that the values of parameters are as follows:

   - On the local device, the interval for sending BFD packets is set to 200 ms, the interval for receiving BFD packets is set to 300 ms, and the detection multiple is set to 4.
   - On the peer device, the interval for sending BFD packets is 100 ms, the interval for receiving BFD packets is 600 ms, and the detection multiple is 5.

   Then,

   - On the local device, the actual interval for sending BFD packets is 600 ms calculated by using the formula max {200 ms, 600 ms}, the interval for receiving BFD packets is 300 ms calculated by using the formula max {100 ms, 300 ms}, and the detection period is 1500 ms calculated by 300 ms multiplied by 5.
   - On the peer device, the actual interval for sending local BFD packets is 300 ms obtained by using the formula max {100 ms, 300 ms}, the interval for receiving BFD packets is 600 ms obtained by using the formula max {200 ms, 600 ms}, and the detection period is 2400 ms obtained by 600 ms multiplied by 4.
4. Run the **mpls bfd min-rx-interval** *interval* command to adjust the minimum interval for receiving BFD packets.

Copyright © Huawei Technologies Co., Ltd.

The minimum interval for receiving BFD packets is adjusted on the local device.

When the device is equipped with an FSU, by default, the value is 10 milliseconds; otherwise, by default, the value is 1000 milliseconds.

If the backward link is an IP link, this parameter is not applicable.

5. Run the **mpls bfd detect-multiplier** *multiplier* command to adjust the local BFD detection multiple.

   The default value is 3.

6. Run the **quit** command to return to the system view.
7. Run the **bfd** *cfg-name* command to enter the BFD session view.

Step 5 Run:

```
commit
```

The configuration is committed.

----End

2.5.5 Checking the Configuration

After the configuration of detecting an LDP LSP through a static BFD session, you can view the BFD configuration, the specified BFD session, and BFD statistics.

Prerequisite

The configurations of the static BFD for LDP LSP function are complete.

Procedure

- Run the **display bfd configuration** { **all** | **static** } command to check the BFD configuration.
- Run the **display bfd session** { **all** | **static** } command to check information about the BFD session.
- Run the **display bfd statistics session** { **all** | **static** } command to check information about BFD statistics.

----End

2.6 Configuring Dynamic BFD for LDP LSP

By configuring a dynamic BFD session to detect an LDP LSP, you does not need to configure BFD parameters. This can speed up link fault detection and reduce workload on configurations.

2.6.1 Establishing the Configuration Task

Before configuring a dynamic BFD session to detect an LDP LSP, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

With dynamic BFD for LDP LSP, failure detection speeds up and the workload of configuring decreases. In addition, LDP FRR is well supported for the LSP for providing better services.

Copyright © Huawei Technologies Co., Ltd.

NOTE

When working in LDP LSP, the dynamic BFD supports only the LDP LSP that is created after the host route is triggered.

BFD for LSP can function properly though the forward path is an LSP and the backward path is an IP link. The forward path and the backward path must be established over the same link; otherwise, if a fault occurs, BFD cannot identify the faulty path. Before deploying BFD, ensure that the forward and backward paths are over the same link so that BFD can correctly identify the faulty path.

Pre-configuration Tasks

Before configuring the dynamic BFD for LDP LSP, complete the following tasks:

- Configuring basic MPLS functions
- Configuring MPLS LDP
- (Optional) Creating the FEC list to enable BFD

Data Preparations

To configure the dynamic BFD for LDP LSP, you need the following data.

No.	Data
1	LSR ID on each node
2	BFD session trigger mode
3	(Optional) FEC list
4	(Optional) BFD parameters

2.6.2 Enabling Global BFD Capability

You need to enable BFD globally on only the ingress node and egress node.

Context

Do as follows on the ingress and egress nodes:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bfd
```

Enable BFD globally.

----End

Copyright © Huawei Technologies Co., Ltd.

2.6.3 Enabling MPLS to Establish BFD Session Dynamically

After enabling BFD on the ingress and egress nodes, you can enable MPLS and dynamically create a BFD session.

Procedure

- Do as follows on the ingress:
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     mpls

     The MPLS view is displayed.
  3. Run:
     mpls bfd enable

     An LDP LSP is enabled with the capability of creating BFD session dynamically.

     The BFD session is not created after this command is run.
- Do as follows on the egress:
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     bfd

     The BFD view is displayed.
  3. Run:
     mpls-passive

     The function of creating BFD session passively is enabled.

     Running this command cannot create a BFD session. The BFD session is not created until the request packet that contains LSP ping of BFD TLV from the ingress.

----End

2.6.4 Configuring the Triggering Policy of Dynamic BFD for LDP LSP

The trigger policies of configuring a dynamic BFD session to detect an LDP LSP are classified into the host mode and FEC list mode, which can be configured as required.

Context

Do as follows on the egress of an LSP to be detected:

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Step 3 Run:

```
mpls bfd-trigger [ host [ nexthop next-hop-address | outgoing-interface interface-type interface-number ] * | fec-list list-name ]
```

The triggering policy to establish the session of dynamic BFD for LDP LSP is configured.

After the command is run, the BFD session is started to create.

There are two triggering policies to establish the session of dynamic BFD for LDP LSP:

- Host mode: is adopted when all host addresses are required to be triggered to create BFD session. You can specify parameters of **nexthop** and **outgoing-interface** to define LSPs that can create a BFD session.
- FEC list mode: is adopted when only a part of host addresses are required to be triggered to create a BFD session. You can use the **fec-list** command to specify host addresses.

----End

2.6.5 (Optional) Adjusting BFD Parameters

By adjusting the BFD detection parameters, you can modify the BFD detection interval and detection multiplier.

Context

Do as follows on the ingress:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bfd
```

The BFD view is displayed.

Step 3 Run:

```
mpls ping interval interval
```

The interval for sending LSP ping packets is adjusted.

Step 4 Run:

```
quit
```


Copyright © Huawei Technologies Co., Ltd.

Exit from the BFD view.

Step 5 Run:

```
mpls
```

The MPLS view is displayed.

Step 6 Run:

```
mpls bfd { min-tx-interval interval | min-rx-interval interval | detect-multiplier multiplier }*
```

BFD time parameters are set.

When the device is equipped with an FSU, by default, the minimum interval for sending BFD packets and the minimum interval for receiving BFD packets are 10 milliseconds; otherwise, by default, the value is 1000 milliseconds. The detection multiple is 3.

Actual interval for the local device to send BFD packets = MAX {Locally configured interval for sending BFD packets, Remotely configured interval for receiving BFD packets}; Actual interval for the local device receive BFD packets = MAX {Remotely configured interval for sending BFD packets, Locally configured interval for receiving BFD packets}; Local detection period = Actual interval for receiving BFD packets x Remotely configured BFD detection multiple.

For example, assume that the values of parameters are as follows:

- On the local device, the interval for sending BFD packets is se to 200 ms, the interval for receiving BFD packets is set to 300 ms, and the detection multiple is set to 4.
- On the peer device, the configured interval for sending BFD packets is 100 ms, the interval for receiving BFD packets is 600 ms, and the detection multiple is 5.

Then,

- On the local device, the actual interval for sending BFD packets is 600 ms calculated by using the formula max {200 ms, 600 ms}, the interval for receiving BFD packets is 300 ms calculated by using the formula max {100 ms, 300 ms}, and the detection period is 1500 ms calculated by 300 ms multiplied by 5.
- On the peer device, the actual interval for sending BFD packets is 300 ms calculated by using the formula max {100 ms, 300 ms}, the interval for receiving BFD packets is 600 ms calculated by using the formula max {200 ms, 600 ms}, and the detection period is 2400 ms calculated by 600 ms multiplied by 4.

----End

2.6.6 Checking the Configuration

After the configuration of detecting an LDP LSP through a dynamic BFD session, you can view the BFD configurations and BFD sessions on the ingress node and egress node.

Prerequisite

The configurations of the dynamic BFD for LDP LSP function are complete.

Procedure

- Run the **display bfd configuration all** [**verbose**] command to check the BFD configuration (ingress).

Copyright © Huawei Technologies Co., Ltd.

- Run the **display bfd configuration passive-dynamic** [**peer-ip** *peer-ip* **remote-discriminator** *discriminator*] [**verbose**] command to check the BFD configuration (egress).
- Run the **display bfd session all** [**verbose**] command to check information about the BFD session (ingress).
- Run the **display bfd session passive-dynamic** [**peer-ip** *peer-ip* **discriminator** *discriminator*] [**verbose**] command to check information about the BFD established passively (egress).
- Run the **display mpls bfd session** [**statistics** | [**protocol** { **ldp** | **cr-static** | **rsvp-te** }] | [**outgoing-interface** *interface-type interface-number*] | [**nexthop** *ip-address*] | [**fec** *fec-address*] | **verbose** | **monitor**] command to check information about BFD session (ingress).

----End

Example

Run the **display bfd session all** command, and you can view the state of BFD session that is established dynamically. The state of the BFD session is Up, and the type of the link that is bound to the session is **LDP_LSP**.

```
<Quidway> display bfd session all verbose
--------------------------------------------------------------------------------
Session MIndex : 256       State : Up        Name : dyn_8192
--------------------------------------------------------------------------------
  Local Discriminator    : 8192           Remote Discriminator   : 8192
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type          : LDP_LSP
  Bind Session Type      : Dynamic
  Bind Peer Ip Address   : 3.3.3.3
  NextHop Ip Address     : 192.168.1.2
  Bind Interface         : Vlanif10
  LSP Token              : 0x3002001
  FSM Board Id           : 3                TOS-EXP                : 6
  Min Tx Interval (ms)   : 100                Min Rx Interval (ms)   : 100
  Actual Tx Interval (ms): 100                Actual Rx Interval (ms): 100
  Local Detect Multi     : 4                Detect Interval (ms)   : 400
  Echo Passive           : Disable          Acl Number             : -
  Destination Port       : 3784             TTL                    : 1
  Proc interface status  : Disable
  WTR Interval (ms)      : --               Process PST            : Enable
  Active Multi           : 3
  Last Local Diagnostic  : No Diagnostic
  Bind Application       : VRRP | LSPM | LSPM | L2VPN | OAM_MANAGER
  Session TX TmrID       : --               Session Detect TmrID   : --
  Session Init TmrID     : --               Session WTR TmrID      : --
  Session Echo Tx TmrID  : -
  PDT Index              : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description    : --
--------------------------------------------------------------------------------
     Total UP/DOWN Session Number : 1/0
```

Run the **display bfd session passive-dynamic verbose** command on the egress, and you can view the state of BFD session that is established passively. The field of BFD bind type is **peer IP address**. This indicates that the BFD packets sent from this ingress are transported through IP routes. BFD parameters cannot be adjusted on the egress. Thus, by default, **min-tx-interval** and **min-tx-interval** are 10 respectively. In fact, however, the actual interval between sending time and the receiving time depends on the negotiation between both ends.

```
<Quidway> display bfd session passive-dynamic verbose
--------------------------------------------------------------------------------
Session MIndex : 256       (Multi Hop) State : Up        Name : dyn_8192
--------------------------------------------------------------------------------
```


Copyright © Huawei Technologies Co., Ltd.

```
  Local Discriminator    : 8192             Remote Discriminator   : 8192
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type          : Peer Ip Address
  Bind Session Type      : Entire_Dynamic
  Bind Peer Ip Address   : 192.168.1.1
  Bind Interface         : --
  FSM Board Id           : 3                TOS-EXP                : 6
  Min Tx Interval (ms)   : 10                Min Rx Interval (ms)   : 10
  Actual Tx Interval (ms): 100               Actual Rx Interval (ms): 100
  Local Detect Multi     : 3                Detect Interval (ms)   : 300
  Echo Passive           : Disable          Acl Number             : -
  Destination Port       : 3784             TTL                    : 253
  Proc Interface Status  : Disable          Process PST            : Disable
  WTR Interval (ms)      : --               Local Demand Mode      : Disable
  Active Multi           : 3
  Last Local Diagnostic  : No Diagnostic
  Bind Application
  Session TX TmrID       : --               Session Detect TmrID   : --
  Session Init TmrID     : --               Session WTR TmrID      : --
  Session Echo Tx TmrID  : -
  PDT Index              : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description    : --
--------------------------------------------------------------------------------
     Total UP/DOWN Session Number : 1/0
```

2.7 Configuring Manual LDP FRR

By configuring Manual LDP FRR, you can quickly switch traffic to the backup LSP when a link fails, which ensures uninterrupted traffic transmission.

2.7.1 Establishing the Configuration Task

Before configuring Manual LDP FRR, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

LDP FRR provides MPLS with a fast reroute function to implement the local port-level backup. In addition, the data loss decreases.

Pre-configuration Tasks

Before configuring LDP FRR, complete the following tasks:

- Configuring MPLS
- Configuring MPLS LDP

If the LDP FRR is based on the BFD, you need to configure the one-hop BFD.

Data Preparation

To configure LDP FRR, you need the following data.

No.	Data
1	Type and number of the interface protected in a primary LSP

Copyright © Huawei Technologies Co., Ltd.

No.	Data
2	Next hop address in a bypass LSP
3	Name of the IP prefix list that can trigger the establishment of bypass LSPs
4	Priority of LSP backup

2.7.2 Enabling Manual LDP FRR

By configuring parameters on the ingress node, you can enable Manual LDP FRR.

Context

Do as follows on the ingress:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

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

The interface view is displayed.

Step 3 Run:

```
mpls ldp frr nexthop nexthop-address [ ip-prefix ip-prefix-name ] [ priority priority ]
```

LDP FRR is enabled on the interface.

On the same interface, you can configure up to 10 LDP FRR entries with different precedences. According to different precedences, only one bypass LSP is generated. The smaller the value is, the higher the precedence is. By default, the precedence value is 50.

NOTE

- LDP FRR cannot be enabled or disabled during the LDP GR.
- If LDP FRR and IP FRR are deployed concurrently, IP FRR is used preferentially.
- When the **undo mpls ldp** command is run to disable the LDP function in the system view or the **undo mpls ldp** command is run to disable the LDP function in the interface view, the LDP FRR configuration in the interface view is not automatically deleted. Only the LDP FRR function is invalid.
- In LDP FRR configuration, the bypass LSP must be in liberal state. That is, the route state of the bypass LSP from ingress to egress must be "Inactive Avd".

----End

2.7.3 (Optional) Configuring Manual LDP FRR Protection Timer

By configuring a Manual LDP FRR protection timer, you can ensure that the primary LDP LSP is not deleted.

Copyright © Huawei Technologies Co., Ltd.

Context

Do as follows on the ingress:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

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

The interface view is displayed.

Step 3 Run:

```
mpls ldp frr timer protect-time protect-time
```

The LDP FRR protection timer is configured on the interface.

----End

Follow-up Procedure

When the LDP FRR protection timer is enabled, and the LDP session goes Down due to an active link failure, the LDP LSP along the active link is not deleted until one of the following conditions is meet:

- LDP FRR protection timer expires.
- The active link route is deleted.
- The interface of the active link goes Down.

2.7.4 (Optional) Allowing BFD to Modify the PST

You need to permit the BFD session to modify the PST only when configuring BFD for Manual LDP FRR.

Context

The procedure is only applicable to configure the LDP FRR based on BFD.

Do as follows on the ingress:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bfd cfg-name
```

The created BFD session view is displayed.

Copyright © Huawei Technologies Co., Ltd.

Step 3 Run:

```
commit
```

The configuration is committed.

By default, BFD does not modify the PST.

----End

2.7.5 Checking the Configuration

After the configuration of Manual LDP FRR, you can view information about Manual LDP FRR-LSPs and BFD-enabled interfaces.

Prerequisite

The configurations of the LDP FRR function are complete.

Procedure

- Run the **display mpls lsp** command to check information about LSPs enabled with LDP FRR.
- Run the **display bfd interface** [*interface-type interface-number*] command to check information about the BFD interface.

----End

2.8 Configuring LDP Auto FRR

By configuring a policy for triggering the setup of backup LSPs, you can control the setup of backup LSPs.

2.8.1 Establishing the Configuration Task

Before configuring LDP Auto FRR, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

In a network where LDP Fast Reroute (FRR) is configured, traffic is fast switched to the backup LSP when a link becomes faulty. In this case, traffic is uninterrupted and is switched within 50 ms.

There are two types of LDP FRR: manual LDP FRR and LDP Auto FRR.

- In the mode of manual LDP FRR, you need to configure a backup LSP by specifying the outbound interfaces or the next hops. The configuration procedure is complex, but the backup LSP can be specified. Therefore, manual LDP FRR is more flexible, and is applicable to the network with a simple structure.
- In the mode of LDP Auto FRR, a backup LSP can be automatically generated according to the triggering policy. The configuration procedure is more simplified. In addition, loops that may occur during the manual configuration can be avoided. Therefore, LDP Auto FRR is applicable to the large-scale network with a complicated structure.

Copyright © Huawei Technologies Co., Ltd.

Pre-configuration Tasks

Before configuring LDP Auto FRR, complete the following tasks:

- Configuring IP addresses for interfaces to ensure that neighboring nodes are reachable at the network layer
- Configuring IS-IS to advertise the network segments connecting to interfaces on each node and to advertise the routes of hosts with Label Switching Router (LSR) IDs
- Configuring MPLS LDP
- Configuring IS-IS Auto FRR

Data Preparation

To configure LDP Auto FRR, you need the following data.

No.	Data
1	Type and number of the interface where a backup LSP is set up
2	Policy for triggering LDP to set up backup LSPs

2.8.2 Enabling LDP Auto FRR

To configure LDP Auto FRR, you need to configure the ingress or transit node.

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:

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

The policy for triggering LDP to set up backup LSPs is configured.

By default, the backup routes with 32-bit addresses trigger LDP to setup backup LSPs.

The **auto-frr lsp-trigger** command is restricted by the **lsp-trigger** command. If both the **auto-frr lsp-trigger** command and the **lsp-trigger** command are configured, the established backup LSPs satisfy both the policy for triggering the setup of LSPs by LDP and the policy for triggering the setup of backup LSPs by LDP.

NOTE

During LDP GR, changing the policy for triggering the setup of backup LSPs is not allowed.

----End

Copyright © Huawei Technologies Co., Ltd.

2.8.3 Checking the Configuration

After the configuration of LDP Auto FRR, you can view information about LDP Auto FRR-LSPs.

Prerequisite

All LDP Auto FRR configurations are complete.

Procedure

- Run the **display mpls lsp** command to view information about the established backup LSP after LDP Auto FRR is enabled.

----End

Example

Enable LDP Auto FRR. You can view that the backup LSP to the destination 2.2.2.9/32 has already been set up. The configuration result is as follows:

```
[Quidway] display mpls lsp

------------------------------------------------------------------------------
                LSP Information: LDP LSP
------------------------------------------------------------------------------
FEC                In/Out Label  In/Out IF                      Vrf Name
2.2.2.9/32         NULL/3        -/Vlanif10
**LDP FRR**         /1025      /Vlanif20
2.2.2.9/32         1024/3        -/Vlanif10
   **LDP FRR**         /1025      /Vlanif20
3.3.3.9/32         NULL/3        -/Vlanif20
   **LDP FRR**         /1025      /Vlanif10
3.3.3.9/32         1025/3        -/Vlanif20
   **LDP FRR**         /1025      /Vlanif10
4.4.4.9/32         NULL/1026     -/Vlanif20
   **LDP FRR**         /1026      /Vlanif10
4.4.4.9/32         1026/1026     -/Vlanif20
   **LDP FRR**         /1026      /Vlanif10
10.1.3.0/24        1027/3        -/Vlanif20
10.1.4.0/24        1028/3        -/Vlanif20
   **LDP FRR**         /1027      /Vlanif10
```

2.9 Configuring Synchronization Between LDP and IGP

By configuring LDP and IGP synchronization, you can delay the route switchback by suppressing the setup of IGP neighbor relationship till an LDP session is established.

2.9.1 Establishing the Configuration Task

Before configuring LDP and IGP synchronization, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

In the networking where primary and backup LSPs are used, synchronization between LDP and IGP is applied to avoid traffic loss in case the primary LSP fails. The situations are as follows:

Copyright © Huawei Technologies Co., Ltd.

- When the primary LSP fails, the IGP traffic and LSP traffic are switched to the backup LSP. When the primary LSP recovers, IGP converges faster than the creation of the LDP session. Thus, IGP traffic is switched back to the primary LSP before the LDP session is set up. This causes the loss of LSP traffic.
- When the primary LSP runs normally whereas the LDP sessions between the nodes along the primary LSP fail, the LSP traffic is switched to the backup LSP. The IGP traffic, however, is still transmitted along the primary LSP. As a result, the LSP traffic is lost.

Pre-configuration Tasks

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

- Configuring MPLS functions
- Configuring MPLS LDP functions globally and on all interfaces

Data Preparation

To configure synchronization between LDP and IGP, you need the following data.

No.	Data
1	Type and number of the interface on which the backup LSP is set up
2	Type and number of the interface on which the timer is configured
3	Timer value

2.9.2 Enabling Synchronization Between LDP and IGP

To enable LDP and IGP synchronization, you need to configure the interfaces of both ends of the link between the crossing node of active and standby links and the LDP neighboring node.

Procedure

- When OSPF runs as an IGP, do as follows on the interfaces of both ends of the link between the crossing node of the active link and the standby link and the LDP neighboring node on the active link:
  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

     Synchronization between LDP and OSPF is enabled on the interface to be protected.
- When IS-IS runs as an IGP, do as follows on the interfaces of both ends of the link between the crossing node of active and standby links and the LDP neighboring node on the active link:

Copyright © Huawei Technologies Co., Ltd.

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 interface to be protected.

----End

2.9.3 (Optional) Setting the Hold-down Timer Value

You can set the value of a hold-down timer, that is, an interval during which an interface waits for the setup of an LDP session without setting up the OSPF neighbor relationship.

Context

Do as follows on the interface:

Procedure

- When OSPF runs as an IGP, do as follows on the interfaces of both ends of the link between the crossing node of active and standby links and the LDP neighboring node on the active link:
  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-down *value*

     The interval OSPF should wait for an LDP session to be established is set.

     By default, the hold-down timer value is 10 seconds.
- When IS-IS runs as an IGP, do as follows on the interfaces of both ends of the link between the crossing node of active and standby links and the LDP neighboring node on the active link:
  1. Run:
     system-view

     The system view is displayed.

Copyright © Huawei Technologies Co., Ltd.

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

   The interface view is displayed.
3. Run:
   isis timer ldp-sync hold-down *value*

   The interval IS-IS should wait for an LDP session to be established is set.

   By default, the hold-down timer value is 10 seconds.

----End

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

You can set the value of a hold-max-cost timer, that is, an interval for advertising the maximum cost through LSAs generated locally.

Context

Do as follows on the interface:

Procedure

- When OSPF runs as an IGP, do as follows on the interfaces of both ends of the link between the crossing node of active and standby links and the LDP neighboring node on the active link:
  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 interval for advertising the maximum cost in the LSAs of local LSRs through OSPF is set.

     By default, the value of the hold-max-cost timer is 10 seconds.

     You can choose different parameters as required.
     - When OSPF carries only LDP services, to ensure that the route selected by OSPF is always the same as the LDP LSP, **infinite** need to be specified.
     - When OSPF carries multiple services including LDP services, to ensure that OSPF route selection and other services still run normally in case the LDP session of the primary LSP fails, *value* can be specified.

     If this command is configured repeatedly, the latest configuration takes effect.
- When IS-IS runs as an IGP, do as follows on the interfaces of both ends of the link between the crossing node of active and standby links and the LDP neighboring node on the active link:

Copyright © Huawei Technologies Co., Ltd.

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 interval for advertising the maximum cost in the LSAs of local LSRs through IS-IS is set.

   By default, the value of the hold-max-cost timer is 10 seconds.

   You can choose different parameters as required.
   - When IS-IS carries only LDP services, to ensure that the route selected by IS-IS is always the same as the LDP LSP, **infinite** need to be specified.
   - When IS-IS carries multiple services including LDP services, to ensure that IS-IS route selection and other services still run normally in case the LDP session of the primary LSP fails, *value* can be specified.

   If this command is configured repeatedly, the latest configuration takes effect.

----End

2.9.5 (Optional) Setting the Delay Timer Value

You can set the value of a delay timer, that is, an period for waiting for the setup of an LSP.

Context

Do as follows on the interfaces of both ends of the link between the crossing node of active and standby links and the LDP neighboring node on the active link:

Procedure

Step 1 Run:
system-view

The system view is displayed.

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

The interface view is displayed.

Step 3 Run:
mpls ldp timer igp-sync-delay *value*

The period of waiting for the LSP setup after the establishment of the LDP session is set.

By default, the value of the delay timer is 10 seconds.

----End

Copyright © Huawei Technologies Co., Ltd.

2.9.6 Checking the Configuration

After the configuration of LDP and IGP synchronization, you can view the synchronization information and route management information on interfaces enabled with LDP and IGP synchronization.

Prerequisite

The configurations of the synchronization between LDP and IGP function are complete.

Procedure

- Run the **display ospf ldp-sync interface** { **all** | *interface-type interface-number* } command to check information about synchronization between LDP and OSPF on the interface.
- Run the **display isis** [*process-id* | **vpn-instance** *vpn-instance-name*] **ldp-sync interface** command to check information about synchronization between LDP and IS-IS on the interface.
- Run the **display rm interface** [*interface-type interface-number* | **vpn-instance** *vpn-instance-name*] command to check information about the route management.

----End

Example

- If the configurations succeed, run the **display ospf ldp-sync** or **display isis ldp-sync** command, and you can view that the status of the interface configured with synchronization between LDP and IGP is Sync-Achieved.
- Run the **display rm interface** command, you can view that the LDP-ISIS or LDP-OSPF is enabled.

2.10 Configuring LDP GTSM

By configuring LDP GTSM, you can detect TTLs to prevent attacks.

2.10.1 Establishing the Configuration Task

Before configuring LDP GTSM, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

The Generalized TTL Security Mechanism (GTSM) prevents attacks by using the TTL detection. An attacker simulates real LDP unicast packets and sends the packets in a large quantity to a node. After receiving the packets, an interface of the LSR directly sends the packets to LDP of the control plane if the interface finds that the packets are sent by the local node, without checking the validity of the packets. Because the control plane of the node needs to process the "legal" packets, the system becomes abnormally busy and CPU usage is high.

GTSM protects the node by checking whether the TTL value in the IP packet header is within a pre-defined range, and thus enhances the system security.

Copyright © Huawei Technologies Co., Ltd.

Pre-configuration Tasks

Before configuring basic LDP GTSM functions, complete the following tasks:

- Enabling MPLS and MPLS LDP

Data Preparation

To configure the basic LDP GTSM functions, you need the following data.

No.	Data
1	LSR ID of an LDP peer
2	Maximum number of valid hops permitted by GTSM

2.10.2 Configuring LDP GTSM

To configure LDP GTSM, you need to configure both LDP peers.

Context

Do as follows on the two LDP peers that need to be configured with GTSM:

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:

```
gtsm peer ip-address valid-ttl-hops hops
```

LDP GTSM is configured.

If the value of *hops* is set to the maximum number of valid hops permitted by GTSM, when the TTL values carried in the packets sent by an LDP peer are within the range [255 - hops + 1, 255], the packets are received; otherwise, the packets are discarded.

----End

2.10.3 Checking the Configuration

After the configuration of LDP GTSM, you can view GTSM statistics.

Prerequisite

The configurations of the LDP GTSM function are complete.

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Run the **display gtsm statistics** { *slot-id* | **all** } command to check the GTSM statistics.

----End

Example

Run the **display gtsm statistics** command, and you can view the GTSM statistics in each slot, including the total number of LDP, BGP, BGP4+, and OSPF packets and the number of packets that are allowed to pass through or the number of dropped packets.

```
<Quidway> display gtsm statistics all
GTSM Statistics Table
------------------------------------------------------------------
SlotId  Protocol  Total Counters  Drop Counters  Pass Counters
------------------------------------------------------------------
 1      BGP       0               0              0
 1      BGPv6     0               0              0
 1      OSPF      0               0              0
 1      LDP       11              0              11
------------------------------------------------------------------
```

2.11 Configuring LDP GR

By configuring LDP GR, you can realize the uninterrupted forwarding during the master/slave switchover or the protocol restart, which can limit the protocol flapping on the control plane.

2.11.1 Establishing the Configuration Task

Before configuring LDP GR, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

It is necessary to enable LDP GR to maintain normal forwarding and resume the LDP session and establish LSPs after the switchover and system update.

NOTE

In practical applications, the system-level GR is usually configured in the hardware environment with dual main control boards. In this manner, the service can be forwarded when the main control board fails.

Pre-configuration Tasks

Before configuring LDP GR, complete the following tasks:

- Configuring the IGP GR function
- Configuring the local MPLS LDP session

Data Preparation

To configure LDP GR, you need the following data.

Copyright © Huawei Technologies Co., Ltd.

No.	Data
1	MPLS LSR ID of the local node
2	Value of the Reconnect timer of the LDP session
3	Value of the LDP Neighbor-liveness timer
4	Value of the LDP Recovery timer

2.11.2 Enabling LDP GR

To enable LDP GR, you need to configure both the GR Restarter and its neighbor.

Context

Do as follows on the LDP GR Restarter and its neighbor nodes:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

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

The local LSR ID is configured.

Step 3 Run:

```
mpls
```

The MPLS function is enabled on the local node and the MPLS view is displayed.

Step 4 Run:

```
quit
```

Return to the system view.

Step 5 Run:

```
mpls ldp
```

The LDP function is enabled on the local node and the LDP view is displayed.

Step 6 Run:

```
graceful-restart
```

The GR function is enabled.

By default, the LDP GR function is disabled.

Copyright © Huawei Technologies Co., Ltd.

NOTE

- When the LDP GR is enabled or disabled, the LDP session is renewed.
- During the LDP GR process, the **undo mpls ldp** and **reset mpls ldp** commands are not permitted.
- During the LDP GR process, the modification of the LSP trigger policy through the **lsp-trigger**, **propagate mapping** and **lsp-trigger bgp-label-route** commands is invalid.
- During the LDP GR process, you are not permitted to run the **mpls ldp frr nexthop** command to enable the LDP FRR. Alternatively, run the **undo mpls ldp frr nexthop** command to disable the LDP FRR.

----End

2.11.3 (Optional) Configuring GR Restarter Timer

You can set the value of a GR Restarter timer, that is, the Neighbor-liveness timer.

Context

Do as follows on the GR restarter:

NOTE

Modifying the values of the LDP GR timers may lead to reestablishment of LDP sessions.

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 neighbor-liveness time
```

The value of the Neighbor-liveness timer is set.

By default, the value of the Neighbor-liveness timer is 600 seconds.

----End

2.11.4 (Optional) Configuring the timer of GR Helper

You can set the values of GR Helper timers, that is, the Reconnect timer for an LDP session and the LSP Recovery timer.

Context

Do as follows on the GR Helper:

NOTE

If any timer value related to LDP GR is modified, the LDP session is recreated.

Copyright © Huawei Technologies Co., Ltd.

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 time
```

The time of the Reconnect timer for the LDP session is set.

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

Step 4 Run:

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

The time of the LSP Recovery timer is set.

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

Step 5 Run:

```
graceful-restart timer neighbor-liveness time
```

The value of the Neighbor-liveness timer is set.

By default, the value of the Neighbor-liveness timer is 600 seconds.

----End

2.11.5 Checking the Configuration

After the configuration of LDP GR, you can view GR information about all protocols related to MPLS, LDP information, and LDP session information.

Prerequisite

The configurations of the LDP GR function are complete.

Procedure

- Run the **display mpls graceful-restart** command to check information about GR of all protocols related to MPLS.
- 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 the LDP session.

----End

Example

- Run the **display mpls ldp** command, and you can view that the state of Graceful Restart is On. That is, LDP GR is enabled.

Copyright © Huawei Technologies Co., Ltd.

- Run the **display mpls ldp** command or the **display mpls ldp session verbose** command, and you can view the values of LDP session Reconnect timer, Neighbor-liveness timer, and LSP Recovery timer.

2.12 Setting MPLS TTL Processing Modes

This section describes how to set the MPLS TTL processing modes.

2.12.1 Establishing the Configuration Task

Applicable Environment

The S9300 provides the following MPLS TTL processing modes:

- If the ingress node is configured with the uniform mode or enabled with the IP TTL propagation function, the IP TTL decreases by one at each hop on an MPLS network. Therefore, the Traceroute output information reflects the actual path where the packet traverses.
- If the ingress node is configured with the pipe mode or disabled with the IP TTL propagation function, the IP TTL does not decrease by one at any hop. The Traceroute output information hides all the hops on the MPLS backbone network, as if the ingress node is directly connected to the egress node.

Pre-configuration Tasks

Before configuring MPLS TTL processing modes, complete the following task:

- Configuring MPLS or MPLS VPN

Data Preparation

None.

2.12.2 Setting MPLS TTL Processing Modes

Context

On an MPLS network, the ingress node and the egress node need to be considered to be directly connected sometimes. In this case, the IP TTL decreases by one on each of the ingress node and the egress node.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
undo ttl propagate
```


Copyright © Huawei Technologies Co., Ltd.

The MPLS TTL processing mode is set to pipe.

By default, the TTL propagate function is enabled and the MPLS TTL processing mode is uniform.

----End

2.13 Setting the Mapping of the Precedence in the MPLS Tunnel Label

This section describes how to set the mapping of the precedence in the MPLS tunnel label.

2.13.1 Establishing the Configuration Task

Applicable Environment

To implement certain QoS functions on an MPLS network, the S9300 needs to determine the packet precedence according to the tunnel label of the MPLS public network. Therefore, you need to map the tunnel label to the EXP field.

Pre-configuration Tasks

Before setting the mapping of the precedence in the tunnel label, complete the following task:

- Creating a DiffServ domain

Data Preparation

None.

2.13.2 Configuring the DiffServ Domain

Context

A DiffServ domain comprises the connected DiffServ nodes, which use the same service policy and implement the same PHBs.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
diffserv domain { default | ds-domain-name }
```

A DiffServ domain is created and the DiffServ domain view is displayed.

Copyright © Huawei Technologies Co., Ltd.

The **default** domain defines the default mappings from packet priorities to PHBs and colors. You can modify the mappings defined in the **default** domain but cannot delete the **default** domain.

----End

2.13.3 Setting the Mapping of the Precedence in the MPLS Tunnel Label

Context

You need to set the mapping of the precedence in the MPLS tunnel label according to the actual situation on the network.

Procedure

- Do as follows on the ingress PE:
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     mpls-qos ingress { **use vpn-label-exp** | **trust upstream** { *ds-name* | **default** | **none** } }

     The public tunnel label is mapped to the EXP field on the ingress PE.
- Do as follows on the P:
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     mpls-qos transit trust upstream { *ds-name* | **default** | **none** }

     The public tunnel label is mapped to the EXP field on the P.
- Do as follows on the egress PE:
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     mpls-qos egress trust upstream { *ds-name* | **default** | **none** }

     The public tunnel label is mapped to the EXP field on the egress PE.

  This command must be run before the public tunnel is set up. If the command is run after the public tunnel is set up, you must restart the MPLS LDP session; otherwise, the command cannot take effect.

----End

Copyright © Huawei Technologies Co., Ltd.

2.14 Setting the DiffServ Mode Supported by MPLS VPNs

This section describes how to set the DiffServ mode supported by the MPLS L3VPN and the MPLS L2VPN.

2.14.1 Establishing the Configuration Task

Applicable Environment

The DiffServ mode supported by the MPLS L3VPN includes three models: pipe, short pipe, and uniform.

- Pipe: The EXP value added to the MPLS label of the packets by the ingress PE is defined by the user. If the EXP value is changed on the MPLS network, the new EXP value is valid only on the MPLS network. The egress PE selects the PHB according to the EXP value of the packet. When the packet leaves the MPLS network, the DSPC value becomes effective again.
- Short pipe: The EXP field added to the MPLS label of the packets by the ingress PE is defined by the user. If the EXP value is changed on the MPLS network, the new EXP value is valid only on the MPLS network. The egress PE selects the PHB according to the DSCP value. When the packet leaves the MPLS network, the DSPC value becomes effective again.
- In the uniform model, the precedences of packets on the IP network and the MPLS network are uniformly defined, that is, the precedence of the packets on the two networks are globally valid. At the ingress PE, each packet is assigned a label and the lower 3 bits in the DSCP field are mapped to the EXP field. If the EXP value is changed on the MPLS network, the change affects the PHB used when the packet leaves the MPLS network. At the egress, the EXP field of the packet is mapped to the DSCP field.

On an L2VPN, the MPLS label is in the outer encapsulation layer of the packet. Therefore, the 802.1p field of the VLAN packets needs to be mapped to the EXP field.

Pre-configuration Tasks

Before configuring the DiffServ mode for the MPLS VPNs, complete the following task:

- Setting the mapping of the precedence in the MPLS tunnel label (for details, see **2.13 Setting the Mapping of the Precedence in the MPLS Tunnel Label**)

Data Preparation

None.

2.14.2 Setting the DiffServ Mode Supported by the MPLS L3VPN

Context

You need to set the DiffServ mode supported by the MPLS L3VPN according to the actual situation of the network.

Copyright © Huawei Technologies Co., Ltd.

NOTE

On F-series boards, when the DiffServ mode is set to short-pipe, a maximum of four domains (with domain IDs 0 to 3) can be configured. If more than four domains are configured, the MPLS short-pipe mode does not take effect after the device restarts. You can query the domain ID by using the **display diffserv domain**.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip vpn-instance vpn-instance-name
```

The VPN instance view is displayed.

Step 3 Run:

```
diffserv-mode { pipe { mpls-exp mpls-exp | domain ds-name } | short-pipe { [ mpls-exp mpls-exp ] domain ds-name } | uniform [ domain ds-name ] }
```

The DiffServ mode supported by the MPLS L3VPN is set.

By default, the DiffServ mode supported by the MPLS L3VPN is uniform.

----End

2.14.3 Setting the DiffServ Mode Supported by MPLS L2VPN

Context

You need to set the DiffServ mode supported by the MPLS L2VPN according to the actual situation of the network.

NOTE

On F-series boards, when the DiffServ mode is set to short-pipe, a maximum of four domains (with domain IDs 0 to 3) can be configured. If more than four domains are configured, the MPLS short-pipe mode does not take effect after the device restarts. You can query the domain ID by using the **display diffserv domain**.

Procedure

- VLL networking
  1. Run:
     ```
     system-view
     ```
     The system view is displayed.
  2. Run:
     ```
     interface interface-type interface-number
     ```
     The AC interface view is displayed.
  3. Run:
     ```
     diffserv-mode { pipe { mpls-exp mpls-exp | domain ds-name } | short-pipe { [ mpls-exp mpls-exp ] domain ds-name } | uniform [ domain ds-name ] }
     ```


Copyright © Huawei Technologies Co., Ltd.

The DiffServ mode applied to the VLL network is set.

By default, the DiffServ mode applied to the VLL network is uniform.

- VPLS networking
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     vsi *vsi-name*

     The VSI view is displayed.
  3. Run:
     diffserv-mode { **pipe** { **mpls-exp** *mpls-exp* | **domain** *ds-name* } | **short-pipe** { [**mpls-exp** *mpls-exp*] **domain** *ds-name* } | **uniform** [**domain** *ds-name*] }

     The DiffServ mode applied to the VPLS network is set.

     By default, the DiffServ mode applied to the VPLS network is uniform.

----End

2.15 Maintaining MPLS LDP

The operations of MPLS LDP maintenance include deleting MPLS statistics, detecting connectivity and reachability of an LSP, and configuring the trap function on an LDP LSP.

2.15.1 Resetting LDP

Resetting LDP may temporarily affect the reestablishment of the LSP. Take care to reset LDP.

Context

CAUTION

Resetting LDP may temporarily affect the reestablishment of the LSP. Take care to reset LDP.

Resetting LDP is prohibited during the LDP GR.

After you confirm to reset LDP, run the following commands in the user view.

Procedure

- Run the **reset mpls ldp** command to reset configurations of the global LDP instance.
- Run the **reset mpls ldp vpn-instance** *vpn-instance-name* command to reset LDP configurations on a specified LDP instance.
- Run the **reset mpls ldp all** command to reset configurations on all LDP instances.
- Run the **reset mpls ldp peer** *peer-id* command to reset a specified peer.

Copyright © Huawei Technologies Co., Ltd.

- Run the **reset mpls ldp vpn-instance** *vpn-instance-name* **peer** *peer-id* command to reset the peer on a specified VPN instance.

----End

2.15.2 Checking the LSP Connectivity and Reachability

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

Context

You can run the following commands in any view to perform MPLS ping and MPLS tracert.

Procedure

- Run:

  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*] [**nexthop** *nexthop-address* | **draft6**]

  MPLS ping is performed.

  If **draft6** is specified, the command is implemented according to draft-ietf-mpls-lsp-ping-06. By default, the command is implemented according to RFC 4379.

- Run:

  tracert lsp [**-a** *source-ip* | **-exp** *exp-value* | **-h** *ttl-value* | **-r** *reply-mode* | **-t** *time-out*] * **ip** *destination-address mask-length* [*ip-address*] [**nexthop** *nexthop-address* | **draft6**]

  MPLS tracert is performed.

  If **draft6** is specified, the command is implemented according to draft-ietf-mpls-lsp-ping-06. By default, the command is implemented according to RFC 4379.

----End

2.15.3 Enabling the Trap Function on the LSP

By configuring the trap function on an LSP, you can notify the NMS of the changes of the LSP status.

Context

Run the following commands in the system view to notify the Network Management System (NMS) of the LSP status change.

By default, the trap function is disabled during the setup of the LDP LSP.

Procedure

- Run the **snmp-agent trap suppress feature-name lsp trap-name** { **mplsxcup** | **mplsxcdown** } **trap-interval** *trap-interval* [**max-trap-number** *max-trap-number*] command in the system view to enable the trap function for the LDP LSP and enable the debugging of excessive mplsxcup or mplsxcdown.

----End

Copyright © Huawei Technologies Co., Ltd.

2.16 Configuration Examples

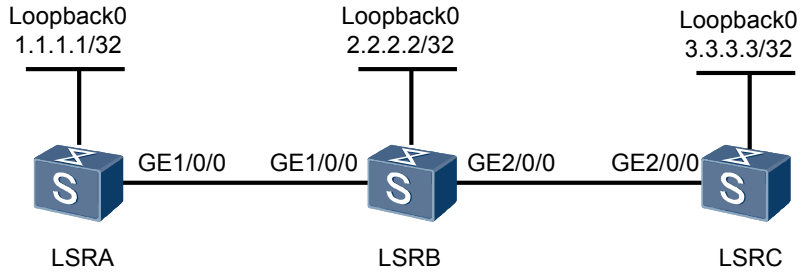
This section provides several configuration examples of MPLS LDP.

2.16.1 Example for Configuring Local LDP Sessions

Networking Requirements

As shown in **Figure 2-1**, local LDP sessions are set up between LSRA and LSRB, and between LSRB and LSRC.

Figure 2-1 Networking diagram for configuring local LDP sessions



Switch	Interface	VLANIF interface	IP address
LSRA	GE1/0/0	VLANIF10	10.1.1.1/24
LSRB	GE1/0/0	VLANIF10	10.1.1.2/24
LSRB	GE2/0/0	VLANIF20	10.2.1.1/24
LSRC	GE2/0/0	VLANIF20	10.2.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and add interfaces to the VLANs, and create VLANIF interfaces.
2. Enable global MPLS and MPLS LDP on the LSRs.
3. Enable MPLS on interfaces of the LSRs.
4. Enable MPLS LDP on interfaces of the two LSRs of the local LDP session.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each interface on each LSR shown in **Figure 2-1**, OSPF process ID, and OSPF area ID
- LSR ID of each node

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Create VLANs on the LSR and add GE interfaces to the VLANs, create VLANIF interfaces, and assign IP addresses to the VLANIF interfaces.

Configure LSRA.

```
<Quidway> system-view
[Quidway] sysname LSRA
[LSRA] interface loopback0
[LSRA-LoopBack0] ip address 1.1.1.1 32
[LSRA-LoopBack0] quit
[LSRA] interface gigabitethernet1/0/0
[LSRA-GigabitEthernet1/0/0] port link-type access
[LSRA-GigabitEthernet1/0/0] quit
[LSRA] vlan 10
[LSRA-vlan10] port gigabitethernet1/0/0
[LSRA-vlan10] quit
[LSRA] interface vlanif 10
[LSRA-Vlanif10] ip address 10.1.1.1 24
```

Configure LSRB.

```
<Quidway> system-view
[Quidway] sysname LSRB
[LSRB] interface loopback0
[LSRB-LoopBack0] ip address 2.2.2.2 32
[LSRB-LoopBack0] quit
[LSRB] interface gigabitethernet1/0/0
[LSRB-GigabitEthernet1/0/0] port link-type access
[LSRB-GigabitEthernet1/0/0] quit
[LSRB] vlan 10
[LSRB-vlan10] port gigabitethernet1/0/0
[LSRB-vlan10] quit
[LSRB] interface vlanif 10
[LSRB-Vlanif10] ip address 10.1.1.2 24
[LSRB-Vlanif10] quit
[LSRB] interface gigabitethernet2/0/0
[LSRB-GigabitEthernet2/0/0] port link-type access
[LSRB-GigabitEthernet2/0/0] quit
[LSRB] vlan 20
[LSRB-vlan20] port gigabitethernet2/0/0
[LSRB-vlan20] quit
[LSRB] interface vlanif 20
[LSRB-Vlanif20] ip address 10.2.1.1 24
```

Configure LSRC.

```
<Quidway> system-view
[Quidway] sysname LSRC
[LSRC] interface loopback0
[LSRC-LoopBack0] ip address 3.3.3.3 32
[LSRC-LoopBack0] quit
[LSRC] interface gigabitethernet2/0/0
[LSRC-GigabitEthernet2/0/0] port link-type access
[LSRC-GigabitEthernet2/0/0] quit
[LSRC] vlan 20
[LSRC-vlan20] port gigabitethernet2/0/0
[LSRC-vlan20] quit
[LSRC] interface vlanif 20
[LSRC-Vlanif20] ip address 10.2.1.2 24
```

Step 2 Configure OSPF to advertise the network segments that the interfaces are connected to and the host route of the LSR ID.

Configure LSRA.

```
[LSRA] ospf 1
[LSRA-ospf-1] area 0
```


Copyright © Huawei Technologies Co., Ltd.

```
[LSRA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[LSRA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
```

Configure LSRB.

```
[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] network 10.1.1.0 0.0.0.255
[LSRB-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
```

Configure LSRC.

```
[LSRC] ospf 1
[LSRC-ospf-1] area 0
[LSRC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[LSRC-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
```

Step 3 Enable MPLS and MPLS LDP on each node.

Configure LSRA.

```
[LSRA] mpls lsr-id 1.1.1.1
[LSRA] mpls
[LSRA-mpls]quit
[LSRA] mpls ldp
```

Configure LSRB.

```
[LSRB] mpls lsr-id 2.2.2.2
[LSRB] mpls
[LSRB-mpls]quit
[LSRB] mpls ldp
```

Configure LSRC.

```
[LSRC] mpls lsr-id 3.3.3.3
[LSRC] mpls
[LSRC-mpls]quit
[LSRC] mpls ldp
```

Step 4 Enable MPLS on each interface.

Configure LSRA.

```
[LSRA] interface vlanif 10
[LSRA-Vlanif10] mpls
[LSRA-Vlanif10] quit
```

Configure LSRB.

```
[LSRB] interface vlanif 10
[LSRB-Vlanif10] mpls
[LSRB-Vlanif10] quit
[LSRB] interface Vlanif 20
[LSRB-Vlanif20] mpls
```

Configure LSRC.

```
[LSRC] interface vlanif 20
[LSRC-Vlanif20] mpls
```

Step 5 Enable MPLS LDP on each interface.

Configure LSRA.

```
[LSRA] interface vlanif 10
[LSRA-Vlanif10] mpls ldp
[LSRA-Vlanif10] quit
```


Copyright © Huawei Technologies Co., Ltd.

Configure LSRB.

```
[LSRB] interface vlanif 10
[LSRB-Vlanif10] mpls ldp
[LSRB-Vlanif10] quit
[LSRB] interface vlanif 20
[LSRB-Vlanif20] mpls ldp
```

Configure LSRC.

```
[LSRC] interface vlanif 20
[LSRC-Vlanif20] mpls ldp
```

Step 6 Verify the configuration.

After the configuration, run the **display mpls ldp session** command. You can view that the status of local LDP sessions between LSRA and LSRB, and between LSRB and LSRC is **Operational**.

Take the display on LSRA as an example.

```
[LSRA] display mpls ldp session

              LDP Session(s) in Public Network
Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
 A '*' before a session means the session is being deleted.
 ------------------------------------------------------------------------------
 Peer-ID            Status      LAM  SsnRole  SsnAge      KA-Sent/Rcv
 ------------------------------------------------------------------------------
 2.2.2.2:0          Operational DU   Passive  000:00:22   91/91
 ------------------------------------------------------------------------------
 TOTAL: 1 session(s) Found.
```

----End

Configuration Files

- Configuration file of LSRA

```
#
 sysname LSRA
#
 vlan batch 10
#
 mpls lsr-id 1.1.1.1
 mpls
#
mpls ldp
#
interface Vlanif 10
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface LoopBack0
 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
#
return
```


Copyright © Huawei Technologies Co., Ltd.

- Configuration file of LSRB

```
#
 sysname LSRB
#
 vlan batch 10 20
#
 mpls lsr-id 2.2.2.2
 mpls
#
mpls ldp
#
interface Vlanif 10
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlanif 20
 ip address 10.2.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack0
 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 10.1.1.0 0.0.0.255
  network 10.2.1.0 0.0.0.255
#
return
```

- Configuration file of LSRC

```
#
 sysname LSRC
#
 vlan batch 20
#
 mpls lsr-id 3.3.3.3
 mpls
#
mpls ldp
#
interface Vlanif 20
 ip address 10.2.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack0
 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 10.2.1.0 0.0.0.255
#
return
```

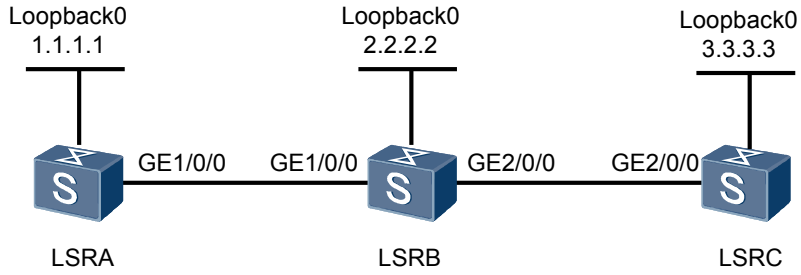

Copyright © Huawei Technologies Co., Ltd.

2.16.2 Example for Configuring a Remote LDP Session

Networking Requirements

As shown in **Figure 2-2**, a remote LDP session is set up between LSRA and LSRC.

Figure 2-2 Networking diagram for configuring a remote LDP session



Switch	Interface	VLANIF interface	IP address
LSRA	GE1/0/0	VLANIF10	10.1.1.1/24
LSRB	GE1/0/0	VLANIF10	10.1.1.2/24
LSRB	GE2/0/0	VLANIF20	10.2.1.1/24
LSRC	GE2/0/0	VLANIF20	10.2.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and add interfaces to the VLANs, and create VLANIF interfaces.
2. Enable global MPLS and MPLS LDP on each LSR.
3. Enable MPLS on interfaces of the LSRs.
4. Enable MPLS LDP on interfaces of the two LSRs of the remote LDP session.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each interface on each LSR shown in **Figure 2-2**, OSPF process ID, and OSPF area ID
- LSR ID of each node

Procedure

Step 1 Create VLANs on the LSR and add GE interfaces to the VLANs, create VLANIF interfaces, and assign IP addresses to the VLANIF interfaces.

Configure LSRA.

Copyright © Huawei Technologies Co., Ltd.

```
<Quidway> system-view
[Quidway] sysname LSRA
[LSRA] interface loopback0
[LSRA-LoopBack0] ip address 1.1.1.1 32
[LSRA-LoopBack0] quit
[LSRA] interface gigabitethernet1/0/0
[LSRA-GigabitEthernet1/0/0] port link-type access
[LSRA-GigabitEthernet1/0/0] quit
[LSRA] vlan 10
[LSRA-Vlan10] port gigabitethernet1/0/0
[LSRA-Vlan10] quit
[LSRA] interface vlanif 10
[LSRA-Vlanif10] ip address 10.1.1.1 24
```

Configure LSRB.

```
<Quidway> system-view
[Quidway] sysname LSRB
[LSRB] interface loopback0
[LSRB-LoopBack0] ip address 2.2.2.2 32
[LSRB-LoopBack0] quit
[LSRB] interface gigabitethernet1/0/0
[LSRB-GigabitEthernet1/0/0] port link-type access
[LSRB-GigabitEthernet1/0/0] quit
[LSRB] vlan 10
[LSRB-Vlan10] port gigabitethernet1/0/0
[LSRB-Vlan10] quit
[LSRB] interface vlanif 10
[LSRB-Vlanif10] ip address 10.1.1.2 24
[LSRB-Vlanif10] quit
[LSRB] interface gigabitethernet2/0/0
[LSRB-GigabitEthernet2/0/0] port link-type access
[LSRB-GigabitEthernet2/0/0] quit
[LSRB] vlan 20
[LSRB-Vlan20] port gigabitethernet2/0/0
[LSRB-Vlan20] quit
[LSRB] interface vlanif 20
[LSRB-Vlanif20] ip address 10.2.1.1 24
```

Configure LSRC.

```
<Quidway> system-view
[Quidway] sysname LSRC
[LSRC] interface loopback0
[LSRC-LoopBack0] ip address 3.3.3.3 32
[LSRC-LoopBack0] quit
[LSRC] interface gigabitethernet2/0/0
[LSRC-GigabitEthernet2/0/0] port link-type access
[LSRC-GigabitEthernet2/0/0] quit
[LSRC] vlan 20
[LSRC-Vlan20] port gigabitethernet2/0/0
[LSRC-Vlan20] quit
[LSRC] interface vlanif 20
[LSRC-Vlanif20] ip address 10.2.1.2 24
```

Step 2 Configure OSPF to advertise the network segments that the interfaces are connected to and the host route of the LSR ID.

Configure LSRA.

```
[LSRA] ospf 1
[LSRA-ospf-1] area 0
[LSRA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[LSRA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
```

Configure LSRB.

```
[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
```


Copyright © Huawei Technologies Co., Ltd.

```
[LSRB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[LSRB-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
```

Configure LSRC.

```
[LSRC] ospf 1
[LSRC-ospf-1] area 0
[LSRC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[LSRC-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
```

Step 3 Enable MPLS and MPLS LDP on each node.

Configure LSRA.

```
[LSRA] mpls lsr-id 1.1.1.1
[LSRA] mpls
[LSRA-mpls]quit
[LSRA] mpls ldp
```

Configure LSRB.

```
[LSRB] mpls lsr-id 2.2.2.2
[LSRB] mpls
[LSRB-mpls]quit
[LSRB] mpls ldp
```

Configure LSRC.

```
[LSRC] mpls lsr-id 3.3.3.3
[LSRC] mpls
[LSRC-mpls] quit
[LSRC] mpls ldp
```

Step 4 Enable MPLS on each interface.

Configure LSRA.

```
[LSRA] interface vlanif 10
[LSRA-Vlanif10] mpls
[LSRA-Vlanif10] quit
```

Configure LSRB.

```
[LSRB] interface vlanif 10
[LSRB-Vlanif10] mpls
[LSRB-Vlanif10] quit
[LSRB] interface vlanif 20
[LSRB-Vlanif20] mpls
```

Configure LSRC.

```
[LSRC] interface vlanif 20
[LSRC-Vlanif20] mpls
```

Step 5 Specify the name and IP address of the remote peer on the two LSRs of a remote LDP session.

Configure LSRA.

```
[LSRA] mpls ldp remote-peer LSRC
[LSRA-mpls-ldp-remote-LSRC] remote-ip 3.3.3.3
[LSRA-mpls-ldp-remote-LSRC] quit
```

Configure LSRC.

```
[LSRC] mpls ldp remote-peer LSRA
[LSRC-mpls-ldp-remote-LSRA] remote-ip 1.1.1.1
[LSRC-mpls-ldp-remote-LSRA] quit
```

Step 6 Verify the configuration.

Copyright © Huawei Technologies Co., Ltd.

After the configuration, run the **display mpls ldp session** command on the node. You can view that the status of the remote LDP session between LSRA and LSRC is **Operational**.

Take the display on LSRA as an example.

```
[LSRA] display mpls ldp session

 LDP Session(s) in Public Network
 ------------------------------------------------------------------------------
 Peer-ID            Status      LAM  SsnRole  SsnAge      KASent/Rcv
 ------------------------------------------------------------------------------
 3.3.3.3:0          Operational DU   Passive  000:00:01   6/6
 ------------------------------------------------------------------------------
 TOTAL: 1 session(s) Found.
 LAM : Label Advertisement Mode      SsnAge Unit : DDD:HH:MM
```

Run the **display mpls ldp remote-peer** command on the two LSRs of the remote LDP session, and you can view information about the remote peer.

----End

Configuration Files

- Configuration file of LSRA

```
#
 sysname LSRA
#
 vlan batch 10
#
 mpls lsr-id 1.1.1.1
 mpls
#
mpls ldp
#
 mpls ldp remote-peer LSRC
 remote-ip 3.3.3.3
 undo remote-ip pwe3
#
interface Vlanif 10
 ip address 10.1.1.1 255.255.255.0
 mpls
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface LoopBack0
 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
#
return
```

- Configuration file of LSRB

```
#
 sysname LSRB
#
 vlan batch 10 20
#
 mpls lsr-id 2.2.2.2
 mpls
#
mpls ldp
#
```


Copyright © Huawei Technologies Co., Ltd.

```
interface Vlanif 10
 ip address 10.1.1.2 255.255.255.0
 mpls
#
interface Vlanif 20
 ip address 10.2.1.1 255.255.255.0
 mpls
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack0
 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 10.1.1.0 0.0.0.255
  network 10.2.1.0 0.0.0.255
#
return
```

- Configuration file of LSRC

```
#
 sysname LSRC
#
 vlan batch 20
#
 mpls lsr-id 3.3.3.3
 mpls
#
mpls ldp
#
 mpls ldp remote-peer LSRA
 remote-ip 1.1.1.1
 undo remote-ip pwe3
#
interface Vlanif 20
 ip address 10.2.1.2 255.255.255.0
 mpls
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack0
 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 10.2.1.0 0.0.0.255
#
return
```

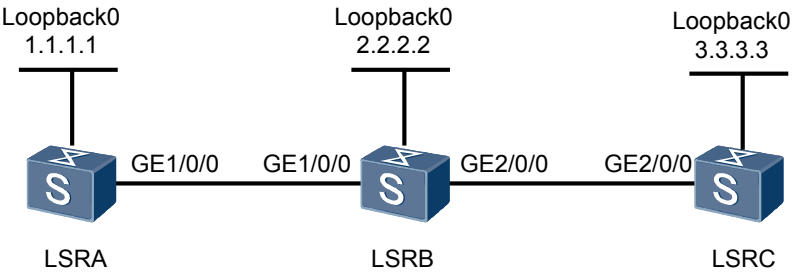
2.16.3 Example for Configuring an LDP LSP

Networking Requirements

As shown in **Figure 2-3**, an LDP LSP is set up between LSRA and LSRC.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-3 Networking diagram for configuring an LDP LSP



Switch	Interface	VLANIF interface	IP address
LSRA	GE1/0/0	VLANIF10	10.1.1.1/24
LSRB	GE1/0/0	VLANIF10	10.1.1.2/24
LSRB	GE2/0/0	VLANIF20	10.2.1.1/24
LSRC	GE2/0/0	VLANIF20	10.2.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a local LDP session.
2. Modify the triggering policy for establishing LDP LSPs on the LSRs.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each interface on each LSR shown in **Figure 2-3**, OSPF process ID, and OSPF area ID
- Modified the policy for triggering the establishment of LDP LSPs.

Procedure

Step 1 Configure the LDP LSP.

After the configuration in **2.16.1 Example for Configuring Local LDP Sessions**, all the LSRs triggers the establishment of LDP LSPs according to the host route, which is the default triggering policy.

Run the **display mpls ldp lsp** command on the LSRs, and you can view that all the host routes trigger the establishment of LDP LSPs.

Take the display on LSRA as an example.

Copyright © Huawei Technologies Co., Ltd.

```
[LSRA] display mpls ldp lsp

LDP LSP Information
 ------------------------------------------------------------------------------
 DestAddress/Mask   In/OutLabel   UpstreamPeer    Next-Hop        Out-Interface
 ------------------------------------------------------------------------------
 1.1.1.1/32         3/NULL        2.2.2.2         127.0.0.1       InLoop0
 2.2.2.2/32         NULL/3        2.2.2.2         10.1.1.2        Vlanif10
 3.3.3.3/32         NULL/1025     2.2.2.2         10.1.1.2        Vlanif10
 ------------------------------------------------------------------------------
 TOTAL: 3 Normal LSP(s) Found.
 TOTAL: 0 Liberal LSP(s) Found.

 A '*' before a LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stale
```

NOTE

Generally, the default triggering policy is used. That is, the establishment of an LDP LSP is triggered by the host route. You can perform the following procedures to modify the policy for triggering the establishment of LDP LSPs as required.

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

Modify the policy for triggering the establishment of as **all** on the LSRs so that all the static routes and IGP routes can trigger the establishment of the LDP LSPs.

Configure LSRA.

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

Configure LSRB.

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

Configure LSRC.

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

Step 3 Verify the configuration.

Run the **display mpls ldp lsp** command, and you can view the establishment of the LDP LSP. Take the display on LSRA as an example.

```
[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   InLoop0
*1.1.1.1/32         Liberal
 2.2.2.2/32         NULL/3        -               10.1.1.2    Vlanif10
 2.2.2.2/32         1024/3        2.2.2.2         10.1.1.2    Vlanif10
 3.3.3.3/32         NULL/1025     -               10.1.1.2    Vlanif10
 3.3.3.3/32         1025/1025     2.2.2.2         10.1.1.2    Vlanif10
 10.1.1.0/30        3/NULL        2.2.2.2         10.1.1.1    Vlanif10
*10.1.1.0/30        Liberal
 10.1.2.0/30        NULL/3        -               10.1.1.2    Vlanif10
 10.1.2.0/30        1026/3        2.2.2.2         10.1.1.2    Vlanif10
 ------------------------------------------------------------------------------
 TOTAL: 8 Normal LSP(s) Found.
 TOTAL: 2 Liberal LSP(s) Found.
```


Copyright © Huawei Technologies Co., Ltd.

```
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 LSRA

```
#
 sysname LSRA
#
 vlan batch 10
#
 mpls lsr-id 1.1.1.1
 mpls
  lsp-trigger all
#
mpls ldp
#
interface Vlanif 10
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface LoopBack0
 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
#
return
```

- Configuration file of LSRB

```
#
 sysname LSRB
#
 vlan batch 10 20
#
 mpls lsr-id 2.2.2.2
 mpls
  lsp-trigger all
#
mpls ldp
#
interface Vlanif 10
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlanif 20
 ip address 10.2.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
```


Copyright © Huawei Technologies Co., Ltd.

```
 port link-type access
 port default vlan 20
#
interface LoopBack0
 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 10.1.1.0 0.0.0.255
  network 10.2.1.0 0.0.0.255
#
return
```

- Configuration file of LSRC

```
#
 sysname LSRC
#
 vlan batch 20
#
 mpls lsr-id 3.3.3.3
 mpls
  lsp-trigger all
#
mpls ldp
#
interface Vlanif 20
 ip address 10.2.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack0
 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 10.2.1.0 0.0.0.255
#
return
```

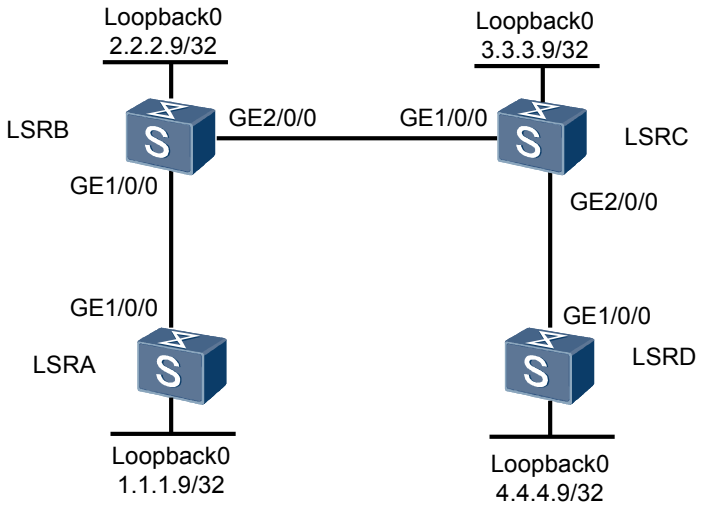
2.16.4 Example for Configuring a Transit LSP Through the IP Prefix List

Networking Requirements

As shown in **Figure 2-4**, the LDP LSPs are set up between the nodes. LSRB, however, permits only the FEC of 4.4.4.9/32 to establish the transit LSP.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-4 Networking diagram for configuring transit LSPs



Switch	Interface	VLANIF interface	IP address
LSRA	GE1/0/0	VLANIF10	10.1.1.1/24
LSRB	GE1/0/0	VLANIF10	10.1.1.2/24
LSRB	GE2/0/0	VLANIF20	10.2.1.1/24
LSRC	GE1/0/0	VLANIF20	10.2.1.2/24
LSRC	GE2/0/0	VLANIF30	10.3.1.1/24
LSRD	GE1/0/0	VLANIF30	10.3.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and add physical interfaces to the VLANs, and create VLANIF interfaces.
2. Configure the IP address of each interface on each node and the address of the loopback interface used as the LSR ID, and configure OSPF to advertise the network segments that the interfaces are connected to and the host route of the LSR ID.
3. Enable MPLS and MPLS LDP globally on the nodes and configure the policy for triggering the establishment of LSPs.
4. Configure the IP prefix list for controlling the LSPs.
5. Filter the routes of transit LSPs by using the IP prefix list on transit node LSRB.
6. Enable MPLS and MPLS LDP on each interface.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each interface on each LSR shown in **Figure 2-4**, OSPF process ID, and OSPF area ID

Copyright © Huawei Technologies Co., Ltd.

- Policy for triggering the establishment of LSPs
- Name of the IP prefix list and routes to be filtered on the transit node

Procedure

Step 1 Create VLANs and add interfaces to the VLANs, and create VLANIF interfaces.

For details, see **2.16.2 Example for Configuring a Remote LDP Session**.

Step 2 Configure the IP address of each interface on each node and configure OSPF to advertise the network segments that the interfaces are connected to and the host route of the LSR ID.

As shown in **Figure 2-4**, configure the IP address and mask of each interface, including the loopback interface, and configure OSPF to advertise the network segments that the interfaces are connected to and the host route of the LSR ID. The configuration details are not mentioned here.

Step 3 Configure the IP prefix list on transit node LSRB.

Configure the IP prefix list on transit node LSRB to permit only 4.4.4.9/32 on LSRD to establish the transit LSP.

```
[LSRB]ip ip-prefix FilterOnTransit permit 4.4.4.9 32
```

Step 4 Configure basic MPLS functions on each node and interface and enable LDP.

Configure LSRA.

```
[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 vlanif10
[LSRA-Vlanif10] mpls
[LSRA-Vlanif10] mpls ldp
[LSRA-Vlanif10] quit
```

Configure LSRB.

```
[LSRB] mpls lsr-id 2.2.2.9
[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 Vlanif10
[LSRB-Vlanif10] mpls
[LSRB-Vlanif10] mpls ldp
[LSRB-Vlanif10] quit
[LSRB] interface Vlanif20
[LSRB-Vlanif20] mpls
[LSRB-Vlanif20] mpls ldp
[LSRB-Vlanif20] quit
```

The configurations of LSRC and LSRD are similar to the configuration of LSRA, and are not mentioned here.

Step 5 Verify the configuration.

Run the **display mpls ldp lsp** command, and you can view the establishment of the LDP LSPs.

Check the LDP LSP on LSRA.

Copyright © Huawei Technologies Co., Ltd.

```
[LSRA] display mpls ldp lsp
LDP LSP Information
 ------------------------------------------------------------------------------
 SN     DestAddress/Mask   In/OutLabel   Next-Hop        In/Out-Interface
 ------------------------------------------------------------------------------
 1      1.1.1.9/32         3/NULL        127.0.0.1       Vlanif10/InLoop0
 2      2.2.2.9/32         NULL/3        10.1.1.2        -------/Vlanif10
 3      4.4.4.9/32         NULL/1027     10.1.1.2        -------/Vlanif10
 4      10.2.1.0/24        NULL/3        10.1.1.2        -------/Vlanif10
 ------------------------------------------------------------------------------
 TOTAL: 4 Normal LSP(s) Found.
 TOTAL: 0 Liberal LSP(s) Found.

 A '*' before a LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stale
```

Check the LDP LSP on LSRB.

```
[LSRB] display mpls ldp lsp
                  LDP LSP Information
 ------------------------------------------------------------------------------
 SN     DestAddress/Mask   In/OutLabel   Next-Hop        In/Out-Interface
 ------------------------------------------------------------------------------
 1      1.1.1.9/32         NULL/3        10.1.1.1        -------/Vlanif10
 2      2.2.2.9/32         3/NULL        127.0.0.1       Vlanif10/InLoop0
 3      2.2.2.9/32         3/NULL        127.0.0.1       Vlanif20/InLoop0
 4      3.3.3.9/32         NULL/3        10.2.1.2        -------/Vlanif20
 5      4.4.4.9/32         NULL/1026     10.2.1.2        -------/Vlanif20
 6      4.4.4.9/32         1027/1026     10.2.1.2        Vlanif20/Vlanif20
 7      10.1.1.0/24        3/NULL        10.1.1.2        Vlanif10/Vlanif10
 8      10.2.1.0/24        3/NULL        10.2.1.1        Vlanif10/Vlanif20
 9      10.3.1.0/24        NULL/3        10.2.1.2        -------/Vlanif20
 ------------------------------------------------------------------------------
 TOTAL: 9 Normal LSP(s) Found.
 TOTAL: 0 Liberal LSP(s) Found.

 A '*' before a LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stal
```

Check the LDP LSP on LSRC.

```
[LSRC] display mpls ldp lsp
                   LDP LSP Information
-------------------------------------------------------------------------------
SN     DestAddress/Mask   In/OutLabel   Next-Hop        In/Out-Interface
-------------------------------------------------------------------------------
1      2.2.2.9/32         NULL/3        10.2.1.1        -------/Vlanif20
2      2.2.2.9/32         1024/3        10.2.1.1        Vlanif20/Vlanif20
3      3.3.3.9/32         3/NULL        127.0.0.1       Vlanif20/InLoop0
4      3.3.3.9/32         3/NULL        127.0.0.1       Vlanif20/InLoop0
5      4.4.4.9/32         NULL/3        10.3.1.2        -------/Vlanif30
6      4.4.4.9/32         1025/3        10.3.1.2        Vlanif10/Vlanif30
7      10.1.1.0/24        NULL/3        10.1.2.1        -------/Vlanif20
8      10.1.1.0/24        1026/3        10.1.2.1        Vlanif30/Vlanif20
9      10.2.1.0/24        3/NULL        10.2.1.2        Vlanif30/Vlanif20
10     10.3.1.0/24       3/NULL        10.3.1.1        Vlanif20/Vlanif30
-------------------------------------------------------------------------------
TOTAL: 10 Normal LSP(s) Found.
TOTAL: 0 Liberal LSP(s) Found.
A '*' before a LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
```

Check the LDP LSP on LSRD.

```
[LSRD] display mpls ldp lsp
                   LDP LSP Information
 ------------------------------------------------------------------------------
 SN     DestAddress/Mask   In/OutLabel   Next-Hop        In/Out-Interface
 ------------------------------------------------------------------------------
 1      2.2.2.9/32         NULL/1024     10.3.1.1        -------/Vlanif30
```


Copyright © Huawei Technologies Co., Ltd.

```
2      3.3.3.9/32         NULL/3        10.3.1.1        -------/Vlanif30
3      4.4.4.9/32         3/NULL        127.0.0.1       Vlanif30/InLoop0
4      10.1.1.0/24        NULL/1025     10.3.1.1        -------/Vlanif30
5      10.2.1.0/24        NULL/3        10.3.1.1        -------/Vlanif30
 ------------------------------------------------------------------------------
TOTAL: 5 Normal LSP(s) Found.
TOTAL: 0 Liberal LSP(s) Found.

A '*' before a LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
```

According to the preceding information, only the LDP LSP to the destination 4.4.4.4/32 that takes LSRB as the transit node exists on each node, and other LDP LSPs that do not take LSRB as the transit node exist on each node. This is because the IP prefix list is configured.

----End

Configuration Files

- Configuration file of LSRA

```
#
 sysname LSRA
#
 vlan batch 10
#
 mpls lsr-id 1.1.1.9
 mpls
  lsp-trigger all
#
mpls ldp
#
interface Vlanif 10
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface LoopBack0
 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
#
return
```

- Configuration file of LSRB

```
#
 sysname LSRB
#
 vlan batch 10 20
#
 mpls lsr-id 2.2.2.9
 mpls
  lsp-trigger all
#
mpls ldp
  propagate mapping for ip-prefix FilterOnTransit
#
interface Vlanif 10
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
```


Copyright © Huawei Technologies Co., Ltd.

```
#
interface Vlanif 20
 ip address 10.2.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack0
 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 10.2.1.0 0.0.0.255
#
 ip ip-prefix FilterOnTransit index 10 permit 4.4.4.9 32
#
return
```

- Configuration file of LSRC

```
#
 sysname LSRC
#
 vlan batch 20 30
#
 mpls lsr-id 3.3.3.9
 mpls
  lsp-trigger all
#
mpls ldp
#
interface Vlanif 20
 ip address 10.2.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlanif 30
 ip address 10.3.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 20
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 30
#
interface LoopBack0
 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 0.0.0.255
  network 10.3.1.0 0.0.0.255
#
return
```

- Configuration file of LSRD

Copyright © Huawei Technologies Co., Ltd.

```
#
 sysname LSRD
#
 vlan batch 30
#
 mpls lsr-id 4.4.4.9
 mpls
  lsp-trigger all
#
mpls ldp
#
interface Vlanif 30
 ip address 10.3.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 30
#
interface LoopBack0
 ip address 4.4.4.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 4.4.4.9 0.0.0.0
  network 10.3.1.0 0.0.0.255
#
return
```

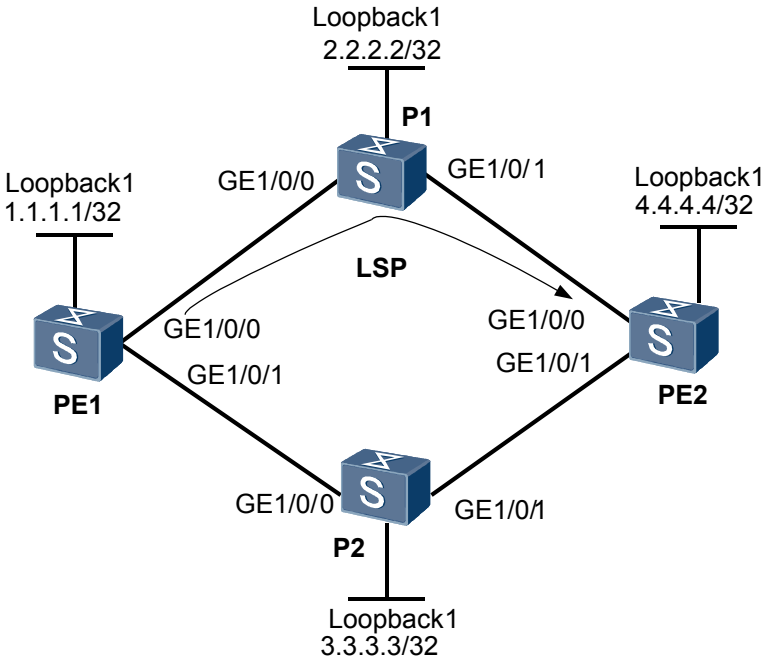
2.16.5 Example for Configuring Static BFD for LDP LSPs

Networking Requirements

As shown in **Figure 2-5**, an LDP LSP is set up along the path PE1 → P1→ PE2 and the path PE2 → P2 → PE1 is an IP link. Static BFD is required to detect the connectivity of the LDP LSP.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-5 Networking diagram for configuring static BFD for LDP LSPs



Device	Interface	VLANIF interface	IP address
PE1	GE1/0/0	VLANIF10	10.1.1.1/24
	GE1/0/1	VLANIF30	10.3.1.1/24
P1	GE1/0/0	VLANIF10	10.1.1.2/24
	GE1/0/1	VLANIF20	10.2.1.1/24
P2	GE1/0/0	VLANIF30	10.3.1.2/24
	GE1/0/1	VLANIF40	10.4.1.1/24
PE2	GE1/0/0	VLANIF20	10.2.1.2/24
	GE1/0/1	VLANIF40	10.4.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANIF interfaces, and use OSPF in the entire MPLS domain to ensure the connectivity between the nodes.
2. Set up an LDP LSP along the path PE1-P1-PE2.
3. On PE1, configure a BFD session that is bound to the LDP LSP.
4. On PE2, configure a BFD session that is bound to the IP link to notify PE1 of the detected LDP LSP faults.

Copyright © Huawei Technologies Co., Ltd.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each interface on each node
- OSPF process ID
- BFD configuration name, local discriminator, and remote discriminator

Procedure

Step 1 Create VLANs on PE and P devices and add GE interfaces to the VLANs, create VLANIF interfaces, and assign IP addresses to the VLANIF interfaces and configure OSPF.

As shown in **Figure 2-5**, configure IP addresses and masks for the interfaces, including loopback interfaces.

Configure OSPF on all the nodes and advertise host routes of the loopback interfaces. The configuration details are not mentioned here.

After the configuration, LSRs can ping each other. Run the **display ip routing-table** command on each LSR, and you can view the routing entries to the LSRs.

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

Configure PE1.

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface vlanif 10
[PE1-Vlanif10] mpls
[PE1-Vlanif10] mpls ldp
```

Configure P1.

```
[P1] mpls lsr-id 2.2.2.2
[P1] mpls
[P1-mpls] quit
[P1] mpls ldp
[P1-mpls-ldp] quit
[P1] interface vlanif 10
[P1-Vlanif10] mpls
[P1-Vlanif10] mpls ldp
[P1] interface vlanif 20
[P1-Vlanif20] mpls
[P1-Vlanif20] mpls ldp
```

Configure PE2.

```
[PE2] mpls lsr-id 4.4.4.4
[PE2] mpls
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface vlanif 20
[PE2-Vlanif20] mpls
[PE2-Vlanif120] mpls ldp
```

Run the **display mpls ldp lsp** command, and you can view that an LDP LSP destined for 4.4.4.9/32 is set up on PE1.

```
<PE1> display mpls ldp lsp
```


Copyright © Huawei Technologies Co., Ltd.

```
                          LDP LSP Information
-------------------------------------------------------------------------------
SN     DestAddress/Mask   In/OutLabel   Next-Hop        In/Out-Interface
-------------------------------------------------------------------------------
1      1.1.1.1/32         3/NULL        127.0.0.1       Vlanif10/InLoop0
2      2.2.2.2/32         NULL/3        10.1.1.2        -------/Vlanif10
3      4.4.4.4/32         NULL/1025     10.1.1.2        -------/Vlanif10
-------------------------------------------------------------------------------
TOTAL: 3 Normal LSP(s) Found.
TOTAL: 0 Liberal LSP(s) Found.

A '*' before a LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
```

Step 3 Enable global BFD on the two nodes of the detected link.

Configure PE1.

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

Configure PE2.

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

Step 4 On the ingress node, configure a BFD session that is bound to the LDP LSP.

Configure PE1.

```
<PE1> system-view
[PE1] bfd pe1tope2 bind ldp-lsp peer-ip 4.4.4.4 nexthop 10.1.1.2 interface
vlanif10
[PE1-bfd-lsp-session-pe1tope2] discriminator local 1
[PE1-bfd-lsp-session-pe1tope2] discriminator remote 2
[PE1-bfd-lsp-session-pe1tope2] process-pst
[PE1-bfd-lsp-session-pe1tope2] commit
[PE1-bfd-lsp-session-pe1tope2] quit
```

Step 5 On the egress node, configure a BFD session that is bound to the IP link to notify the ingress node of LDP LSP faults.

Configure PE2.

```
<PE2> system-view
[PE2] bfd pe2tope1 bind  peer-ip 1.1.1.1
[PE2-bfd-session-pe2tope1] discriminator local 2
[PE2-bfd-session-pe2tope1] discriminator remote 1
[PE2-bfd-session-pe2tope1] commit
[PE2-bfd-session-pe2tope1] quit
```

Step 6 Verify the configuration.

After the configuration, run the **display bfd session all verbose** command on the ingress node, and you can view that the State field is displayed as **Up** and the BFD Bind Type field is displayed as **LDP_LSP**.

```
[PE1] display bfd session all verbose
-------------------------------------------------------------------------------
Session MIndex : 256          State : Up           Name : pe1tope2
-------------------------------------------------------------------------------
  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   : 4.4.4.4
  NextHop Ip Address     : 10.1.1.2
```


Copyright © Huawei Technologies Co., Ltd.

```
  Bind Interface         : Vlanif10
  LSP Token              : 0x10000
  FSM Board Id           : 1                TOS-EXP                : 7
  Min Tx Interval (ms)   : 1000             Min Rx Interval (ms)   : 1000
  Actual Tx Interval (ms): 1000             Actual Rx Interval (ms): 1000
  Local Detect Multi     : 3                Detect Interval (ms)   : 3000
  Echo Passive           : Disable          Acl Number             : -
  Proc Interface Status  : Disable          Process PST            : Enable
  WTR Interval (ms)      : -                Local Demand Mode      : Disable
  Active Multi           : 3
  Last Local Diagnostic  : Neighbor Signaled Session Down(Receive AdminDown)
  Bind Application       : LSPM | L2VPN | OAM_MANAGER
  Session TX TmrID       : 94               Session Detect TmrID   : 95
  Session Init TmrID     : -                Session WTR TmrID      : -
  Session Echo Tx TmrID  : -
  PDT Index              : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description    : -
--------------------------------------------------------------------------------

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

After the configuration, run the **display bfd session all verbose** command on the egress node, and you can view that the (Multi Hop) State field is displayed as **Up** and the BFD Bind Type field is displayed as **Peer IP Address**.

```
[PE2] display bfd session all verbose
--------------------------------------------------------------------------------
Session MIndex : 256       (Multi Hop) State : Up        Name : pe2tope1
--------------------------------------------------------------------------------
  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   : 1.1.1.1
  Bind Interface         : -
  FSM Board Id           : 1                TOS-EXP                : 7
  Min Tx Interval (ms)   : 1000             Min Rx Interval (ms)   : 1000
  Actual Tx Interval (ms): 1000             Actual Rx Interval (ms): 1000
  Local Detect Multi     : 3                Detect Interval (ms)   : 3000
  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  : -
  PDT Index              : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description    : -
--------------------------------------------------------------------------------

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

----End

Configuration Files

- Configuration file of PE1

```
#
 sysname PE1
#
 vlan batch 10 30
#
 bfd
#
 mpls lsr-id 1.1.1.1
 mpls
```


Copyright © Huawei Technologies Co., Ltd.

```
#
mpls ldp
#
interface Vlanif 10
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface Vlanif 30
 ip address 10.3.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet1/0/1
 port link-type access
 port default vlan 30
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
bfd pe1tope2 bind ldp-lsp peer-ip 4.4.4.9 nexthop 10.1.1.2 interface vlanif10
 discriminator local 1
 discriminator remote 2
 process-pst
 commit
#
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
  network 10.3.1.0 0.0.0.255
#
return
```

- Configuration file of P1

```
#
 sysname P1
#
 vlan batch 10 20
#
 mpls lsr-id 2.2.2.2
 mpls
#
mpls ldp
#
interface Vlanif 10
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlanif 20
 ip address 10.2.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet1/0/1
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
ospf 1
 area 0.0.0.0
```


Copyright © Huawei Technologies Co., Ltd.

```
  network 2.2.2.2 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.2.1.0 0.0.0.255
#
return
```

- Configuration file of P2

```
#
 sysname P2
#
 vlan batch 30 40
#
interface Vlanif 30
 ip address 10.3.1.2 255.255.255.0
#
interface Vlanif 40
 ip address 10.4.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 30
#
interface GigabitEthernet1/0/1
 port link-type access
 port default vlan 40
#
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 10.3.1.0 0.0.0.255
  network 10.4.1.0 0.0.0.255
#
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
 vlan batch 20 40
#
 bfd
#
 mpls lsr-id 4.4.4.4
 mpls
#
mpls ldp
#
interface Vlanif 20
 ip address 10.2.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlanif 40
 ip address 10.4.1.2 255.255.255.0
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 20
#
interface GigabitEthernet1/0/1
 port link-type access
 port default vlan 40
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
#
bfd 4to1 bind peer-ip 1.1.1.1
```


Copyright © Huawei Technologies Co., Ltd.

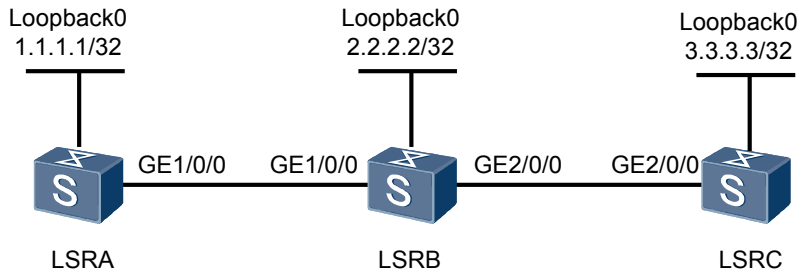
```
 discriminator local 2
 discriminator remote 1
 commit
#
ospf 1
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.4.1.0 0.0.0.255
#
return
```

2.16.6 Example for Configuring Dynamic BFD for LDP LSPs

Networking Requirements

As shown in **Figure 2-6**, LSRA, LSRB, and LSRC belong to one MPLS domain; an LDP LSP is established between LSRA and LSRC. Dynamic BFD is required to detect the connectivity of the LDP LSP.

Figure 2-6 Networking diagram for configuring dynamic BFD for LDP LSPs



switch	Interface	VLANIF interface	IP address
LSRA	GE1/0/0	VLANIF10	10.1.1.1/24
LSRB	GE1/0/0	VLANIF10	10.1.1.2/24
LSRB	GE2/0/0	VLANIF20	10.2.1.1/24
LSRC	GE2/0/0	VLANIF20	10.2.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Establish an LDP LSP between LSRA and LSRC.
2. Configure BFD.
3. Adjust BFD parameters.

Data Preparation

To complete the configuration, you need the following data:

Copyright © Huawei Technologies Co., Ltd.

- LSR ID of each node and IP address of each interface
- BFD parameters

Procedure

Step 1 Create VLANs on PE and P devices and add GE interfaces to the VLANs, create VLANIF interfaces, and assign IP addresses to the VLANIF interfaces and configure OSPF.

As shown in **Figure 2-6**, configure IP addresses and masks for the interfaces, including loopback interfaces.

Configure OSPF on all the nodes and advertise host routes of the loopback interfaces. The configuration details are not mentioned here.

After the configuration, LSRs can ping each other. Run the **display ip routing-table** command on each LSR, and you can view the routing entries to the LSRs.

Step 2 Establish an LDP LSP between LSRA and LSRC.

Configure LSRA.

```
<LSRA> system-view
[LSRA] mpls lsr-id 1.1.1.1
[LSRA] mpls
[LSRA-mpls] quit
[LSRA] mpls ldp
[LSRA-mpl-ldp] quit
[LSRA] interface vlanif 10
[LSRA-Vlanif10] mpls
[LSRA-Vlanif10] mpls ldp
[LSRA-Vlanif10] quit
```

Configure LSRB.

```
<LSRB> system-view
[LSRB] mpls lsr-id 2.2.2.2
[LSRB] mpls
[LSRB-mpls] quit
[LSRB] mpls ldp
[LSRB-mpl-ldp] quit
[LSRB] interface vlanif 10
[LSRB-Vlanif10] mpls
[LSRB-Vlanif10] mpls ldp
[LSRB-Vlanif10] quit
[LSRB] interface vlanif 20
[LSRB-Vlanif20] mpls
[LSRB-Vlanif20] mpls ldp
```

Configure LSRC.

```
<LSRC> system-view
[LSRC] mpls lsr-id 3.3.3.3
[LSRC] mpls
[LSRC-mpls] quit
[LSRC] mpls ldp
[LSRC-mpl-ldp] quit
[LSRC] interface vlanif 20
[LSRC-Vlanif20] mpls
[LSRC-Vlanif20] mpls ldp
[LSRC-Vlanif20] quit
```

After the configuration, run the **display mpls ldp lsp** command on LSRA, and you can view that an LDP LSP is set up between LSRA and LSRC. Take the display on LSRA as an example.

```
[LSRA] display mpls ldp lsp
```


Copyright © Huawei Technologies Co., Ltd.

```
                  LDP LSP Information
-------------------------------------------------------------
 SN DestAddress/Mask In/OutLabel Next-Hop        In/Out-Interface
-------------------------------------------------------------
 1      1.1.1.1/32         3/NULL        127.0.0.1       Vlanif10/InLoop0
 2      2.2.2.2/32         NULL/3        100.1.1.2       -------/Vlanif10
 3      3.3.3.3/32         NULL/1025     100.1.1.2       -------/Vlanif10
-------------------------------------------------------------
 TOTAL: 3 Normal LSP(s) Found.
 TOTAL: 0 Liberal LSP(s) Found.
 A '*' before an LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stale
```

Step 3 Configure dynamic BFD to detect the connectivity of the LDP LSP between LSRA and LSRC.

Configure an FEC list on LSRA to ensure that BFD detects only the connectivity of the LDP LSP between LSRA and LSRC.

```
[LSRA] fec-list tortc
[LSRA-fec-list-tortc] fec-node 3.3.3.3
```

Enable BFD on LSRA, specify the FEC list that triggers a BFD session dynamically, and adjust BFD parameters.

```
[LSRA] bfd
[LSRA-bfd] quit
[LSRA] mpls
[LSRA-mpls] mpls bfd-trigger fec-list tortc
[LSRA-mpls] mpls bfd enable
[LSRA-mpls] mpls bfd min-tx-interval 100 min-rx-interval 600 detect-multiplier 4
```

Enable BFD for LSPs passively on LSRC.

```
[LSRC] bfd
[LSRC-bfd] mpls-passive
```

Step 4 Verify the configuration.

Run the **display bfd session all verbose** command, and you can view the BFD session status that is created dynamically.

```
[LSRA] display bfd session all verbose
-------------------------------------------------------------
Session MIndex : 256      (One Hop) State : Up       Name : bfd1
-------------------------------------------------------------
  Local Discriminator: 8192     Remote Discriminator  : 8193
  Session Detect Mode  : Asynchronous Mode Without Echo Function
  BFD Bind Type          : LDP_LSP
  Bind Session Type      : Dynamic
  Bind Peer Ip Address   : 3.3.3.3
  NextHop Ip Address     : 10.1.1.2
  Bind Interface         : Vlanif10
  LSP Token              : 0x10000
  FSM Board Id           : 1        TOS-EXP            : 7
  Min Tx Interval (ms)   : 100      Min Rx Interval (ms)   : 600
  Actual Tx Interval (ms): 10      Actual Rx Interval (ms): 30
  Local Detect Multi     : 4      Detect Interval (ms)   : 1800
  Echo Passive           : Disable     Acl Number         : --
  Proc interface status  : Disable   Process PST          : Enable
  WTR Interval (ms)      : --       Local Demand Mode    : Disable
  Active Multi           : 3
  Last Local Diagnostic  : No Diagnostic
  Bind Application       : LSPM | L2VPN | OAM_MANAGER
  Session TX TmrID       : 16000   Session Detect TmrID   : 16820
  Session Init TmrID     : --      Session WTR TmrID      : --
  Session Echo Tx TmrID  : --
  PDT Index              : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description    : --
```


Copyright © Huawei Technologies Co., Ltd.

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

Check the status of the BFD session created dynamically on LSRC. The BFD Bind Type field is displayed as **Peer IP Address**, which indicates that BFD packets sent by LSRC are transmitted through the IP route.

```
[LSRC] display bfd session passive-dynamic verbose
------------------------------------------------------------
Session MIndex : 257    (Multi Hop) State : Up       Name : bfd2
------------------------------------------------------------
  Local Discriminator    : 8193    Remote Discriminator   : 8192
  Session Detect Mode  : Asynchronous Mode Without Echo Function
  BFD Bind Type          : Peer Ip Address
  Bind Session Type      : Entire_Dynamic
  Bind Peer Ip Address   : 1.1.1.1
  Bind Interface         : --
  FSM Board Id           : 1      TOS-EXP                : 7
  Min Tx Interval (ms)   : 100    Min Rx Interval (ms)   : 600
  Actual Tx Interval (ms): 600     Actual Rx Interval (ms): 100
  Local Detect Multi     : 3       Detect Interval (ms)   : 400
  Echo Passive           : Disabl  Acl Number             : --
  Proc interface status  : Disable   Process PST        : Disable
  WTR Interval (ms)      : --      Local Demand Mode      : Disable
  Active Multi           : 4
  Last Local Diagnostic  : No Diagnostic
  Bind Application
  Session TX TmrID       : 75      Session Detect TmrID   : 76
  Session Init TmrID     : --      Session WTR TmrID      : --
  Session Echo Tx TmrID  : --
  PDT Index              : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description    : --
------------------------------------------------------------

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

----End

Configuration Files

- Configuration file of LSRA

```
#
 sysname LSRA
#
 vlan batch 10
#
 bfd
#
 mpls lsr-id 1.1.1.1
 mpls
  mpls bfd enable
  mpls bfd-trigger fec-list tortc
  mpls bfd min-tx-interval 100 min-rx-interval 600 detect-multiplier 4
#
 fec-list tortc
   fec-node 3.3.3.3
#
mpls ldp
#
interface Vlanif 10
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
```


Copyright © Huawei Technologies Co., Ltd.

```
interface LoopBack0
 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
#
return
```

- Configuration file of LSRB

```
#
 sysname LSRB
#
 vlan batch 10 20
#
 mpls lsr-id 2.2.2.2
 mpls
#
mpls ldp
#
interface Vlanif 10
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlanif 20
 ip address 10.2.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack0
 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 10.1.1.0 0.0.0.255
  network 10.2.1.0 0.0.0.255
#
return
```

- Configuration file of LSRC

```
#
 sysname LSRC
#
 bfd
 mpls-passive
#
 vlan batch 20
#
 mpls lsr-id 3.3.3.3
 mpls
#
mpls ldp
#
interface Vlanif 20
 ip address 10.2.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
```


Copyright © Huawei Technologies Co., Ltd.

```
 port link-type access
 port default vlan 20
#
interface LoopBack0
 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 10.2.1.0 0.0.0.255
#
return
```

2.16.7 Example for Configuring Manual LDP FRR

Networking Requirements

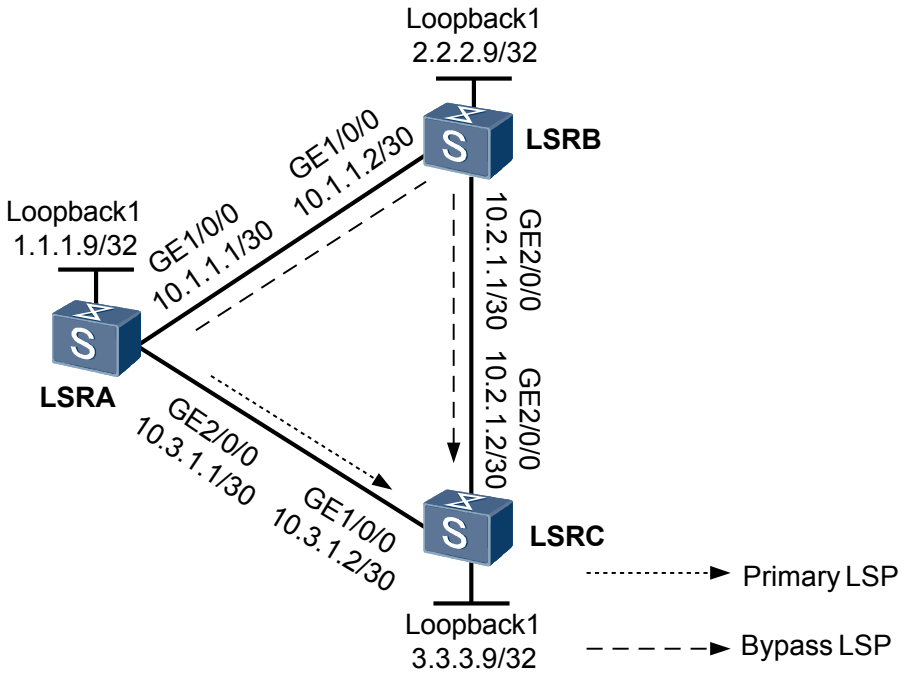
As shown in **Figure 2-7**, two LSPs are required from LSRA to LSRC. One is the primary LSP along the path LSRA → LSRC and another is the bypass LSP along the path LSRA → LSRB → LSRC. Manual LDP FRR is required on LSRA for local interface backup to reduce data loss.

Here, only LSRA must support Manual LDP FRR.

NOTE

In networking of Manual LDP FRR, the bypass LSP must be in liberal state. That is, on an LSR that is enabled with FRR, run the **display ip routing-table** *ip-address* **verbose** command to view the route state of the bypass LSP is "Inactive Adv".

Figure 2-7 Networking diagram of configuring Manual LDP FRR



Switch	Interface	VLANIF interface	IP address
LSRA	GigabitEthernet1/0/0	VLANIF 10	10.1.1.1/30
LSRA	GigabitEthernet2/0/0	VLANIF 20	10.3.1.1/30

Copyright © Huawei Technologies Co., Ltd.

LSRB	GigabitEthernet1/0/0	VLANIF 10	10.1.1.2/30
LSRB	GigabitEthernet2/0/0	VLANIF 30	10.2.1.1/30
LSRC	GigabitEthernet1/0/0	VLANIF 20	10.3.1.2/30
LSRC	GigabitEthernet2/0/0	VLANIF 30	10.2.1.2/30

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the IP address of the interfaces, set the loopback address as the LSR ID, and use OSPF to advertise the network segments that the interfaces are connected to and the LSR ID host route.
2. Enable MPLS and MPLS LDP globally on the LSRs.
3. Enable MPLS and MPLS LDP on the interfaces.
4. Specify the next hop address that is used by Manual LDP FRR for generating the backup LSP on the protected interface.
5. Configure the Manual LDP FRR protection timer on the interface.

Data Preparation

To complete the configuration, you need the following data:

- IP address of the interfaces, OSPF process ID, and area ID
- Policy for triggering the establishment of LSPs
- Next hop address of the backup LSP
- Value of Manual LDP FRR protection timer

Procedure

Step 1 Configure VLANs that interfaces belong to.

```
<Quidway> system-view
[Quidway] sysname LSRA
[LSRA] vlan batch 10 20
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] port hybrid pvid vlan 10
[LSRA-GigabitEthernet1/0/0] port hybrid untagged vlan 10
[LSRA-GigabitEthernet1/0/0] quit
[LSRA] interface gigabitethernet 2/0/0
[LSRA-GigabitEthernet2/0/0] port hybrid pvid vlan 20
[LSRA-GigabitEthernet2/0/0] port hybrid untagged vlan 20
[LSRA-GigabitEthernet2/0/0] quit
```

The configurations of LSRB and LSRC are similar to the configuration of LSRA, and are not mentioned here.

Step 2 Configure an IP address for each VLANIF interface.

```
[LSRA] interface vlanif 10
[LSRA-Vlanif10] ip address 10.1.1.1 30
[LSRA-Vlanif10] quit
[LSRA] interface vlanif 20
[LSRA-Vlanif20] ip address 10.3.1.1 30
[LSRA-Vlanif20] quit
```


Copyright © Huawei Technologies Co., Ltd.

The configurations of LSRB and LSRC are similar to the configuration of LSRA, and are not mentioned here.

Step 3 Configure OSPF to advertise the LSR ID host route and network segments that the interfaces are connected to.

Configure LSRA.

```
<LSRA> system-view
[LSRA] ospf 1
[LSRA-ospf-1] area 0
[LSRA-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[LSRA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.3
[LSRA-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.3
[LSRA-ospf-1-area-0.0.0.0] quit
[LSRA-ospf-1] quit
```

Configure LSRB.

```
<LSRB> system-view
[LSRB] ospf 1
[LSRB-ospf-1] area 0
[LSRB-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[LSRB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.3
[LSRB-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.3
[LSRB-ospf-1-area-0.0.0.0] quit
[LSRB-ospf-1] quit
```

Configure LSRC.

```
<LSRC> system-view
[LSRC] ospf 1
[LSRC-ospf-1] area 0
[LSRC-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[LSRC-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.3
[LSRC-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.3
[LSRC-ospf-1-area-0.0.0.0] quit
[LSRC-ospf-1] quit
```

After the configuration, run the **display ip routing-table** command on each LSR, and you can view that the LSRs learn the routes from each other.

Take the display on LSRA as an example.

```
<LSRA> display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 12        Routes : 13

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        Vlanif10
        3.3.3.9/32  OSPF    10   2           D   10.3.1.2        Vlanif20
       10.1.1.0/30  Direct  0    0           D   10.1.1.1        Vlanif10
       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        Vlanif10
       10.2.1.0/30  OSPF    10   2           D   10.3.1.2        Vlanif20
                    OSPF    10   2           D   10.1.1.2        Vlanif10
       10.3.1.0/30  Direct  0    0           D   10.3.1.1        Vlanif20
       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        Vlanif20
      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 4 Configure the MPLS and MPLS LDP functions on the nodes globally and on the interfaces to forward the MPLS traffic over the network.

Configure LSRA.

Copyright © Huawei Technologies Co., Ltd.

```
[LSRA] mpls lsr-id 1.1.1.9
[LSRA] mpls
[LSRA-mpls] quit
[LSRA] mpls ldp
[LSRA-mpls-ldp] quit
[LSRA] interface vlanif 10
[LSRA-Vlanif10] mpls
[LSRA-Vlanif10] mpls ldp
[LSRA-Vlanif10]  quit
[LSRA] interface vlanif 20
[LSRA-Vlanif20] mpls
[LSRA-Vlanif20] mpls ldp
[LSRA-Vlanif20] quit
```

Configure LSRB.

```
[LSRB] mpls lsr-id 2.2.2.9
[LSRB] mpls
[LSRB-mpls] quit
[LSRB] mpls ldp
[LSRB-mpls-ldp] quit
[LSRB] interface vlanif 10
[LSRB-Vlanif10] mpls
[LSRB-Vlanif10] mpls ldp
[LSRB-Vlanif10] quit
[LSRB] interface vlanif 30
[LSRB-Vlanif30] mpls
[LSRB-Vlanif30] mpls ldp
[LSRB-Vlanif30] quit
```

Configure LSRC.

```
[LSRC] mpls lsr-id 3.3.3.9
[LSRC] mpls
[LSRC-mpls] quit
[LSRC] mpls ldp
[LSRC-mpls-ldp] quit
[LSRC] interface vlanif 20
[LSRC-Vlanif20] mpls
[LSRC-Vlanif20] mpls ldp
[LSRC-Vlanif20] quit
[LSRC] interface vlanif 30
[LSRC-Vlanif30] mpls
[LSRC-Vlanif30] mpls ldp
[LSRC-Vlanif30] quit
```

After the configuration, LDP sessions are established between neighboring LSRs. Run the **display mpls ldp session** command on each LSR, and you can view that **Status** is displayed as **Operational**.

Take the display on LSRA as an example.

```
<LSRA> display mpls ldp session
```

Step 5 Enable Manual LDP FRR on the Vlanif20 on LSRA, and specify the next hop address for generating the backup LSP.

Configure LSRA.

```
[LSRA] interface vlanif 20
[LSRA-Vlanif20] mpls ldp frr nexthop 10.1.1.2
```

Step 6 Configure Manual LDP FRR protection timer on Vlanif20 of LSRA

Configure LSRA.

```
[LSRA] interface vlanif 20
[LSRA-Vlanif20] mpls ldp frr timer protect-time 11
```


Copyright © Huawei Technologies Co., Ltd.

Step 7 Verify the configuration.

Run the **display mpls lsp** command on LSRA, and you can view that Manual LDP FRR is enabled on the LSP of LSRC.

```
<LSRA> display mpls lsp
------------------------------------------------------------------------
                LSP Information: LDP LSP
------------------------------------------------------------------------
FEC                 In/Out Label  In/Out IF                      Vrf Name
3.3.3.9/32          NULL/3        -/Vlanif20
   **LDP FRR**          /1025      /Vlanif10
3.3.3.9/32          1025/3        -/Vlanif20
   **LDP FRR**          /1025      /Vlanif10
2.2.2.9/32          NULL/3        -/Vlanif10
2.2.2.9/32          1024/3        -/Vlanif10
```

----End

Configuration Files

- Configuration file of LSRA

```
#
sysname LSRA
#
vlan batch 10 20
#
 mpls lsr-id 1.1.1.9
 mpls
#
mpls ldp
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.252
mpls
 mpls ldp
#
interface Vlanif20
 ip address 10.3.1.1 255.255.255.252
mpls
 mpls ldp
mpls ldp frr timer protect-time 11
mpls ldp frr nexthop 10.1.1.2
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
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
  network 10.3.1.0 0.0.0.3
#
return
```

- Configuration file of LSRB

```
#
sysname LSRB
#
vlan batch 10 30
```


Copyright © Huawei Technologies Co., Ltd.

```
#
mpls lsr-id 2.2.2.9
 mpls
#
mpls ldp
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.252
mpls
 mpls ldp
#
interface Vlanif30
 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
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
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 LSRC

```
#
sysname LSRC
#
vlan batch 20 30
#
mpls lsr-id 3.3.3.9
 mpls
#
mpls ldp
#
interface Vlanif20
 ip address 10.3.1.2 255.255.255.252
mpls
 mpls ldp
#
interface Vlanif30
 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
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
ospf 1
 area 0.0.0.0
  network 3.3.3.9 0.0.0.0
```


Copyright © Huawei Technologies Co., Ltd.

```
  network 10.3.1.0 0.0.0.3
  network 10.2.1.0 0.0.0.3
#
Return
```

2.16.8 Example for Configuring LDP Auto FRR

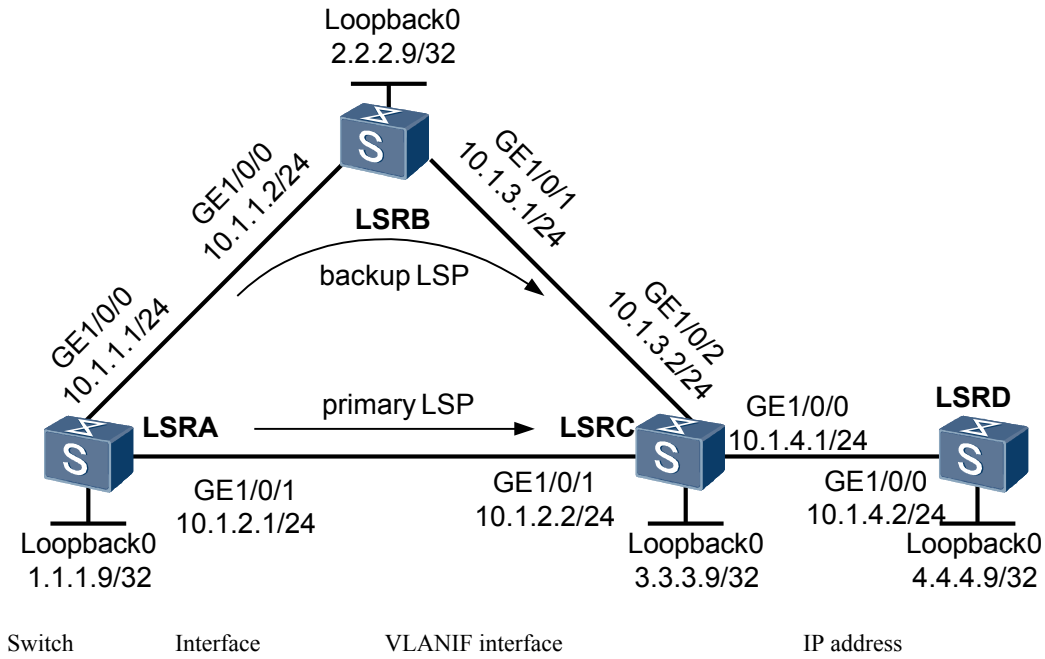
Networking Requirements

With the development of networks, new services that have stringent requirements for real-time transmission are emerging, for example, Voice over IP (VoIP) and on-line video services. A large number of services are based on VPN. Currently, VPN services are generally implemented by using LDP tunnels. In case of data loss due to faults over the link, these services will be seriously affected.

The Manual LDP FRR is a technique that ensures that when a fault occurs, service traffic on the public network is forwarded along the backup LSP before routes are converged and a new primary LSP is established. This mechanism ensures that the service interruption lasts for only as long as it takes the fault to be detected and traffic to be switched to the backup LSP. Therefore, packet loss lasts for less than 50 ms. But the time that is required for VPN services to be switched to a new LSP after routes convergence is completed depends on the actual VPN implementation. This means that the speed at which VPN services are switched to the new primary LSP must be raised so as to ensure that VPN services are interrupted for less than 50 ms. This issue can be solved by configuring LDP Auto FRR.

As shown in **Figure 2-8**, the primary and backup LSPs are set up between LSRA and LSRC. The primary LSP is along the path from LSRA to LSRC, and the backup LSP is along the path LSRA -> LSRB -> LSRC. When the primary LSP becomes faulty, traffic must be rapidly switched to the backup LSP. After LDP Auto FRR is configured on LSRA, in case of a fault over the link, a backup LSP is automatically set up to reduce traffic loss.

Figure 2-8 Networking diagram of configuring LDP Auto FRR



Copyright © Huawei Technologies Co., Ltd.

LSRA	GE1/0/0	VLANIF10	10.1.1.1/24
LSRA	GE1/0/1	VLANIF20	10.1.2.1/24
LSRB	GE1/0/0	VLANIF10	10.1.1.2/24
LSRB	GE1/0/1	VLANIF40	10.1.3.1/24
LSRC	GE1/0/1	VLANIF20	10.1.2.2/24
LSRC	GE1/0/0	VLANIF30	10.1.4.1/24
LSRC	GE1/0/2	VLANIF40	10.1.3.2/24
LSRD	GE1/0/0	VLANIF30	10.1.4.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Assign IP addresses to interfaces on each node and configure the loopback address that is used as the LSR ID.
2. Configure IS-IS to advertise the network segments connecting to interfaces on each node and to advertise the routes of hosts with LSR IDs.
3. Enable global and interface-based MPLS and MPLS LDP on each node.
4. Enable IS-IS Auto FRR on the LSR from which the protected traffic is originated.
5. Change the LSP triggering policy to trigger the setup of LSPs for all routes.
6. Configure a policy for triggering the setup of backup LSPs on the LSR from which the protected traffic is originated.

Data Preparation

To complete the configuration, you need the following data:

- IP addresses of the interfaces on each node, as listed in **Figure 2-8**, IS-IS process IDs, and the area where each nodes resides
- Policy for triggering the setup of backup LSPs

Procedure

Step 1 Configure VLANs that interfaces belong to and configure an IP address for each VLANIF interface.

Configure LSRA.

```
<Quidway> system-view
[Quidway] sysname LSRA
[LSRA] interface loopback1
[LSRA-LoopBack1] ip address 1.1.1.9 32
[LSRA-LoopBack1] quit
[LSRA] interface gigabitethernet1/0/0
[LSRA-GigabitEthernet1/0/0] port link-type access
[LSRA-GigabitEthernet1/0/0] quit
[LSRA] vlan 10
[LSRA-vlan10] port gigabitethernet1/0/0
[LSRA-vlan10] quit
```


Copyright © Huawei Technologies Co., Ltd.

```
[LSRA] interface vlanif 10
[LSRA-Vlanif10] ip address 10.1.1.1 24
[LSRA-Vlanif10] quit
[LSRA] interface gigabitethernet2/0/0
[LSRA-GigabitEthernet2/0/0] port link-type access
[LSRA-GigabitEthernet2/0/0] quit
[LSRA] vlan 20
[LSRA-vlan20] port gigabitethernet2/0/0
[LSRA-vlan20] quit
[LSRA] interface vlanif 20
[LSRA-Vlanif20] ip address 10.1.2.1 24
[LSRA-Vlanif20] quit
```

The configurations of LSRB, LSRC and LSRD are similar to the configuration of LSRA, and are not mentioned here.

Step 2 Enable IS-IS to advertise the network segments connecting to interfaces on each node and to advertise the routes of hosts with LSR IDs.

Configure LSRA.

```
<LSRA> system-view
[LSRA] isis 1
[LSRA-isis-1] network-entity 10.0000.0000.0001.00
[LSRA-isis-1] quit
[LSRA] interface vlanif 10
[LSRA-Vlanif10] isis enable 1
[LSRA-Vlanif10] quit
[LSRA] interface vlanif 20
[LSRA-Vlanif20] isis enable 1
[LSRA-Vlanif20] quit
[LSRA] interface loopBack 0
[LSRA-LoopBack0] isis enable 1
[LSRA-LoopBack0] quit
```

Configure LSRB.

```
<LSRB> system-view
[LSRB] isis 1
[LSRB-isis-1] network-entity 10.0000.0000.0002.00
[LSRB-isis-1] quit
[LSRB] interface vlanif 10
[LSRB-Vlanif10] isis enable 1
[LSRB-Vlanif10] quit
[LSRB] interface vlanif 40
[LSRB-Vlanif40] isis enable 1
[LSRB-Vlanif40] quit
[LSRB] interface loopBack 0
[LSRB-LoopBack0] isis enable 1
[LSRB-LoopBack0] quit
```

Configure LSRC.

```
<LSRC> system-view
[LSRC] isis 1
[LSRC-isis-1] network-entity 10.0000.0000.0003.00
[LSRC-isis-1] quit
[LSRC] interface vlanif 30
[LSRC-Vlanif30] isis enable 1
[LSRC-Vlanif30] quit
[LSRC] interface vlanif 20
[LSRC-Vlanif20] isis enable 1
[LSRC-Vlanif20] quit
[LSRC] interface vlanif 40
[LSRC-Vlanif40] isis enable 1
[LSRC-Vlanif40] quit
[LSRC] interface loopBack 0
[LSRC-LoopBack0] isis enable 1
[LSRC-LoopBack0] quit
```


Copyright © Huawei Technologies Co., Ltd.

Configure LSRD.

```
<LSRD> system-view
[LSRD] isis 1
[LSRD-isis-1] network-entity 10.0000.0000.0004.00
[LSRD-isis-1] quit
[LSRD] interface vlanif 30
[LSRD-Vlanif30] isis enable 1
[LSRD-Vlanif30] quit
[LSRD] interface loopBack 0
[LSRD-LoopBack0] isis enable 1
[LSRD-LoopBack0] quit
```

Step 3 Configure global and interface-based MPLS and MPLS LDP on each node. Enable the network to forward MPLS traffic and view the setup of the LSPs.

Configure LSRA.

```
[LSRA] mpls lsr-id 1.1.1.9
[LSRA] mpls
[LSRA-mpls] quit
[LSRA] mpls ldp
[LSRA-mpls-ldp] quit
[LSRA] interface vlanif 10
[LSRA-Vlanif10] mpls
[LSRA-Vlanif10] mpls ldp
[LSRA-Vlanif10] quit
[LSRA] interface vlanif 20
[LSRA-Vlanif20] mpls
[LSRA-Vlanif20] mpls ldp
[LSRA-Vlanif20] quit
```

Configure LSRB.

```
[LSRB] mpls lsr-id 2.2.2.9
[LSRB] mpls
[LSRB-mpls] quit
[LSRB] mpls ldp
[LSRB-mpls-ldp] quit
[LSRB] interface vlanif 10
[LSRB-Vlanif10] mpls
[LSRB-Vlanif10] mpls ldp
[LSRB-Vlanif10] quit
[LSRB] interface vlanif 40
[LSRB-Vlanif40] mpls
[LSRB-Vlanif40] mpls ldp
[LSRB-Vlanif40] quit
```

Configure LSRC.

```
[LSRC] mpls lsr-id 3.3.3.9
[LSRC] mpls
[LSRC-mpls] quit
[LSRC] mpls ldp
[LSRC-mpls-ldp] quit
[LSRC] interface vlanif 30
[LSRC-Vlanif30] mpls
[LSRC-Vlanif30] mpls ldp
[LSRC-Vlanif30] quit
[LSRC] interface vlanif 20
[LSRC-Vlanif20] mpls
[LSRC-Vlanif20] mpls ldp
[LSRC-Vlanif20] quit
[LSRC] interface vlanif 40
[LSRC-Vlanif40] mpls
[LSRC-Vlanif40] mpls ldp
[LSRC-Vlanif40] quit
```

Configure LSRD.

Copyright © Huawei Technologies Co., Ltd.

```
[LSRD] mpls lsr-id 4.4.4.9
[LSRD] mpls
[LSRD-mpls] quit
[LSRD] mpls ldp
[LSRD-mpls-ldp] quit
[LSRD] interface vlanif 30
[LSRD-Vlanif30] mpls
[LSRD-Vlanif30] mpls ldp
[LSRD-Vlanif30] quit
```

After the configuration is complete, run the **display mpls lsp** command on LSRA to view the established LSP.

```
[LSRA] display mpls lsp

------------------------------------------------------------------------------
                LSP Information: LDP LSP
------------------------------------------------------------------------------
FEC                In/Out Label  In/Out IF                      Vrf Name
2.2.2.9/32         NULL/3        -/Vlanif10
2.2.2.9/32         1024/3        -/Vlanif10
3.3.3.9/32         NULL/3        -/Vlanif20
3.3.3.9/32         1025/3        -/Vlanif20
4.4.4.9/32         NULL/1026     -/Vlanif20
4.4.4.9/32         1026/1026     -/Vlanif20
```

The preceding command output shows that by default, the setup of LSPs is triggered by LDP for the routes with 32-bit addresses.

Step 4 Enable IS-IS Auto FRR on LSRA. View the routing information and the setup of the LSPs.

Enable IS-IS Auto FRR on LSRA.

```
[LSRA] isis
[LSRA-isis-1] frr
[LSRA-isis-1-frr] loop-free-alternate
[LSRA-isis-1-frr] quit
[LSRA-isis-1] quit
```

Display information about the route between LSRA and the link connecting LSRC and LSRD.

```
[LSRA] display ip routing-table 10.1.4.0 verbose

Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1

Destination: 10.1.4.0/24
     Protocol: ISIS            Process ID: 1
   Preference: 15                    Cost: 20
      NextHop: 10.1.2.2         Neighbour: 0.0.0.0
        State: Active Adv             Age: 00h05m38s
          Tag: 0                 Priority: low
        Label: NULL               QoSInfo: 0x0
   IndirectID: 0x0
 RelayNextHop: 0.0.0.0           Interface: Vlanif20
     TunnelID: 0x0                   Flags: D
    BkNextHop: 10.1.1.2         BkInterface: Vlanif10
      BkLabel: NULL             SecTunnelID: 0x0
 BkPETunnelID: 0x0          BkPESecTunnelID: 0x0
 BkIndirectID: 0x0
```

The preceding command output shows that a backup IS-IS route is generated after IS-IS Auto FRR is enabled.

Run the **display mpls lsp** command on LSRA to view the setup of the LSPs.

```
[LSRA] display mpls lsp
```


Copyright © Huawei Technologies Co., Ltd.

```
------------------------------------------------------------------------------
                LSP Information: LDP LSP
------------------------------------------------------------------------------
FEC                In/Out Label  In/Out IF                      Vrf Name
2.2.2.9/32         NULL/3        -/Vlanif10
   **LDP FRR**         /1025      /Vlanif20
2.2.2.9/32         1024/3        -/Vlanif10
   **LDP FRR**         /1025      /Vlanif20
3.3.3.9/32         NULL/3        -/Vlanif20
   **LDP FRR**         /1025      /Vlanif10
3.3.3.9/32         1025/3        -/Vlanif20
   **LDP FRR**         /1025      /Vlanif10
4.4.4.9/32         NULL/1026     -/Vlanif20
   **LDP FRR**         /1026      /Vlanif10
4.4.4.9/32         1026/1026     -/Vlanif20
   **LDP FRR**         /1026      /Vlanif10
```

The preceding command output shows that by default, the setup of a backup LSP is triggered by LDP for the routes with 32-bit addresses.

Step 5 Run the **lsp-trigger** command on LSRC to change the LSP triggering policy to trigger the setup of LSPs for all routes. Then, view the setup of the LSPs.

Run the **lsp-trigger** command on LSRC to change the LSP triggering policy to trigger the setup of LSPs for all routes.

```
[LSRC] mpls
[LSRC-mpls] lsp-trigger all
```

Run the **display mpls lsp** command on LSRA to view information about the established LSPs.

```
[LSRA] display mpls lsp

------------------------------------------------------------------------------
                LSP Information: LDP LSP
------------------------------------------------------------------------------
FEC                In/Out Label  In/Out IF                      Vrf Name
2.2.2.9/32         NULL/3        -/Vlanif10
   **LDP FRR**         /1025      /Vlanif20
2.2.2.9/32         1024/3        -/Vlanif10
   **LDP FRR**         /1025      /Vlanif20
3.3.3.9/32         NULL/3        -/Vlanif20
   **LDP FRR**         /1025      /Vlanif10
3.3.3.9/32         1025/3        -/Vlanif20
   **LDP FRR**         /1025      /Vlanif10
4.4.4.9/32         NULL/1026     -/Vlanif20
   **LDP FRR**         /1026      /Vlanif10
4.4.4.9/32         1026/1026     -/Vlanif20
   **LDP FRR**         /1026      /Vlanif10
10.1.3.0/24        1027/3        -/Vlanif20
10.1.4.0/24        1028/3        -/Vlanif20
```

The preceding command output shows that the setup of LSPs is triggered by LDP for the routes with 24-bit addresses.

Step 6 Configure a triggering policy to trigger the setup of backup LSPs for all backup routes.

Run the **auto-frr lsp-trigger** command on LSRA to trigger the setup of backup LSPs for all backup routes.

```
[LSRA] mpls ldp
[LSRA-mpls-ldp] auto-frr lsp-trigger all
[LSRA-mpls-ldp] quit
```

Step 7 Verify the configuration.

Copyright © Huawei Technologies Co., Ltd.

After the preceding configuration is complete, run the **display mpls lsp** command on LSRA to view the setup of backup LSPs.

```
[LSRA] display mpls lsp

------------------------------------------------------------------------------
                LSP Information: LDP LSP
------------------------------------------------------------------------------
FEC                 In/Out Label  In/Out IF                      Vrf Name
2.2.2.9/32          NULL/3        -/Vlanif10
   **LDP FRR**          /1025      /Vlanif20
2.2.2.9/32          1024/3        -/Vlanif10
   **LDP FRR**          /1025      /Vlanif20
3.3.3.9/32          NULL/3        -/Vlanif20
   **LDP FRR**          /1025      /Vlanif10
3.3.3.9/32          1025/3        -/Vlanif20
   **LDP FRR**          /1025      /Vlanif10
4.4.4.9/32          NULL/1026     -/Vlanif20
   **LDP FRR**          /1026      /Vlanif10
4.4.4.9/32          1026/1026     -/Vlanif20
   **LDP FRR**          /1026      /Vlanif10
10.1.3.0/24         1027/3        -/Vlanif20
10.1.4.0/24         1028/3        -/Vlanif20
   **LDP FRR**          /1027      /Vlanif10
```

The preceding command output shows that backup LSP is set up between LSRA and the link connecting LSRC and LSRD.

----End

Configuration Files

- Configuration file of LSRA

```
#
 sysname LSRA
#
vlan batch 10 20
#
 mpls lsr-id 1.1.1.9
 mpls
#
mpls ldp
 auto-frr lsp-trigger all
#
aaa
 authentication-scheme default
 #
 authorization-scheme default
 #
 accounting-scheme default
 #
 domain default
 #
#
isis 1
 frr
  loop-free-alternate level-1
  loop-free-alternate level-2
 network-entity 10.0000.0000.0001.00
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
#
interface Vlanif20
```


Copyright © Huawei Technologies Co., Ltd.

```
 ip address 10.1.2.1 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
 isis enable 1
#
interface GigabitEthernet 1/0/0
 port link-type access
 port default vlan 10

#
interface GigabitEthernet 1/0/1
 port link-type access
 port default vlan 20
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

- Configuration file of LSRB

```
#
 sysname LSRB
#
#
vlan batch 10 40
#
 mpls lsr-id 2.2.2.9
 mpls
#
aaa
 authentication-scheme default
 #
 authorization-scheme default
 #
 accounting-scheme default
 #
 domain default
 #
isis 1
 network-entity 10.0000.0000.0002.00
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
#
interface Vlanif40
 ip address 10.1.3.1 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
 isis enable 1
#
interface GigabitEthernet 1/0/0
 port link-type access
 port default vlan 10

#
interface GigabitEthernet 1/0/1
 port link-type access
 port default vlan 40
```


Copyright © Huawei Technologies Co., Ltd.

```
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

- Configuration file of LSRC

```
#
 sysname LSRC
#
vlan batch 30 20 40
#
 mpls lsr-id 3.3.3.9
 mpls
  lsp-trigger all
#
aaa
 authentication-scheme default
 #
 authorization-scheme default
 #
 accounting-scheme default
 #
 domain default
#
isis 1
 network-entity 10.0000.0000.0003.00
#
interface Vlanif30
  ip address 10.1.4.1 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
#
interface Vlanif20
 ip address 10.1.2.2 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
#
interface Vlanif40
 ip address 10.1.3.2 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
 isis enable 1
#
interface GigabitEthernet 1/0/0
 port link-type access
 port default vlan 30
#
interface GigabitEthernet 1/0/1
 port link-type access
 port default vlan 20
#
interface GigabitEthernet 1/0/2
 port link-type access
 port default vlan 40
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

- Configuration file of LSRD

Copyright © Huawei Technologies Co., Ltd.

```
#
 sysname LSRD
#
vlan batch 30
#
 mpls lsr-id 4.4.4.9
 mpls
#
aaa
 authentication-scheme default
 #
 authorization-scheme default
 #
 accounting-scheme default
 #
 domain default
 #
#
isis 1
 network-entity 10.0000.0000.0004.00
#
interface Vlanif30
 ip address 10.1.4.2 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 4.4.4.9 255.255.255.255
 isis enable 1
#
interface GigabitEthernet 1/0/0
 port link-type access
 port default vlan 30
#
user-interface con 0
user-interface vty 0 4
user-interface vty 16 20
#
return
```

2.16.9 Example for Configuring Synchronization of LDP and an IGP

Networking Requirements

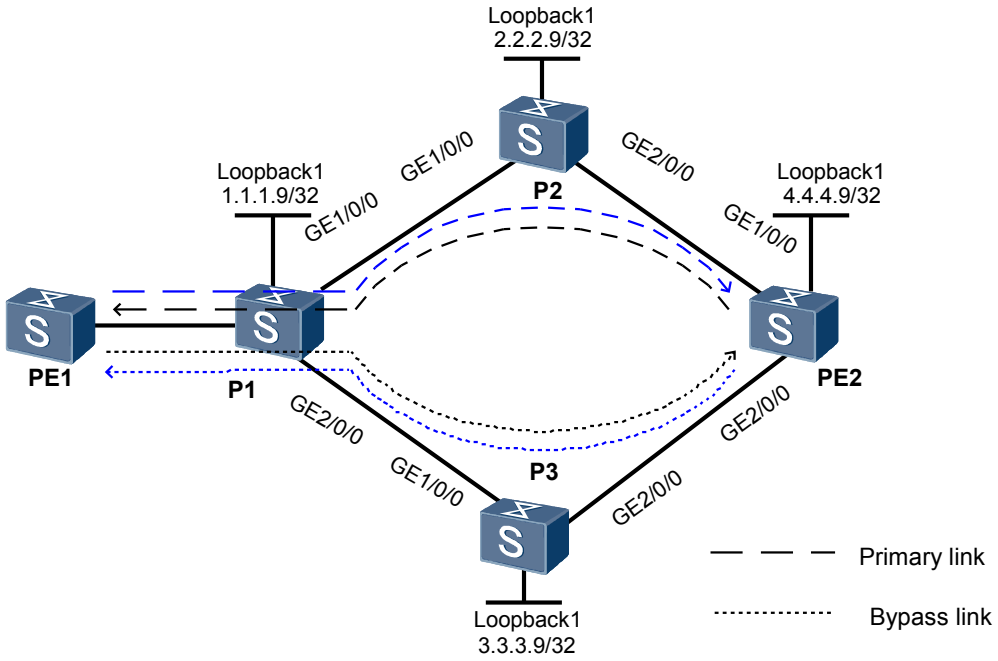
As shown in **Figure 2-9**, two links are established between PE1 and PE2. The link PE1->P1->P2->PE2 is an active link and the link PE1->P1->P3->PE2 is a standby link.

Configure synchronization of LDP and an IGP on the interfaces of both ends of the link between crossing node P1 of the active link and the standby link and LDP neighboring node P2 on the active link. After the faulty active link is recovered, the synchronization function can be used to shorten the interval for switching the traffic from the standby link to the active link and reduce the interruption at the millisecond level.

P and PE devices are the S9300s.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-9 Networking diagram for configuring synchronization of LDP and an IGP



switch	Interface	VLANIF interface	IP address
P1	GE1/0/0	VLANIF10	10.1.1.1/24
P1	GE2/0/0	VLANIF30	10.3.1.1/24
P2	GE1/0/0	VLANIF10	10.1.1.2/24
P2	GE2/0/0	VLANIF20	10.2.1.1/24
P3	GE1/0/0	VLANIF30	10.3.1.2/24
P3	GE2/0/0	VLANIF40	10.4.1.1/24
PE2	GE1/0/0	VLANIF20	10.2.1.2/24
PE2	GE2/0/0	VLANIF40	10.4.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and VLANIF interfaces.

Copyright © Huawei Technologies Co., Ltd.

2. Configure synchronization of LDP and an IGP on the interfaces of both ends of the link between crossing node P1 of the active link and the standby link and LDP neighboring node P2 on the active link.
3. Set the values of the hold-down timer, hold-max-cost timer, and delay timer on the interfaces of both ends of the link between crossing node P1 of the active link and the standby link and LDP neighboring node P2 on the active link.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each interface on each node shown in **Figure 2-9**, OSPF process ID, and OSPF area ID
- Values of the hold-down timer, hold-max-cost timer, and delay timer

Procedure

Step 1 Create VLANs on the S9300 and add GE interfaces to the VLANs, create VLANIF interfaces, and assign IP addresses to the VLANIF interfaces.

As shown in **Figure 2-9**, configure IP addresses and masks for the interfaces, including loopback interfaces. Configure OSPF to advertise the network segments that the interfaces are connected to and the host route of the LSR ID. The configuration details are not mentioned here.

The link PE1 → P1 → P2 → PE2 is an active link and the link PE1 → P1 → P3 → PE2 is a standby link. The cost of VLANIF 30 on P1 is 1000.

After the configuration, run the **display ip routing-table** command on each node, and you can view that the nodes learn routes from each other. The outgoing interface of the route from P1 to P2 is VLANIF 10.. Take the display on P1 as an example.

```
<P1> display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 14        Routes : 14

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.9/32  Direct  0    0           D   127.0.0.1       InLoopBack1
        2.2.2.9/32  OSPF    10   2           D   10.1.1.2        Vlanif10
        3.3.3.9/32  OSPF    10   4           D   10.1.1.2        Vlanif10
        4.4.4.9/32  OSPF    10   3           D   10.1.1.2        Vlanif10
       10.1.1.0/24  Direct  0    0           D   10.1.1.1        Vlanif10
       10.1.1.1/32  Direct  0    0           D   127.0.0.1       InLoopBack1
       10.1.1.2/32  Direct  0    0           D   10.1.1.2        Vlanif10
       10.2.1.0/24  OSPF    10   2           D   10.1.1.2        Vlanif10
       10.3.1.0/24  Direct  0    0           D   10.3.1.1        Vlanif30
       10.3.1.1/32  Direct  0    0           D   127.0.0.1       InLoopBack1
       10.3.1.2/32  Direct  0    0           D   10.3.1.2        Vlanif30
       10.4.1.0/24  OSPF    10   3           D   10.1.1.2        Vlanif10
      127.0.0.0/32  Direct  0    0           D   127.0.0.1       InLoopBack1
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack1
```

Step 2 Enable MPLS and MPLS LDP globally and on all the interfaces of the nodes.

Configure P1.

```
<P1> system-view
[P1] mpls lsr-id 1.1.1.9
[P1] mpls
[P1-mpls] quit
[P1] mpls ldp
```


Copyright © Huawei Technologies Co., Ltd.

```
[P1-mpls-ldp] quit
[P1] interface vlanif 10
[P1-Vlanif10] mpls
[P1-Vlanif10] mpls ldp
[P1-Vlanif10] quit
[P1] interface vlanif 30
[P1-Vlanif30] mpls
[P1-Vlanif30] mpls ldp
[P1-Vlanif30] quit
```

Configure P2.

```
<P2> system-view
[P2] mpls lsr-id 2.2.2.9
[P2] mpls
[P2-mpls] quit
[P2] mpls ldp
[P2-mpls-ldp] quit
[P2] interface vlanif 10
[P2-Vlanif10] mpls
[P2-Vlanif10] mpls ldp
[P2-Vlanif10] quit
[P2] interface vlanif 20
[P2-Vlanif20] mpls
[P2-Vlanif20] mpls ldp
[P2-Vlanif20] quit
```

Configure P3.

```
<P3> system-view
[P3] mpls lsr-id 3.3.3.9
[P3] mpls
[P3-mpls] quit
[P3] mpls ldp
[P3-mpls-ldp] quit
[P3] interface vlanif 30
[P3-Vlanif30] mpls
[P3-Vlanif30] mpls ldp
[P3-Vlanif30] quit
[P3] interface vlanif 40
[P3-Vlanif40] mpls
[P3-Vlanif40] mpls ldp
[P3-Vlanif40] quit
```

Configure PE2.

```
<PE2> system-view
[PE2] mpls lsr-id 4.4.4.9
[PE2] mpls
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface vlanif 20
[PE2-Vlanif20] mpls
[PE2-Vlanif20] mpls ldp
[PE2-Vlanif20] quit
[PE2] interface vlanif 40
[PE2-Vlanif40] mpls
[PE2-Vlanif40] mpls ldp
[PE2-Vlanif40] quit
```

After the configuration, LDP sessions are established between neighboring nodes. Run the **display mpls ldp session** command on each node, and you can view that Status is displayed as **Operational**. Take the display on P1 as an example.

```
<P1> display mpls ldp session
               LDP Session(s) in Public Network
 ------------------------------------------------------------------------------
 Peer-ID            Status      LAM  SsnRole  SsnAge      KA-Sent/Rcv
```


Copyright © Huawei Technologies Co., Ltd.

```
--------------------------------------------------------------------------------
2.2.2.9:0          Operational DU   Passive  000:00:56   227/227
3.3.3.9:0          Operational DU   Passive  000:00:56   227/227
--------------------------------------------------------------------------------
TOTAL: 2 session(s) Found.
LAM : Label Advertisement Mode      SsnAge Unit : DDD:HH:MM
```

Step 3 Configure synchronization of LDP and an IGP on the interfaces of both ends of the link between crossing node P1 of the active link and the standby link and LDP neighboring node P2 on the active link.

Configure P1.

```
<P1> system-view
[P1] interface vlanif 10
[P1-Vlanif10] ospf ldp-sync
[P1-Vlanif10] quit
```

Configure P2.

```
<P2> system-view
[P2] interface vlanif 10
[P2-Vlanif20] ospf ldp-sync
[P2-Vlanif20] quit
```

Step 4 Set the value of the hold-down timer on the interfaces of both ends of the link between crossing node P1 of the active link and the standby link and LDP neighboring node P2 on the active link.

Configure P1.

```
<P1> system-view
[P1] interface vlanif 10
[P1-Vlanif10] ospf timer ldp-sync hold-down 8
[P1-Vlanif10] quit
```

Configure P2.

```
<P2> system-view
[P2] interface vlanif 10
[P2-Vlanif10] ospf timer ldp-sync hold-down 8
[P2-Vlanif10] quit
```

Step 5 Set the value of the hold-max-cost timer on the interfaces of both ends of the link between crossing node P1 of the active link and the standby link and LDP neighboring node P2 on the active link.

Configure P1.

```
<P1> system-view
[P1] interface vlanif 10
[P1-Vlanif10] ospf timer ldp-sync hold-max-cost 9
[P1-Vlanif10] quit
```

Configure P2.

```
<P2> system-view
[P2] interface vlanif 10
[P2-Vlanif10] ospf timer ldp-sync hold-max-cost 9
[P2-Vlanif10] quit
```

Step 6 Set the value of the delay timer on the interfaces of both ends of the link between crossing node P1 of the active link and the standby link and LDP neighboring node P2 on the active link.

Configure P1.

```
<P1> system-view
[P1] interface vlanif 10
```


Copyright © Huawei Technologies Co., Ltd.

```
[P1-Vlanif10] mpls ldp timer igp-sync-delay 6
[P1-Vlanif10] quit
```

Configure P2.

```
<P2> system-view
[P2] interface vlanif 10
[P2-Vlanif10] mpls ldp timer igp-sync-delay 6
[P2-Vlanif10] quit
```

Step 7 Verify the configuration.

After the configuration, run the **display ospf ldp-sync** command on P1, and you can view that the interface status is **Sync-Achieved**.

```
<P1> display ospf ldp-sync interface vlanif 10
Interface Vlanif10
HoldDown Timer: 8       HoldMaxCost Timer: 9
LDP State: Up             OSPF Sync State: Sync-Achieved
```

----End

Configuration Files

- Configuration file of P1

```
#
 sysname P1
#
 vlan batch 10 30
#
mpls lsr-id 1.1.1.9
 mpls
#
mpls ldp
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 ospf ldp-sync
 ospf timer ldp-sync holddown 8
 ospf timer ldp-sync holdmaxcost 9
 mpls
 mpls ldp
 mpls ldp timer igp-sync-delay 6
#
interface Vlanif30
 ip address 10.3.1.1 255.255.255.0
 ospf cost 1000
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 30
#
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 10.3.1.0 0.0.0.255
#
return
```


Copyright © Huawei Technologies Co., Ltd.

- Configuration file of P2

```
#
 sysname P2
#
 vlan batch 10 20
#
 mpls lsr-id 2.2.2.9
 mpls
#
mpls ldp
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 ospf ldp-sync
 ospf timer ldp-sync holddown 8
 ospf timer ldp-sync holdmaxcost 9
 mpls
 mpls ldp
 mpls ldp timer igp-sync-delay 6
#
interface vlanif20
 ip address 10.2.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
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 10.2.1.0 0.0.0.255
#
return
```

- Configuration file of P3

```
#
 sysname P3
#
 vlan batch 30 40
#
 mpls lsr-id 3.3.3.9
 mpls
#
mpls ldp
#
interface Vlanif30
 ip address 10.3.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlanif40
 ip address 10.4.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 30
#
```


Copyright © Huawei Technologies Co., Ltd.

```
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 40
#
ospf 1
 area 0.0.0.0
  network 3.3.3.9 0.0.0.0
  network 10.3.1.0 0.0.0.255
  network 10.4.1.0 0.0.0.255
#
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
 vlan batch 20 30
#
mpls lsr-id 4.4.4.9
#
 mpls
#
mpls ldp
#
interface Vlanif20
 ip address 10.2.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlanif40
 ip address 10.4.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 20
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 40
#
interface LoopBack1
 ip address 4.4.4.9 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 4.4.4.9 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.4.1.0 0.0.0.255
#
return
```

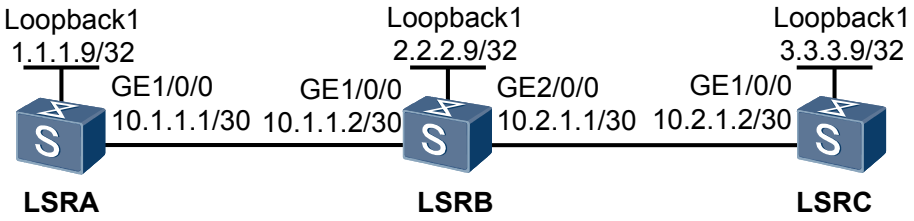
2.16.10 Example for Configuring LDP GTSM

Networking Requirements

As shown in **Figure 2-10**, each node runs MPLS and MPLS LDP. It is required to enable GTSM on LSR B.

Copyright © Huawei Technologies Co., Ltd.

Figure 2-10 Networking diagram for configuring LDP GTSM



Switch	Interface	VLANIF interface	IP address
LSRA	GigabitEthernet1/0/0	VLANIF 10	10.1.1.1/30
LSRB	GigabitEthernet1/0/0	VLANIF 10	10.1.1.2/30
LSRB	GigabitEthernet2/0/0	VLANIF 20	10.2.1.1/30
LSRC	GigabitEthernet1/0/0	VLANIF 20	10.2.1.2/30

Configuration Roadmap

The configuration roadmap is as follows:

- Configure basic MPLS and MPLS LDP functions.
- Configure GTSM on the two LDP peers.

Data Preparation

To complete the configuration, you need the following data:

- LSR ID of each LDP peer
- Maximum number of valid hops permitted by GTSM

Configuration Procedure

1. Configure VLANs that interfaces belong to.

```
<Quidway> system-view
[Quidway] sysname LSRA
[LSRA] vlan batch 10
[LSRA] interface gigabitethernet1/0/0
[LSRA-GigabitEthernet1/0/0] port hybrid pvid vlan 10
[LSRA-GigabitEthernet1/0/0] port hybrid untagged vlan 10
[LSRA-GigabitEthernet1/0/0] quit
```

   The configurations of LSRB and LSRC are similar to the configuration of LSRA, and are not mentioned here.

2. Configure an IP address for each VLANIF interface.

```
[LSRA] interface vlanif 10
[LSRA-Vlanif10] ip address 10.1.1.1 30
[LSRA-Vlanif10] quit
```

   The configurations of LSRB and LSRC are similar to the configuration of LSRA, and are not mentioned here.

3. Configure OSPF to advertise the network segments connected to the interfaces of the LSRs and host routes of LSR IDs. The configuration details are not mentioned here.

Copyright © Huawei Technologies Co., Ltd.

4. Configure each router with MPLS and MPLS LDP functions on each interface. The configuration details are not mentioned here.

   After the preceding configurations, run the **display mpls ldp session** command on each node, and you can view the setup of LDP sessions. Take LSR A as an example.

```
<LSRA> display mpls ldp session
 LDP Session(s) in Public Network
 Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD: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  0000:00:02  9/9

------------------------------------------------------------------------------
 TOTAL: 1 session(s) Found.
```

5. Configure LDP GTSM.

   # On LSR A, configure the range of valid TTL values carried in LDP packets received from LSR B to be from 253 to 255.

```
<LSRA> system-view
[LSRA] mpls ldp
[LSRA-mpls-ldp] gtsm peer 2.2.2.9 valid-ttl-hops 3
```

   # On LSR B, configure the range of valid TTL values carried in the LDP packets received from LSR A to be from 252 to 255, and the range of valid TTL values carried in LDP packets received from LSR C to be from 251 to 255.

```
<LSRB> system-view
[LSRB] mpls ldp
[LSRB-mpls-ldp] gtsm peer 1.1.1.9 valid-ttl-hops 4
[LSRB-mpls-ldp] gtsm peer 3.3.3.9 valid-ttl-hops 5
```

   # On LSR C, configure the range of valid TTL values carried in LDP packets received from LSR B to be from 250 to 255.

```
<LSRC> system-view
[LSRC] mpls ldp
[LSRC-mpls-ldp] gtsm peer 2.2.2.9 valid-ttl-hops 6
```

   Then, if the host PC simulates the LDP packets of LSR A to attack LSR B, LSR B discards the packets directly because the TTL values carried in the LDP packets are not within the range of 252 to 255. In the GTSM statistics on LSR B, the number of discarded packets increases.

Configuration Files

- Configuration file of LSR A

```
#
 sysname LSRA
#
vlan batch 10
#
 mpls lsr-id 1.1.1.9
 mpls
#
mpls ldp
gtsm peer 2.2.2.9 valid-ttl-hops 3
#
interface Vlanif10
ip address 10.1.1.1 255.255.255.252
mpls
 mpls ldp
#
```


Copyright © Huawei Technologies Co., Ltd.

```
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
interface GigabitEthernet1/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
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
#
vlan batch 10 20
#
 mpls lsr-id 2.2.2.9
 mpls
#
mpls ldp
gtsm peer 1.1.1.9 valid-ttl-hops 4
gtsm peer 3.3.3.9 valid-ttl-hops 5
#
interface Vlanif10
ip address 10.1.1.2 255.255.255.252
mpls
 mpls ldp
#
interface Vlanif20
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
#
interface GigabitEthernet1/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet2/0/0
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
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
#
vlan batch 20
#
 mpls lsr-id 3.3.3.9
 mpls
#
mpls ldp
gtsm peer 2.2.2.9 valid-ttl-hops 6
#
interface Vlanif20
ip address 10.2.1.2 255.255.255.252
```


Copyright © Huawei Technologies Co., Ltd.

```
mpls
 mpls ldp
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
interface GigabitEthernet1/0/0
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
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
```

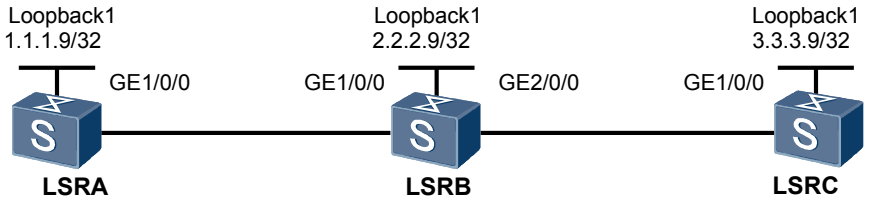
2.16.11 Example for Configuring LDP GR

Networking Requirements

As shown in **Figure 2-11**, LSRA, S9300-B, and LSRC are S9300s with dual main control boards. The three S9300s belong to the same OSPF area and are interconnected through OSPF. All of them support the GR mechanism.

LDP sessions are established between LSRA, S9300-B, and LSRC. When the main control board of S9300-B fails and traffic is switched, the LDP GR mechanism is used for synchronization with neighboring nodes.

Figure 2-11 Networking diagram for configuring LDP GR



switch	Interface	VLANIF interface	IP address
LSRA	GE1/0/0	VLANIF10	10.1.1.1/24
LSRB	GE1/0/0	VLANIF10	10.1.1.2/24
LSRB	GE2/0/0	VLANIF20	10.2.1.1/24
LSRC	GE1/0/0	VLANIF20	10.2.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and VLANIF interfaces.

Copyright © Huawei Technologies Co., Ltd.

2. Configure IP address of each interface on each node and the address of the loopback interface used as the LSR ID, and configure OSPF to advertise the network segments that the interfaces are connected to and the host route of the LSR ID.
3. Configure OSPF GR on each node.
4. Enable MPLS and MPLS LDP on each node globally.
5. Enable MPLS and MPLS LDP on each interface.
6. Set parameters during LDP session negotiation on LSRB.
7. Enable GR of MPLS LDP on each node.
8. Configure the GR session of MPLS LDP and neighboring parameters on LSRB.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each interface on each node shown in **Figure 2-11**, OSPF process ID, and OSPF area ID
- Interval for performing OSPF GR
- Value of the LDP Reconnect timer (300 seconds by default)
- Value of the LDP Neighbor-liveness timer (600 seconds by default)
- Value of the LDP Recovery timer (300 seconds by default)

Procedure

Step 1 Create VLANs and VLANIF interfaces.

See **Figure 2-11**.

Step 2 Assign an IP address to each interface.

See **Figure 2-11**.

Step 3 Configure OSPF to advertise the network segments that the interfaces are connected to and the host route of the LSR ID.

Step 4 Configure OSPF GR.

Configure LSRA.

```
<LSRA> system-view
[LSRA] ospf 1
[LSRA-ospf-1] opaque-capability enable
[LSRA-ospf-1] graceful-restart
[LSRA-ospf-1] quit
```

Configure LSRB.

```
<S9300-B> system-view
[LSRB] ospf 1
[LSRB-ospf-1] opaque-capability enable
[LSRB-ospf-1] graceful-restart
[LSRB-ospf-1] quit
```

Configure LSRC.

```
<S9300-C> system-view
[LSRC] ospf 1
[LSRC-ospf-1] opaque-capability enable
```


Copyright © Huawei Technologies Co., Ltd.

```
[LSRC-ospf-1] graceful-restart
[LSRC-ospf-1] quit
```

Step 5 Configure MPLS and MPLS LDP on each node globally.

Configure LSRA.

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

Configure LSRB.

```
[S9300-B] mpls lsr-id 2.2.2.9
[LSRB] mpls
[LSRB-mpls] quit
[LSRB] mpls ldp
[LSRB-mpls-ldp] quit
```

Configure LSRC.

```
[S9300-C] mpls lsr-id 3.3.3.9
[LSRC] mpls
[LSRC-mpls] quit
[LSRC] mpls ldp
[LSRC-mpls-ldp] quit
```

Step 6 Configure MPLS and MPLS LDP on each interface.

Configure LSRA.

```
[LSRA] interface vlanif 10
[LSRA-Vlanif10] mpls
[LSRA-Vlanif10] mpls ldp
[LSRA-Vlanif10] quit
```

Configure LSRB.

```
[S9300-B] interface vlanif 10
[LSRB-Vlanif10] mpls
[LSRB-Vlanif10] mpls ldp
[LSRB-Vlanif10] quit
[LSRB] interface vlanif 20
[LSRB-Vlanif20] mpls
[LSRB-Vlanif20] mpls ldp
[LSRB-Vlanif20] quit
```

Configure LSRC.

```
[S9300-C] interface vlanif 20
[LSRC-Vlanif20] mpls
[LSRC-Vlanif20] mpls ldp
[LSRC-Vlanif20] quit
```

After the configuration, the local LDP sessions between S9300-A and LSRB, and between S9300-B and LSRC are established.

Run the **display mpls ldp session** command on each node, and you can view the establishment of the LDP session. Take the display on LSRA as an example.

```
[S9300-A] 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  000:00:02   9/9
------------------------------------------------------------------------------
```


Copyright © Huawei Technologies Co., Ltd.

```
TOTAL: 1 Session(s) Found.
LAM : Label Advertisement Mode      SsnAge Unit : DDD:HH:MM
```

Step 7 Configure LDP GR.

Configure LSRA.

```
[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] quit
```

Configure LSRB.

```
[S9300-B] 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] quit
```

Configure LSRC.

```
[S9300-C] 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] quit
```

Step 8 Configure the parameters of LDP GR on the GR restarter.

Configure LSRB.

```
[LSRB] mpls ldp
[LSRB-mpls-ldp] graceful-restart timer reconnect 300
Warning: All the related sessions will be deleted if the operation is performed
!Continue? (y/n)y
[LSRB-mpls-ldp] graceful-restart timer neighbor-liveness 600
Warning: All the related sessions will be deleted if the operation is performed
!Continue? (y/n)y
[LSRB-mpls-ldp] graceful-restart timer recovery 300
Warning: All the related sessions will be deleted if the operation is performed
!Continue? (y/n)y
[LSRB-mpls-ldp] quit
```

Step 9 Verify the configuration.

After the configuration, run the **display mpls ldp session verbose** command on the LSR, and you can view that the Session FT Flag field is displayed as **on**. Take the display on S9300-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   : 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       : 1/1 (Message Count)
 Label Advertisement Mode          : Downstream Unsolicited
 Label Resource Status(Peer/Local) : Available/Available
 Session Age                       : 000:00:00  (DDD:HH:MM)

 Addresses received from peer: (Count: 3)
 10.1.1.2           10.2.1.1           2.2.2.9
```


Copyright © Huawei Technologies Co., Ltd.

```
 --------------------------------------------------------------------------
```

Or, run the **display mpls ldp peer verbose** command on the LSR, and you can view that the Peer FT Flag field is displayed as **on**. Take the display on S9300-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
 Peer Loop Detection : Off              Peer Path Vector Limit : ----
 Peer FT Flag        : On               Peer Keepalive Timer   : 45 Sec
 Recovery Timer      : 300 Sec          Reconnect Timer        : 300 Sec

 Peer Label Advertisement Mode : Downstream Unsolicited
 Peer Discovery Source         : Vlanif10

 --------------------------------------------------------------------------
```

----End

Configuration Files

- Configuration file of LSRA

```
#
 sysname LSRA
#
 vlan batch 10
#
 mpls lsr-id 1.1.1.9
 mpls
#
mpls ldp
 graceful-restart
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
ospf 1
 opaque-capability enable
 graceful-restart
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
return
```

- Configuration file of LSRB

```
#
 sysname LSRB
#
 vlan batch 10 20
#
 mpls lsr-id 2.2.2.9
 mpls
#
mpls ldp
```


Copyright © Huawei Technologies Co., Ltd.

```
 graceful-restart
 graceful-restart timer reconnect 300
 graceful-restart timer neighbor-liveness 600
 graceful-restart timer recovery 300
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlanif20
 ip address 10.2.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#
ospf 1
 opaque-capability enable
 graceful-restart
 area 0.0.0.0
  network 2.2.2.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.2.1.0 0.0.0.255
#
return
```

- Configuration file of LSRC

```
#
 sysname LSRC
#
 vlan batch 20
#
 mpls lsr-id 3.3.3.9
 mpls
#
mpls ldp
 graceful-restart
#
interface Vlanif20
 ip address 10.2.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
ospf 1
 opaque-capability enable
 graceful-restart
 area 0.0.0.0
  network 3.3.3.9 0.0.0.0
  network 10.2.1.0 0.0.0.255
#
Return
```


Copyright © Huawei Technologies Co., Ltd.

3 MPLS TE Configuration

About This Chapter

MPLS TE tunnels transmit MPLS L2VPN (VLL and VPLS) services and MPLS L3VPN services and thus provide high security and guarantees reliable QoS for VPN services.

Copyright © Huawei Technologies Co., Ltd.

Copyright © Huawei Technologies Co., Ltd.

3.1 MPLS TE Overview

MPLS TE reserves resources for tunnels to be set up, allowing traffic to be load-balanced among nodes without passing through congested nodes.

TE

Network resource insufficiency and load imbalance result in congestion on a network, affecting the performance of a backbone network. TE prevents network congestion and optimizes the network resources.

TE dynamically monitors traffic and load on network elements and adjusts parameters relevant to traffic control, routing, and resource constraints in real time. This optimizes utilization of network resources and prevents imbalance-triggered congestion.

MPLS TE

As a combination of MPLS and TE, MPLS TE load-balances traffic on a network by setting up an LSP over a specified path to reserve resources for traffic that will not pass through congested nodes.

An LSP with a higher priority preempts bandwidth resources of LSPs with lower priorities, providing sufficient bandwidth for services on the LSP with a higher priority in the case of bandwidth insufficiency.

If a link fault or a node fault occurs, MPLS TE uses path backup and fast reroute (FRR) to ensure uninterrupted traffic.

Administrators use MPLS TE to create LSPs to eliminate network congestions and use special offline utility to analyze traffic if the number of LSPs increases to a certain extent.

3.2 MPLS TE Features Supported by the S9300

MPLS TE features supported by the system include RSVP-TE tunnels, MPLS TE reliability, MPLS TE QoS, and MPLS TE security.

NOTE

This section describes MPLS TE features that are supported by the S9300. For details about MPLS TE features, see the section "MPLS TE" in the Quidway S9300 Terabit Routing Switch *Feature Description - MPLS*.

Static MPLS TE Tunnel

A static MPLS TE tunnel allows labels to be allocated manually, without signaling protocols exchanging control packets. Static MPLS TE tunnels are established on devices of low performance on a stable network.

Static MPLS TE tunnels have the highest priority among tunnels and therefore their bandwidth is not preemptive. In addition, static MPLS TE tunnels do not preempt bandwidth of other types of CR-LSPs.

Copyright © Huawei Technologies Co., Ltd.

RSVP-TE Tunnel

RSVP-TE tunnels are set up by the RSVP-TE signaling protocol and change dynamically according to the network topology.

RSVP-TE features supported by the S9300 are as follows:

- Collecting and advertising link information

  RSVP-TE uses an extended IGP (OSPF-TE or ISIS-TE) to collect and advertise TE link information and creates a traffic engineering database (TEDB). An extended IGP floods the link information periodically. If a link goes Up or Down, link attributes change, or the reservable bandwidth on the link changes to a certain extent, the extended IGP floods the link information. The flood threshold is adjusted by using command lines.

- Path calculation

  On the S9300, the path of a TE tunnel is calculated by using CSPF. When multiple paths share the same weights, one path is selected by using the configured tie-breaking.

  In addition to the reservable bandwidth and management group attributes, the following attributes are configurable:

  - Tunnel bandwidth
  - Affinity attribute
  - Explicit path
  - Maximum hop limit
  - Shared Risk Link Group (SRLG)

- Establishment of an RSVP-TE tunnel

  If configured, the system records routes and labels, or detects loops during the establishment of an RSVP-TE tunnel. When the resources are insufficient, preemption is triggered based on the setup and the holding priorities.

  If an RSVP-TE tunnel fails to be established, the system re-establishes the RSVP-TE tunnel periodically.

- Signaling mechanism

  RSVP-TE reserves resources in either fixed filter (FF) or shared-explicit (SE) mode. The following extended RSVP mechanisms are supported by the S9300 to relieve network burden and improve reliability:

  - Confirmation and retransmission for RSVP messages
  - Summary refreshing
  - Hello mechanism

  In addition, RSVP authentication is supported by the S9300 to improve network security.

- Traffic forwarding

  VPN traffic is directed to TE tunnels by using configured policy-based routes. Non-VPN traffic is directed to TE tunnels by using static routes, policy-based routes, IGP shortcut, or forwarding adjacency.

- Tunnel optimization and adjustment

  After tunnels are set up, the tunnels are adjusted and optimized by using the following features:

Copyright © Huawei Technologies Co., Ltd.

- Tunnel re-optimization: A path of a CR-LSP is calculated periodically. If a better path is discovered, a new CR-LSP is established over a better path, and traffic switches to the new CR-LSP.
- Route pinning: The path of an established tunnel is pinned, which means that the path of the tunnel is not optimized if a better path is discovered.

Reliability

The S9300 supports the following reliability features applied to MPLS TE tunnels:

- FRR

  FRR is a local protection mechanism in RSVP-TE. FRR protects traffic on CR-LSP links and nodes if faults occur. FRR is classified into manual FRR and automatic FRR.

- CR-LSP backup

  CR-LSP backup protects traffic on an entire RSVP-TE CR-LSP from end to end. If a primary CR-LSP fails, the system establishes a backup CR-LSP; if the backup CR-LSP fails, the system attempts to establish a best-effort path.

- BFD

  BFD detects a fault in a CR-LSP at millisecond level. BFD allows rapid detection, requirements for which hardware detection does not satisfy.

- RSVP GR

  RSVP GR is a status recovery mechanism for RSVP-TE tunnels. If a switchover on the control plane triggered by a fault or an operation, RSVP GR helps the system to properly forwarding data on the forwarding plane and restore the RSVP-TE LSP on the control plane. FRR is supported by the S9300 during the GR process.

- MPLS tunnel protection group

  An MPLS tunnel protection group provides an end-to-end mechanism applicable to MPLS TE tunnels, including but not limited to RSVP-TE tunnels. In an MPLS tunnel protection group, one tunnel protects traffic on other tunnels.

  NOTE

  For configurations of an MPLS tunnel protection group, see the section "MPLS OAM."

DS-TE

DS-TE maps different service types of traffic (such as voice, video, or data traffic) to LSPs. The path through which traffic passes is consistent with traffic engineering constraints of a specific service type.

DS-TE supports either non-IETF or IETF mode on the S9300.

- The non-IETF (non-standard) mode supports combinations between two CTs (CT0 and CT1) and eight priorities (0 to 7) and the Bandwidth Constraints models (RDM and MAM).

  Class-Type (CT) refers to the class mapped to a service. The priority refers to the LSP preemption priority.

- The IEFT (standard) mode supports combinations between eight CTs (CT0 to CT7) and eight priorities (0 to 7). In addition, it supports the following Bandwidth Constraints models: RDM, MAM, and extended-MAM.

A DS-TE tunnel supports TE FRR, hot standby, protection group, and CT traffic statistics.

Copyright © Huawei Technologies Co., Ltd.

3.3 Configuring Static CR-LSP

The configuration of a static CR-LSP is simple and label allocation is performed manually, rather than by using a signaling protocol to exchange control packets. This consumes a few resources.

3.3.1 Establishing the Configuration Task

Before configuring a static CR-LSP, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you rapidly and correctly finish the configuration task.

Applicable Environment

The configuration of a static CR-LSP is a simple process. Labels are manually allocated and the signaling protocol does not need to exchange control packets. The setup of a static CR-LSP consumes a few resources. In addition, you need to configure neither the IGP TE nor CSPF for the static CR-LSP.

The static CR-LSP cannot dynamically adapt to a changing network. Therefore, its application is very limited.

The static CR-LSP is a special static LSP that has the same setup constraints and uses the same label space ranging from 16 to 1023.

Pre-configuration Tasks

Before configuring a static CR-LSP, complete the following tasks:

- Configuring the static route or IGP to ensure the reachability between LSRs
- Configuring an MPLS LSR ID on each LSR
- Enabling basic MPLS functions on each LSR globally and on each interface

Data Preparation

To configure a static CR-LSP, you need the following data.

No.	Data
1	Physical links through which a static CR-LSP passes
2	Nodes through which the static CR-LSP passes
3	Values for outgoing labels on LSRs along the static CR-LSP
4	Number, tunnel ID, and destination address of the tunnel interface
5	Destination address of the static CR-LSP
6	Next hop address or outgoing interface on the ingress
7	Incoming interface, next hop address, or outgoing interface on each transit
8	Incoming interface on the egress

Copyright © Huawei Technologies Co., Ltd.

No.	Data
9	Bandwidth of the ingress and the transit node(s)

NOTE

- The value of the outgoing label on each node is the value of the incoming label of its next node.
- The destination address of a static CR-LSP is the destination address of the TE tunnel interface.

3.3.2 Enabling MPLS TE

Before setting up a static CR-LSP, you must enable MPLS TE.

Context

Do as follows on each node along the static CR-LSP:

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 on the node globally.

To enable MPLS TE on each interface, enable MPLS TE globally in the MPLS view first.

Step 4 Run:

```
quit
```

Return to the system view.

Step 5 Run:

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

The view of the interface is displayed.

Step 6 Run:

```
mpls
```

The MPLS is enabled on the interface.

Step 7 Run:

```
mpls te
```

The MPLS TE is enabled on the interface.

Copyright © Huawei Technologies Co., Ltd.

NOTE

When the MPLS TE is disabled in the interface view, all the CR-LSPs on the current interface change to Down.

When the MPLS TE is disabled in the MPLS view, the MPLS TE on each interface is disabled, and all CR-LSPs are deleted.

----End

3.3.3 Configuring the MPLS TE Tunnel Interface

Before setting up an MPLS TE tunnel, you must create a tunnel interface.

Context

Do as follows on the ingress node of a static CR-LSP:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The tunnel interface is created and the tunnel interface view is displayed.

Step 3 To configure the IP address of the tunnel interface, select one of the following commands.

- Run:

  ```
  ip address ip-address { mask | mask-length } [ sub ]
  ```

  The IP address of the tunnel interface is configured.

  The secondary IP address of the tunnel interface can be configured only after the primary IP address is configured.

- Or, run:

  ```
  ip address unnumbered interface interface-type interface-number
  ```

  The tunnel interface is configured to borrow an IP address from other interfaces.

To forward traffic, the tunnel interface must have an IP address; however, because the MPLS TE tunnel is unidirectional, no peer address is needed. Therefore, it is unnecessary to configure the IP address separately for the tunnel interface. The tunnel interface often borrows an LSR ID of the ingress node as the address.

NOTE

Because the type of the packet forwarded by the MPLS TE tunnel is MPLS, the commands, such as the **ip verify source-address** and **urpf** commands, related to IP packet forwarding configured on this interface are invalid.

Step 4 Run:

```
tunnel-protocol mpls te
```

MPLS TE is configured to be the tunnel protocol.

Step 5 Run:

```
destination ip-address
```


Copyright © Huawei Technologies Co., Ltd.

The destination address of the tunnel is configured, which is usually the LSR ID of the egress node.

Different types of tunnels need different destination addresses. When the tunnel protocol is changed to MPLS TE from other different protocols, the configured **destination** is deleted automatically and needs to be reconfigured.

Step 6 Run:

```
mpls te tunnel-id tunnel-id
```

The tunnel ID is configured.

Step 7 Run:

```
mpls te signal-protocol cr-static
```

The signal protocol of the tunnel is configured to be CR-static.

Step 8 Run:

```
mpls te commit
```

The current tunnel configuration is committed.

NOTE

If MPLS TE parameters on a tunnel interface are modified, you need to run the **mpls te commit** command to activate them.

----End

3.3.4 Configuring the Ingress of the Static CR-LSP

To set up a static CR-LSP, you need to specify the ingress node of the CR-LSP.

Context

Do as follows on the ingress of a static CR-LSP:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
static-cr-lsp ingress { tunnel-interface tunnel interface-number | tunnel-name }
destination destination-address { nexthop next-hop-address | outgoing-interface
interface-type interface-number } * out-label out-label [ bandwidth [ ct0 | ct1 |
ct2 | ct3 | ct4 | ct5 | ct6 | ct7 ] bandwidth ]
```

The LSR is set as the ingress of the specified static CR-LSP.

tunnel *interface-number* specifies the MPLS TE tunnel interface that uses this static CR-LSP. By default, the Bandwidth Constraints value is **ct0**, and the value of bandwidth is 0. The bandwidth used by the tunnel cannot be higher than the maximum reservable bandwidth of the link.

The value of *tunnel-name* cannot be spaces or abbreviations. For example, if a tunnel interface named Tunnel 2/0/0 is specified in the **interface tunnel 2/0/0** command, tunnel-name specified

Copyright © Huawei Technologies Co., Ltd.

in the **static-cr-lsp ingress** command must be Tunnel2/0/0; otherwise, the tunnel cannot be set up. For the transit and egress, tunnel name consistency is not required.

The next hop or outgoing interface is determined by the route from the ingress to the egress. For the difference between the next hop and outgoing interface, refer to "Static Route Configuration" in the Quidway S9300 Terabit Routing Switch *Configuration Guide - IP Routing*.

----End

3.3.5 Configuring the Transit of the Static CR-LSP

To set up a static CR-LSP, you need to specify the transit nodes of the CR-LSP. This procedure is optional because the CR-LSP can have no transit node.

Context

If the static CR-LSP has only the ingress and egress, this configuration is not needed. If the static CR-LSP has one or more transits, do as follows on the transit node:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
static-cr-lsp transit lsp-name incoming-interface interface-type interface-number
in-label in-label-value { nexthop next-hop-address | outgoing-interface interface-
type interface-number } * out-label out-label-value [ bandwidth [ ct0 | ct1 | ct2
| ct3 | ct4 | ct5 | ct6 | ct7 ] bandwidth ]
```

The LSR is set as the transit node of the specified static CR-LSP.

No restriction is specified for the *lsp-name* of the transit and the egress, but the *lsp-name* should not be a duplicate of the existing tunnel name on the node.

----End

3.3.6 Configuring the Egress of the Static CR-LSP

To set up a static CR-LSP, you need to specify the egress node of the CR-LSP.

Context

Do as follows on the egress of the static CR-LSP:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
static-cr-lsp egress lsp-name incoming-interface interface-type interface-number
in-label in-label [ lsrid ingress-lsr-id tunnel-id tunnel-id ]
```


Copyright © Huawei Technologies Co., Ltd.

The LSR is configured as the egress of the specified static CR-LSP.

----End

3.3.7 Checking the Configuration

After the configuration of a static CR-LSP, you can view the static CR-LSP status.

Prerequisite

The configurations of the static MPLS TE tunnel function are complete.

Procedure

- Run the **display mpls static-cr-lsp** [*lsp-name*] [{ **include** | **exclude** } *ip-address mask-length*] [**verbose**] command to check information about the static CR-LSP.
- Run the **display mpls te tunnel** [**destination** *ip-address*] [**lsp-id** *ingress-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*] [**te-class0** | **te-class1** | **te-class2** | **te-class3** | **te-class4** | **te-class5** | **te-class6** | **te-class7**] [**verbose**] command to check information about the tunnel.
- Run the **display mpls te tunnel statistics** or **display mpls lsp statistics** command to check the tunnel statistics.
- Run the **display mpls te tunnel-interface** [**tunnel** *tunnel-number*] command to check information about the tunnel interface on the ingress.

----End

Example

If the configurations succeed, run the preceding commands, and you can view the following information:

- Information about the static CR-LSP name, the incoming and outgoing labels, and the incoming and outgoing interfaces. The status of CR-LSP is Up.
- Statistics of tunnel status on the LSR.
- Details of the tunnel interface, including the tunnel name, state description, and attributes. The tunnel attributes include the LSP ID, ingress, egress, and signaling protocol.

3.4 Configuring an RSVP-TE Tunnel

An RSVP-TE tunnel is the prerequisite for the configuration of TE attributes.

3.4.1 Establishing the Configuration Task

Before configuring an RSVP-TE tunnel, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and efficiently.

Copyright © Huawei Technologies Co., Ltd.

Applicable Environment

A dynamic signaling protocol adjusts the path of a TE tunnel on the basis of network topology changes. To implement advanced features such as TE FRR and CR-LSP backup, establishing an MPLS TE tunnel by using the RSVP-TE signaling protocol is recommended.

Pre-configuration Tasks

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

- Configuring OSPF or IS-IS to ensure the reachability between LSRs
- Configuring an LSR ID for every LSR
- Enabling MPLS on every LSR globally and on each interface

Data Preparation

To configure an RSVP-TE tunnel, you need the following data.

No.	Data
1	Nodes through which an RSVP CR-LSP passes
2	Links through which an MPLS TE tunnel passes
3	Maximum bandwidth and the maximum reservable bandwidth for a link
4	OSPF area ID or IS-IS level of a device enabled with TE
5	Tunnel ID
6	Destination address of a tunnel
7	Constraints for an MPLS TE tunnel, such as explicit path or tunnel bandwidth
8	(Optional) RSVP resource reservation style (the default style is Shared-Explicit)

3.4.2 Enabling MPLS TE and RSVP-TE

Enabling MPLS TE and RSVP-TE is the prerequisite for configuring MPLS TE attributes.

Context

NOTE

- If MPLS TE is disabled in the interface view, all CR-LSPs on the current interface go Down.
- If MPLS TE is disabled in the MPLS view, MPLS TE on each interface is disabled and all CR-LSPs go Down.
- If RSVP-TE on a node is disabled, RSVP-TE on all interfaces of this node is disabled.

Do as follows on each node along a TE tunnel:

Copyright © Huawei Technologies Co., Ltd.

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 on the node globally.

Step 4 Run:

```
mpls rsvp-te
```

RSVP-TE is enabled on the node globally.

Step 5 Run:

```
quit
```

Return to the system view.

Step 6 Run:

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

The interface view of the MPLS-TE-enabled interface is displayed.

Step 7 Run:

```
mpls te
```

MPLS TE is enabled on the interface.

Step 8 Run:

```
mpls rsvp-te
```

RSVP-TE is enabled on the interface.

----End

3.4.3 Configuring OSPF TE

A Traffic Engineering DataBase (TEDB) will be generated on a network if OSPF TE is configured. After OSPF TE is configured, a CR-LSP is established by using OSPF routes not the routes calculated by CSPF.

Context

By default, an OSPF area does not support TE.

The OSPF TE extension uses Opaque Type 10 LSA to carry the TE attribute of a link. Therefore, the Opaque capability of OSPF must be enabled. TE LSAs are generated only when at least one neighbor is in the FULL state.

Copyright © Huawei Technologies Co., Ltd.

NOTE

If OSPF TE is not configured, no TE LSA exists and thus no TEDB is generated on a network. In this case, a CR-LSP is established by using IGP routes not routes calculated by CSPF calculation.

Do as follows on each node along a TE tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

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

The OSPF view is displayed.

Step 3 Run:

```
opaque-capability enable
```

The OSPF opaque capability is enabled.

Step 4 (Optional) Run:

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

The MPLS LSR ID is advertised to multiple OSPF areas. This step is necessary only on an Area Border Router (ABR) in multiple OSPF areas.

Step 5 Run:

```
area area-id
```

The OSPF area view is displayed.

Step 6 Run:

```
mpls-te enable [ standard-complying ]
```

TE is enabled in the current OSPF area.

----End

3.4.4 Configuring IS-IS TE

A TEDB will be generated on a network only if IS-IS TE is configured. After IS-IS TE is configured, a CR-LSP is established by using IS-IS routes not the routes calculated by CSPF.

Context

Do as follows on each node along a TE tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

Copyright © Huawei Technologies Co., Ltd.

```
isis [ process-id ]
```

The IS-IS view is displayed.

Step 3 Run:

```
cost-style { compatible [ relax-spf-limit ] | wide | wide-compatible }
```

The IS-IS Wide Metric attribute is configured.

The IS-IS TE extension uses a sub-TLV of IS-reachable TLV (22) to carry TE attributes. The IS-IS Wide Metric attribute configured as wide, compatible or wide-compatible. By default, IS-IS sends or receives packets that express route metric in Narrow mode.

Step 4 Run:

```
traffic-eng [ level-1 | level-2 | level-1-2 ]
```

IS-IS TE is enabled.

By default, IS-IS does not support TE.

If a level is not specified after IS-IS TE is enabled, IS-IS TE is valid for both Level-1 and Level-2.

Step 5 (Optional) Run:

```
te-set-subtlv { bw-constraint value | lo-multiplier value | unreserve-bw-sub-pool value }*
```

The TLV type for the sub-TLVs used to carry the DS-TE parameters is set.

By default, the BW-constraint sub-TLV is 252; the Local Overbooking Multipliers (LOM) sub-TLV is 253; the unreserve-BW-sub-pool sub-TLV is 251.

----End

3.4.5 (Optional) Configuring an MPLS TE Explicit Path

An explicit path is created, over which a CR-LSP is established.

Context

An explicit path consists of a series of nodes. These nodes form a vector path in the sequence of configuration.

The IP address of an explicit path is the IP address of an interface on the node. Often, the IP address of a loopback interface on the egress node is used as the destination address of the explicit path.

Adjacent nodes are connected in the following modes on an explicit path:

- Strict: The two nodes are connected directly.
- Loose: Other LSRs may exist between the two nodes.

The strict mode and the loose mode are used separately or together.

By default, the **include strict** mode is used. This means that the next hop added to the explicit path must be directly connected to the previous node. A constraint for an explicit path is that the nodes through which traffic must pass or cannot pass are selectable.

include indicates that an established LSP must pass through the specified nodes.

exclude indicates that an established LSP cannot pass through the specified nodes.

Copyright © Huawei Technologies Co., Ltd.

TE tunnels are classified into intra-area tunnels and inter-area tunnels.

- Intra-area tunnel: indicates that TE tunnels are in a single area. An area is either an OSPF area or an IS-IS area, not a BGP AS.
- Inter-area tunnel: indicates that TE tunnels traverse through multiple areas. Areas are OSPF areas or IS-IS areas not BGP ASs.

A loose explicit path must be used to establish an inter-area TE tunnel and the next node of the explicit path must be an ABR or an ASBR.

Do as follows on the ingress of a TE tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
explicit-path path-name
```

The explicit path is created and the explicit path view is displayed.

Step 3 Run:

```
next hop ip-address [ include [ strict | loose ] | exclude ]
```

The next IP address of the explicit path is specified.

Step 4 Run:

```
add hop ip-address1 [ include [ strict | loose ] | exclude ] { after | before } ip-address2
```

A node is added to the explicit path.

Step 5 Run:

```
modify hop ip-address1 ip-address2 [ include [ strict | loose ] | exclude ]
```

The address of a node on the explicit path is modified.

Step 6 Run:

```
delete hop ip-address
```

A node is deleted from the explicit path.

Step 7 Run:

```
list hop [ ip-address ]
```

Information about the explicit path is displayed.

----End

3.4.6 Configuring the MPLS TE Tunnel Interface

A tunnel interface must be created and tunnel configurations must be configured on the tunnel interface before an RSVP-TE tunnel is established.

Context

Do as follows on the ingress node of a TE tunnel:

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel interface-number
```

A tunnel interface is created and the tunnel interface view is displayed.

CAUTION

Configuring a tunnel interface on the main control board is recommended. The slot ID of the main control board is the slot ID in *tunnel-number*, which is usually 0. In the situation where a tunnel interface is configured on an interface board, the tunnel interface will be deleted if the interface board is pulled out.

Step 3 To configure the IP address of a tunnel interface, run one of the following commands.

- To assign an IP address to the tunnel interface, run:
  ```
  ip address ip-address { mask | mask-length } [ sub ]
  ```
  The secondary IP address of the tunnel interface is configured only after the primary IP address is configured.
- To use an unnumbered IP address, run:
  ```
  ip address unnumbered interface interface-type interface-number
  ```

A tunnel interface must have an IP address to forward traffic. It is unnecessary to configure an IP address separately for the tunnel interface as an MPLS TE tunnel is unidirectional. The tunnel interface often borrows the LSR ID of the ingress node as the address.

NOTE

Because the type of the packet forwarded by the MPLS TE tunnel is MPLS, the commands, such as the **ip verify source-address** and **urpf** commands, related to IP packet forwarding configured on this interface are invalid.

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 node.

Different types of tunnels have different requirements for a destination address. If the tunnel protocol is changed to MPLS TE, the configuration of the **destination** command is deleted automatically and needs to be re-configured.

Step 6 Run:

```
mpls te tunnel-id tunnel-id
```


Copyright © Huawei Technologies Co., Ltd.

The tunnel ID is configured.

Step 7 Run:

```
mpls te signal-protocol  rsvp-te
```

RSVP-TE is configured as the signaling protocol for a tunnel.

Step 8 Run:

```
mpls te commit
```

The current tunnel configuration is committed.

NOTE

If MPLS TE parameters on a tunnel interface are changed, run the **mpls te commit** command to make them take effect.

----End

3.4.7 (Optional) Configuring RSVP Resource Reservation Style

By configuring a resource reservation style, you can configure different LSPs over the same link to use the same or different reserved resources.

Context

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 tunnel interface view of the MPLS TE tunnel is displayed.

Step 3 Run:

```
mpls te resv-style { ff | se }
```

The resource reservation style for the tunnel is specified.

By default, the resource reservation style is the Shared-Explicit (SE) style.

In TE applications, the SE style is used in the make-before-break mechanism, and the Fixed-Filter (FF) style is seldom used.

Step 4 Run:

```
mpls te commit
```

The tunnel configuration is committed.

----End

Copyright © Huawei Technologies Co., Ltd.

3.4.8 Configuring CSPF

An IGP uses SPF to calculate the shortest path to each node on a network; MPLS TE uses CSPF to calculate the path to a certain node.

Context

Do as follows on the ingress of a TE tunnel:

NOTE

Configuring CSPF on all the transit nodes is recommended, preventing incomplete path computation on the ingress.

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 on the local LSR is enabled.

Step 4 (Optional) Run:

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

The preferred IGP protocol is configured.

By default, CSPF is disabled.

----End

3.4.9 Checking the Configuration

After the configuration of an RSVP-TE tunnel, you can view statistics about the RSVP-TE tunnel and its status.

Prerequisite

The configurations of the RSVP-TE tunnel function are complete.

Procedure

- Run the **display mpls te link-administration bandwidth-allocation** [**interface** *interface-type interface-number*] command to check the allocation of the link bandwidth.
- Run the **display ospf** [*process-id*] **mpls-te** [**area** *area-id*] [**self-originated**] command to check OSPF TE information.

Copyright © Huawei Technologies Co., Ltd.

- Run the **display isis traffic-eng advertisements** [{ **level-1** | **level-2** | **level-1-2** } | { *lsp-id* | **local** }] * [*process-id* | [**vpn-instance** *vpn-instance-name* | **vpn6-instance** *vpn6-instance-name*] *] command to check the IS-IS TE status.
- Run the **display isis traffic-eng link** [{ **level-1** | **level-2** | **level-1-2** } | **verbose**] * [*process-id* | [**vpn-instance** *vpn-instance-name* | **vpn6-instance** *vpn6-instance-name*] *] command to check the IS-IS TE status.
- Run the **display isis traffic-eng network** [**level-1** | **level-2** | **level-1-2**] [*process-id* | [**vpn-instance** *vpn-instance-name* | **vpn6-instance** *vpn6-instance-name*] *] command to check the IS-IS TE status.
- Run the **display isis traffic-eng statistics** [*process-id* | [**vpn-instance** *vpn-instance-name* | **vpn6-instance** *vpn6-instance-name*] *] command to check the IS-IS TE status.
- Run the **display isis traffic-eng sub-tlvs** [*process-id* | [**vpn-instance** *vpn-instance-name* | **vpn6-instance** *vpn6-instance-name*] *] command to check the IS-IS TE status.
- Run the **display explicit-path** [*path-name*] [**verbose**] command to check the 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 path information for CSPF.
- Run the **display mpls te cspf tedb** { **all** | **area** *area-id* | **interface** *ip-address* | **network-lsa** | **node** [*router-id*] } command to check TEDB information for CSPF.
- Run the **display mpls rsvp-te** [**interface** [*interface-type interface-number*]] command to check information about RSVP.
- Run the **display mpls rsvp-te established** [**interface** *interface-type interface-number peer-ip-address*] command to check the established RSVP-TE tunnel.
- Run the **display mpls rsvp-te peer** [**interface** *interface-type interface-number*] command to check RSVP information of neighbors.
- Run the **display mpls rsvp-te reservation** [**interface** *interface-type interface-number peer-ip-address*] command to check the RSVP reserved resource.
- Run the **display mpls rsvp-te request** [**interface** *interface-type interface-number peer-ip-address*] command to check information about the resources that are requsted.
- Run the **display mpls rsvp-te sender** [**interface** *interface-type interface-number peer-ip-address*] command to check information about the RSVP sender.
- Run the **display mpls rsvp-te statistics** { **global** | **interface** [*interface-type interface-number*] } command to check statistics about RSVP-TE.
- Run the **display mpls te link-administration admission-control** [**interface** *interface-type interface-number* | **stale-interface** *interface-index*] command to check the tunnel permitted by the local node.
- Run the **display mpls te tunnel** [**destination** *ip-address*] [**lsp-id** *ingress-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 tunnel information.
- Run the **display mpls te tunnel statistics** or **display mpls lsp statistics** command to check tunnel statistics.

Copyright © Huawei Technologies Co., Ltd.

- Run the **display mpls te tunnel-interface** [**tunnel** *tunnel-number*] command to check the tunnel interface on the ingress.

----End

Example

If the configurations succeed, run the preceding commands, and you can view the following information:

- Information about links, including the physical bandwidth and available bandwidth of the link
- Information about OSPF TE LSAs generated by every node
- Information about IS-IS TE on every node
- Information about MPLS RSVP-TE timers, the status of interfaces enabled RSVP-TE, the bandwidth, the parameters for RSVP neighbors, sender information, and statistics
- Tunnel name, incoming and outgoing labels, and incoming and outgoing interfaces.
- Tunnel status statistics on the LSR
- Detailed information about the tunnel interface on the tunnel ingress, including the tunnel's name, status, and attributes (including the LSP ID, ingress, and egress)

3.5 Referencing the CR-LSP Attribute Template to Set Up a CR-LSP

By configuring a CR-LSP attribute template to set up CR-LSPs, you can simply the configurations and make the configurations of CR-LSPs more flexible.

3.5.1 Establishing the Configuration Task

Before using a CR-LSP attribute template to set up a CR-LSP, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

You can create a CR-LSP by using the following methods:

- Creating a CR-LSP without using a CR-LSP attribute template
- Creating a CR-LSP by using a CR-LSP attribute template

  It is recommended to use a CR-LSP attribute template to set up a CR-LSP because this method has the following advantages:

  - A CR-LSP attribute template can greatly simplify the configurations of CR-LSPs.
  - A maximum of three CR-LSP attribute templates can be created for a hot-standby CR-LSP or an ordinary backup CR-LSP; thus, you can set up a hot-standby CR-LSP or an ordinary backup CR-LSP with different path options. (Among the three attribute templates, the template with the smallest sequence number is firstly used. If the setup fails, the template with a greater sequence number is used.)

Copyright © Huawei Technologies Co., Ltd.

- If configurations of a CR-LSP attribute template are modified, configurations of the CR-LSPs established by using the CR-LSP attribute template are automatically updated, which makes the configurations of CR-LSPs more flexible.

NOTE

The preceding two methods can be used together. If the TE attribute configured in the tunnel interface view and the TE attribute configured through a CR-LSP attribute template coexist, the former takes precedence over the latter.

Pre-configuration Tasks

Before using a CR-LSP attribute template to set up a CR-LSP, complete the following tasks:

- Configuring an IGP on the P and PE on the MPLS backbone network to ensure IP connectivity
- Enable MPLS, MPLS TE, and RSVP TE on the MPLS backbone network

Data Preparation

To use a CR-LSP attribute template to set up a CR-LSP, you need the following data.

No.	Data
1	Names of the primary CR-LSP attribute template, hot-standby CR-LSP attribute template, or ordinary backup CR-LSP attribute template
2	(Optional) Bandwidth of the CR-LSP attribute template
3	(Optional) Name of the explicit path referenced by the CR-LSP attribute template
4	(Optional) Affinity value and affinity mask of the CR-LSP attribute template
5	(Optional) Setup priority and hold priority of the CR-LSP attribute template
6	(Optional) Hop limit of the CR-LSP attribute template
7	Tunnel interface which will use the attribute template
8	Sequence of using the hot-standby CR-LSP attribute template and ordinary backup CR-LSP attribute template

3.5.2 Configuring a CR-LSP Attribute Template

You need to configure a CR-LSP attribute template before using the CR-LSP attribute template to set up a CR-LSP.

Context

Do as follows on the ingress of the CR-LSP:

Steps 3 to 10 are optional.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
lsp-attribute lsp-attribute-name
```

A CR-LSP attribute template is created and the LSP attribute view is displayed.

NOTE

A CR-LSP attribute template can be deleted only when it is not used by any tunnel interface.

Step 3 (Optional) Run:

```
bandwidth { ct0 bandwidth | ct1 bandwidth | ct2 bandwidth | ct3 bandwidth | ct4 bandwidth | ct5 bandwidth | ct6 bandwidth | ct7 bandwidth }*
```

The bandwidth is set for the CR-LSP attribute template. The optional bandwidth type varies with DS-TE modes. In non-DS-TE mode, only CT0 and CT1 are supported. In DS-TE mode, if no TE-Class mapping table is configured, only CT0, CT1, CT2, and CT3 are supported; if a TE-Class mapping table is configured, the CT types configured in the TE-Class mapping table are adopted.

NOTE

If an MPLS TE tunnel to be set up requires a bandwidth larger than 67105 kbit/s, it is recommended that the 1/1000 of the configured bandwidth to be reserved.

Step 4 (Optional) Run:

```
explicit-path path-name
```

An explicit path is configured for the CR-LSP attribute template.

Step 5 (Optional) Run:

```
affinity property affinity-value [ mask mask-value ]
```

The affinity attribute is set for the CR-LSP attribute template.

By default, both the affinity value and the affinity mask are 0x0.

Step 6 (Optional) Run:

```
priority setup_priority_value [ hold_priority_value ]
```

The setup priority and hold priority are set for the CR-LSP attribute template.

By default, both the setup priority and the hold priority are 7.

Step 7 (Optional) Run:

```
hop-limit hop-limit
```

The hop limit is set for the CR-LSP attribute template.

By default, the hop limit is 32.

Step 8 (Optional) Run:

```
fast-reroute [ bandwidth ]
```

FRR is enabled for the CR-LSP attribute template.

By default, FRR is disabled.

Copyright © Huawei Technologies Co., Ltd.

NOTE

Before enabling or disabling FRR for the CR-LSP attribute template, note the following:

- After FRR is enabled, the route recording function is automatically enabled for the CR-LSP.
- After FRR is disabled, attributes of the bypass tunnel are automatically deleted.

Step 9 (Optional) Run:

```
record-route [ label ]
```

The route recording function is enabled for the CR-LSP attribute template.

By default, the route recording function is disabled.

NOTE

The **undo mpls te record-route** command can take effect only when FRR is disabled.

Step 10 (Optional) Run:

```
bypass-attributes { bandwidth bandwidth | priority setup_priority_value
[ hold_priority_value ] }
```

The bypass tunnel attributes are configured for the CR-LSP attribute template.

By default, the bypass tunnel attributes are not configured.

NOTE

This command can take effect only when the following conditions are met:

- The CR-LSP attribute template has been enabled with FRR allowing bandwidth protection.
- The bandwidth for the bypass tunnel is lower than or equal to the bandwidth for the CR-LSP attribute template.
- The setup priority and hold priority of the bypass tunnel are smaller than the setup priority and hold priority of the CR-LSP attribute template.

Step 11 Run:

```
commit
```

Configurations of the CR-LSP attribute template are committed.

NOTE

When the CR-LSP attribute template is used to set up a CR-LSP:

- The CR-LSP is removed and a new CR-LSP is created if the Break-Before-Make attribute (the priority attribute) of the CR-LSP attribute template is modified.
- The CR-LSP is removed after an eligible CR-LSP is created and traffic switches to the new CR-LSP if the Make-Before-Break attribute of the CR-LSP attribute template is modified.

----End

3.5.3 Setting Up a CR-LSP by Using a CR-LSP Attribute Template

You can use a CR-LSP attribute template to set up the primary CR-LSP, hot-standby CR-LSP, and ordinary backup CR-LSP.

Context

Do as follows on the ingress of the CR-LSP:

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run:

```
system-view
```

The system view is display.

Step 2 Run:

```
interface tunnel tunnel-number
```

The tunnel interface view is displayed.

To configure the TE tunnel interface, refer to the section **Configuring MPLS TE Tunnel Interfaces**.

Step 3 Run:

```
mpls te primary-lsp-constraint { dynamic | lsp-attribute lsp-attribute-name }
```

The primary CR-LSP is set up through the specified CR-LSP attribute template.

If **dynamic** is used, it indicates that when a CR-LSP attribute template is used to set up a primary CR-LSP, all attributes in the template adopt the default values.

Step 4 (Optional) Run:

```
mpls te hotstandby-lsp-constraint number { dynamic | lsp-attribute lsp-attribute-name }
```

The hot-standby CR-LSP is set up by using the specified CR-LSP attribute template.

A maximum of three CR-LSP attribute templates can be used to set up a hot-standby CR-LSP. The hot-standby CR-LSP must be consistent with the primary CR-LSP in the attributes of the setup priority, hold priority, and bandwidth type. To set up a hot-standby CR-LSP, you should keep on attempting to use CR-LSP attribute templates one by one in ascending order of the number of the attribute templates until the hot-standby CR-LSP is set up.

If **dynamic** is used, it indicates that the hot-standby CR-LSP is assigned the same bandwidth and priority as the primary CR-LSP, but specified with a different path from the primary CR-LSP.

Step 5 (Optional) Run:

```
mpls te backup hotstandby-lsp-constraint wtr interval
```

The Wait to Restore (WTR) time is set for the traffic to switch back from the hot-standby CR-LSP to the primary CR-LSP.

By default, the WTR time for the traffic to switch back from the hot-standby CR-LSP to the primary CR-LSP is 10 seconds.

NOTE

The hot-standby CR-LSP specified in the **mpls te backup hotstandby-lsp-constraint wtr** command must be an existing one established by running the **mpls te hotstandby-lsp-constraint** command.

Step 6 (Optional) Run:

```
mpls te ordinary-lsp-constraint number { dynamic | lsp-attribute lsp-attribute-name }
```

The ordinary backup CR-LSP is set up by using the specified CR-LSP attribute template.

A maximum of three CR-LSP attribute templates can be used to set up an ordinary backup CR-LSP. The ordinary backup CR-LSP must be consistent with the primary CR-LSP in the attributes

Copyright © Huawei Technologies Co., Ltd.

of the setup priority, hold priority, and bandwidth type. To set up an ordinary backup CR-LSP, you should keep on attempting to use CR-LSP attribute templates one by one in ascending order of the number of the attribute template until the ordinary backup CR-LSP is set up.

If **dynamic** is used, it indicates that the ordinary backup CR-LSP is assigned the same bandwidth and priority as the primary CR-LSP.

Step 7 Run:

```
mpls te commit
```

The configurations of the CR-LSP are committed.

----End

3.5.4 Checking the Configuration

After referencing a CR-LSP attribute template to set up CR-LSPs, you can view information about the established MPLS TE CR-LSPs.

Prerequisite

All configurations of the CR-LSP set up by using the CR-LSP attribute template are complete.

Procedure

Step 1 Run the **display explicit-path** [*path-name*] [**tunnel-interface** | **lsp-attribute** | **verbose**] command to view information about the explicit path configured for the CR-LSP attribute template.

Step 2 Run the **display mpls te tunnel-interface lsp-constraint** [**tunnel** *tunnel-number*] command to view information about the CR-LSP attribute template on the TE tunnel interface.

Step 3 Run the **display mpls te tunnel-interface** [**auto-bypass-tunnel** *tunnel-name* | **tunnel** *tunnel-number*] command to view information about the MPLS TE tunnel using the CR-LSP attribute template.

----End

Example

If the configurations succeed, you can view the following information:

- List of CR-LSP attribute templates that use the specified explicit path
- Information about the CR-LSP attribute templates on the specified TE tunnel interface
- Information about the CR-LSPs that are set up through the specified CR-LSP attribute template

3.6 Adjusting RSVP Signaling Parameters

RSVP-TE provides various parameters, which meet the requirements for reliability, network resources, and advanced MPLS features.

Copyright © Huawei Technologies Co., Ltd.

3.6.1 Establishing the Configuration Task

Before adjusting RSVP signaling parameters, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

RSVP TE supports diversified signaling parameters. It ensures reliability and network resource efficiency, and offers certain MPLS TE advanced features.

Before performing the configuration tasks described in this section, you must know in detail the purpose of each task and the influences they have on networks.

Pre-configuration Tasks

Before optimizing the RSVP-TE tunnel, complete the following task:

- **Configuring RSVP-TE Tunnel**

Data Preparation

To optimize the RSVP TE tunnel, you need the following data.

No.	Data
1	Refresh interval of RSVP message
2	PSB, RSB, and BSB timeout multiplier of RSVP
3	Retransmission timer and increment of RSVP
4	Transmission interval and allowable maximum loss numbers of Hello messages

3.6.2 Configuring RSVP Hello Extension

The RSVP Hello extension mechanism can detect reachability of RSVP neighbors.

Context

Do as follows on each node along the TE tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Copyright © Huawei Technologies Co., Ltd.

Step 3 Run:

```
mpls rsvp-te hello
```

RSVP Hello extension is enabled on this node.

By default, the RSVP hello extension is disabled.

Step 4 Run:

```
mpls rsvp-te hello-lost times
```

The permitted maximum times of Hello message loss is set.

When the RSVP Hello extension is enabled, by default, Hello ACK messages cannot be received for consecutive 3 times, exceeding which the link is regarded as faulty, and the TE tunnel is torn down.

Step 5 Run:

```
mpls rsvp-te timer hello interval
```

The refresh interval of Hello messages is set.

When the RSVP Hello extension is enabled, by default, the refresh interval of Hello message is seconds.

If the refresh interval is modified, the modification takes effect after the timer times out.

Step 6 Run:

```
quit
```

Return to the system view.

Step 7 Run:

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

The interface view of the RSVP-TE-enabled interface is displayed.

Step 8 Run:

```
mpls rsvp-te hello
```

The RSVP Hello extension mechanism is enabled on the interface.

The RSVP Hello extension mechanism is used to detect the reachability of RSVP neighboring nodes. For details, refer to RFC 3209 and RFC 3473.

----End

3.6.3 Configuring RSVP Timers

By configuring the RSVP status timer, you can set the refresh interval of Path messages and Resv messages and the timeout multiplier when RSVP is in the blocked state.

Context

Do as follows on each node along the TE tunnel:

Procedure

Step 1 Run:

```
system-view
```


Copyright © Huawei Technologies Co., Ltd.

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 for refreshing Path/Resv messages is set.

By default, the refresh interval of Path/Resv message is 30 seconds.

If the refresh interval is modified, the modification takes effect after the timer expires.

It is not recommended to set a long refresh interval or modify the refresh interval frequently.

Step 4 Run:

mpls rsvp-te keep-multiplier *number*

The timeout multiplier of PSB and RSB is configured.

By default, the timeout multiplier of PSB and RSB is 3.

Step 5 Run:

mpls rsvp-te blockade-multiplier *number*

The timeout multiplier of blockade state is set.

By default, the timeout multiplier of blockade state is 4.

----End

3.6.4 Configuring RSVP Refresh Mechanism

Enabling Srefresh on the interface that connects two neighboring devices can reduce the cost and improve the performance. After Srefresh is enabled, the retransmission of Srefresh messages is automatically enabled on the interface.

Context

Enabling Srefresh in the interface view or the mpls view on two nodes that are the neighbors of each other can reduce the cost and improve the performance of a network. In the interface view, Srefresh can be enabled only on this interface; in the MPLS view, Srefresh can be enabled on the entire device. After Srefresh is enabled, the retransmission of Srefresh messages is automatically enabled on the interface or the device.

Assume that a node initializes the retransmission interval as *Rf* seconds. If receiving no ACK message within *Rf* seconds, the node retransmits the RSVP message after (1 + *Delta*) x *Rf* seconds. The value of *Delta* depends on the link rate. The node retransmits the message until it receives an ACK message or the times of retransmission reach the threshold (that is, retransmission increment value).

Procedure

Step 1 Run:

system-view

Copyright © Huawei Technologies Co., Ltd.

The system view is displayed.

Step 2 Run one of the following commands to enter the interface view or the MPLS view.

- To enter the interface view of the MPLS TE tunnel, run:

  interface *interface-type interface-number*

  The Srefresh mechanism that is configured in the interface view takes effect only on the current interface.

- To enter the MPLS view, run:

  mpls

  The Srefresh mechanism that is configured in the MPLS view takes effect globally. The Srefresh mechanism in MPLS view is applied to the TE FRR networking. By doing this, both the usage of network resources and the reliability of the Srefresh mechanism can be improved.

Step 3 Run:

mpls rsvp-te srefresh

Srefresh is enabled.

By default, Srefresh is disabled on the interface.

Step 4 (Optional) Run:

mpls rsvp-te timer retransmission { **increment-value** *increment* | **retransmit-value** *interval* } *

The retransmission parameters are set.

By default, *increment* is set to 1, and *interval* is set to 500 milliseconds.

----End

3.6.5 Enabling Reservation Confirmation Mechanism

Receiving an ResvConf message does not mean that the resource reservation succeeds. It means that resources are reserved successfully only on the farthest upstream node where this Resv message arrives. These resources, however, may be preempted by other applications later.

Context

Do as follows on the egress of the TE tunnel:

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

The reservation confirmation mechanism is enabled.

Copyright © Huawei Technologies Co., Ltd.

The reservation confirmation is initiated by the receiver of Path message. An object that requires confirming the reservation is carried along the Resv message sent by the receiver.

NOTE

Receiving ResvConf messages does not mean that the resource reservation succeeds. 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.

----End

3.6.6 Checking the Configuration

After adjusting RSVP signaling parameters, you can view the refresh parameters, the status of RSVP reservation confirmation and RSVP Hello extension, and the RSVP status timer configuration.

Procedure

- Run the **display mpls rsvp-te** [**interface** [*interface-type interface-number*]] command to check related information about RSVP-TE.
- Run the **display mpls rsvp-te psb-content** [*ingress-lsr-id tunnel-id lsp-id*] command to check information about RSVP-TE PSB.
- Run the **display mpls rsvp-te rsb-content** [*ingress-lsr-id tunnel-id lsp-id*] command to check information about RSVP-TE RSB.
- Run the **display mpls rsvp-te statistics** { **global** | **interface** [*interface-type interface-number*] } command to check RSVP-TE statistics.

----End

Example

If the configurations succeed, run the preceding commands and you can view the following information:

- Refresh parameters of the interface
- Confirmation of the resource reservation, the state of the Hello extension, and the configurations of RSVP-TE status timers.

3.7 Configuring RSVP Authentication

RSVP authentication prevents unauthorized nodes from setting up RSVP neighbor relationships with the local node and prevents spoofing of forged packets.

3.7.1 Establishing the Configuration Task

Before configuring RSVP authentication, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

RSVP key authentication prevents an unauthorized node from setting up RSVP neighbor relationships with the local node or generating forged packets to attack the local node.

Copyright © Huawei Technologies Co., Ltd.

RSVP key authentication prevents the following unauthorized means of setting up RSVP neighbor relationships, protecting the local node from attacks (such as malicious reservation of high bandwidth):

- An unauthorized node attempts to set up a neighbor relationship with the local node.
- A remote node generates and sends forged RSVP messages to set up a neighbor relationship with the local node.

The message window function and the handshake function, together with RSVP key authentication, prevent anti-replay attacks or authentication interruption between RSVP neighbors resulted from RSVP message mis-sequence during network congestion.

The RSVP authentication lifetime is configured, preventing unceasing RSVP authentication. In the situation where no CR-LSP exists between RSVP neighbors, the neighbor relationship is kept Up until the RSVP authentication lifetime expires.

Pre-configuration Tasks

Before configuring RSVP authentication, complete the following task:

- **Configuring an RSVP-TE Tunnel**

Data Preparation

To configure RSVP authentication, you need the following data.

No.	Data
1	RSVP authentication key
2	(Optional) Local password used in handshake authentication
3	(Optional) RSVP message window size (being 1 by default)

3.7.2 Configuring RSVP Key Authentication

RSVP key authentication is performed on interfaces of two RSVP neighbors. The keys configured on the interfaces of the RSVP neighbors must be the same; otherwise, RSVP authentication fails and the received RSVP packets are discarded.

Context

RSVP authentication uses authentication objects in RSVP messages to authenticate the RSVP messages, preventing malicious attacks initiated by the modified or forged RSVP messages and improving the network reliability and security.

The RSVP key authentication is configured either in the interface view or the MPLS RSVP-TE neighbor view:

- In the interface view, RSVP key authentication configured is performed between directly-connected nodes.
- In the MPLS RSVP-TE neighbor view, the RSVP key authentication is performed between neighboring nodes, which is recommended.

Copyright © Huawei Technologies Co., Ltd.

HMAC-MD5 or keychain authentication is enabled by configuring one of the following optional parameters:

- **cipher**: configures HMAC-MD5 authentication with keys displayed in cipher text.
- **plain**: configures HMAC-MD5 authentication with keys displayed in plaintext.
- **keychain**: configures keychain authentication by using a globally configured keychain.

NOTE

Characters $@$@ are used as the prefix and suffix of passwords with variable lengths, and they cannot be both configured at the beginning and end of a plain text password.

Procedure

- Configure RSVP key authentication in the interface view.

  Do as follows on each interface between two directly-connected nodes:

  NOTE

  The configurations must be complete on either of the two directly-connected interfaces within a period of time three times the interval at which a Path Refresh message is sent; otherwise, the RSVP session goes Down.

  1. Run:
     system-view

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

     The view of the MPLS TE link interface is displayed.
  3. Run:
     mpls rsvp-te authentication { **cipher** | **plain** } *auth-key*

     The authentication key is configured.

     RSVP key authentication configured in the interface view takes effect only on the current interface and has the lowest preference.
- Configure RSVP key authentication in the MPLS RSVP-TE neighbor view.

  Do as follows on each neighboring node:

  NOTE

  The configurations must be complete on either of the two directly-connected interfaces within a period of time three times the interval at which a Path Refresh message is sent; otherwise, the RSVP session goes Down.

  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     mpls rsvp-te peer *ip-address*

     The MPLS RSVP-TE neighbor view is displayed.

     - When *ip-address* is specified as an interface address but not the LSR ID of the RSVP neighbor, key authentication is based on this neighbor's interface address. This means that RSVP key authentication takes effect only on the specified

Copyright © Huawei Technologies Co., Ltd.

interface of the neighbor, providing high security. In this case, RSVP key authentication has the highest preference.

- When *ip-address* is specified as an address equal to the LSR ID of the RSVP neighbor, key authentication is based on the neighbor's LSR ID. This means that RSVP key authentication takes effect on all interfaces of the neighbor. In this case, this RSVP key authentication has the higher preference than that configured in the interface view, but has the lower preference than that configured based on the neighbor interface address.

3. Run:

   mpls rsvp-te authentication { **cipher** | **plain** } *auth-key*

   The authentication key is configured.

----End

3.7.3 (Optional) Configuring the RSVP Authentication Lifetime

By setting the RSVP authentication lifetime, you enable a device to retain an RSVP neighbor relationship for a specified period of time though no CR-LSP exists between the RSVP neighbors.

Context

RSVP neighbors to remain the neighbor relationship when no CR-LSP exists between them until the RSVP authentication lifetime expires. Configuring the RSVP authentication time does not affect the existing CR-LSPs.

Do as follows on each node along the tunnel:

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Run either of the following commands to enter the interface view or the MPLS RSVP-TE neighbor view:

- To enter the interface view of an MPLS TE tunnel, run:

  interface *interface-type interface-number*

  The RSVP authentication lifetime that is configured in the interface view takes effect only on the current interface.

- To enter the MPLS RSVP-TE neighbor view, run:

  mpls rsvp-te peer *ip-address*

  - If *ip-address* is specified as an interface address but not the LSR ID of the RSVP neighbor, the RSVP authentication lifetime takes effect only on the interface.
  - If *ip-address* is specified as an address equal to the LSR ID, the RSVP authentication lifetime takes effect on the entire device.

Step 3 Run:

mpls rsvp-te authentication lifetime *lifetime*

The RSVP authentication lifetime is set.

Copyright © Huawei Technologies Co., Ltd.

lifetime is in the format of HH:MM:SS. The value ranges from 00:00:01 to 23:59:59. By default, the time is 00:30:00, that is, 30 minutes.

----End

3.7.4 (Optional) Configuring the Handshake Function

RSVP key authentication is the prerequisite for configuring the RSVP handshake function.

Context

Do as follows on each node along a tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run either of the following commands to enter the interface view or the MPLS RSVP-TE neighbor view:

- To enter the interface view of the MPLS TE tunnel, run:

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

  The handshake function that is configured in the interface view takes effect only on the current interface.

- To enter the MPLS RSVP-TE neighbor view, run:

  ```
  mpls rsvp-te peer ip-address
  ```

  - When *ip-address* is specified as an interface address but not the LSR ID of the RSVP neighbor, the handshake function is configured based on the neighbor interface address. In this case, the handshake function takes effect only on the interface.
  - When *ip-address* is specified as an address equal to the LSR ID of the neighbor, the handshake function is configured based on the neighbor LSR ID. In this case, the handshake function takes effect on the entire device.

Step 3 Run:

```
mpls rsvp-te authentication handshake local-secret
```

The handshake function is configured.

As *local-secret* is meaningful only on the local side, different values of *local-secret* can be set on a device and its neighbor.

The handshake function helps a device to establish an RSVP neighbor relationship with its neighbor. If a device receives RSVP messages from a neighbor, with which the device has not established an RSVP authentication relationship, the device will send Challenge messages carrying *local-secret* to this neighbor. After receiving the Challenge messages, the neighbor returns Response messages carrying *local-secret* the same as that in the Challenge messages. After receiving the Response messages, the local end checks *local-secret* carried in the Response messages. If *local-secret* in the Response messages is the same as the local set configured *local-secret*, the device determines to establish an RSVP authentication relationship with its neighbor.

Copyright © Huawei Technologies Co., Ltd.

NOTE

If you run the **mpls rsvp-te authentication lifetime** command after configuring the handshake function, note that the RSVP authentication lifetime must be greater than the interval for sending RSVP refresh messages.

If the RSVP authentication lifetime is smaller than the interval for sending RSVP refresh messages, the RSVP authentication relationship may be deleted because no RSVP refresh message is received within the RSVP authentication lifetime. In such a case, after the next RSVP refresh message is received, the handshake operation is triggered. Repeated handshake operations may cause RSVP tunnels unable to be set up or cause RSVP tunnels to be deleted.

----End

3.7.5 (Optional) Configuring the Message Window Function

The message window function is configured to prevent mis-sequence of RSVP messages.

Context

The default window size is 1, which means that a device saves only the largest sequence number of the RSVP message from neighbors.

When **window-size** is larger than 1, it means that a device accepts several valid sequence numbers.

Do as follows on each node along a tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run either of the following commands to enter the interface view or the MPLS RSVP-TE neighbor view:

- To enter the interface view of the MPLS TE tunnel, run:

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

  The message window function that is configured in the interface view takes effect only on the current interface.

- To enter the MPLS RSVP-TE neighbor view, run:

  ```
  mpls rsvp-te peer ip-address
  ```

  - When *ip-address* is specified as an interface address but not the LSR ID of an RSVP neighbor, the message window function is configured based on the neighbor interface address. In this case, the handshake function takes effect only on the interface.
  - When *ip-address* is specified as an address equal to the LSR ID of the RSVP neighbor, the message window function is configured based on the neighbor LSR ID. In this case, the message window function takes effect on the entire device.

Step 3 Run:

```
mpls rsvp-te authentication window-size window-size
```

The message window function is configured.

window-size is the number of valid sequence numbers carried in RSVP messages that a device can save.

Copyright © Huawei Technologies Co., Ltd.

RSVP Authentication must be configured before the message window function is configured.

NOTE

If RSVP is enabled on an Eth-Trunk interface or an IP-Trunk interface, only one neighbor relationship is established on the trunk link between RSVP neighbors. Therefore, any member interface of the trunk interface receives RSVP messages in a random order, resulting in RSVP message mis-sequence. Configuring RSVP message window size prevents RSVP message mis-sequence.

The window size larger than 32 is recommended. If the window size is set too small, the RSVP packets are discarded because the sequence number is beyond the range of the window size, causing an RSVP neighbor relationship to be terminated.

----End

3.7.6 Checking the Configuration

After the configuration of RSVP key authentication, you can view information about RSVP-TE of a physical outgoing interface.

Prerequisite

The configurations of RSVP key authentication are complete.

Procedure

Step 1 Run the **display mpls rsvp-te peer** [**interface** *interface-type interface-number*] command to view information about the RSVP neighbor on an RSVP-TE-enabled interface.

----End

Example

After the configurations are successful, run the **display mpls rsvp-te peer** command on an interface, and you can view that the number of RSBs in the RSVP-TE neighbor information is not zero.

3.8 Adjusting the Path of CR-LSP

You can adjust and configure the method of calculating CR-LSPs.

3.8.1 Establishing the Configuration Task

Before adjusting the path calculation method of CR-LSPs, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

CSPF uses the TEDB and constraints to calculate appropriate paths and establishes CR-LSPs through the signaling protocol. MPLS TE provides many methods to affect CSPF computation to adjust the CR-LSP path, including the following modes:

- Tie-breaking

  CSPF calculates only a shortest path to reach the tunnel destination. During the path computation, if there are several paths with the same metric, the device select one of them.

Copyright © Huawei Technologies Co., Ltd.

Tie-breaking methods for selecting the path are as follows:

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

NOTE

Tie-breaking selects the link based on bandwidth ratio. If the ratios are the same, such as no reservable bandwidth or the equal bandwidth is used, the link that is found firstly is selected, even if **least-fill** or **most-fill** is configured.

- Route pinning

  A successfully-established CR-LSP does not vary with the route change. This is called route pinning.

- Administrative group and affinity property

  The affinity property of the MPLS TE tunnel determines the links used by the tunnel. The affinity property cooperates with link administrative group to determine which links the tunnel uses.

- SRLG

  A shared risk link group (SRLG) is a set of links which are likely to fail concurrently due to sharing a physical resource. Links in the group have a shared risk. That is, if one of the links fails, other links in the group may fail too.

  In MPLS TE, SRLG is a feature that enhances the path reliability for hot-standby tunnel or the TE FRR tunnel. The two or more links can have a common risk when they share common physical resource. For example, the sub-interfaces share the risk with their main interface since the sub-interface definitely goes down when its main interface goes down. If the backup or bypass tunnel goes through a link which shares a same risk with the primary tunnel, the probability of backup tunnel going down along with the primary tunnel is high.

- Hop limit

  Hop limit is a rule for path selection for setting up a CR-LSP. It limits the number of hops that a CR-LSP allows.

- Re-optimization

  Dynamically optimizing a CR-LSP is to periodically recompute routes for the CR-LSP. If the route in recomputation is better than the route in use, then a new CR-LSP is established according to the recomputed route. Meanwhile, services are switched from the old CR-LSP to the new CR-LSP, and the old one is deleted.

Pre-configuration Tasks

The configuration tasks described in this section are some special configurations for CSPF in MPLS TE. Before performing these configuration tasks, you need to know their influences on the system.

Before adjusting the selection of the CR-LSP, complete the following task:

- **Configuring RSVP-TE Tunnel**

Copyright © Huawei Technologies Co., Ltd.

Data Preparation

To adjust the selection of the CR-LSP, you need the following data.

No.	Data
1	Tie-breaking policy for the node and the tunnel
2	Administrative group of links and affinity property of tunnels
3	Re-optimization interval of CR-LSP
4	SRLG number, SRLG path calculation mode (preferred or strict)

3.8.2 Configuring Administrative Group and Affinity Property

The configuration of the administrative group affects only LSPs to be set up; the configuration of the affinity property affects established LSPs by recalculating the paths.

Context

Do as follows on the ingress of the CR-LSP tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

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

The interface view of the MPLS-TE-enabled interface is displayed.

Step 3 Run:

```
mpls te link administrative group value
```

The administrative group of the MPLS TE link is configured.

Step 4 Run:

```
quit
```

Return to the system view.

Step 5 Run:

```
interface tunnel tunnel-number
```

The tunnel interface view of the MPLS TE tunnel is displayed.

Step 6 Run:

```
mpls te affinity property properties [ mask mask-value ] [ best-effort | secondary ]
```

The affinity for the tunnel is configured.

Copyright © Huawei Technologies Co., Ltd.

By default, the values of administrative group, affinity property, and mask are all 0x0.

Step 7 Run:

```
mpls te commit
```

The current tunnel configuration is committed.

----End

Follow-up Procedure

The modification of administrative group takes effect only on LSPs that are established after modification.

After the modified affinity property is committed, the established LSP in this tunnel may be affected and the system recalculates the path for the TE tunnel.

3.8.3 Configuring SRLG

In the networking scenario where the hot standby CR-LSP is set up or TE FRR is enabled, you need to configure the SRLG attribute on the outgoing tunnel interface of the ingress and the other member links of the SRLG to which the outgoing interface belongs.

Context

Configuring SRLG includes:

- **Configuring SRLG for the link**
- **Configuring SRLG path calculation mode for the tunnel**

Procedure

- Configuring SRLG for the link

  Do as follows on the links which are in the same SRLG.

  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 srlg srlg-number
     ```
     The interface is configured as an SRLG member.

     In application scenario of the hot-standby tunnel or the TE FRR tunnel, you just need to configure SRLG on the out interface of the ingress node and on anyone out interface of the links which are in the same SRLG as the protected interface(s).

- Configuring SRLG path calculation mode for the tunnel

  Do as follows on the ingress node of the hot-standby tunnel or the TE FRR tunnel.

Copyright © Huawei Technologies Co., Ltd.

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 you specify the **strict** keyword, the CSPF always considers the SRLG as a constraint when calculating the path for the backup CR-LSP or the hot-standby CR-LSP.
   - If you specify the **preferred** keyword, CSPF tries to calculate the path which avoids the links in the same SRLG as the protected interface(s); if the calculation fails, CSPF does not consider the SRLG as a constraint anymore.

----End

3.8.4 Configuring CR-LSP Hop Limit

Similar to the administrative group and the affinity property, the hop limit is a condition for CR-LSP path selection and is used to specify the number of hops along a CR-LSP to be set up.

Context

Do as follows on the ingress of the CR-LSP:

Procedure

Step 1 Run:
system-view

The system view is displayed.

Step 2 Run:
interface tunnel *tunnel-number*

The tunnel interface view of the MPLS TE tunnel is displayed.

Step 3 Run:
mpls te hop-limit *hop-limit-value* [**best-effort** | **secondary**]

The number of hops along the CR-LSP is set.

Step 4 Run:
mpls te commit

The current tunnel configuration is committed.

----End

3.8.5 Configuring Metrics for Path Calculation

You can configure the metric type that is used for setting up a tunnel.

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Specifying the metric type used by the tunnel

  Do as follows on the ingress along a CR-LSP tunnel:

  1. Run:
     system-view

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

     The tunnel interface view is displayed.
  3. Run:
     mpls te path metric-type { **igp** | **te** }

     The metric type for path computation is configured.
  4. Run:
     mpls te commit

     The current configuration of the tunnel is committed.
  5. Run:
     quit

     Return to the system view.
  6. (Optional) Run:
     mpls

     The MPLS view is displayed.
  7. (Optional) Run:
     mpls te path metric-type { **igp** | **te** }

     The path metric type used by the tunnel during route selection is specified.

     If the **mpls te path metric-type** command is not run in the tunnel interface view, the metric type in the MPLS view is adopted; otherwise, the metric type in the tunnel interface view is used.

     By default, path metric type used by the tunnel during route selection is TE.

- (Optional) Configuring the TE metric value of the path

  If the metric type of a specified tunnel is TE, you can modify the TE metric value of the path on the outgoing interface of the ingress and the transit node through the following configurations:

  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:

Copyright © Huawei Technologies Co., Ltd.

mpls te metric *value*

The TE metric value of the path is configured.

By default, the path uses the IGP metric value as the TE metric value.

----End

3.8.6 Configuring Tie-Breaking of CSPF

You can configure the CSPF tie-breaking function to select a path from multiple paths with the same weight value.

Context

Do as follows on the ingress of the CR-LSP tunnel:

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 tie-breaking { **least-fill** | **most-fill** | **random** }

CR-LSP tie-breaking policy for the LSR is configured.

The default tie-breaking policy is random.

Step 4 Run:
quit

Return to the system view.

Step 5 Run:
interface tunnel *tunnel-number*

The tunnel interface view of the MPLS TE tunnel is displayed.

Step 6 Run:
mpls te tie-breaking { **least-fill** | **most-fill** | **random** }

The CR-LSP tie-breaking policy for current tunnel is configured.

Step 7 Run:
mpls te commit

The current tunnel configuration is committed.

The tunnel preferentially takes the tie-breaking policy configured in its tunnel interface view. If the tie-breaking policy is not configured in the tunnel interface view, the configuration in the MPLS view is adopted.

----End

Copyright © Huawei Technologies Co., Ltd.

3.8.7 Configuring Failed Link Timer

By configuring a failed-link timer, you can prevent a failed link from repeatedly participating in the CSPF calculation.

Context

CSPF uses a locally-maintained traffic-engineering database (TEDB) to calculate the shortest path to the destination address. Then, the signaling protocol applies for and reserves resources for the path. In the case of a link on a network is faulty, if the routing protocol fails to notify CSPF of updating the TEDB in time, this may cause the path calculated by CSPF to contain the faulty link.

As a result, the control packets, such as RSVP Path messages, of a signaling protocol are discarded on the faulty link. Then, the signaling protocol returns an error message to the upstream node. Receiving the link error message on the upstream node triggers CSPF to recalculate a path. The path recalculated by CSPF and returned to the signaling protocol still contains the faulty link because the TEDB is not updated. The control packets of the signaling protocol are still discarded and the signaling protocol returns an error message to trigger CSPF to recalculate a path. The procedure repeats until the TEDB is updated.

To avoid the preceding situation, when the signaling protocol returns an error message to notify CSPF of a link failure, CSPF sets the status of the faulty link to INACTIVE and enables a failed link timer. Then, CSPF does not use the faulty link in path calculation until CSPF receives a TEDB update event or the failed link timer expires.

Before the failed link timer expires, if a TEDB update event is received, CSPF deletes the failed link timer.

Do as follows on the ingress along a CR-LSP tunnel:

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 timer failed-link interval
```

The failed link timer is configured.

By default, the failed link timer is set to 10 seconds.

The failed link timer is a local configuration. If the failed link timers of nodes are set to different values, a failed link that is in ACTIVE state on one node may be in INACTIVE state on other nodes.

----End

Copyright © Huawei Technologies Co., Ltd.

3.8.8 Configuring Loop Detection

By configuring the loop detection function, you can prevent loops.

Context

In the loop detection mechanism, a maximum number of 32 hops are allowed on an LSP. If information about the local LSR is recorded in the path information table, or the number of hops on the path exceeds 32, this indicates that a loop occurs and the LSP fails to be set up.

Do as follows on the ingress of the CR-LSP tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The tunnel interface view of the MPLS TE tunnel is displayed.

Step 3 Run:

```
mpls te loop-detection
```

The loop detection on tunnel creation is enabled.

By default, loop detection is disabled.

Step 4 Run:

```
mpls te commit
```

The current tunnel configuration is committed.

----End

3.8.9 Configuring Route Pinning

By configuring the route pinning function, you can use the path that is originally selected, rather than another eligible path, to set up a CR-LSP.

Context

By default, route pinning is disabled.

NOTE

If route pinning is enabled, the MPLS TE re-optimization cannot be used at the same time.

Do as follows on the ingress of the CR-LSP tunnel:

Procedure

Step 1 Run:

```
system-view
```


Copyright © Huawei Technologies Co., Ltd.

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The tunnel interface view of the MPLS TE tunnel is displayed.

Step 3 Run:

```
mpls te record-route [ label ]
```

Route record and label record are enabled.

Step 4 Run:

```
mpls te route-pinning
```

Route pinning is enabled.

Step 5 Run:

```
mpls te commit
```

The current tunnel configuration is committed.

----End

3.8.10 Checking the Configuration

After the adjustment of CR-LSP path selection, you can view the status of the CSPF tie-breaking function, status of the route pinning function, interval for optimizing a CR-LSP, and affinity property and its mask.

Prerequisite

All configurations of adjusting the patch for CR-LSP are complete.

Procedure

Step 1 Run the **display mpls te tunnel-interface** [**tunnel** *tunnel-number*] command to check information about the tunnel interface.

----End

Example

If the configuration is successful, run the preceding command and you can view the following items:

- Tie-breaking policy
- If routing pinning is enabled, the status is displayed as "Enabled"
- If re-optimization is enabled, the status is displayed as "Enabled" and the interval is also displayed
- Affinity property and its mask

3.9 Adjusting the Establishment of MPLS TE Tunnels

By configuring multiple attributes of an MPLS TE tunnel, you can adjust the parameters during the establishment of the MPLS TE tunnel.

Copyright © Huawei Technologies Co., Ltd.

3.9.1 Establishing the Configuration Task

Before adjusting the establishment of an MPLS TE tunnel, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

During the establishment of an MPLS TE tunnel, specific configurations are required in the practical application. This section describes the special configuration.

Pre-configuration Tasks

Note that tasks introduced in this section are of special configuration in MPLS TE. Before performing these configuration tasks, you must know their influences on the system.

Before adjusting the establishment of the MPLS TE tunnel, complete the following task:

- **Configuring RSVP-TE Tunnel**

Data Preparation

To adjust the establishment of the MPLS TE tunnel, you need the following data.

No.	Data
1	Number of attempts to reestablish a tunnel and the reestablishment interval
2	Setup priority and holding priority of tunnels

3.9.2 Configuring the Tunnel Priority

In the process of establishing a CR-LSP, if no path with the required bandwidth exists, you can perform bandwidth preemption according to setup priorities and holding priorities.

Context

Do as follows on the ingress of the CR-LSP tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The tunnel interface view of the MPLS TE tunnel is displayed.

Step 3 Run:

Copyright © Huawei Technologies Co., Ltd.

mpls te priority *setup-priority* [*hold-priority*]

The priority for the tunnel is configured.

Both the setup priority and the holding priority range from 0 to 7. The smaller the value is, the higher the priority is.

By default, both the setup priority and the holding priority are 7. When only the setup priority is to be configured, ensure that the setup priority must be identical with the holding priority.

NOTE

The value of the setup priority must not be less than that of the holding priority. That is, the setup priority should not be higher than the holding priority.

Step 4 Run:

mpls te commit

The current tunnel configuration is committed.

----End

3.9.3 Configuring Re-optimization for CR-LSP

By configuring the tunnel re-optimization function, you can periodically recompute routes for a CR-LSP. If the recomputed routes are better than the routes in use, a new CR-LSP is then established according to the recomputed routes. In addition, services are switched to the new CR-LSP, and the previous CR-LSP is deleted.

Context

NOTE

- If the re-optimization is enabled, the route pinning cannot be used at the same time.
- The CR-LSP re-optimization cannot be configured when the resource reservation style is FF.

Do as follows on the ingress of the CR-LSP tunnel:

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Run:

interface tunnel *tunnel-number*

The tunnel interface view of the MPLS TE tunnel is displayed.

Step 3 Run:

mpls te reoptimization [**frequency** *interval*]

Periodic re-optimization is enabled.

By default, re-optimization is disabled. The default periodic re-optimization interval is 3600 seconds.

Step 4 Run:

mpls te commit

Copyright © Huawei Technologies Co., Ltd.

The current tunnel configuration is committed.

Step 5 Run:

```
return
```

Back to the user view.

Step 6 (Optional) Run:

```
mpls te reoptimization
```

The TE tunnel is re-optimized immediately.

After configuring the timing re-optimization in the tunnel view, return to the user view and run the **mpls te reoptimization** command to re-optimize the optimized tunnels immediately. Once the re-optimization is performed, the timing re-optimization timer is reset and count time again.

----End

3.9.4 Configuring Tunnel Reestablishment Parameters

By configuring the tunnel reestablishment function, you can periodically recompute the route for a CR-LSP. If the route in recomputation is better than the route in use, a new CR-LSP is then established according to the recomputed route. In addition, services are switched to the new CR-LSP, and the previous CR-LSP is deleted.

Context

Do as follows on the ingress of the CR-LSP tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The tunnel interface view of the MPLS TE tunnel is displayed.

Step 3 Run:

```
mpls te retry times
```

The number of attempts to re-establish a tunnel is specified.

By default, the creation retry times is 5.

Step 4 Run:

```
mpls te timer retry interval
```

The interval for re-establishing a tunnel is specified.

By default, the interval for re-establishing a tunnel is 30 seconds.

Step 5 Run:

```
mpls te commit
```

The current tunnel configuration is committed.

Copyright © Huawei Technologies Co., Ltd.

If the establishment of a tunnel fails, the system attempts to reestablish the tunnel within the set interval and the maximum number of attempts is the set reestablishment times.

----End

3.9.5 Configuring Route Record and Label Record

By configuring route record and label record, you can determine whether to record routes and labels during the establishment of an RSVP-TE tunnel.

Context

By default, routes and labels are not recorded.

Do as follows on the ingress of the CR-LSP tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The tunnel interface view of the MPLS TE tunnel is displayed.

Step 3 Run:

```
mpls te record-route [ label ]
```

The route and label are recorded when establishing the tunnel.

Step 4 Run:

```
mpls te commit
```

The current tunnel configuration is committed.

----End

3.9.6 Configuring the RSVP Signaling Delay-Trigger Function

In the case that a fault occurs on an MPLS network, a great number of RSVP CR-LSPs need to be reestablished. This causes consumption of a large number of system resources. By configuring the delay for triggering the RSVP signaling, you can reduce the consumption of system resources when establishing an RSVP CR-LSP.

Context

When there are numerous RSVP CR-LSPs to be reestablished on the MPLS network, it may take up many system resources. In this case, if the RSVP signaling delay-trigger function is configured, the system resources can be efficiently used.

Do as follows on each node on which multiple RSVP CR-LSPs need to be reestablished:

Copyright © Huawei Technologies Co., Ltd.

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 signaling-delay-trigger enable
```

The RSVP signaling delay-trigger function is enabled.

By default, the RSVP signaling delay-trigger function is not enabled.

----End

3.9.7 Checking the Configuration

After adjusting the establishment of an MPLS TE tunnel, you can view the TE tunnel attributes.

Prerequisite

All configurations of adjusting the establishment of an MPLS TE tunnel are complete.

Procedure

Step 1 Run the **display mpls te tunnel-interface** [**tunnel** *tunnel-number*] command to view information about the tunnel interface.

----End

Example

If the configurations are successful, run the preceding commands, and you can view the following items:

- The route record and label record of the tunnel are enabled.
- The times and interval of tunnel reestablishment attempts are displayed.
- The tunnel setup priority and holding priority are displayed.

3.10 Adjusting the Traffic Forwarding of an MPLS TE Tunnel

By adjusting the forwarding of MPLS TE traffic, you can modify the path along which IP traffic or MPLS traffic is transmitted, or limit the types of traffic that can be transmitted along a TE tunnel.

Copyright © Huawei Technologies Co., Ltd.

3.10.1 Establishing the Configuration Task

Before adjusting the forwarding of MPLS TE traffic, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

In MPLS TE, traffic forwarding is affected by the configurations that changes the path through which IP traffic or MPLS traffic passes or the configuration that can limit traffic types of the TE tunnel.

This section describes several measures to adjust traffic forwarding in MPLS TE.

Pre-configuration Tasks

The configuration described in this section should be used together with CSPF and the dynamic signaling protocol (such as RSVP-TE).

Before adjusting the traffic forwarding, complete the following task:

- **Configuring RSVP-TE Tunnel**

Data Preparation

To adjust the traffic forwarding, you need the following data.

No.	Data
1	Number for TE tunnel interface
2	TE metric of the MPLS TE link
3	IGP metric of the TE tunnel

3.10.2 Configuring IGP Shortcut

By configuring IGP shortcut, you can prevent a route to an LSP from being advertised to neighbors. In this manner, other nodes cannot use this LSP.

Context

NOTE

The IGP shortcut and the Forwarding Adjacency cannot be used together.

Do as follows on the ingress along a CR-LSP tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Run:

```
interface tunnel tunnel-number
```

The interface view of the MPLS TE tunnel is displayed.

Step 3 Run:

```
mpls te igp shortcut [ isis | ospf ]
```

The IGP shortcut is configured.

NOTE

By default, the IGP shortcut is not configured.

If the IGP type is not specified when the IGP shortcut is configured, both IS-IS and OSPF are supported by default.

Step 4 Run:

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

The IGP metric value for the tunnel is configured.

By default, the metric value used by the TE tunnel is the same as that of the IGP.

IS-IS does not support the relative metric.

You can specify a metric value used by the TE tunnel when path is calculated in the IGP shortcut feature.

- If the **absolute** metric is used, the TE tunnel is equal to the configured metric value.
- If the **relative** metric is used, the TE tunnel is equal to the sum of the metric value of the corresponding IGP path and relative metric value.

Step 5 Run:

```
mpls te commit
```

The current TE tunnel configuration is committed.

Step 6 For IS-IS, run:

```
isis enable [ process-id ]
```

IS-IS is enabled on the tunnel interface.

Step 7 For OSPF, run the following commands in sequence.

- Run the **quit** command to return to the system view.
- Run the **ospf** [*process-id*] command to enter the OSPF view.
- Run the **enable traffic-adjustment** command to configure OSPF IGP shortcut.

----End

3.10.3 Configuring Forwarding Adjacency

By configuring the forwarding adjacency, you can advertise a route of an LSP to neighbors. In this manner, other nodes can use this LSP.

Context

The routing protocol performs bidirectional detection on a link. When using the forwarding adjacency to advertise LSP links to other nodes, configure another tunnel for transferring data packets in the reverse direction. Then, enable the forwarding adjacency on these two tunnels.

Copyright © Huawei Technologies Co., Ltd.

NOTE

By default, the forwarding adjacency is disabled.

If the Forwarding Adjacency is used, then the IGP shortcut cannot be used at the same time.

Do as follows on the ingress along a CR-LSP tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The tunnel interface view is displayed.

Step 3 Run:

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

The forwarding adjacency is enabled.

Step 4 Run:

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

The IGP metric value for the tunnel is configured.

NOTE

IS-IS does not support relative metric.

The IGP metric value should be set properly to ensure that the LSP is advertised and used correctly. For example, the metric of a TE tunnel should be less than that of IGP routes to ensure that the TE tunnel is used as a route link.

Step 5 Run:

```
mpls te commit
```

The current tunnel configuration is committed.

Step 6 For IS-IS, run:

```
isis enable [ process-id ]
```

The IS-IS process on the tunnel interface is enabled.

Step 7 For OSPF, run one of the following commands.

- Run the **quit** command to return to the system view.
- Run the **ospf** [*process-id*] command to enter the OSPF view.
- Run the **enable traffic-adjustment advertise** command to enable the forwarding adjacency.

----End

3.10.4 Configuring Switching Delay and Deletion Delay

To ensure that the original CR-LSP can be deleted only after a new CR-LSP is set up, you need to configure the switching delay and the deletion delay, which avoids traffic interruption.

Copyright © Huawei Technologies Co., Ltd.

Context

MPLS TE adopts a make-before-break mechanism. When attributes of an MPLS TE tunnel such as bandwidth and path change, a new CR-LSP with new attributes, also called Modified LSP, must be established. To prevent data loss during traffic switching, the new CR-LSP must be established before the original CR-LSP is torn down. Through the make-before-break mechanism, the system does not need to calculate the bandwidth to be reserved for the new CR-LSP. That is, the new CR-LSP shares the bandwidth with the original CR-LSP.

In practical applications, if the upstream nodes are not as busy as the downstream nodes, the original CR-LSP may be deleted in advance, causing temporary traffic interruption.

To avoid this problem, you can configure the switch delay and deletion delay on the ingress of the tunnel.

Do as follows on the ingress:

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 delete-time
```

The switching delay and deletion delay are configured.

By default, the switching delay is 5 seconds and the deletion delay is 7 seconds.

----End

3.11 Configuring MPLS TE FRR

MPLS TE FRR is a local protection technique and is used to protect a CR-LSP against link faults and node faults. MPLS TE FRR needs to be configured manually.

3.11.1 Establishing the Configuration Task

Before configuring MPLS TE FRR, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

MPLS TE Fast ReRoute (FRR) is a local protection technique.

NOTE

The RSVP-TE tunnel of SE style supports FRR; the static TE tunnel does not support FRR.

Copyright © Huawei Technologies Co., Ltd.

Additional bandwidth is occupied because the bypass tunnel used by the FRR needs to be pre-established. When idle network bandwidth is insufficient, the FRR should be used only for important nodes or links.

- Supporting board hot pulling-out protection

  When the interface board where an outgoing interface of a primary tunnel on a PLR resides is pulled out, the MPLS TE traffic is swiftly switched to the bypass tunnel. When the interface board is re-inserted and the outgoing interface of the primary tunnel is available, MPLS TE traffic is switched back to the primary tunnel. The TE FRR with board hot pulling-out protection is used to protect the outgoing interface of the primary tunnel on a PLR.

  When board hot pulling-out protection is used, note that the tunnel interface of the primary tunnel on a PLR, the tunnel interface of the bypass tunnel, and the outgoing interface of the bypass tunnel must not reside on the interface board to be pulled out. It is recommended to configure the TE tunnel interfaces of a PLR on the main control board.

  NOTE

  When the interface where the LSP or CR-LSP resides is deleted, or when the board where the interface resides is pulled out, the interface goes to the Stale state and becomes a staled interface. If the number of staled interfaces on a node reaches the maximum specified in the license, the node cannot provide FRR protection for the primary tunnel in the following cases:

  - The **undo mpls** command is run on the outgoing interface of the primary tunnel.
  - The interface board where the outgoing interface of the primary tunnel resides is pulled out or the interface board fails.

- Supporting FRR during RSVP GR

  In the S9300, the FRR can be performed to reduce the fault duration when the PLR node, PLR upstream node, MP, or MP downstream node is restarted or the switchover is performed; meanwhile, the outgoing interface of the primary tunnel of the PLR fails.

  During the RSVP GR, the Down event of the outgoing interface on the tunnel triggers FRR switchover.

- Not supporting simultaneous failure of multiple nodes

  The FRR does not take effect when multiple nodes fail simultaneously. That is, if the FRR is performed, data is switched from the primary LSP to the bypass LSP. During the period that data is transmitted on the bypass LSP, the bypass LSP must be in the Up state all the time. If the bypass LSP goes Down during this period, the protected data cannot be forwarded through MPLS. Data transmission then is interrupted and the FRR function is invalidated. Although the bypass LSP goes Up again, it cannot forward data. Data can be forwarded only after the primary LSP is restored or re-created.

When configuring a bypass LSP, you must specify the link or node protected by the bypass LSP and ensure that this bypass LSP does not pass through the link or node it protects. Otherwise, the protection does not take effect.

Pre-configuration Tasks

Before configuring MPLS TE fast reroute, complete the following tasks:

- Establishing the primary LSP by using the RSVP-TE signaling protocol
- Enabling MPLS TE and RSVP TE in the MPLS view and physical interface view of the node along the bypass tunnel (See **Enabling MPLS TE and RSVP TE**.)
- Enabling CSPF on the PLR node

Copyright © Huawei Technologies Co., Ltd.

- (Optional) Configuring the explicit path of the bypass tunnel

Data Preparation

To configure TE FRR, you need the following data.

No.	Data
1	Protection policy of FRR, that is, a node or a link that is the object to be protected
2	(Optional) Bandwidth of the bypass tunnel
3	(Optional) Scanning interval of TE FRR

3.11.2 Enabling TE Fast Reroute

Before configuring manual TE FRR, you must enable TE FRR.

Context

By default, the TE FRR is disabled.

Do as follows on the ingress node along the primary LSP:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel interface-number
```

The tunnel interface view of the primary LSP is displayed.

Step 3 Run:

```
mpls te fast-reroute [ bandwidth ]
```

FRR is enabled.

NOTE

The primary tunnel in a tunnel protection group can be configured with the TE FRR for dual protection. On the ingress, the tunnel protection group and TE FRR cannot be configured together. Otherwise, neither the tunnel protection group nor TE FRR takes effect. The protection tunnel in the tunnel protection group, however, cannot be configured with the TE FRR.

For example, assume Tunnel 1/0/0 and Tunnel 2/0/0 are MPLS TE tunnel interfaces and the ID of Tunnel 2/0/0 is 200. The **mpls te protection tunnel** *200* and **mpls te fast-reroute** commands can be run on Tunnel 1/0/0. That is, Tunnel 1/0/0 can be the primary tunnel in the protection group and the TE FRR function. When the **mpls te protection tunnel** *200* command is run on Tunnel 1/0/0, the **mpls te fast-reroute** command cannot be run on Tunnel 2/0/0.

Step 4 Run:

```
mpls te commit
```


Copyright © Huawei Technologies Co., Ltd.

The current tunnel configuration is committed.

----End

3.11.3 Configuring Bypass Tunnels

To configure MPLS TE FRR, you need to configure a path and the attributes for a bypass tunnel.

Context

Do as follows on the PLR node:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel interface-number
```

The interface view of the MPLS TE tunnel is displayed.

Step 3 To configure the IP address for the bypass tunnel interface, run the following commands as required.

- Run:

  ```
  ip address ip-address { mask | mask-length } [ sub ]
  ```

  The IP address of the bypass tunnel interface is configured.

  The secondary IP address of the interface can be configured only after the primary IP address is configured.

- Run:

  ```
  ip address unnumbered interface
  ```

  The bypass tunnel interface borrows an IP address from another interface.

  NOTE

  To forward traffic, the tunnel interface must be configured with an IP address. An MPLS TE tunnel is unidirectional and no peer address exists. Therefore, a tunnel interface needs not to be assigned with an IP address. The tunnel interface borrows the loopback interface address that is used as the LSR ID of the local node.

Step 4 Run:

```
tunnel-protocol mpls te
```

MPLS TE is specified as the tunneling protocol.

Step 5 Run:

```
destination ip-address
```

The destination address of the bypass tunnel is configured as the LSR ID of the MP node.

Step 6 Run:

```
mpls te tunnel-id tunnel-id
```

The ID of the bypass tunnel is configured.

Copyright © Huawei Technologies Co., Ltd.

Step 7 (Optional) Run:

mpls te path explicit-path *path-name*

The explicit path used by the bypass tunnel is configured.

The physical link that the bypass tunnel passes through cannot overlap through which the primary tunnel passes.

Step 8 Run:

mpls te bypass-tunnel

The bypass tunnel are configured.

NOTE

One tunnel interface cannot serve as the bypass tunnel and backup tunnel at the same time, nor as the bypass tunnel and the protect tunnel in a protection group. That is, the **mpls te bypass-tunnel** and **mpls te backup** commands cannot be configured on the same interface, and the **mpls te bypass-tunnel** and **mpls te protection tunnel** commands also cannot be configured on the same interface.

Step 9 Run:

mpls te protected-interface *interface-type interface-number*

The interface to be protected by the bypass tunnel is specified.

NOTE

The **mpls te protected-interface** and **mpls te backup** commands cannot be run on the same tunnel interface at the same time.

Step 10 Run:

mpls te commit

The current tunnel configuration is committed.

----End

Follow-up Procedure

After the bypass tunnel is configured, the route record is enabled.

One bypass tunnel protects up to three physical interfaces. After a tunnel is specified to protect a physical interface, its corresponding LSP becomes the bypass LSP. The establishment of a bypass LSP can be triggered when an explicit path on the PLR is configured.

During the FRR period, if the bypass LSP goes Down, the protected data cannot be forwarded over an MPLS network; thus traffic may be interrupted and the FRR fails. Even after the bypass LSP goes Up again, traffic cannot be forwarded. Traffic can be forwarded only after the primary LSP is restored or re-established.

NOTE

- The **mpls te fast-reroute** command and the **mpls te bypass-tunnel** command cannot be configured on the same interface.
- The **mpls te reoptimization** command and the **mpls te bypass-tunnel** command cannot be configured on the same interface.
- If the FRR switching occurs, the data flow is switched from the primary LSP to the bypass LSP. During the period when the data flow is forwarded through the bypass LSP, the bypass LSP must be in Up state. Otherwise, the FRR fails.

Copyright © Huawei Technologies Co., Ltd.

3.11.4 (Optional) Configuring the Scanning Timer for FRR

By configuring a TE FRR scanning timer, you can search for the eligible LSPs that can function as bypass LSPs and then bind the optimal LSP to the primary LSP.

Context

Do as follows on the PLR node:

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 timer fast-reroute [ weight ]
```

The scanning timer for FRR is configured.

If *weight* is specified, the system can calculate the scanning interval according to the following formula:

Scanning interval = *Weight* x 1000 x 200/Maximum number of RSVP LSPs

If the calculated scanning interval is greater than 1000 milliseconds, it is the actual scanning interval; otherwise, 1000 ms is the scanning interval.

By default, the interval of the scanning timer is 1000 milliseconds.

After configuring FRR, the PLR performs scheduled scanning to search for LSPs that can serve as bypass LSPs and binds the optimal bypass LSP to the primary LSP. After the FRR switching, if the protected LSP is restored or another LSP is established, traffic is switched to the original LSP or the newly-established LSP.

----End

3.11.5 (Optional) Modifying PSB and RSB Timeout Multiplier

To perform TE FRR during the RSVP GR process, you need to modify the timeout multiplier of the PSB or RSB.

Context

Do as follows on each node along the tunnel to support the FRR during the RSVP GR:

Procedure

Step 1 Run:

```
system-view
```


Copyright © Huawei Technologies Co., Ltd.

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Step 3 Run:

```
mpls rsvp-te keep-multiplier number
```

The timeout multiplier of the path state block (PSB) and reserved state block (RSB) is configured.

The timeout multiplier of the PSB and RSB is recommended to be equal to or greater than five to avoid the PSB and RSB loss because of large numbers of RSVP LSPs.

----End

3.11.6 Checking the Configuration

After the configuration of MPLS TE FRR, you can view detailed information about a bypass tunnel.

Prerequisite

The configurations of the MPLS TE 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 LSP.
- 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 LSP or bypass tunnel.
- Run the **display mpls te tunnel-interface** [**tunnel** *tunnel-number*] command to check details about interfaces on the primary tunnel 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 the primary tunnel or bypass tunnel.

----End

3.12 Configuring MPLS TE Auto FRR

MPLS TE Auto FRR is a local protection technique and is used to protect a CR-LSP against link faults and node faults. MPLS TE Auto FRR does not need to be configured manually.

3.12.1 Establishing the Configuration Task

Before configuring MPLS TE Auto FRR, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Applicable Environment

On the network that requires high reliability, the FRR protection is configured to improve the reliability of the network. If the network topology is complex and multiple links need to be

Copyright © Huawei Technologies Co., Ltd.

configured, the configuration procedure is complicated. The Auto FRR can set up a bypass tunnel automatically to meet the requirements to reduce the workload and improve the network reliability.

Similar to the common MPLS TE FRR, MPLS TE Auto FRR also supports board hot pulling-out protection and FRR during RSVP GR. For details, see **Configuring MPLS TE FRR**.

Pre-configuration Tasks

Before configuring the Auto FRR, complete the following tasks:

- Establishing the primary LSP by using the RSVP-TE signaling protocol
- Enabling MPLS, MPLS TE and RSVP TE globally and in the physical interface view of the node along the bypass tunnel (See **Enabling MPLS TE and RSVP TE**.)
- Enabling CSPF on the ingress node and the transit node of the primary tunnel

Data Preparation

To configure the MPLS Auto FRR, you need the following data.

No.	Data
1	Protection policy of the Auto FRR, that is, the link or the node to be protected
2	(Optional) Bandwidth of the bypass tunnel
3	(Optional) Scanning interval of TE FRR

3.12.2 Enabling the TE Auto FRR

Before configuring TE Auto FRR, you must enable TE Auto FRR.

Context

Do as follows on the ingress node of the tunnel:

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
```

The TE Auto FRR is enabled globally.

Copyright © Huawei Technologies Co., Ltd.

Step 4 Run:

```
quit
```

Return to the system view.

Step 5 Run:

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

The interface view of the outgoing interface of the primary tunnel is displayed.

Step 6 (Optional) Run:

```
mpls te auto-frr { link | node | default }
```

The TE Auto FRR is enabled on the outgoing interface on the ingress node of the primary tunnel.

By default, after Auto FRR is enabled globally, all the MPLS TE interfaces are automatically configured with the **mpls te auto-frr default** command. To disable Auto FRR on some interfaces, run the **undo mpls te auto-frr** command on these interfaces. Then, these interfaces no longer have Auto FRR capability even if Auto FRR is enabled or is to be re-enabled globally.

By default, the TE Auto FRR is disabled.

NOTE

- If the **mpls te auto-frr default** command is configured in the interface view, the Auto FRR capability of the interface is consistent with the global Auto FRR capability.
- After the node protection is enabled, if the topology does not meet the requirement to set up an automatic bypass tunnel for node protection, the penultimate hop (but not other hops) on the primary tunnel attempts to set up an automatic bypass tunnel for link protection.

----End

3.12.3 Enabling the TE FRR and Configuring the Auto Bypass Tunnel Attributes

After TE Auto FRR is enabled, the system automatically sets up a bypass tunnel.

Context

Do as follows on the ingress node of the primary tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The tunnel interface view of the primary tunnel is displayed.

Step 3 Run:

```
mpls te fast-reroute [ bandwidth ]
```

The TE FRR is enabled.

Copyright © Huawei Technologies Co., Ltd.

To guarantee the tunnel bandwidth, you must specify the parameter **bandwidth**.

Step 4 (Optional) Run:

```
mpls te bypass-attributes bandwidth bandwidth [ priority setup-priority [ hold-priority ] ]
```

The attributes of the bypass tunnel are configured.

NOTE

- The bypass tunnel attributes can be configured only after the **mpls te fast-reroute bandwidth** command is run on the primary tunnel.
- The bandwidth of the bypass tunnel cannot be greater than the bandwidth of the primary tunnel.
- When the attributes of the automatic bypass tunnel are not configured, by default, the bandwidth of the automatic bypass tunnel is the same as the bandwidth of the primary tunnel.
- The setup priority of the bypass tunnel cannot be higher than the holding priority. Both priorities cannot be higher than the priority of the primary tunnel.
- When the bandwidth of the primary tunnel is changed or the FRR is disabled, the attributes of the bypass tunnel are cleared automatically.
- On one TE tunnel interface, the bandwidth of the bypass tunnel cannot be configured together with the multi-CT.

Step 5 Run:

```
mpls te commit
```

The current configuration of the tunnel is committed.

----End

3.12.4 (Optional) Configuring the Scanning Timer for FRR

By configuring a TE FRR scanning timer, you can search for the eligible LSPs that can function as bypass LSPs and then bind the optimal LSP to the primary LSP.

Context

Do as follows on the PLR node:

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 timer fast-reroute [ weight ]
```

The scanning timer for FRR is configured.

If *weight* is specified, the system can calculate the scanning interval according to the following formula:

Scanning interval = *Weight* x 1000 x 200/Maximum number of RSVP LSPs

Copyright © Huawei Technologies Co., Ltd.

If the calculated scanning interval is greater than 1000 milliseconds, it is the actual scanning interval; otherwise, 1000 ms is the scanning interval.

By default, the interval of the scanning timer is 1000 milliseconds.

After configuring FRR, the PLR performs scheduled scanning to search for LSPs that can serve as bypass LSPs and binds the optimal bypass LSP to the primary LSP. After the FRR switching, if the protected LSP is restored or another LSP is established, traffic is switched to the original LSP or the newly-established LSP.

----End

3.12.5 (Optional) Modifying PSB and RSB Timeout Multiplier

To perform TE FRR during the RSVP GR process, you need to modify the timeout multiplier of the PSB or RSB.

Context

Do as follows on each node along the tunnel to support the FRR during the RSVP GR:

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 timeout multiplier of the path state block (PSB) and reserved state block (RSB) is configured.

The timeout multiplier of the PSB and RSB is recommended to be equal to or greater than five to avoid the PSB and RSB loss because of large numbers of RSVP LSPs.

----End

3.12.6 Checking the Configuration

After the configuration of MPLS TE Auto FRR, you can view detailed information about a bypass tunnel.

Prerequisite

The configurations of the MPLS TE auto FRR function are complete.

Procedure

- Run the **display mpls te tunnel verbose** command to check binding information about the primary tunnel and the auto bypass tunnel.

Copyright © Huawei Technologies Co., Ltd.

- Run the **display mpls te tunnel-interface** [**tunnel** *tunnel-number* | **auto-bypass-tunnel** *tunnel-name*] command to check detailed information about the auto 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 path information about the primary tunnel and the auto bypass tunnel.

----End

3.13 Configuring CR-LSP Backup

By configuring CR-LSP backup, you can provide end-to-end protection for a CR-LSP.

3.13.1 Establishing the Configuration Task

Before configuring CR-LSP backup, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This helps you complete the configuration task quickly and accurately.

Applicable Environment

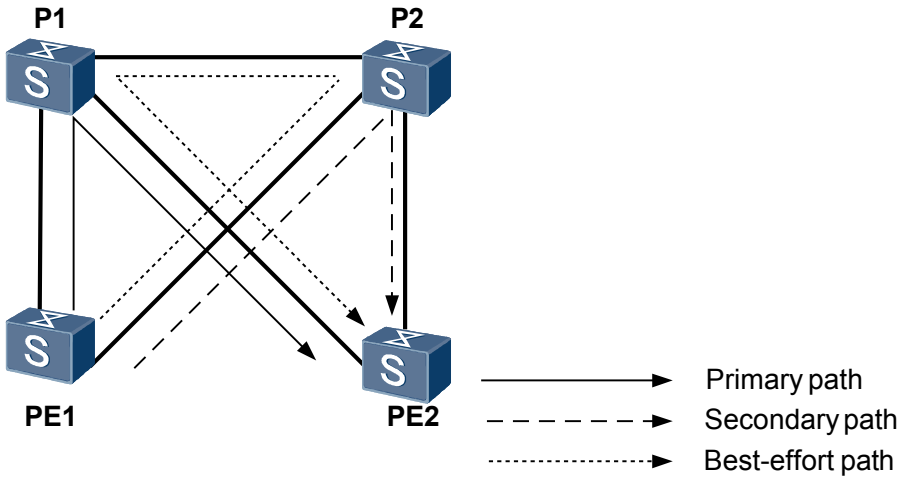
A backup CR-LSP provides an end-to-end path protection over an entire LSP.

A backup CR-LSP is classified into the following types:

- Hot-standby CR-LSP: A hot-standby CR-LSP is established at the same time a primary CR-LSP is set up. If the primary CR-LSP forwarding services fails, traffic rapidly switches to the hot-standby CR-LSP. Additional bandwidth is needed in hot-standby mode.
- Ordinary backup CR-LSP: An ordinary backup CR-LSP is set up only if a primary CR-LSP fails. No additional bandwidth is needed in ordinary backup mode. If a primary CR-LSP fails, traffic switches only after an ordinary backup CR-LSP has been successfully set up.

Hot-standby CR-LSPs support best-effort paths. If both the primary and backup CR-LSPs fail, the system establishes a temporary CR-LSP, which is called a best-effort path, and switches traffic to this best effort path. On the network shown in **Figure 3-1**, the primary CR-LSP is along the path PE1 -> P1 -> PE2 and the backup CR-LSP is along the path PE1 -> P2 -> PE2. If both of them fail, a best-effort LSP is set up along the path PE1 -> P2 -> P1 -> PE2.

Figure 3-1 Schematic diagram of a best-effort LSP



Copyright © Huawei Technologies Co., Ltd.

Pre-configuration Tasks

Before configuring CR-LSP backup, complete the following tasks:

- Enabling MPLS, MPLS TE, and RSVP TE globally and in the interface view of each node along a backup CR-LSP (See **Enabling MPLS TE and RSVP TE**.)

Data Preparation

To configure CR-LSP backup, you need the following data.

No.	Data
1	Backup mode
2	(Optional) Explicit path for the backup CR-LSP
3	(Optional) Affinity property of the backup CR-LSP
4	(Optional) Hop limit of the backup CR-LSP

3.13.2 Configuring CR-LSP Backup

CR-LSP backup is configured on the ingress of a primary CR-LSP. Hot standby and ordinary backup are mutually exclusive.

Context

By default, the CR-LSP backup is not enabled. After the CR-LSP backup is configured on the ingress of a tunnel, the system automatically selects the path of the backup CR-LSP without manual interruption.

NOTE

The CR-LSP backup cannot be configured with re-optimization at the same time.

Do as follows on the ingress node of the primary tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The tunnel interface view of the MPLS TE tunnel is displayed.

Step 3 Run:

```
mpls te backup { hot-standby [ wtr interval ] | ordinary }
```

The mode of establishing the CR-LSP backup is configured.

Copyright © Huawei Technologies Co., Ltd.

NOTE

A primary CR-LSP cannot function as a bypass tunnel or a backup CR-LSP for another CR-LSP. That is, the **mpls te protected-interface** or **mpls te bypass-tunnel** are mutually exclusive.

Step 4 (Optional) Run:

mpls te path explicit-path *path-name* **secondary**

The explicit path used by the backup CR-LSP is specified.

NOTE

When an explicit path is used to set up a hot-standby CR-LSP, it cannot completely overlap the path of the primary CR-LSP; otherwise, the hot-standby CR-LSP cannot protect the primary CR-LSP.

Step 5 (Optional) Run:

mpls te affinity property *properties* [**mask** *mask-value*] **secondary**

The affinity property used by the backup CR-LSP is configured.

By default, the affinity property used by the backup CR-LSP is 0x0.

Step 6 (Optional) Run:

mpls te hop-limit *hop-limit-value* **secondary**

The number of hops of the backup CR-LSP is limited.

By default, the hop limit of a backup CR-LSP is 32.

Step 7 Run:

mpls te commit

The current tunnel configuration is committed.

----End

3.13.3 (Optional) Configuring a Best-Effort LSP

By configuring a best-effort path, you can switch traffic to the best-effort path when both the primary CR-LSP and the backup CR-LSP fail.

Context

In best-effort mode, do as follows on the ingress node of the TE tunnel:

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Run:

interface tunnel *tunnel-number*

The tunnel interface view is displayed.

Step 3 Run:

mpls te backup ordinary best-effort

A best-effort LSP is configured.

Copyright © Huawei Technologies Co., Ltd.

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 used in the best-effort LSP is configured.

By default, the value of the affinity property used by the best-effort LSP is 0x0.

Step 5 (Optional) Run:

mpls te hop-limit *hop-limit-value* **best-effort**

The number of hops of the best-effort LSP is limited.

By default, the hop limit of a backup CR-LSP is 32.

Step 6 Run:

mpls te commit

The current tunnel configuration is committed.

----End

Follow-up Procedure

After a best-effort LSP is configured, the device triggers the setup of a best-effort LSP when both the primary LSP and the backup LSP fail.

3.13.4 Checking the Configuration

After the configuration of CR-LSP backup, you can view information about a backup CR-LSP.

Procedure

- Run the **display mpls te tunnel-interface** [**tunnel** *tunnel-number*] command to check information about the tunnel interface.
- Run the **display mpls te hot-standby state** { **all** [**verbose**] | **interface tunnel** *interface-number* } command to check the hot standby status.
- Run the **display mpls te tunnel** [**destination** *ip-address*] [**lsp-id** *ingress-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*] [**te-class0** | **te-class1** | **te-class2** | **te-class3** | **te-class4** | **te-class5** | **te-class6** | **te-class7**] [**verbose**] command to check information about the tunnel.

----End

Example

In hot standby mode, after the configuration, run the **display mpls te tunnel-interface** command, and you can view information about a backup CR-LSP.

```
[Quidway] display mpls te tunnel-interface
=============================================================
                              Tunnel1/0/0
    =========================================================
    Tunnel State Desc   :  UP
```


Copyright © Huawei Technologies Co., Ltd.

```
    Active LSP          :  Hot-Standby LSP
    Session ID          :  100
    Ingress LSR ID      :  4.4.4.4          Egress LSR ID:  3.3.3.3
    Admin State         :  UP               Oper State   :  UP
    Primary LSP State      : DOWN
      Main LSP State       : SETTING UP
    Hot-Standby LSP State  : UP
      Main LSP State       : READY              LSP ID  : 32769
      Modify LSP State     : SETTING UP
```

Run the **display mpls te hot-standby state** command, and you can view information about the hot standby.

```
<Quidway> display mpls te hot-standby state interface Tunnel 1/0/0
-------------------------------------------------------------
Verbose information about the Tunnel1/0/0 hot-standby state
-------------------------------------------------------------
tunnel name                              : Tunnel1/0/0
session id                               : 100
main LSP token                           : 0x100201a
hot-standby LSP token                    : 0x100201b
HSB switch result                        : Best-Effort LSP
WTR                                      : 15s
```

Run the **display mpls te tunnel** to check information about the tunnel.

```
<Quidway>  display mpls te tunnel verbose
    No                      :  1
    Tunnel-Name             :  Tunnel1/0/0
    TunnelIndex             :  0           LSP Index         :  1024
    Session ID              :  100         LSP ID            :  1
    Lsr Role                :  Ingress
    Ingress LSR ID          :  1.1.1.1
    Egress LSR ID           :  2.2.2.2
    In-Interface            :  -
    Out-Interface           :  Pos1/0/0
    Sign-Protocol           :  Static CR   Resv Style        :
    IncludeAnyAff           :  0x0         ExcludeAnyAff     :  0x0
    IncludeAllAff           :  0x0
    ER-Hop Table Index      :  -           AR-Hop Table Index:  -
    C-Hop Table Index       :  -
    PrevTunnelIndexInSession:  -           NextTunnelIndexInSession:  -
    PSB Handle              :  0
    Created Time            :  2008/04/03 19:31:14
    --------------------------------
              DS-TE Information
    --------------------------------
    Bandwidth Reserved Flag :  Unreserved
    CT0 Bandwidth(Kbit/sec) :  0           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          :  0           Hold-Priority          :  0
    --------------------------------
                FRR Information
    --------------------------------
    Primary LSP Info
    TE Attribute Flag       :  0xe3        Protected Flag    : 0x04
    Bypass In Use           :  Not Exists
    Bypass Tunnel Id        :  -
    BypassTunnel            :  -
    Bypass Lsp ID           :  -           FrrNextHop        :  -
    ReferAutoBypassHandle   :  -
    FrrPrevTunnelTableIndex :  -           FrrNextTunnelTableIndex:  -
    Bypass Attribute(Not configured)
    Setup Priority          :  -           Hold Priority     :  -
    HopLimit                :  -           Bandwidth         :  -
    IncludeAnyGroup         :  -           ExcludeAnyGroup   :  -
    IncludeAllGroup         :  -
    Bypass Unbound Bandwidth Info(Kbit/sec)
```


Copyright © Huawei Technologies Co., Ltd.

```
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         :  -
```

3.14 Configuring Synchronization of the Bypass Tunnel and the Backup CR-LSP

This section describes that after the primary CR-LSP is faulty, the system starts the TE FRR bypass tunnel and tries to restore the primary CR-LSP the same time it sets up a backup CR-LSP.

3.14.1 Establishing the Configuration Task

Before configuring synchronization of the bypass tunnel and the backup CR-LSP, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the required data. This can help you complete the configuration task quickly and accurately.

Application Environment

To protect important links and nodes, you can configure the TE FRR bypass tunnel and the end-to-end backup CR-LSP together. The backup CR-LSP is more reliable than the TE FRR bypass tunnel. Therefore, to improve the security of the tunnel, you are recommended to configure synchronization of the TE FRR bypass tunnel and the backup CR-LSP.

- In ordinary backup mode, the following situations occur:
  - When the protected link or node is faulty, the system switches traffic to the TE FRR bypass tunnel and tries to restore the primary CR-LSP. At the same time, the system tries to set up a backup CR-LSP.
  - When the backup CR-LSP is set up successfully and the primary CR-LSP is not restored, traffic is switched to the backup CR-LSP.
  - When the backup CR-LSP fails to be set up and the primary CR-LSP is not restored, traffic still passes through the TE FRR bypass tunnel.
- In hot standby mode, the following situations occur:
  - If the backup CR-LSP is in the Up state and the protected link or node is faulty, traffic is switched to the TE FRR bypass tunnel and then immediately switched to the backup CR-LSP. At the same time, the system tries to restore the primary CR-LSP.
  - If the backup CR-LSP is in the Down state, the processing of hot standby is the same as the processing of ordinary backup.

When the primary CR-LSP is Up and the hot standby CR-LSP is also in the Up state, more bandwidth resources are needed. The ordinary CR-LSP is set up only when the primary CR-LSP is in the FRR-in-use state. That is, when the primary CR-LSP works normally, no more bandwidth resources are needed. Therefore, the ordinary backup is recommended.

Copyright © Huawei Technologies Co., Ltd.

Pre-configuration Tasks

Before configuring synchronization of the bypass tunnel and the backup CR-LSP, you need to complete the following tasks:

- Setting up the primary tunnel
- Configuring manual MPLS TE FRR or MPLS TE Auto FRR (See the section **Configuring MPLS TE FRR** or the section **Configuring MPLS Auto TE FRR**.)
- Configuring the backup CR-LSP (except for the best-effort path) in either hot standby mode or ordinary backup mode (See the section **Configuring CR-LSP Backup**.)

Data Preparation

To configure synchronization of the bypass tunnel and the backup CR-LSP, you need the following data.

No.	Data
1	Protection policy of TE FRR, that is, to protect the link or the node
2	Backup mode

3.14.2 Enabling Synchronization of the Bypass Tunnel and the Backup CR-LSP

By configuring synchronization of the bypass tunnel and the backup CR-LSP, you can protect the entire CR-LSP.

Context

Do as follows on the ingress LSR of the primary tunnel:

NOTE

Before the configuration, you must configure the end-to-end protection (except for the best-effort path) in either hot standby mode or ordinary backup mode and the TE FRR partial protection.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The tunnel interface view of the MPLS TE tunnel is displayed.

Step 3 Run:

```
mpls te backup frr-in-use
```


Copyright © Huawei Technologies Co., Ltd.

When the primary CR-LSP is faulty (that is, the primary CR-LSP is in FRR-in-use state), the system starts the TE FRR bypass tunnel and tries to restore the primary CR-LSP. At the same time, the system tries to set up a backup CR-LSP.

Step 4 Run:

```
mpls te commit
```

The tunnel configurations are committed.

Step 5 Run:

```
quit
```

Return to the system view.

----End

3.14.3 Checking the Configuration

After the configuration of synchronization of the bypass tunnel and the backup CR-LSP, you can view information about the bypass tunnel and the backup CR-LSP.

Prerequisite

All configurations of synchronization of the bypass tunnel and the backup CR-LSP are complete.

Procedure

- Run the **display mpls te tunnel-interface** [**tunnel** *tunnel-number* | **auto-bypass-tunnel** *tunnel-name*] command, and you can view information about the tunnel.

----End

3.15 Configuring RSVP GR

This section describes how to configure RSVP-TE GR so that devices along an RSVP-TE tunnel can retain RSVP sessions during a master/slave switchover.

3.15.1 Establishing the Configuration Task

Before configuring RSVP-TE GR, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

When an RSVP node performs an active/standby switchover, an RSVP adjacency relationship between the local node and its neighbor is torn down because of signaling protocol timeout, resulting in removal of a CR-LSP and a temporary traffic interruption.

RSVP GR resolves the preceding problem. The RSVP GR mechanism allows the adjacency relationship to be reestablished between neighbors without tearing down RSVP sessions.

On the S9300, FRR switching is performed during the RSVP GR process. FRR protects traffic if a switchover is performed on the PLR node, PLR upstream node, MP, or MP downstream node and the outgoing interface of the PLR primary tunnel fails, reducing the fault period.

Copyright © Huawei Technologies Co., Ltd.

NOTE

When FRR is performed during the RSVP GR process, setting the timeout multiplier in the PSB and RSB to a value equal to or greater than five is recommended, preventing PSB and RSB loss due to oversized data. For detailed configurations, see **(Optional) Modifying the PSB and RSB Timeout Multiplier**.

Pre-configuration Tasks

Before configuring RSVP GR, complete the following tasks:

- Configuring an RSVP-TE tunnel
- Enabling IS-IS GR or OSPF GR on each LSR

Data Preparation

To configure RSVP GR, you need the following data.

No.	Data
1	IGP parameters: ● IS-IS: IS-IS process ID, Network Entity Title (NET), and IS-IS level of each node ● OSPF: OSPF process ID and AS number
2	MPLS LSR ID of each node
3	Tunnel interface number and tunnel ID
4	(Optional) Basic RSVP GR time

3.15.2 Enabling the RSVP Hello Extension Function

By configuring the RSVP Hello extension, you can enable a device to quickly check reachability between RSVP nodes.

Context

Do as follows on a GR node and its 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 hello
```


Copyright © Huawei Technologies Co., Ltd.

The RSVP Hello extension function is enabled globally.

Step 4 Run:

```
quit
```

The system view is displayed.

Step 5 Run:

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

The RSVP interface view is displayed.

Step 6 Run:

```
mpls rsvp-te hello
```

The RSVP Hello extension function is enabled on the interface.

By default, although the RSVP Hello extension function has been enabled globally, it is disabled on RSVP-enabled interfaces.

----End

3.15.3 Enabling Full GR of RSVP

By enabling RSVP full GR, you can ensure uninterrupted data transmission on the forwarding plane.

Context

Do as follows on a GR node:

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 full-gr
```

The RSVP GR function and the function of supporting RSVP GR on a neighbor are enabled.

By default, the RSVP GR function and RSVP GR support function are disabled.

----End

3.15.4 (Optional) Enabling the RSVP GR Support Function

By being enabled with RSVP GR, a device supports the GR capability of its neighbor.

Copyright © Huawei Technologies Co., Ltd.

Context

RSVP GR takes effect on the RSVP GR-enabled neighbor automatically after the neighbor is enabled with RSVP full GR. If the GR node's neighbor is a GR node, do not perform the following steps. If the GR node's neighbor is not a GR node, do as follows:

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 function is enabled on the local node.

Step 5 Run:

```
mpls rsvp-te hello support-peer-gr
```

The function of supporting RSVP GR on the neighbor is enabled.

----End

3.15.5 (Optional) Configuring Hello Sessions Between RSVP GR Nodes

On a network enabled with TE FRR, a Hello session needs to be set up between a PLR and an MP.

Context

If TE FRR is deployed, a hello session is required between a PLR and an MP. Do as follows on the PLR and MP:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Copyright © Huawei Technologies Co., Ltd.

Step 3 Run:

```
mpls rsvp-te
```

RSVP-TE is enabled.

Step 4 Run:

```
mpls rsvp-te hello
```

The RSVP Hello function is enabled on the local node.

Step 5 Run:

```
mpls rsvp-te hello nodeid-session ip-address
```

A Hello session is set up between a restarting node and a neighbor node.

ip-address is the LSR ID of the RSVP neighbor.

----End

3.15.6 (Optional) Modifying Basic Time

By setting the basic time and the number of ingress LSPs, you can modify the restart time.

Context

After an active/standby switchover starts, an RSVP GR node has an RSVP smoothing period, during which the data plane continues forwarding data if the control plane is not restored. After RSVP smoothing is completed, a restart timer is started.

Restart timer value = Basic time + Number of ingress LSPs x 60 ms

In this formula, the default basic time is 90 seconds and is configurable by using a command line, and the number of LSPs is the number of LSPs with the local node being the ingress.

After the restart timer expires, the recovery timer is started.

Recovery timer = Restart time + Total number of LSPs x 40 ms

Do as follows on the GR node to modify the basic time:

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 modified.

By default, the RSVP GR basic time is 90 seconds.

----End

Copyright © Huawei Technologies Co., Ltd.

3.15.7 Checking the Configuration

After the configuration of RSVP GR, you can view that the TE tunnel properly forward data during the GR process.

Procedure

- Run the **display mpls rsvp-te graceful-restart** command to check the status of the local RSVP GR.
- Run the **display mpls rsvp-te graceful-restart peer** [{ **interface** *interface-type interface-number* | **node-id** } [*ip-address*]] command to check the status of RSVP GR on a neighbor.

----End

Example

Run the **display mpls rsvp-te graceful-restart** command on a restarted node. If "GR-Self GR-Support" is displayed in the Graceful-Restart Capability field, it means that the local device has the RSVP GR function. During the GR process, in the output of the **display mpls rsvp-te graceful-restart** command, "Restart time going on" or "Recovery time going on" is displayed in the GR Status field.

Run the **display mpls rsvp-te graceful-restart peer** command on the restarted node.

Information displayed in the Neighbor Capability field has specific meanings:

- Can Do Self GR: means that the neighbor node is enabled with the RSVP GR capability.
- Can Support GR: means that the neighbor node is enabled with the RSVP GR supporting capability.
- Both "Can Do Self GR" and "Can Support GR": mean that the neighbor node is enabled with the RSVP GR function and the RSVP GR support function.

3.16 Configuring Static BFD for CR-LSP

This section describes how to configure a static BFD session to detect link faults in static CR-LSPs or RSVP CR-LSPs.

3.16.1 Establishing the Configuration Task

Before configuring static BFD for CR-LSP, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

BFD detects the following types of CR-LSPs:

- Static CR-LSP
- RSVP CR-LSP

BFD for static CR-LSP and BFD for RSVP CR-LSP can be used to replace MPLS OAM to detect the MPLS TE tunnel protection groups and trigger primary/backup CR-LSP switchover. BFD for CR-LSP is applicable to the hot-standby CR-LSP. It detects the primary and backup CR-LSPs and triggers CR-LSPs switchover.

Copyright © Huawei Technologies Co., Ltd.

For details about MPLS OAM configuration, refer to the chapter "MPLS OAM Configuration" in the *Configuration Guide - MPLS*.

NOTE

For the same CR-LSP, MPLS OAM and BFD cannot be configured simultaneously.

In the scenario that static BFD for CR-LSP is applied and the BFD status is Up, if the tunnel interface to which CR-LSP belongs is shut down, the BFD status remains Up.

BFD for LSP can function properly though the forward path is an LSP and the backward path is an IP link. The forward path and the backward path must be established over the same link; otherwise, if a fault occurs, BFD cannot identify the faulty path. Before deploying BFD, ensure that the forward and backward paths are over the same link so that BFD can correctly identify the faulty path.

Pre-configuration Tasks

Before configuring static BFD for CR-LSP, complete the following task:

- **Configuring Static MPLS TE Tunnel** or **Configuring RSVP-TE Tunnel** or MPLS TE tunnel protection group

NOTE

For details about the configuration of the MPLS TE tunnel protection group for the MPLS TE tunnel, refer to the chapter "MPLS OAM Configuration" in the *Quidway S9300 Terabit Routing Switch Configuration Guide - MPLS*.

Data Preparation

To configure static BFD for CR-LSP, you need the following data.

No.	Data
1	BFD session name
2	Backward channel (IP link, dynamic LSP, static LSP, or MPLS TE tunnel)
3	Local and remote discriminators of the BFD session
4	Minimum interval for sending BFD packets
5	Minimum interval for receiving BFD packets
6	Local BFD detection multiplier

3.16.2 Enabling BFD Globally

To configure static BFD for CR-LSP, you must enable BFD globally on the ingress node and the egress node of a tunnel.

Context

Do as follows on the ingress node and egress node of the tunnel:

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bfd
```

BFD is enabled globally.

----End

3.16.3 Configuring BFD Parameters on the Ingress of the Tunnel

The BFD parameters configured on the ingress node include the local and remote discriminators, local minimum intervals at which BFD packets are sent and received, and BFD detection multiplier, which determine the establishment of a BFD session.

Context

Do as follows on the ingress node of a tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

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

BFD is configured to detect the primary or backup CR-LSP bound to a specified tunnel.

The parameter **backup** means that backup CR-LSPs are to be checked.

Step 3 Run:

```
discriminator local discr-value
```

The local discriminator is set.

Step 4 Run:

```
discriminator remote discr-value
```

The remote discriminator is set.

Step 5 (Optional) Run:

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

The local minimum interval at which BFD packets are sent is set.

The default value is specified in the license.

Step 6 (Optional) Run:

```
min-rx-interval interval
```

The local minimum interval at which BFD packets are received is set.

Copyright © Huawei Technologies Co., Ltd.

The default value is specified in the license.

Step 7 (Optional) Run:

detect-multiplier *multiplier*

The local detection multiplier is adjusted.

By default, the local detection multiplier is 3.

Step 8 Run:

commit

The current configuration is committed.

NOTE

Actual local sending interval = MAX { Configured local sending interval, Configured remote receiving interval }

Actual local receiving interval = MAX { Configured remote sending interval, Configured local receiving interval }

Actual local detection interval = Actual local receiving interval x Configured remote detection multiplier

For example:

- The local sending and receiving intervals are set to 200 ms and 300 ms respectively and the detection multiplier is set to 4.
- The remote sending and receiving intervals are set to 100 ms and 600 ms respectively and the detection multiplier is set to 5.

Then,

- Actual local sending interval = MAX {200 ms, 600 ms} = 600 ms; Actual local receiving interval = MAX {100 ms, 300 ms} = 300 ms; Actual local detection interval is 300 ms x 5 = 1500 ms.
- Actual remote sending interval = MAX {100 ms, 300 ms} = 300 ms; Actual remote receiving interval = MAX {200 ms, 600 ms} = 600 ms; Actual remote detection interval is 600 ms x 4 = 2400 ms.

----End

3.16.4 Configuring BFD Parameters on the Egress of the Tunnel

The BFD parameters configured on the egress node include the local and remote discriminators, local minimum intervals at which BFD packets are sent and received, and BFD detection multiplier, which determine the establishment of a BFD session.

Context

Do as follows on the egress node of a tunnel:

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Configure a reverse tunnel to inform the ingress of a fault if the fault occurs. The reverse tunnel can be the IP link, LSP, or TE tunnel. To prevent affecting BFD detection, an IP link is usually selected to inform the ingress of an LSP fault. If the configured reverse tunnel requires BFD detection, configure a pair of BFD sessions for it. Choose one of the following configurations as required:

Copyright © Huawei Technologies Co., Ltd.

- For an IP link, run:
  bfd *cfg-name* **bind peer-ip** *ip-address* [**vpn-instance** *vpn-name*] [**interface** *interface-type interface-number*] [**source-ip** *ip-address*]
- For an LDP LSP, run:
  bfd *cfg-name* **bind ldp-lsp peer-ip** *ip-address* **nexthop** *ip-address* [**interface** *interface-type interface-number*]
- For a static LSP, run:
  bfd *cfg-name* **bind static-lsp** *lsp-name*
- For a CR-LSP, run:
  bfd *cfg-name* **bind mpls-te interface tunnel** *tunnel-number* **te-lsp** [**backup**]
- For a TE tunnel, run:
  bfd *cfg-name* **bind mpls-te interface tunnel** *tunnel-number*

Step 3 Run:

discriminator local *discr-value*

The local discriminator is set.

Step 4 Run:

discriminator remote *discr-value*

The remote discriminator is set.

Step 5 (Optional) Run:

min-tx-interval *interval*

The minimum interval at which the local end sends BFD packets is set.

The default value is specified by the license.

Step 6 (Optional) Run:

min-rx-interval *interval*

The minimum interval at which the local end receives BFD packets is set.

The default value is specified by the license.

Step 7 (Optional) Run:

detect-multiplier *multiplier*

The local detection multiplier is set.

Step 8 Run:

commit

The configuration is committed.

----End

3.16.5 Checking the Configuration

After the configuration of static BFD for CR-LSP, you can view that the status of a BFD session is Up.

Procedure

- Run the **display bfd configuration mpls-te interface tunnel** *interface-number* **te-lsp** [**verbose**] command to check BFD configurations on the ingress.
- Run the following commands to check BFD configurations on the egress:

Copyright © Huawei Technologies Co., Ltd.

- Run the **display bfd configuration all** [**for-ip** | **for-lsp** | **for-te**] [**verbose**] command to check all BFD configurations.
- Run the **display bfd configuration static** [**for-ip** | **for-lsp** | **for-te** | **name** *cfg-name*] [**verbose**] command to check the static BFD configurations.
- Run the **display bfd configuration peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] [**verbose**] command to check the configurations of BFD with the reverse path being an IP link.
- Run the **display bfd configuration static-lsp** *lsp-name* [**verbose**] command to check the configurations of BFD with the reverse path being a static LSP.
- Run the **display bfd configuration ldp-lsp peer-ip** *peer-ip* **nexthop** *nexthop-address* [**interface** *interface-type interface-number*] [**verbose**] command to check the configurations of BFD with the backward channel being an LDP LSP.
- Run the **display bfd configuration mpls-te interface tunnel** *interface-number* **te-lsp** [**verbose**] command to check the configurations of BFD with the backward channel being a CR-LSP.
- Run the **display bfd configuration mpls-te interface tunnel** *interface-number* [**verbose**] command to check the configurations of BFD with the backward channel being a TE tunnel.

- Run the **display bfd session mpls-te interface tunnel** *interface-number* **te-lsp** [**verbose**] command to check BFD session configurations on the ingress.
- Run the following commands to check BFD session configurations on the egress:
  - Run the **display bfd session all** [**for-ip** | **for-lsp** | **for-te**] [**verbose**] command to check all the BFD configurations.
  - Run the **display bfd session static** [**for-ip** | **for-lsp** | **for-te**] [**verbose**] command to check the static BFD configurations.
  - Run the **display bfd session peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] [**verbose**] command to check the configurations of BFD with the backward channel being an IP link.
  - Run the **display bfd session static-lsp** *lsp-name* [**verbose**] command to check the configurations of BFD with the backward channel being a static LSP.
  - Run the **display bfd session ldp-lsp peer-ip** *peer-ip* **nexthop** *nexthop-address* [**interface** *interface-type interface-number*] [**verbose**] command to check the configurations of BFD with the backward channel being an LDP LSP.
  - Run the **display bfd session mpls-te interface tunnel** *interface-number* **te-lsp** [**verbose**] command to check the configurations of BFD with the backward channel being a CR-LSP.
  - Run the **display bfd session mpls-te interface tunnel** *interface-number* [**verbose**] command to check the configurations of BFD with the backward channel being a TE tunnel.
- Run the following command to check BFD statistics:
  - Run the **display bfd statistics session all** [**for-ip** | **for-lsp** | **for-te**] command to check all BFD session statistics.
  - Run the **display bfd statistics session peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] command to check statistics about the BFD session that detects faults in the IP link.

Copyright © Huawei Technologies Co., Ltd.

- Run the **display bfd statistics session static-lsp** *lsp-name* command to check statistics about the BFD session that detects faults in the static LSP.
- Run the **display bfd statistics session ldp-lsp peer-ip** *peer-ip* **nexthop** *nexthop-address* [**interface** *interface-type interface-number*] command to check statistics of the BFD session that detects faults in the LDP LSP.
- Run the **display bfd statistics session mpls-te interface tunnel** *interface-number* **te-lsp** command to check statistics about the BFD session that detects faults in the CR-LSP.

----End

Example

After the configuration, run the preceding commands to check BFD session status, and you can view that the BFD session is Up.

3.17 Configuring Static BFD for TE

This section describes how to configure a static BFD session to detect faults in a TE tunnel.

3.17.1 Establishing the Configuration Task

Before configuring static BFD for TE, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

BFD for TE allows applications such as VPN FRR or VLL FRR to fast switch traffic if the primary tunnel fails, preventing service interruption.

NOTE

MPLS OAM and BFD cannot be configured together on a TE tunnel.

BFD for LSP can function properly though the forward path is an LSP and the backward path is an IP link. The forward path and the backward path must be established over the same link; otherwise, if a fault occurs, BFD cannot identify the faulty path. Before deploying BFD, ensure that the forward and backward paths are over the same link so that BFD can correctly identify the faulty path.

Pre-configuration Tasks

Before configuring static BFD for TE, complete the following task:

- **Configuring Static MPLS TE Tunnel** or **Configuring RSVP-TE Tunnel**

Data Preparation

To configure static BFD for TE, you need the following data.

No.	Data
1	Name of the BFD session

Copyright © Huawei Technologies Co., Ltd.

No.	Data
2	Backward channel (IP link, dynamic LSP, static LSP, or MPLS TE tunnel)
3	Local and remote discriminators of the BFD session
4	(Optional) Local minimum interval at which BFD packets are sent
5	(Optional) Local minimum interval at which BFD packets are received
6	(Optional) Local detection multiplier

3.17.2 Enabling BFD Globally

To configure static BFD for TE, you need to enable BFD globally on the ingress and egress nodes of a tunnel.

Context

Do as follows on the ingress and egress of a tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bfd
```

BFD is enabled globally.

----End

3.17.3 Configuring BFD Parameters on the Ingress of the Tunnel

The BFD parameters configured on the ingress node include the local and remote discriminators, local minimum intervals at which BFD packets are sent and received, and BFD detection multiplier, which determine the establishment of a BFD session.

Context

Do as follows on the ingress of a tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bfd cfg-name bind mpls-te interface tunnel tunnel-number
```


Copyright © Huawei Technologies Co., Ltd.

BFD is configured to detect faults in a specified tunnel.

Step 3 Run:

discriminator local *discr-value*

The local discriminator is configured.

Step 4 Run:

discriminator remote *discr-value*

The remote discriminator is configured.

Step 5 (Optional) Run:

min-tx-interval *interval*

The local minimum interval at which BFD packets are sent is set.

Step 6 (Optional) Run:

min-rx-interval *interval*

The local minimum interval at which BFD packets are received is set.

Step 7 (Optional) Run:

detect-multiplier *multiplier*

The local detection multiplier is set.

Step 8 Run:

commit

The BFD configuration is committed.

NOTE

If the status of the tunnel to be checked is Down, the BFD session cannot be set up.

Actual local sending interval = MAX { Configured local sending interval, Configured remote receiving interval }

Actual local receiving interval = MAX { Configured remote sending interval, Configured local receiving interval }

Actual local detection interval = Actual local receiving interval x Configured remote detection multiplier.

For example:

- The local sending and receiving intervals are set to 200 ms and 300 ms respectively and the detection multiplier is set to 4.
- The remote sending and receiving intervals are set to 100 ms and 600 ms respectively and the detection multiplier is set to 5.

Then,

- Actual local sending interval = MAX {200 ms, 600 ms} = 600 ms; Actual local receiving interval = MAX {100 ms, 300 ms} = 300 ms; actual local detection interval is 300 ms x 5 = 1500 ms.
- Actual remote sending interval = MAX {100 ms, 300 ms} = 300 ms; Actual remote receiving interval = MAX {200 ms, 600 ms} = 600 ms; Actual remote detection interval is 600 ms x 4 = 2400 ms.

----End

3.17.4 Configuring BFD Parameters on the Egress of the Tunnel

The BFD parameters configured on the egress node include the local and remote discriminators, local minimum intervals at which BFD packets are sent and received, and BFD detection multiplier, which determine the establishment of a BFD session.

Copyright © Huawei Technologies Co., Ltd.

Context

Do as follows on the egress node of a tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Configure a reverse tunnel to inform the ingress of a fault if the fault occurs. The reverse tunnel can be the IP link, LSP, or TE tunnel. To prevent affecting BFD detection, an IP link is usually selected to inform the ingress of an LSP fault. If the configured reverse tunnel requires BFD detection, configure a pair of BFD sessions for it. Choose one of the following configurations as required:

- For an IP link, run:
  bfd *cfg-name* **bind peer-ip** *ip-address* [**vpn-instance** *vpn-name*] [**interface** *interface-type interface-number*] [**source-ip** *ip-address*]
- For an LDP LSP, run:
  bfd *cfg-name* **bind ldp-lsp peer-ip** *ip-address* **nexthop** *ip-address* [**interface** *interface-type interface-number*]
- For a static LSP, run:
  bfd *cfg-name* **bind static-lsp** *lsp-name*
- For a TE tunnel, run:
  bfd *cfg-name* **bind mpls-te interface tunnel** *tunnel-number*

Step 3 Run:

```
discriminator local discr-value
```

The local discriminator is configured.

Step 4 Run:

```
discriminator remote discr-value
```

The remote discriminator is configured.

Step 5 (Optional) Run:

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

The local minimum interval at which BFD packets are sent is set.

The default value is determined by the License.

Step 6 (Optional) Run:

```
min-rx-interval interval
```

The local minimum interval at which BFD packets are received is set.

The default value is specified in the license.

Step 7 (Optional) Run:

```
detect-multiplier multiplier
```

The local detection multiplier is set.

Step 8 Run:

```
commit
```


Copyright © Huawei Technologies Co., Ltd.

The current configuration is committed.

----End

3.17.5 Checking the Configuration

After the configuration of static BFD for TE, you can view that the status of a BFD session is Up.

Procedure

- Run the **display bfd configuration mpls-te interface tunnel** *interface-number* [**verbose**] command to check BFD configurations on the ingress.
- Run the following commands to check BFD configurations on the egress:
  - Run the **display bfd configuration all** [**for-ip** | **for-lsp** | **for-te**] [**verbose**] command to check all information about BFD.
  - Run the **display bfd configuration static** [**for-ip** | **for-lsp** | **for-te** | **name** *cfg-name*] [**verbose**] command to check the static BFD configurations.
  - Run the **display bfd configuration peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] [**verbose**] command to check the configurations of BFD with the backward channel being an IP link.
  - Run the **display bfd configuration static-lsp** *lsp-name* [**verbose**] command to check the configurations of BFD with the backward channel being a static LSP.
  - Run the **display bfd configuration ldp-lsp peer-ip** *peer-ip* **nexthop** *nexthop-address* [**interface** *interface-type interface-number*] [**verbose**] command to check the configurations of BFD with the backward channel being an LDP LSP.
  - Run the **display bfd configuration mpls-te interface tunnel** *interface-number* **te-lsp** [**verbose**] command to check the configurations of BFD with the backward channel being a CR-LSP.
  - Run the **display bfd configuration mpls-te interface tunnel** *interface-number* [**verbose**] command to check the configurations of BFD with the backward channel being a TE tunnel.
- Run the **display bfd session mpls-te interface tunnel** *interface-number* [**verbose**] command to check BFD session configurations on the ingress.
- Run the following commands to check BFD session configurations on the egress:
  - Run the **display bfd session all** [**for-ip** | **for-lsp** | **for-te**] [**verbose**] command to check all BFD configurations.
  - Run the **display bfd session static** [**for-ip** | **for-lsp** | **for-te**] [**verbose**] command to check the configurations of static BFD.
  - Run the **display bfd session peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] [**verbose**] command to check the configurations of BFD with the backward channel being an IP link.
  - Run the **display bfd session static-lsp** *lsp-name* [**verbose**] command to check the configurations of BFD with the backward channel being a static LSP.
  - Run the **display bfd session ldp-lsp peer-ip** *peer-ip* **nexthop** *nexthop-address* [**interface** *interface-type interface-number*] [**verbose**] command to check the configurations of BFD with the backward channel being an LDP LSP.

Copyright © Huawei Technologies Co., Ltd.

- Run the **display bfd session mpls-te interface tunnel** *interface-number* **te-lsp** [**verbose**] command to check the configurations of BFD with the backward channel being a CR-LSP.
- Run the **display bfd session mpls-te interface tunnel** *interface-number* [**verbose**] command to check the configurations of BFD with the backward channel being a TE tunnel.

- Run the following command to check BFD statistics:
  - Run the **display bfd statistics** command to check all BFD statistics.
  - Run the **display bfd statistics session all** [**for-ip** | **for-lsp** | **for-te**] command to check all BFD session statistics.
  - Run the **display bfd statistics session peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] command to check statistics of the BFD session that detects faults in the IP link.
  - Run the **display bfd statistics session static-lsp** *lsp-name* command to check statistics about the BFD session that detects faults in the static LSP.
  - Run the **display bfd statistics session ldp-lsp peer-ip** *peer-ip* **nexthop** *nexthop-address* [**interface** *interface-type interface-number*] command to check statistics of the BFD session that detects faults in the LDP LSP.
  - Run the **display bfd statistics session mpls-te interface tunnel** *interface-number* **te-lsp** command to check statistics of the BFD session that detects faults in the CR-LSP.

----End

Example

After the configuration, run the preceding commands to check BFD session status, and you can view that the BFD session is Up.

3.18 Configuring Dynamic BFD for CR-LSP

This section describes how to configure a dynamic BFD session to detect link faults in a static CR-LSP or an RSVP CR-LSP.

3.18.1 Establishing the Configuration Task

Before configuring dynamic BFD for CR-LSP, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

Compared with static BFD, dynamically creating BFD sessions simplifies configurations and reduces configuration errors.

BFD detects faults in the following CR-LSPs:

- Static CR-LSP
- RSVP CR-LSP

Currently, dynamic BFD for CR-LSP cannot detect faults in the entire TE tunnel.

Copyright © Huawei Technologies Co., Ltd.

NOTE

MPLS OAM and BFD cannot be configured together for one CR-LSP.

If a dynamic BFD session for CR-LSP is Up but the tunnel interface of the detected CR-LSP is shut down, the BFD session is still Up.

BFD for LSP can function properly though the forward path is an LSP and the backward path is an IP link. The forward path and the backward path must be established over the same link; otherwise, if a fault occurs, BFD cannot identify the faulty path. Before deploying BFD, ensure that the forward and backward paths are over the same link so that BFD can correctly identify the faulty path.

Pre-configuration Tasks

Before configuring dynamic BFD for CR-LSP, complete the following tasks:

- **Configuring Static MPLS TE Tunnel** or **Configuring an RSVP-TE Tunnel**

Data Preparation

To configure dynamic BFD for CR-LSP, you need the following data.

No.	Data
1	Local minimum interval at which BFD packets are sent
2	Local minimum interval at which BFD packets are received
3	Local BFD detection multiplier

3.18.2 Enabling BFD Globally

To configure dynamic BFD for CR-LSP, you need to enable BFD globally on the ingress node and the egress node of a tunnel.

Context

Do as follows on the ingress and the egress of a TE tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bfd
```

BFD is enabled globally.

----End

Copyright © Huawei Technologies Co., Ltd.

3.18.3 Enabling the Capability of Dynamically Creating BFD Sessions on the Ingress

You can enable the ingress node to dynamically create BFD sessions on a TE tunnel in either of two modes, that is, enabling BFD globally and enabling BFD on a tunnel interface.

Context

Enabling the capability of dynamically creating BFD sessions on a TE tunnel can be implemented in either of the following methods:

- **Enabling MPLS TE BFD Globally** if most TE tunnels on the ingress need to dynamically create BFD sessions
- **Enabling MPLS TE BFD on the Tunnel Interface** if certain TE tunnels on the ingress need to dynamically create BFD sessions

Procedure

- Enable MPLS TE BFD globally.

  Do as follows on the ingress:

  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     mpls

     The MPLS view is displayed.
  3. Run:
     mpls te bfd enable

     The capability of dynamically creating BFD sessions is enabled on the TE tunnel.

     After this command is run in the MPLS view, dynamic BFD for TE is enabled on all the tunnel interfaces, excluding the interfaces on which dynamic BFD for TE are blocked.
  4. (Optional) Block the capability of dynamically creating BFD sessions for TE on the tunnel interfaces of the TE tunnels that do not need dynamic BFD for TE.

     (1) Run:
     interface tunnel *interface-number*

     The TE tunnel interface view is displayed.

     (2) Run:
     mpls te bfd block

     The capability of dynamically creating BFD sessions on the tunnel interface is blocked.

     (3) Run:
     mpls te commit

     The current configuration on this tunnel interface is committed.
- Enable MPLS TE BFD on a tunnel interface.

  Do as follows on the ingress:

Copyright © Huawei Technologies Co., Ltd.

1. Run:
   system-view

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

   The TE tunnel interface view is displayed.
3. Run:
   mpls te bfd enable

   The capability of dynamically creating BFD sessions is enabled on the TE tunnel.

   The command configured in the tunnel interface view takes effect only on the current tunnel interface.
4. Run:
   mpls te commit

   The configuration of the TE tunnel is committed.

----End

3.18.4 Enabling the Capability of Passively Creating BFD Sessions on the Egress

On a unidirectional LSP, creating a BFD session on the active role (ingress node) triggers the sending of LSP ping request messages to the passive role (egress node). Only after the passive role receives the ping packets, a BFD session can be automatically set up.

Context

Do as follows on the egress:

Procedure

Step 1 Run:
system-view

The system view is displayed.

Step 2 Run:
bfd

The BFD view is displayed.

Step 3 Run:
mpls-passive

The capability of passively creating BFD sessions is enabled.

After this command is run, a BFD session can be created only after the egress receives an LSP Ping request containing a BFD TLV from the ingress.

----End

Copyright © Huawei Technologies Co., Ltd.

3.18.5 (Optional) Adjusting BFD Parameters

BFD parameters are adjusted on the ingress of a tunnel in either of two modes, that is, adjusting BFD parameters globally and on a tunnel interface.

Context

BFD parameters are adjusted on the ingress of a TE tunnel either of the following modes:

- **Adjusting Global BFD Parameters** if most TE tunnels on the ingress use the same BFD parameters
- **Adjusting BFD Parameters on an Interface** if certain TE tunnels on the ingress need BFD parameters different from global BFD parameters

NOTE

Actual local sending interval = MAX { Configured local sending interval, Configured remote receiving interval }

Actual local receiving interval = MAX { Configured remote sending interval, Configured local receiving interval }

Actual local detection interval = Actual local receiving interval x Configured remote detection multiplier

On the egress of the TE tunnel enabled with the capability of passively creating BFD sessions, the default values of the receiving interval, sending interval and detection multiplier cannot be adjusted. The default values of these three parameters are the minimum configurable values on the ingress. Therefore, the BFD detection interval on the ingress and that on the egress of a TE tunnel are as follows:

- Actual detection interval on the ingress = Configured receiving interval on the ingress x 3
- Actual detection interval on the egress = Configured sending interval on the ingress x Configured detection multiplier on the ingress

Procedure

- Adjust global BFD parameters.

  Do as follows on the ingress of a TE tunnel:

  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     mpls

     The MPLS view is displayed.
  3. Run:
     mpls te bfd { **min-tx-interval** *tx-interval* | **min-rx-interval** *tx-interval* | **detect-multiplier** *multiplier* }*

     BFD time parameters are adjusted globally.
- Adjust BFD parameters on the tunnel interface.
  1. Run:
     system-view

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

Copyright © Huawei Technologies Co., Ltd.

The TE tunnel interface view is displayed.

3. Run:

   mpls te bfd { **min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier* }*

   BFD time parameters are adjusted.

4. Run:

   mpls te commit

   The current configurations of the TE tunnel interface are committed.

----End

3.18.6 Checking the Configuration

After the configuration of dynamic BFD for CR-LSP, you can view that a CR-LSP is Up and a BFD session is successfully set up.

Procedure

- Run the **display bfd configuration dynamic** [**verbose**] command to check the configuration of dynamic BFD on the ingress.
- Run the **display bfd configuration passive-dynamic** [**peer-ip** *peer-ip* **remote-discriminator** *discriminator*] [**verbose**] command to check the configuration of dynamic BFD on the egress.
- Run the **display bfd session dynamic** [**verbose**] command to check information about the BFD session on the ingress.
- Run the **display bfd session passive-dynamic** [**peer-ip** *peer-ip* **discriminator** *discriminator*] [**verbose**] command to check information about the BFD session passively created on the egress.
- Check the BFD statistics.
  - Run the **display bfd statistics** command to check statistics about all BFD sessions.
  - Run the **display bfd statistics session dynamic** command to check statistics about dynamic BFD sessions.
- Run the **display mpls bfd session** [**statistics** | [**protocol** { **ldp** | **cr-static** | **rsvp-te** }] | [**outgoing-interface** *interface-type interface-number*] | [**nexthop** *ip-address*] | [**fec** *fec-address*] | **verbose** | **monitor**] command to check information about the MPLS BFD session.

----End

Example

Run the **display bfd session all verbose** command on the ingress, and you can view that the status of the BFD sessions is Up and the links bound to the sessions are TE LSPs.

Run the **display bfd session passive-dynamic verbose** command on the egress, and you can view that the BFD session created on the egress is a multi-hop BFD session bound to the peer IP address.

Copyright © Huawei Technologies Co., Ltd.

3.19 Configuring Dynamic BFD for RSVP

This section describes how to configure a dynamic BFD session to detect faults in links between RSVP neighbors.

3.19.1 Establishing the Configuration Task

Before configuring dynamic BFD for RSVP, familiarize yourself with the applicable environment, complete the pre-configuration tasks, and obtain the data required for the configuration. This will help you complete the configuration task quickly and accurately.

Applicable Environment

BFD for RSVP is applied to a scenario where TE FRR is used and a Layer 2 device exists on the primary LSP between a PLR and its downstream neighbors. On a network where GR is enabled on the PLR and MP, BFD for RSVP is also recommended.

By default, the interval at which RSVP Hello messages are sent is 3 seconds. The interval at which a neighbor is declared Down is three times the interval at which RSVP Hello messages are sent. This allows devices to detect a fault in an RSVP neighbor at seconds level.

If a Layer 2 device exists on a link between RSVP neighboring nodes, the neighboring node cannot rapidly detect the fault after the link fails, resulting in a great loss of data.

BFD detects faults at millisecond level in protected links or nodes. BFD for RSVP rapidly detects faults in an RSVP neighbor, allowing packets to switch to a backup LSP rapidly.

NOTE

BFD for LSP can function properly though the forward path is an LSP and the backward path is an IP link. The forward path and the backward path must be established over the same link; otherwise, if a fault occurs, BFD cannot identify the faulty path. Before deploying BFD, ensure that the forward and backward paths are over the same link so that BFD can correctly identify the faulty path.

Pre-configuration Tasks

Before configuring BFD for RSVP, complete the following tasks:

- **Configuring RSVP-TE Tunnel**

Data Preparation

To configure BFD for RSVP, you need the following data.

No.	Data
1	Local minimum interval at which BFD packets are sent
2	Local minimum interval at which BFD packets are received
3	Local BFD detection multiplier

Copyright © Huawei Technologies Co., Ltd.

When modifying BFD session parameters, select the parameters for the BFD sessions shared by different protocols as follows:

- If the interval at which BFD packets are sent, interval at which BFD packets are received, and local detection multiplier are set globally and on the interfaces of a node, the parameters configured on the interfaces are used by a local RSVP protocol.
- If BFD for RSVP and other protocols share a BFD session on a node, the node selects the smallest time parameters among all protocols as the local parameters.
- The following formulas are applied:
  - Actual local sending interval = MAX { Configured local sending interval, Configured remote receiving interval }
  - Actual local receiving interval = MAX { Configured remote sending interval, Configured local receiving interval }
  - Actual local detection interval = Actual local receiving interval x Configured remote detection multiplier

3.19.2 Enabling BFD Globally

To configure dynamic BFD for RSVP, you must enable BFD on both ends of RSVP neighbors.

Context

Do as follows on the two RSVP neighboring nodes between which a Layer 2 device resides:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
bfd
```

BFD is enabled globally.

----End

3.19.3 Enabling BFD for RSVP

You can enable BFD for RSVP in either of two modes, that is, enabling BFD for RSVP globally and enabling BFD for RSVP on RSVP interfaces.

Context

Enabling BFD for RSVP in the following manners:

- **Enabling BFD for RSVP Globally** if most RSVP interfaces on a node need BFD for RSVP.
- **Enabling BFD for RSVP on the RSVP Interface** if certain RSVP interfaces on a node need BFD for RSVP.

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Enable BFD for RSVP globally.

  Do as follows on both RSVP neighboring nodes between which a Layer 2 device resides:

  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     mpls

     The MPLS view is displayed.
  3. Run:
     mpls rsvp-te bfd all-interfaces enable

     BFD for RSVP is enabled globally.

     After this command is run in the MPLS view, BFD for RSVP is enabled on all RSVP interfaces except the interfaces with BFD for RSVP that are blocked.
  4. (Optional) Block BFD for RSVP on the RSVP interfaces that need not BFD for RSVP.
     (1) Run:
     interface *interface-type interface-number*

     The view of the RSVP-TE-enabled interface is displayed.
     (2) Run:
     mpls rsvp-te bfd block

     BFD for RSVP is blocked on the interface.

- Enable BFD for RSVP on the RSVP interface.

  Do as follows on the two RSVP neighboring nodes between which a Layer 2 device resides:

  1. Run:
     system-view

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

     The view of the RSVP-TE-enabled interface is displayed.
  3. Run:
     mpls rsvp-te bfd enable

     BFD for RSVP is enabled on the RSVP interface.

----End

3.19.4 (Optional) Adjusting BFD Parameters

BFD parameters are adjusted on the ingress of a tunnel in either of two modes, that is, adjusting BFD parameters globally and on a tunnel interface.

Context

BFD for RSVP parameters are adjusted on the ingress of a TE tunnel either of the following modes:

Copyright © Huawei Technologies Co., Ltd.

- **Adjusting Global BFD Parameters** if most RSVP interfaces on a node use the same BFD parameters
- **Adjusting BFD Parameters on an RSVP Interface** if certain RSVP interfaces require BFD parameters different from global BFD parameters

Procedure

- Adjust global BFD parameters globally.

  Do as follows on the two RSVP neighboring nodes between which a Layer 2 device resides:

  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     mpls

     The MPLS view is displayed.
  3. Run:
     mpls rsvp-te bfd all-interfaces { **min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier* }*

     BFD parameters are set globally.

     NOTE

     Parameters are described as follows:

     - *tx-interval* indicates the Desired Min Tx Interval (DMTI), that is, the desired minimum interval for the local end sending BFD control packets.
     - *rx-interval* indicates the Required Min Rx Interval (RMRI), that is, the supported minimum interval for the local end receiving BFD control packets.
     - *multiplier* indicates the BFD detection multiplier.

     BFD detection parameters that take effect on the local node may be different from the configured parameters:

     - Actual local sending interval = MAX { Locally-configured DMTI, Remotely-configured RMRI }
     - Actual local receiving interval = MAX { Remotely-configured DMTI, Locally-configured RMRI }
     - Actual local detection interval = Actual local receiving interval x Configured remote detection multiplier

- Adjust BFD parameters on an RSVP interface.

  Do as follows on the two RSVP neighboring nodes between which a Layer 2 device resides:

  1. Run:
     system-view

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

     The view of the RSVP-TE-enabled interface is displayed.
  3. Run:
     mpls rsvp-te bfd { **min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier* }*

Copyright © Huawei Technologies Co., Ltd.

BFD parameters on the RSVP interface are adjusted.

----End

3.19.5 Checking the Configuration

After the configuration of dynamic BFD for RSVP, you can view that the status of a BFD session for RSVP is Up.

Procedure

- Run the **display mpls rsvp-te bfd session** { **all** | **interface** *interface-type interface-number* | **peer** *ip-address* } [**verbose**] command to check information about the BFD for RSVP session.
- Run the **display mpls rsvp-te** [**interface** [*interface-type interface-number*]] command to check the configuration of RSVP-TE.
- Run the **display mpls rsvp-te peer** [**interface** *interface-type interface-number*] command to check information about the RSVP neighbor.
- Run the **display mpls rsvp-te statistics** { **global** | **interface** [*interface-type interface-number*] } command to check statistics about RSVP-TE.

----End

Example

If the configurations are successful, you can view that the status of the BFD session for RSVP is Up.

NOTE

Information about the BFD session can be checked only after the BFD session parameters are configured and the session is created successfully.

3.20 Maintaining MPLS TE

This section describes how to clear operation information about MPLS TE, and reset the automatic bandwidth adjustment.

3.20.1 Checking the Connectivity of the TE Tunnel

This section describes how to check connectivity of a TE tunnel between the ingress and egress.

Prerequisite

The configurations of the TE tunnel detection are complete.

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 the connectivity of the TE tunnel between the ingress and egress.

Copyright © Huawei Technologies Co., Ltd.

- 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 trace the hops of a TE tunnel.

----End

Example

After configuring MPLS TE, run the **ping lsp** command on the ingress of the TE tunnel, and you can view whether or not the ingress pings the egress. If the ping fails, run the **tracert lsp** command to locate the fault. If the **hot-standby** parameter is specified, the hot-standby CR-LSP can be tested. If **draft6** is specified, the command is implemented in compliance with draft-ietf-mpls-lsp-ping-06. By default, the command is implemented in compliance with RFC 4379.

3.20.2 Checking a TE Tunnel By Using NQA

After the configuration of MPLS TE, you can use NQA to detect the connectivity and jitter of a TE tunnel.

Context

After configuring MPLS TE, you can use NQA to check the connectivity and jitter of the TE tunnel. For detailed configurations, see the chapter "NQA Configuration" in the Quidway S9300 Terabit Routing Switch *Configuration Guide - System Management*.

3.20.3 Checking Information About Tunnel Faults

If an RSVP-TE tunnel interface goes Down, you can view information about the fault.

Context

If an RSVP-TE tunnel interface goes Down, you can run the following command to view information about tunnel faults.

Procedure

Step 1 Run **display mpls te tunnel-interface last-error** [*tunnel-name*] command to view information about tunnel faults.

----End

Example

Run the **display mpls te tunnel-interface last-error** command on the ingress, and you can view last errors of a local node or last errors carried in a PathErr message received from the downstream node. The errors can be as follows:

- CSPF computation failures
- Errors that occur during the RSVP GR process
- 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 of the TE tunnel.

Copyright © Huawei Technologies Co., Ltd.

3.20.4 Clearing the Operation Information

This section describes how to clear statistics about RSVP-TE.

Context

Run the **reset** command in the user view to clear the operation information.

Procedure

Step 1 Run the **reset mpls rsvp-te statistics** { **global** | **interface** [*interface-type interface-number*] } command in the user view to clear statistics about RSVP-TE.

----End

3.20.5 Resetting the Tunnel Interface

By resetting a tunnel interface, you can activate configurations of the tunnel.

Context

To make the tunnel-related configuration take effect, you can run the **mpls te commit** command in the tunnel interface view and run the **reset** command in the user view.

NOTE

If the configuration is modified in the interface view of the TE tunnel but the **mpls te commit** command is not configured, the system cannot execute the **reset mpls te tunnel-interface tunnel** command to re-establish the tunnel.

Procedure

Step 1 Run the **reset mpls te tunnel-interface tunnel** *interface-number* command to reset the tunnel interface.

----End

3.20.6 Resetting the RSVP Process

By resetting the RSVP process, you can re-establish all RSVP CR-LSPs or verify the RSVP operation process.

Context

CAUTION

Resetting the RSVP process results in the release and reestablishment of all RSVP CR-LSPs.

To re-establish all RSVP CR-LSPs or verify the operation process of RSVP, run the following **reset** command.

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Run the **reset mpls rsvp-te** command to reset the RSVP process.

----End

3.20.7 Deleting or Resetting the Bypass Tunnel

In the scenario where MPLS TE Auto FRR is enabled, you can delete or re-establish a bypass tunnel.

Context

In a scenario where MPLS TE Auto FRR is used, you can run the following **reset** command to release or re-establish bypass tunnels.

Procedure

- Run the **reset mpls te auto-frr** { **lsp-id** *ingress-lsr-id tunnel-id* | **name** *bypass-tunnel-name* } command to delete or reset the Auto FRR bypass tunnel.

----End

3.20.8 Enabling the Trap Function on the LSP

By configuring the trap function on an LSP, you can notify the NMS of the changes of the LSP status.

Context

Run the following commands in the system view to notify the Network Management System (NMS) of the LSP status change.

By default, the trap function is disabled during the setup of the LDP LSP.

Procedure

- Run the **snmp-agent trap suppress feature-name lsp trap-name** { **mplsxcup** | **mplsxcdown** } **trap-interval** *trap-interval* [**max-trap-number** *max-trap-number*] command in the system view to enable the trap function for the LDP LSP and enable the debugging of excessive mplsxcup or mplsxcdown.

----End

3.20.9 Debugging MPLS TE

If a fault occurs, you can run the debug command in the user view to debug MPLS TE and view debugging information to locate the fault.

Context

If a fault occurs, run the following **debugging** commands in the user view to debug MPLS TE information and locate the fault.

For the procedure of outputting the debugging information, see the Quidway S9300 Terabit Routing Switch *Configuration Guide - System Management*.

Copyright © Huawei Technologies Co., Ltd.

CAUTION

Debugging affects system performance. After debugging, run the **undo debugging all** command to disable it immediately.

Procedure

- Run the **debugging mpls rsvp-te** { **all** | **authentication** | **bfd** | **bundle** | **encdec** | **error** | **graceful-restart** | **gr-hello** | **hello** | **hsb** | **lsp-id** | **main** | **msg-hex** | **packet-verbose** | **path** | **peer** | **perr** | **ptear** | **rconf** | **rerr** | **resv** | **rtear** | **socket** | **srefresh** | **timer** | **tool** | **traffic-control** | **tunnel-id** { *tunnel-id* | **all** } | **warning** } command to enable the debugging of RSVP-TE.
- Run the **debugging mpls te management** { **all** | **auto-frr** | **error** | **events** | **fast-reroute** | **interface** | **link-administration** | **lspid** { **all** | *ingress-lsr-id session-id local-lsp-id* } | **process** | **reoptimization** | **states** | **tunnel** | **warning** } command to enable the debugging of MPLS-TE management.
- Run the **debugging mpls te cspf** { **all** | **computation** | **errors** | **events** | **tedb** } command to enable the debugging of CSPF.
- Run the **debugging ospf** [*process-id*] **mpls-te** command to enable the debugging of OSPF TE.
- Run the **debugging isis traffic-eng** { **advertisement** | **event** } [*process-id* | **vpn-instance** *vpn-instance-name*] command to enable the debugging of IS-IS TE.

----End

3.21 Configuration Examples

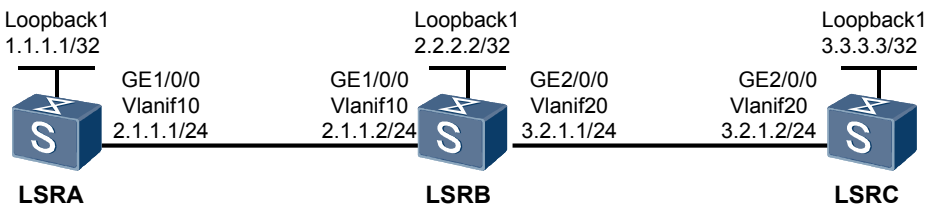
This section provides several configuration examples of MPLS TE.

3.21.1 Example for Configuring Static MPLS TE Tunnels

Networking Requirements

As shown in **Figure 3-2**, a static TE tunnel from LSRA to LSRC and a static TE tunnel from LSRC to LSRA need to be set up. The bandwidth of the two tunnels is 10 Mbit/s.

Figure 3-2 Networking diagram for configuring static CR-LSPs



Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and VLANIF interfaces.
2. Configure IP address of each interface on each node and the address of the loopback interface used as the LSR ID, and configure OSPF to advertise the network segments that the interfaces are connected to and the host route of the LSR ID.
3. Set the LSR ID and enable MPLS and MPLS TE globally on each node and each interface.
4. Set the maximum bandwidth and the maximum reservable bandwidth of the link on each outgoing interface of each node along the tunnel.
5. Create a tunnel interface, and specify the IP address, protocol, destination IP address, tunnel ID of the tunnel, and signaling type used for setting up the tunnel on the ingress node.
6. Configure the static LSP bound to the tunnel, specify the next hop address and outgoing label on the ingress node, specify the incoming interface, next hop address, and outgoing label on the transit node, and specify the incoming label and incoming interface on the egress node.

NOTE

- The value of the outgoing label of each node is the value of the incoming label of its next node.
- When running the **static-cr-lsp ingress** {**tunnel-interface tunnel** *tunnel-number* | *tunnel-name* } **destination** *destination-address* { **nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number* } **out-label** *out-label-value* [**bandwidth** [**ct0** | **ct1** | **ct2** | **ct3** | **ct4** | **ct5** | **ct6** | **ct7**] *bandwidth*] command to configure the ingress node of a CR-LSP, note that *tunnel-name* must be the same as the tunnel name created by using the **interface tunnel** *tunnel-number* command. *tunnel-name* is a string of case-sensitive characters without spaces. For example, the name of the tunnel created by using the **interface tunnel 2/0/0** command is Tunnel 2/0/0. In this case, the parameter of the ingress node of the static CR-LSP is Tunnel 2/0/0; otherwise, the tunnel cannot be created. There is no such limit on the transit node and egress node.

Data Preparation

To complete the configuration, you need the following data:

- OSPF process ID and area ID of each node
- Numbers of tunnel interfaces, IP addresses of tunnel interfaces, destination IP addresses, tunnel IDs, and signaling protocols (CR-static) on LSRA and LSRC
- Maximum bandwidth and maximum reservable bandwidth of each link
- Next hop address and outgoing label of the ingress node of the static CR-LSP
- Incoming interface, next hop address, and outgoing label of the transit node of the static CR-LSP
- Incoming interface of the egress node of the static CR-LSP

Procedure

Step 1 Create VLANs and VLANIF interfaces, and assign IP addresses to the VLANIF interfaces.

Configure LSRA.

```
<Quidway> system-view
[Quidway] sysname LSRA
[LSRA] interface loopback1
[LSRA-LoopBack1] ip address 1.1.1.1 32
[LSRA-LoopBack1] quit
```


Copyright © Huawei Technologies Co., Ltd.

```
[LSRA] interface gigabitethernet 1/0/0
[LSRA-GigabitEthernet1/0/0] port link-type access
[LSRA-GigabitEthernet1/0/0] quit
[LSRA] vlan 10
[LSRA-vlan10] port gigabitethernet 1/0/0
[LSRA-vlan10] quit
[LSRA] interface vlanif 10
[LSRA-Vlanif10] ip address 2.1.1.1 24
[LSRA-Vlanif10] quit
```

Configure LSRB.

```
<Quidway> system-view
[Quidway] sysname LSRB
[LSRB] interface loopback1
[LSRB-LoopBack1] ip address 2.2.2.2 32
[LSRB-LoopBack1] quit
[LSRB] interface gigabitethernet 1/0/0
[LSRB-GigabitEthernet1/0/0] port link-type access
[LSRB-GigabitEthernet1/0/0] quit
[LSRB] interface gigabitethernet 2/0/0
[LSRB-GigabitEthernet2/0/0] port link-type access
[LSRB-GigabitEthernet2/0/0] quit
[LSRB] vlan 10
[LSRB-vlan10] port gigabitethernet 1/0/0
[LSRB-vlan10] quit
[LSRB] interface vlanif 10
[LSRB-Vlanif10] ip address 2.1.1.2 24
[LSRB-Vlanif10] quit
[LSRB] vlan 20
[LSRB-vlan20] port gigabitethernet 2/0/0
[LSRB-vlan20] quit
[LSRB] interface vlanif 20
[LSRB-Vlanif20] ip address 3.2.1.1 24
```

Configure LSRC.

```
<Quidway> system-view
[Quidway] sysname LSRC
[LSRC] interface loopback1
[LSRC-LoopBack1] ip address 3.3.3.3 32
[LSRC-LoopBack1] quit
[LSRC] interface gigabitethernet 2/0/0
[LSRC-GigabitEthernet1/0/0] port link-type access
[LSRC-GigabitEthernet1/0/0] quit
[LSRC] vlan 20
[LSRC-vlan20] port gigabitethernet 1/0/0
[LSRC-vlan20] quit
[LSRC] interface vlanif 20
[LSRC-Vlanif20] ip address 3.2.1.2 24
[LSRC-Vlanif20] quit
```

Step 2 Configure the routing protocol to connect the LSRs at the network layer.

The configuration details are not mentioned here.

Step 3 Configure basic MPLS functions and enable MPLS TE.

Configure LSRA.

```
[LSRA] mpls lsr-id 1.1.1.1
[LSRA] mpls
[LSRA-mpls] mpls te
[LSRA] interface vlanif 10
[LSRA-Vlanif10] mpls
[LSRA-Vlanif10] mpls te
[LSRA-Vlanif10] quit
[LSRA-mpls] quit
```


Copyright © Huawei Technologies Co., Ltd.

The configurations of LSRB and LSRC are similar to the configuration of LSRA, and are not mentioned here.

Step 4 Configure MPLS TE tunnels.

Create an MPLS TE tunnel from LSRA to LSRC on LSRA.

```
[LSRA] interface tunnel 1/0/0
[LSRA-Tunnel1/0/0] ip address unnumbered interface loopback 1
[LSRA-Tunnel1/0/0] tunnel-protocol mpls te
[LSRA-Tunnel1/0/0] destination 3.3.3.3
[LSRA-Tunnel1/0/0] mpls te tunnel-id 100
[LSRA-Tunnel1/0/0] mpls te signal-protocol cr-static
[LSRA-Tunnel1/0/0] mpls te commit
[LSRA-Tunnel1/0/0] quit
```

Create an MPLS TE tunnel from LSRC to LSRA on LSRC.

```
[LSRC] interface tunnel 2/0/0
[LSRC-Tunnel2/0/0] ip address unnumbered interface loopback 1
[LSRC-Tunnel2/0/0] tunnel-protocol mpls te
[LSRC-Tunnel2/0/0] destination 1.1.1.1
[LSRC-Tunnel2/0/0] mpls te tunnel-id 200
[LSRC-Tunnel2/0/0] mpls te signal-protocol cr-static
[LSRC-Tunnel2/0/0] mpls te commit
[LSRC-Tunnel2/0/0] quit
```

Step 5 Create a static CR-LSP from LSRA to LSRC.

Configure LSRA as the ingress node of the static CR-LSP.

```
[LSRA] static-cr-lsp ingress tunnel-interface tunnel 1/0/0 destination 3.3.3.3
nexthop 2.1.1.2 out-label 20 bandwidth ct0 10000
```

Configure LSRB as the transit node of the static CR-LSP.

```
[LSRB] static-cr-lsp transit tunnel1/0/0 incoming-interface vlanif 10 in-label 20
nexthop 3.2.1.2 out-label 30 bandwidth ct0 10000
```

Configure LSRC as the ingress node of the static CR-LSP.

```
[LSRC] static-cr-lsp egress tunnel1/0/0 incoming-interface vlanif 20 in-label 30
```

Step 6 Create a static CR-LSP from LSRC to LSRA.

Configure LSRC as the ingress node of the static CR-LSP.

```
[LSRC] static-cr-lsp ingress tunnel-interface tunnel 2/0/0 destination 1.1.1.1
nexthop 3.2.1.1 out-label 120 bandwidth ct0 10000
```

Configure LSRB as the transit node of the static CR-LSP.

```
[LSRB] static-cr-lsp transit tunnel2/0/0 incoming-interface vlanif 20 in-label 120
nexthop 2.1.1.1 out-label 130 bandwidth ct0 10000
```

Configure LSRA as the egress node of the static CR-LSP.

```
[LSRA] static-cr-lsp egress tunnel2/0/0 incoming-interface vlanif 10 in-label 130
```

Step 7 Verify the configuration.

After the configuration, run the **display interface tunnel** command on LSRA, and you can view that the status of the tunnel interface is Up.

Run the **display mpls te tunnel** command on each node, and you can view the establishment of MPLS TE tunnels.

```
[LSRA] display mpls te tunnel
LSP-Id                  Destination           In/Out-If
```


Copyright © Huawei Technologies Co., Ltd.

```
1.1.1.1:100:1             3.3.3.3              -/Vlanif10
-                         -                    Vlanif10/-

[LSRB] display mpls te tunnel
LSP-Id                     Destination            In/Out-If
-                          -                      Vlanif10/Vlanif20
-                          -                      Vlanif20/Vlanif10

[LSRC] display mpls te tunnel
LSP-Id                    Destination          In/Out-If
3.3.3.3:200:1             1.1.1.1              -/Vlanif20
-                         -                    Vlanif20/-
```

Run the **display mpls lsp** or **display mpls static-cr-lsp** command on each node, and you can view the establishment of static CR-LSPs.

Check the configuration on LSRA.

```
[LSRA] display mpls lsp
------------------------------------------------------------------------------
                 LSP Information: STATIC CRLSP
------------------------------------------------------------------------------
FEC                In/Out Label  In/Out IF                      Vrf Name
3.3.3.3/32         NULL/20       -/Vlanif10
-/-                130/NULL      Vlanif10/-


[LSRA] display mpls static-cr-lsp
TOTAL          : 2     STATIC CRLSP(S)
UP             : 2     STATIC CRLSP(S)
DOWN           : 0     STATIC CRLSP(S)
Name            FEC              I/O Label  I/O If                    Stat
Tunnel1/0/0    3.3.3.3/32        NULL/20    -/Vlanif10                Up
tunnel2/0/0    -/-               130/NULL   Vlanif10/-                Up
```

Check the configuration on LSRB.

```
[LSRB] display mpls lsp
------------------------------------------------------------------------------
                 LSP Information: STATIC CRLSP
------------------------------------------------------------------------------
FEC                In/Out Label  In/Out IF                      Vrf Name
-/-                20/30         Vlanif10/Vlanif20
-/-                120/130       Vlanif20/Vlanif10

[LSRB] display mpls static-cr-lsp
TOTAL          : 2     STATIC CRLSP(S)
UP             : 2     STATIC CRLSP(S)
DOWN           : 0     STATIC CRLSP(S)
Name            FEC              I/O Label  I/O If                     Stat
tunnel1/0/0    -/-               20/30      Vlanif10/Vlanif20          Up
tunnel2/0/0    -/-               120/130    Vlanif20/Vlanif10          Up
```

Check the configuration on LSRC.

```
[LSRC] display mpls lsp
------------------------------------------------------------------------------
                 LSP Information: STATIC CRLSP
------------------------------------------------------------------------------
FEC                In/Out Label  In/Out IF                      Vrf Name
1.1.1.1/32         NULL/120      -/Vlanif20
-/-                30/NULL       Vlanif20/-


[LSRC] display mpls static-cr-lsp
TOTAL          : 2     STATIC CRLSP(S)
UP             : 2     STATIC CRLSP(S)
DOWN           : 0     STATIC CRLSP(S)
Name            FEC                I/O Label  I/O If                    Stat
```


Copyright © Huawei Technologies Co., Ltd.

```
Tunnel2/0/0    1.1.1.1/32          NULL/120   -/Vlanif20               Up
tunnel1/0/0    -/-                 30/NULL    Vlanif20/-               Up
```

When the static CR-LSP is used to establish the MPLS TE tunnel, the packets on the transit node and the egress node are forwarded according to the specified incoming label and outgoing label. Therefore, information such as FEC is null is shown in the display of LSRB and LSRC.

----End

Configuration Files

- Configuration file of LSRA

```
#
 sysname LSRA
#
 vlan batch 10
#
 mpls lsr-id 1.1.1.1
 mpls
  mpls te
#
interface Vlanif10
 ip address 2.1.1.1 255.255.255.0
 mpls
 mpls te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te tunnel-id 100
 mpls te signal-protocol cr-static
 mpls te commit
#
ospf 1
 area 0.0.0.0
  network 2.1.1.0 0.0.0.255
  network 1.1.1.1 0.0.0.0
#
static-cr-lsp ingress tunnel-interface Tunnel1/0/0 destination 3.3.3.3 nexthop
2.1.1.2 out-label 20 bandwidth ct0 10000
static-cr-lsp egress tunnel2/0/0 incoming-interface vlanif 10 in-label 130
#
return
```

- Configuration file of LSRB

```
#
 sysname LSRB
#
 vlan batch 10 20
#
 mpls lsr-id 2.2.2.2
 mpls
  mpls te
#
interface Vlanif10
 ip address 2.1.1.2 255.255.255.0
 mpls
 mpls te
#
```


Copyright © Huawei Technologies Co., Ltd.

```
interface Vlanif20
 ip address 3.2.1.1 255.255.255.0
 mpls
 mpls te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 2.1.1.0 0.0.0.255
  network 3.2.1.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
#
static-cr-lsp transit tunnel1/0/0 incoming-interface Vlanif 10 in-label 20
nexthop 3.2.1.2 out-label 30 bandwidth ct0 10000
static-cr-lsp transit tunnel2/0/0 incoming-interface Vlanif20 in-label 120
nexthop 2.1.1.1 out-label 130 bandwidth ct0 10000
#
return
```

- Configuration file of LSRC

```
#
 sysname LSRC
#
 vlan batch 20
#
 mpls lsr-id 3.3.3.3
 mpls
  mpls te
#
interface Vlanif20
 ip address 3.2.1.2 255.255.255.0
 mpls
 mpls te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
interface Tunnel2/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 1.1.1.1
 mpls te signal-protocol cr-static
 mpls te tunnel-id 200
 mpls te commit
#
ospf 1
 area 0.0.0.0
  network 3.2.1.0 0.0.0.255
  network 3.3.3.3 0.0.0.0
#
static-cr-lsp ingress tunnel-interface Tunnel2/0/0 destination 1.1.1.1 nexthop
3.2.1.1 out-label 120 bandwidth ct0 10000
static-cr-lsp egress tunnel1/0/0 incoming-interface vlanif 20 in-label 30
#
```


Copyright © Huawei Technologies Co., Ltd.

```
return
```

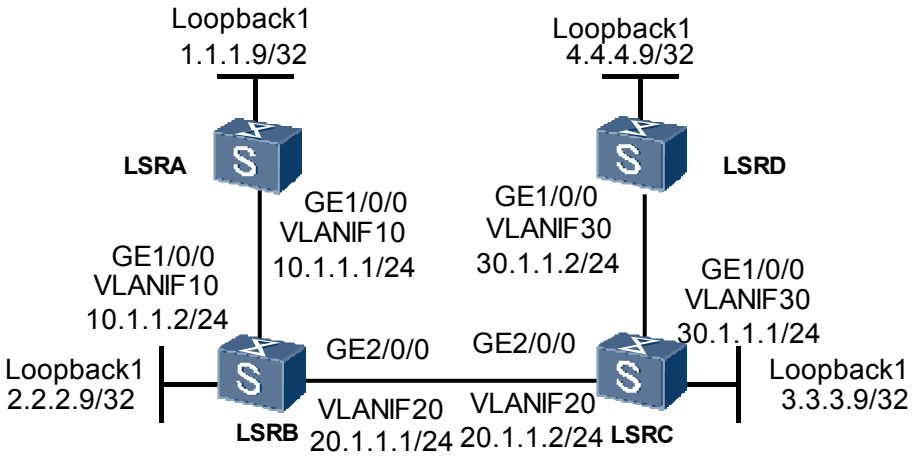
3.21.2 Example for Configuring an RSVP-TE Tunnel

Networking Requirements

As shown in **Figure 3-3**, IS-IS is run on LSRA, LSRB, LSRC, and LSRD. They are all Level 2 devices.

RSVP-TE is used to establish a TE tunnel from LSRA to LSRD.

Figure 3-3 Networking diagram for configuring an RSVP-TE tunnel



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and VLANIF interfaces.
2. Configure the IP address of each interface and configure the loopback address as the LSR ID.
3. Enable global ISIS, set the NET, change the cost type to enable ISIS TE, and enable ISIS on each interface, including the loopback interface.
4. Set the LSR ID and enable MPLS, MPLS TE, MPLS RSVP-TE, and MPLS CSPF globally.
5. Enable MPLS, MPLS TE, and MPLS RSVP-TE on each interface.
6. Create a tunnel interface and specify the IP address, tunneling protocol, destination IP address, tunnel ID, dynamic signaling protocol RSVP-TE and bandwidth for the tunnel on the ingress node.

Data Preparation

To complete the configuration, you need the following data:

- IS-IS area ID, originating system ID, and IS-IS level of each node

Copyright © Huawei Technologies Co., Ltd.

- Maximum bandwidth and maximum reservable bandwidth of the link along the tunnel
- Number of the tunnel interface, IP address, destination IP address, tunnel ID, signaling protocol (RSVP-TE), and tunnel bandwidth

Procedure

Step 1 Create VLANs and VLANIF interfaces, and assign IP addresses to the VLANIF interfaces.

Configure LSRA.

```
<Quidway> system-view
[Quidway] sysname LSRA
[LSRA] interface loopback1
[LSRA-LoopBack1] ip address 1.1.1.9 32
[LSRA-LoopBack1] quit
[LSRA] interface gigabitethernet1/0/0
[LSRA-GigabitEthernet1/0/0] port link-type access
[LSRA-GigabitEthernet1/0/0] quit
[LSRA] vlan 10
[LSRA-vlan10] port gigabitethernet1/0/0
[LSRA-vlan10] quit
[LSRA] interface vlanif 10
[LSRA-Vlanif10] ip address 10.1.1.1 24
[LSRA-Vlanif10] quit
```

Configure LSRB.

```
<Quidway> system-view
[Quidway] sysname LSRB
[LSRB] interface loopback1
[LSRB-LoopBack1] ip address 2.2.2.9 32
[LSRB-LoopBack1] quit
[LSRB] interface gigabitethernet1/0/0
[LSRB-GigabitEthernet1/0/0] port link-type access
[LSRB-GigabitEthernet1/0/0] quit
[LSRB] vlan 10
[LSRB-vlan10] port gigabitethernet1/0/0
[LSRB-vlan10] quit
[LSRB] interface gigabitethernet2/0/0
[LSRB-GigabitEthernet2/0/0] port link-type access
[LSRB-GigabitEthernet2/0/0] quit
[LSRB] vlan 20
[LSRB-vlan20] port gigabitethernet2/0/0
[LSRB-vlan20] quit
[LSRB] interface vlanif 10
[LSRB-Vlanif10] ip address 10.1.1.2 24
[LSRB-Vlanif10] quit
[LSRB] interface vlanif 20
[LSRB-Vlanif20] ip address 20.1.1.1 24
[LSRB-Vlanif20] quit
```

Configure LSRC.

```
<Quidway> system-view
[Quidway] sysname LSRC
[LSRC] interface loopback1
[LSRC-LoopBack1] ip address 3.3.3.9 32
[LSRC-LoopBack1] quit
[LSRC] vlan 20
[LSRC] interface gigabitethernet2/0/0
[LSRC-GigabitEthernet2/0/0] port link-type access
[LSRC-GigabitEthernet2/0/0] quit
[LSRC-vlan20] port gigabitethernet2/0/0
[LSRC-vlan20] quit
[LSRC] interface gigabitethernet1/0/0
[LSRC-GigabitEthernet1/0/0] port link-type access
[LSRC-GigabitEthernet1/0/0] quit
```


Copyright © Huawei Technologies Co., Ltd.

```
[LSRC] vlan 30
[LSRC-vlan30] port gigabitethernet1/0/0
[LSRC-vlan30] quit
[LSRC] interface vlanif 20
[LSRC-Vlanif20] ip address 20.1.1.2 24
[LSRC-Vlanif20] quit
[LSRC] interface vlanif 30
[LSRC-Vlanif30] ip address 30.1.1.1 24
[LSRC-Vlanif30] quit
```

Configure LSRD.

```
<Quidway> system-view
[Quidway] sysname LSRD
[LSRD] interface loopback1
[LSRD-LoopBack1] ip address 4.4.4.9 32
[LSRD-LoopBack1] quit
[LSRD] vlan 30
[LSRD] interface gigabitethernet1/0/0
[LSRD-GigabitEthernet1/0/0] port link-type access
[LSRD-GigabitEthernet1/0/0] quit
[LSRD-vlan30] port gigabitethernet1/0/0
[LSRD-vlan30] quit
[LSRD] interface vlanif 30
[LSRD-Vlanif30] ip address 30.1.1.2 24
[LSRD-Vlanif30] quit
```

Step 2 Configure IS-IS to advertise routes.

Configure LSRA.

```
[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 vlanif 10
[LSRA-Vlanif10] isis enable 1
[LSRA-Vlanif10] quit
[LSRA] interface loopback 1
[LSRA-LoopBack1] isis enable 1
[LSRA-LoopBack1] quit
```

Configure LSRB.

```
[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 vlanif 10
[LSRB-Vlanif10] isis enable 1
[LSRB-Vlanif10] quit
[LSRB] interface vlanif 20
[LSRB-Vlanif20] isis enable 1
[LSRB-Vlanif20] quit
[LSRB] interface loopback 1
[LSRB-LoopBack1] isis enable 1
[LSRB-LoopBack1] quit
```

Configure LSRC.

```
[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 vlanif 20
[LSRC-Vlanif20] isis enable 1
[LSRC-Vlanif20] quit
[LSRC] interface vlanif 30
[LSRC-Vlanif30] isis enable 1
[LSRC-Vlanif30] quit
```


Copyright © Huawei Technologies Co., Ltd.

```
[LSRC] interface loopback 1
[LSRC-LoopBack1] isis enable 1
[LSRC-LoopBack1] quit
```

Configure LSRD.

```
[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 vlanif 30
[LSRD-Vlanif30] isis enable 1
[LSRD-Vlanif30] quit
[LSRD] interface loopback 1
[LSRD-LoopBack1] isis enable 1
[LSRD-LoopBack1] quit
```

After the configuration, run the **display ip routing-table** command on each node, and you can view that the nodes learn the routes from each other. Take the display on LSRA as an example.

```
[LSRA] display ip routing-table
Route Flags: R - relied, D - download to fib
------------------------------------------------------------------------------
Routing Tables: 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       InLoopBack1
      2.2.2.9/32  ISIS   15   10       D    10.1.1.2       Vlanif10
      3.3.3.9/32  ISIS   15   20       D    10.1.1.2       Vlanif10
      4.4.4.9/32  ISIS   15   30       D    10.1.1.2       Vlanif10
     10.1.1.0/24  Direct 0    0        D     10.1.1.1      Vlanif10
     10.1.1.1/32  Direct 0    0        D     127.0.0.1     InLoopBack1
     20.1.1.0/24  ISIS   15   20       D     10.1.1.2      Vlanif10
     30.1.1.0/24  ISIS   15   30       D     10.1.1.2      Vlanif10
    127.0.0.0/8   Direct 0    0        D     127.0.0.1     InLoopBack1
    127.0.0.1/32  Direct 0    0        D     127.0.0.1     InLoopBack1
```

Step 3 Configure basic MPLS functions and enable MPLS TE, RSVP-TE, and CSPF.

Enable MPLS, MPLS TE, and RSVP-TE globally on each node, enable MPLS, MPLS TE, and RSVP-TE on all tunnel interfaces, and enable CSPF in the system view on the ingress node.

Configure LSRA.

```
[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 vlanif 10
[LSRA-Vlanif10] mpls
[LSRA-Vlanif10] mpls te
[LSRA-Vlanif10] mpls te bandwidth max-reservable-bandwidth 1000
[LSRA-Vlanif10] mpls te bandwidth bc0 1000
[LSRA-Vlanif10] mpls rsvp-te
[LSRA-Vlanif10] quit
```

Configure LSRB.

```
[LSRB] mpls lsr-id 2.2.2.9
[LSRB] mpls
[LSRB-mpls] mpls te
[LSRB-mpls] mpls rsvp-te
[LSRB-mpls] mpls te cspf
[LSRB-mpls] quit
[LSRB] interface vlanif 10
[LSRB-Vlanif10] mpls
[LSRB-Vlanif10] mpls te
```


Copyright © Huawei Technologies Co., Ltd.

```
[LSRB-Vlanif10] mpls te bandwidth max-reservable-bandwidth 1000
[LSRB-Vlanif10] mpls te bandwidth bc0 1000
[LSRB-Vlanif10] mpls rsvp-te
[LSRB-Vlanif10] quit
[LSRB] interface vlanif 20
[LSRB-Vlanif20] mpls
[LSRB-Vlanif20] mpls te
[LSRB-Vlanif20] mpls te bandwidth max-reservable-bandwidth 1000
[LSRB-Vlanif20] mpls te bandwidth bc0 1000
[LSRB-Vlanif20] mpls rsvp-te
[LSRB-Vlanif20] quit
```

Configure LSRC.

```
[LSRC] mpls lsr-id 3.3.3.9
[LSRC] mpls
[LSRC-mpls] mpls te
[LSRC-mpls] mpls te cspf
[LSRC-mpls] mpls rsvp-te
[LSRC-mpls] quit
[LSRC] interface vlanif 20
[LSRC-Vlanif20] mpls
[LSRC-Vlanif20] mpls te
[LSRC-Vlanif20] mpls te bandwidth max-reservable-bandwidth 1000
[LSRC-Vlanif20] mpls te bandwidth bc0 1000
[LSRC-Vlanif20] mpls rsvp-te
[LSRC-Vlanif20] quit
[LSRC] interface vlanif 30
[LSRC-Vlanif30] mpls
[LSRC-Vlanif30] mpls te
[LSRC-Vlanif30] mpls te bandwidth max-reservable-bandwidth 1000
[LSRC-Vlanif30] mpls te bandwidth bc0 1000
[LSRC-Vlanif30] mpls rsvp-te
[LSRC-Vlanif30] quit
```

Configure LSRD.

```
[LSRD] mpls lsr-id 4.4.4.9
[LSRD] mpls
[LSRD-mpls] mpls te
[LSRD-mpls] mpls te cspf[LSRD-mpls] mpls rsvp-te
[LSRD-mpls] quit
[LSRD] interface vlanif 30
[LSRD-Vlanif30] mpls
[LSRD-Vlanif30] mpls te
[LSRD-Vlanif30] mpls te bandwidth max-reservable-bandwidth 1000
[LSRD-Vlanif30] mpls te bandwidth bc0 1000
[LSRD-Vlanif30] mpls rsvp-te
[LSRD-Vlanif30] quit
```

Step 4 Configure IS-IS TE.

Configure LSRA.

```
[LSRA] isis 1
[LSRA-isis-1] cost-style wide
[LSRA-isis-1] traffic-eng level-2
[LSRA-isis-1] quit
```

Configure LSRB.

```
[LSRB] isis 1
[LSRB-isis-1] cost-style wide
[LSRB-isis-1] traffic-eng level-2
[LSRB-isis-1] quit
```

Configure LSRC.

```
[LSRC] isis 1
[LSRC-isis-1] cost-style wide
```


Copyright © Huawei Technologies Co., Ltd.

```
[LSRC-isis-1] traffic-eng level-2
[LSRC-isis-1] quit
```

Configure LSRD.

```
[LSRD] isis 1
[LSRD-isis-1] cost-style wide
[LSRD-isis-1] traffic-eng level-2
[LSRD-isis-1] quit
```

Step 5 Configure the MPLS TE tunnel interface.

Create tunnel interfaces on the ingress node, and configure IP addresses for the tunnel interfaces, tunneling protocol, destination IP address, tunnel ID, dynamic signaling protocol, and tunnel bandwidth, and make the configurations take effect by using the **mpls te commit** command.

Configure LSRA.

```
[LSRA] interface tunnel 1/0/0
[LSRA-Tunnel1/0/0] ip address unnumbered interface loopback 1
[LSRA-Tunnel1/0/0] tunnel-protocol mpls te
[LSRA-Tunnel1/0/0] destination 4.4.4.9
[LSRA-Tunnel1/0/0] mpls te tunnel-id 100
[LSRA-Tunnel1/0/0] mpls te signal-protocol rsvp-te
[LSRA-Tunnel1/0/0] mpls te commit
[LSRA-Tunnel1/0/0] quit
```

Step 6 Verify the configuration.

After the configuration, run the **display interface tunnel** command on LSRA, and you can view that the status of the tunnel interface is Up.

```
[LSRA] display interface tunnel
Tunnel1/0/0 current state : UP
Line protocol current state : UP
Last up time: 2009-05-30, 02:39:24
Description:HUAWEI, Quidway Series, Tunnel1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is unnumbered, using address of LoopBack10(1.1.1.9/32)
Encapsulation is TUNNEL, loopback not set
Tunnel destination 4.4.4.9
Tunnel up/down statistics 1
Tunnel protocol/transport MPLS/MPLS, ILM is available,
primary tunnel id is 0x10001, secondary tunnel id is 0x0
    300 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets output,  0 bytes
    0 output error
```

Run the **display mpls te tunnel-interface** command on LSRA, and you can view detailed information about the tunnel.

```
[LSRA] display mpls te tunnel-interface
  Tunnel Name         :  Tunnel1/0/0
  Tunnel State Desc   :  CR-LSP is Up
  Tunnel Attributes   :
    LSP ID              :  1.1.1.9:0
    Session ID          :  100
    Admin State         :  UP                   Oper State   :  UP
    Ingress LSR ID      :  1.1.1.9              Egress LSR ID:  4.4.4.9
    Signaling Protocol  :  RSVP                 Resv Style   :  SE
    Class Type          :  CLASS 0              Tunnel BW    :  0 kbps
    Reserved BW         :  0 kbps
    Setup Priority      :  7                    Hold Priority:  7
    Hop Limit           :  -
    Secondary Hop Limit :  -
    BestEffort Hop Limit:  -
    Affinity Prop/Mask  :  0x0/0x0
```


Copyright © Huawei Technologies Co., Ltd.

```
Explicit Path Name  :  -
Secondary Affinity Prop/Mask:  0x0/0x0
Secondary Explicit Path Name:  -
BestEffort Affinity Prop/Mask:  0x0/0x0
Tie-Breaking Policy :  None
Metric Type         :  None
Record Route        :  Disabled             Record Label :  Disabled
FRR Flag            :  Disabled             BackUpBW Flag:  Not Supported
BackUpBW Type       :  -                    BackUpBW     :  -
Route Pinning       :  Disabled
Retry Limit         :  5                    Retry Interval:  10 sec
Reopt               :  Disabled             Reopt Freq   :  -
Back Up Type        :  None
Back Up LSPID       :  -
Auto BW             :  Disabled             Auto BW Freq :  -
Min BW              :  -                    Max BW       :  -
Current Collected BW:  -
Interfaces Protected:  -
Car Policy          :  Disabled
Tunnel  Group       :  Primary
Primary Tunnel Sum  :  -
Primary Tunnel      :  -
Backup  Tunnel      :  -
IPTN    InLabel     :  -
Group   Status      :  Up
Oam     Status      :  -
Bfd Capability      :  Disabled
BestEffort          :  Disabled             IsBestEffortPath:  Non-existent
```

Run the **display mpls te cspf tedb all** command on LSRA, and you can view link information in the TEDB.

```
[LSRA] display mpls te cspf tedb all
Maximum Node Supported: 128              Maximum Link Supported: 256
Current Total Node Number: 4             Current Total Link Number: 6
Id     Router-Id     IGP      Process-Id   Area         Link-Count
1      3.3.3.9       ISIS     1            Level-2       2
2      2.2.2.9       ISIS     1            Level-2       2
3      4.4.4.9       ISIS     1            Level-2       1
4      1.1.1.9       ISIS     1            Level-2       1
```

----End

Configuration Files

- Configuration file of LSRA

```
#
 sysname LSRA
#
 vlan batch 10
#
 mpls lsr-id 1.1.1.9
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 00.0005.0000.0000.0001.00
 traffic-eng level-2
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
```


Copyright © Huawei Technologies Co., Ltd.

```
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
 isis enable 1
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 4.4.4.9
 mpls te tunnel-id 100
 mpls te commit
#
return
```

- Configuration file of LSRB

```
#
 sysname LSRB
#
 vlan batch 10 20
#
 mpls lsr-id 2.2.2.9
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 00.0005.0000.0000.0002.00
 traffic-eng level-2
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif20
 ip address 20.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of LSRC

```
#
 sysname LSRC
#
 vlan batch 20 30
```


Copyright © Huawei Technologies Co., Ltd.

```
#
 mpls lsr-id 3.3.3.9
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 00.0005.0000.0000.0003.00
 traffic-eng level-2
#
interface Vlanif20
 ip address 20.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif30
 ip address 30.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 30
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of LSRD

```
#
 sysname LSRD
#
 vlan batch 30
#
 mpls lsr-id 4.4.4.9
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 00.0005.0000.0000.0004.00
traffic-eng level-2
#
interface Vlanif30
 ip address 30.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 30
#
```


Copyright © Huawei Technologies Co., Ltd.

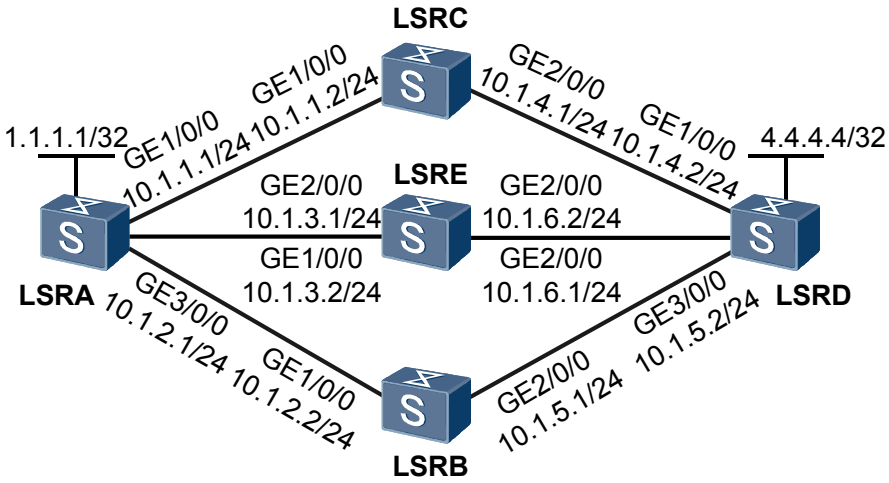
```
interface LoopBack1
 ip address 4.4.4.9 255.255.255.255
 isis enable 1
#
return
```

3.21.3 Example for Setting Up CR-LSPs by Using CR-LSP Attribute Templates

Networking Requirements

As shown in **Figure 3-4**, a primary CR-LSP with LSRA being the ingress and LSRD being the egress needs to be set up, and the primary CR-LSP needs to be configured with the hot-standby CR-LSP and ordinary backup CR-LSP. In this manner, when the primary CR-LSP fails, the traffic can be switched to the hot-standby CR-LSP or ordinary backup CR-LSP.

Figure 3-4 Networking diagram of setting up CR-LSPs by using CR-LSP attribute templates



Switch	Interface	VLANIF interface	IP address
LSRA	GigabitEthernet1/0/0	VLANIF 10	10.1.1.1/24
LSRA	GigabitEthernet2/0/0	VLANIF 20	10.1.3.1/24
LSRA	GigabitEthernet3/0/0	VLANIF 30	10.1.2.1/24
LSRB	GigabitEthernet1/0/0	VLANIF 30	10.1.2.2/24
LSRB	GigabitEthernet2/0/0	VLANIF 40	10.1.5.1/24
LSRC	GigabitEthernet1/0/0	VLANIF 10	10.1.1.2/24
LSRC	GigabitEthernet2/0/0	VLANIF 60	10.1.4.1/24
LSRD	GigabitEthernet1/0/0	VLANIF 60	10.1.4.2/24
LSRD	GigabitEthernet2/0/0	VLANIF 50	10.1.6.2/24
LSRD	GigabitEthernet3/0/0	VLANIF 40	10.1.5.2/24
LSRE	GigabitEthernet1/0/0	VLANIF 20	10.1.3.2/24
LSRE	GigabitEthernet2/0/0	VLANIF 50	10.1.6.1/24

Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure IP addresses and a routing protocol for interfaces so that they can communicate at the network layer.
2. Enable MPLS and MPLS TE in the system view and in each interface view.
3. Configure CR-LSP attribute templates on the ingress of the CR-LSPs.
4. Create the CR-LSPs on the TE tunnel interface by using the CR-LSP attribute templates.

Data Preparation

To complete the configuration, you need the following data:

- LSR ID of each router
- Name of each CR-LSP attribute template and attributes of each template
- IP address of the tunnel interface, destination address of the tunnel, and tunnel ID

Procedure

Step 1 Configure VLANs that interfaces belong to.

```
<Quidway> system-view
[Quidway] sysname LSRA
[LSRA] vlan batch 10 20 30
[LSRA] interface gigabitEthernet 1/0/0
[LSRA-GigabitEthernet1/0/0] port hybrid pvid vlan 10
[LSRA-GigabitEthernet1/0/0] port hybrid untagged vlan 10
[LSRA-GigabitEthernet1/0/0] quit
[LSRA] interface gigabitEthernet 2/0/0
[LSRA-GigabitEthernet2/0/0] port hybrid pvid vlan 20
[LSRA-GigabitEthernet2/0/0] port hybrid untagged vlan 20
[LSRA-GigabitEthernet2/0/0] quit
[LSRA] interface gigabitEthernet 3/0/0
[LSRA-GigabitEthernet3/0/0] port hybrid pvid vlan 30
[LSRA-GigabitEthernet3/0/0] port hybrid untagged vlan 30
[LSRA-GigabitEthernet3/0/0] quit
```

The configurations of LSRB, LSRC, LSRD and LSRE are similar to the configuration of LSRA, and are not mentioned here.

Step 2 Configure IP addresses and an IGP for the interfaces so that they can communicate at the network layer.

The configuration details are not mentioned here.

Step 3 Configure the LSR ID for each router, and enable MPLS and MPLS TE in the system view and in each interface view on each router.

Configure LSRA.

```
<LSRA> system-view
[LSRA] mpls lsr-id 1.1.1.1
[LSRA] mpls
[LSRA-mpls] mpls te
[LSRA-mpls] mpls rsvp-te
[LSRA-mpls] quit
[LSRA] interface vlanif 10
[LSRA-Vlanif10] mpls
```


Copyright © Huawei Technologies Co., Ltd.

```
[LSRA-Vlanif10] mpls te
[LSRA-Vlanif10] mpls rsvp-te
[LSRA-Vlanif10] quit
[LSRA] interface vlanif 20
[LSRA-Vlanif20] mpls
[LSRA-Vlanif20] mpls te
[LSRA-Vlanif20] mpls rsvp-te
[LSRA-Vlanif20] quit
[LSRA] interface vlanif 30
[LSRA-Vlanif30] mpls
[LSRA-Vlanif30] mpls te
[LSRA-Vlanif30] mpls rsvp-te
[LSRA-Vlanif30] quit
```

NOTE

The configurations of LSRB, LSRC, LSRD, and LSRE are similar to those of LSRA, and are not mentioned here.

Step 4 Configure CR-LSP attribute templates and their explicit paths.

On LSRA, configure the explicit path named up_path as LSRA->LSRC->LSRD.

```
[LSRA] explicit-path up_path
[LSRA-explicit-path-up_path] next hop 10.1.1.2
[LSRA-explicit-path-up_path] next hop 10.1.4.2
[LSRA-explicit-path-up_path] quit
```

On LSRA, configure the explicit path named down_path as LSRA->LSRB->LSRD.

```
[LSRA] explicit-path down_path
[LSRA-explicit-path-down_path] next hop 10.1.2.2
[LSRA-explicit-path-down_path] next hop 10.1.5.2
[LSRA-explicit-path-down_path] quit
```

On LSRA, configure the explicit path named middle_path as LSRA->LSRE->LSRD.

```
[LSRA] explicit-path middle_path
[LSRA-explicit-path-middle_path] next hop 10.1.3.2
[LSRA-explicit-path-middle_path] next hop 10.1.6.2
[LSRA-explicit-path-middle_path] quit
```

On LSRA, configure the CR-LSP attribute template named lsp_attribute_1.

```
[LSRA] lsp-attribute lsp_attribute_1
[LSRA-lsp-attribuLSP_attribute_1] explicit-path up_path
[LSRA-lsp-attribuLSP_attribute_1] priority 5 5
[LSRA-lsp-attribuLSP_attribute_1] hop-limit 12
[LSRA-lsp-attribuLSP_attribute_1] commit
```

On LSRA, configure the CR-LSP attribute template named lsp_attribute_2.

```
[LSRA] lsp-attribute lsp_attribute_2
[LSRA-lsp-attribuLSP_attribute_2] explicit-path down_path
[LSRA-lsp-attribuLSP_attribute_2] priority 5 5
[LSRA-lsp-attribuLSP_attribute_2] hop-limit 15
[LSRA-lsp-attribuLSP_attribute_2] commit
```

On LSRA, configure the CR-LSP attribute template named lsp_attribute_3.

```
[LSRA] lsp-attribute lsp_attribute_3
[LSRA-lsp-attribuLSP_attribute_3] explicit-path middle_path
[LSRA-lsp-attribuLSP_attribute_3] priority 5 5
[LSRA-lsp-attribuLSP_attribute_3] commit
```

NOTE

The priorities of the CR-LSP attribute templates configured on the same tunnel interface must be the same.

Step 5 Set up the CR-LSP with LSRA being the ingress and LSRD being the egress by using the CR-LSP attribute template.

Copyright © Huawei Technologies Co., Ltd.

Set up the CR-LSP with LSRA being the ingress and LSRD being the egress.

```
[LSRA] interface tunnel1/0/0
[LSRA-Tunnel1/0/0] tunnel-protocol mpls te
[LSRA-Tunnel1/0/0] destination 4.4.4.4
[LSRA-Tunnel1/0/0] mpls te tunnel-id 100
[LSRA-Tunnel1/0/0] mpls te primary-lsp-constraint lsp-attribute lsp_attribute_1
[LSRA-Tunnel1/0/0] mpls te hotstandby-lsp-constraint 1 lsp-attribute
lsp_attribute_2
[LSRA-Tunnel1/0/0] mpls te ordinary-lsp-constraint 1 lsp-attribute lsp_attribute_3
[LSRA-Tunnel1/0/0] mpls te commit
```

Step 6 Verify the configuration.

Run the **display mpls te tunnel-interface lsp-constraint** command on LSRA. You can view the configurations of the LSP attribute templates.

```
<LARA> display mpls te tunnel-interface lsp-constraint
    Tunnel Name                     :  Tunnel1/0/0
    Primary-lsp-constraint Name     :  lsp_attribute_1
    Hotstandby-lsp-constraint Number:  1
    Hotstandby-lsp-constraint Name  :  lsp_attribute_2
    Ordinary-lsp-constraint Number  :  1
    Ordinary-lsp-constraint Name    :  lsp_attribute_3
```

Run the **display mpls te tunnel-interface** command on LSRA. You can view that the LSP attribute template lsp_attribute_1 is used to set up the CR-LSP.

```
<LSRA> display mpls te tunnel-interface tunnel1/0/0
    Tunnel Name       :  Tunnel1/0/0
    Tunnel State Desc :  Primary CR-LSP Up and HotBackup CR-LSP Up
    Tunnel Attributes   :
    Session ID          :  100
    Ingress LSR ID      :  1.1.1.1              Egress LSR ID:  4.4.4.4
    Admin State         :  UP                   Oper State   :  UP
    Signaling Protocol  :  RSVP
    Tie-Breaking Policy :  None                 Metric Type  :  None
    BypassBW Flag       :  Not Supported
    BypassBW Type       :  -                    Bypass BW    :  -
    Bfd Cap             :  None                 Retry Int    :  10 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
    Secondary HopLimit  :  -
    BestEffort HopLimit :  -
    Secondary Explicit Path Name:  -
    Secondary Affinity Prop/Mask:  0x0/0x0
    BestEffort Affinity Prop/Mask:  0x0/0x0
    IsConfigLspConstraint:  Yes

    Primary LSP ID      :  1.1.1.1:1
    Setup Priority      :  5                    Hold Priority:  5
    Affinity Prop/Mask  :  0x0/0x0              Resv Style   :  SE
    CT0 Bandwidth(Kbit/sec) :  0          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(kbps):  -
    Explicit Path Name  :  up_path              Hop Limit    :  12
```


Copyright © Huawei Technologies Co., Ltd.

```
    Record Route        :  Enabled              Record Label :  Disabled
    Route Pinning       :  Disabled
    FRR Flag            :  Disabled
    IdleTime Remain     :  -
    Lsp-constraint Name :  lsp_attribute_1

    Backup LSP ID       :  1.1.1.1:32769
    Backup LSP Type     :  Hot-standby
    Setup Priority      :  5                    Hold Priority:  5
    Affinity Prop/Mask  :  0x0/0x0              Resv Style   :  SE
    CT0 Bandwidth(Kbit/sec) :  0          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  :  down_path            Hop Limit    :  15
    Record Route        :  Enabled              Record Label :  Disabled
    Route Pinning       :  Disabled
    FRR Flag            :  -
    IdleTime Remain     :  -
    Lsp-constraint Number:  1
    Lsp-constraint Name :  lsp_attribute_2
```

After shutting down Vlanif10 on LSRC, you can find that **Tunnel State Desc** of the LSP attribute template is changed.

```
<LSRA> display mpls te tunnel-interface tunnel1/0/0
    Tunnel Name       :  Tunnel1/0/0
    Tunnel State Desc :  Backup CR-LSP In use and Primary CR-LSP setting Up
    Tunnel Attributes   :
    Session ID          :  100
    Ingress LSR ID      :  1.1.1.1              Egress LSR ID:  4.4.4.4
    Admin State         :  UP                   Oper State   :  UP
    Signaling Protocol  :  RSVP
    Tie-Breaking Policy :  None                 Metric Type  :  None
    BypassBW Flag       :  Not Supported
    BypassBW Type       :  -                    Bypass BW    :  -
    Bfd Cap             :  None                 Retry Int    :  10 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
    Secondary HopLimit  :  -
    BestEffort HopLimit :  -
    Secondary Explicit Path Name:  -
    Secondary Affinity Prop/Mask:  0x0/0x0
    BestEffort Affinity Prop/Mask:  0x0/0x0
    IsConfigLspConstraint:  Yes

    Primary LSP ID      :  1.1.1.1:1
    Setup Priority      :  5                    Hold Priority:  5
    Affinity Prop/Mask  :  0x0/0x0              Resv Style   :  SE
    CT0 Bandwidth(Kbit/sec) :  0          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(kbps):  -
    Explicit Path Name  :  up_path              Hop Limit    :  12
    Record Route        :  Enabled              Record Label :  Disabled
    Route Pinning       :  Disabled
    FRR Flag            :  Disabled
    IdleTime Remain     :  -
```


Copyright © Huawei Technologies Co., Ltd.

```
    Lsp-constraint Name :  lsp_attribute_1

    Backup LSP ID       :  1.1.1.1:32769
    Backup LSP Type     :  Hot-standby
    Setup Priority      :  5                    Hold Priority:  5
    Affinity Prop/Mask  :  0x0/0x0              Resv Style   :  SE
    CT0 Bandwidth(Kbit/sec) :  0          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  :  down_path            Hop Limit    :  15
    Record Route        :  Enabled              Record Label :  Disabled
    Route Pinning       :  Disabled
    FRR Flag            :  -
    IdleTime Remain     :  -
    Lsp-constraint Number:  1
    Lsp-constraint Name :  lsp_attribute_2
```

After shutting down Vlanif30 on LSRB, you can find that **Tunnel State Desc** of the LSP attribute template is changed again.

```
<LSRA> display mpls te tunnel-interface Tunnel 1/0/0
    Tunnel Name       :  Tunnel1/0/0
    Tunnel State Desc :  Backup CR-LSP In use and Primary CR-LSP setting Up
    Tunnel Attributes   :
    Session ID          :  100
    Ingress LSR ID      :  1.1.1.1              Egress LSR ID:  4.4.4.4
    Admin State         :  UP                   Oper State   :  UP
    Signaling Protocol  :  RSVP
    Tie-Breaking Policy :  None                 Metric Type  :  None
    BypassBW Flag       :  Not Supported
    BypassBW Type       :  -                    Bypass BW    :  -
    Bfd Cap             :  None                 Retry Int    :  10 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
    Secondary HopLimit  :  -
    BestEffort HopLimit :  -
    Secondary Explicit Path Name:  -
    Secondary Affinity Prop/Mask:  0x0/0x0
    BestEffort Affinity Prop/Mask:  0x0/0x0
    IsConfigLspConstraint:  Yes

    Primary LSP ID      :  1.1.1.1:1
    Setup Priority      :  5                    Hold Priority:  5
    Affinity Prop/Mask  :  0x0/0x0              Resv Style   :  SE
    CT0 Bandwidth(Kbit/sec) :  0          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(kbps):  -
    Explicit Path Name  :  up_path              Hop Limit    :  12
    Record Route        :  Enabled              Record Label :  Disabled
    Route Pinning       :  Disabled
    FRR Flag            :  Disabled
    IdleTime Remain     :  -
    Lsp-constraint Name :  lsp_attribute_1

    Backup LSP ID       :  1.1.1.1:32771
    Backup LSP Type     :  Ordinary
```


Copyright © Huawei Technologies Co., Ltd.

```
Setup Priority      :  5                    Hold Priority:  5
Affinity Prop/Mask  :  0x0/0x0              Resv Style   :  SE
CT0 Bandwidth(Kbit/sec) :  0          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  :  middle_path          Hop Limit    :  -
Record Route        :  Enabled              Record Label :  Disabled
Route Pinning       :  Disabled
FRR Flag            :  -
IdleTime Remain     :  -
Lsp-constraint Number:  1
Lsp-constraint Name :  lsp_attribute_3
```

----End

Configuration Files

- Configuration file of LSRA

```
#
 sysname LSRA
#
vlan batch 10 20 30
#
 mpls lsr-id 1.1.1.1
 mpls
  mpls te
mpls rsvp-te
#
 explicit-path middle_path
  next hop 10.1.3.2
  next hop 10.1.6.2
#
 explicit-path up_path
  next hop 10.1.1.2
  next hop 10.1.4.2
#
 explicit-path down_path
  next hop 10.1.2.2
  next hop 10.1.5.2
#
 lsp-attribute lsp_attribute_1
  explicit-path up_path
  priority 5
  hop-limit 12
commit
#
 lsp-attribute lsp_attribute_2
  explicit-path down_path
  priority 5
  hop-limit 15
commit
#
 lsp-attribute lsp_attribute_3
  explicit-path middle_path
  priority 5
commit

#
interface Vlanif10
ip address 10.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif20
ip address 10.1.3.1 255.255.255.0
 mpls
```


Copyright © Huawei Technologies Co., Ltd.

```
 mpls te
 mpls rsvp-te
#
interface Vlanif30
ip address 10.1.2.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
interface Tunnel1/0/0
 tunnel-protocol mpls te
 destination 4.4.4.4
 mpls te tunnel-id 100
 mpls te primary-lsp-constraint lsp-attribute lsp_attribute_1
 mpls te hotstandby-lsp-constraint 1 lsp-attribute lsp_attribute_2
 mpls te ordinary-lsp-constraint 1 lsp-attribute lsp_attribute_3
 mpls te commit
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface GigabitEthernet 3/0/0
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
  network 10.1.3.0 0.0.0.255
  mpls-te enable
#
return
```

- Configuration file of LSRB

```
#
 sysname LSRB
#
vlan batch 30 40
#
mpls lsr-id 10.1.5.1
 mpls
  mpls te
  mpls rsvp-te
#
interface Vlanif30
ip address 10.1.2.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif40
 ip address 10.1.5.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
```


Copyright © Huawei Technologies Co., Ltd.

```
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 10.1.5.0 0.0.0.255
  mpls-te enable
#
return
```

- Configuration file of LSRC

```
#
 sysname LSRC
#
vlan batch 10 60
#
mpls lsr-id 10.1.4.1
 mpls
  mpls te
  mpls rsvp-te
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif60
ip address 10.1.4.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 60
 port hybrid untagged vlan 60
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.4.0 0.0.0.255
  mpls-te enable
#
return
```

- Configuration file of LSRD

```
#
 sysname LSRD
#
vlan batch 60 50 40
#
 mpls lsr-id 4.4.4.4
 mpls
  mpls te
  mpls rsvp-te
#
interface Vlanif60
ip address 10.1.4.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
```


Copyright © Huawei Technologies Co., Ltd.

```
#
interface Vlanif50
ip address 10.1.6.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif40
ip address 10.1.5.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 60
 port hybrid untagged vlan 60
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
interface GigabitEthernet 3/0/0
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 10.1.4.0 0.0.0.255
  network 10.1.5.0 0.0.0.255
  network 10.1.6.0 0.0.0.255
  mpls-te enable
#
return
```

- Configuration file of LSRE

```
#
 sysname LSRE
#
vlan batch 20 50
#
 mpls lsr-id 10.1.6.1
 mpls
  mpls te
mpls rsvp-te
#
interface Vlanif20
ip address 10.1.3.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif50
ip address 10.1.6.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
```


Copyright © Huawei Technologies Co., Ltd.

```
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 10.1.3.0 0.0.0.255
  network 10.1.6.0 0.0.0.255
  mpls-te enable
#
return
```

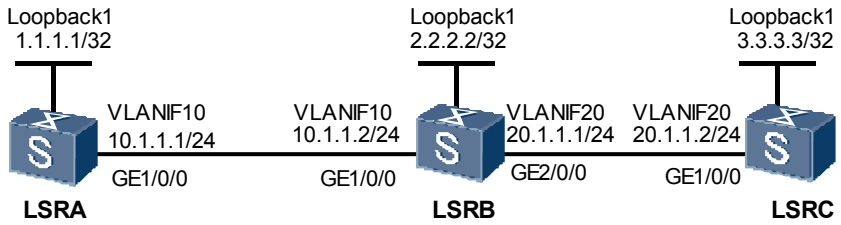
3.21.4 Example for Configuring RSVP Authentication

Networking Requirements

As shown in **Figure 3-5**, the VLANIF member interface between LSRA and LSRB is GE 1/0/0. An MPLS TE tunnel from LSRA to LSRC is set up by using RSVP.

The handshake function is required to be configured so that RSVP authentication is performed between LSRA and LSRB. This prevents pseudo RSVP requests for reserving resources from causing resource exhaustion. In addition, the message window function is required to be configured to prevent the RSVP messages that are out of sequence.

Figure 3-5 Networking diagram for configuring RSVP authentication



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the MPLS network and set up an RSVP-TE tunnel.
2. Configure authentication on the interface to authenticate RSVP messages.
3. Configure the handshake function on the interface.
4. Set the side of the sliding window on the interface so that the interface can save 32 sequence numbers.

NOTE

It is recommended that you set the value of *window-size* to be greater than 32, smaller than 64. If the value of *window-size* is set to be very small, certain received RSVP messages may be beyond the window and are discarded, which can close the RSVP neighbor relationship.

Data Preparation

To complete the configuration, you need the following data:

Copyright © Huawei Technologies Co., Ltd.

- OSPF process ID and OSPF area ID of each node
- Authentication password of the local interface and authentication key
- Size of the sliding window for RSVP authentication

Procedure

Step 1 Create VLANs and VLANIF interfaces, and assign IP addresses to the VLANIF interfaces.

Configure IP addresses and masks for the interfaces according to **Figure 3-5**. The configuration details are not mentioned here, see the configuration files in this example.

Step 2 Configure OSPF.

Configure OSPF to advertise the routes of network segments and the host routes of the LSR IDs. For detailed configuration, see the configuration files in this example.

After the configuration, run the **display ip routing-table** command on each node, and you can view that the nodes learn the routes from each other.

Step 3 Configure basic MPLS functions and enable MPLS TE, MPLS RSVP-TE, and CSPF.

Configure LSRA.

```
[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 vlanif 10
[LSRA-Vlanif10] mpls
[LSRA-Vlanif10] mpls te
[LSRA-Vlanif10] mpls rsvp-te
[LSRA-Vlanif10] quit
```

NOTE

The configurations on LSRB and LSRC are similar to the configuration on LSRA, and are not mentioned here.

Step 4 Configure OSPF TE.

Configure LSRA.

```
[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] quit
```

Configure LSRB.

```
[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] quit
```

Configure LSRC.

```
[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] quit
```


Copyright © Huawei Technologies Co., Ltd.

Step 5 Configure the MPLS TE tunnel.

Create an MPLS TE tunnel on LSRA.

```
[LSRA] interface tunnel 1/0/0
[LSRA-Tunnel1/0/0] ip address unnumbered interface loopback 1
[LSRA-Tunnel1/0/0] tunnel-protocol mpls te
[LSRA-Tunnel1/0/0] destination 3.3.3.3
[LSRA-Tunnel1/0/0] mpls te signal-protocol rsvp-te
[LSRA-Tunnel1/0/0] mpls te tunnel-id 1
[LSRA-Tunnel1/0/0] mpls te commit
[LSRA-Tunnel1/0/0] quit
```

After the configuration, run the **display interface tunnel** command on LSRA, and you can view that the status of the tunnel interface is Up.

```
[LSRA] display interface tunnel 1/0/0
Tunnel1/0/0 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Tunnel1/0/0 Interface
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 NONE
    300 seconds input rate 0 bits/sec, 0 packets/sec
    300 seconds output rate 0 bits/sec, 0 packets/sec
    0 seconds input rate 0 bits/sec, 0 packets/sec
    0 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets input,  0 bytes
    0 input error
    0 packets output,  0 bytes
    0 output error
    Input:
      Unicast: 0 packets, Multicast: 0 packets
    Output:
      Unicast: 0 packets, Multicast: 0 packets
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Step 6 On LSRA and LSRB, configure RSVP authentication on the interfaces that are connected to the MPLS TE link.

Configure LSRA.

```
[LSRA] interface vlanif 10
[LSRA-Vlanif10] mpls rsvp-te authentication plain 123456789
[LSRA-Vlanif10] mpls rsvp-te authentication handshake 12345678
[LSRA-Vlanif10] mpls rsvp-te authentication window-size 32
```

Configure LSRB.

```
[LSRB] interface vlanif 10
[LSRB-Vlanif10] mpls rsvp-te authentication plain 123456789
[LSRB-Vlanif10] mpls rsvp-te authentication handshake 12345678
[LSRB-Vlanif10] mpls rsvp-te authentication window-size 32
```

Step 7 Verify the configuration.

Run the **reset mpls rsvp-te** command, and then run the **display interface tunnel** command on LSRA. You can view that the tunnel interface is Up.

Run the **display mpls rsvp-te interface** command on LSRA or LSRB, and you can view information about RSVP authentication.

```
[LSRA] display mpls rsvp-te interface
Interface: Vlanif10
 Interface Address: 10.1.1.1
 Interface state: UP                  Interface Index: 0x406
```


Copyright © Huawei Technologies Co., Ltd.

```
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
Challenge: ENABLE                     WindowSize: 32
Next Seq # to be sent:3957701863 40   Key ID: ee9f61f80000
Bfd Enabled: DISABLE                  Bfd Min-Tx: 10
Bfd Min-Rx: 10                       Bfd Detect-Multi: 3
```

----End

Configuration Files

- Configuration file of LSRA

```
#
 sysname LSRA
#
 vlan batch 10
#
 mpls lsr-id 1.1.1.1
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
 mpls rsvp-te authentication plain 123456789
 mpls rsvp-te authentication handshake 12345678
 mpls rsvp-te authentication window-size 32
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te tunnel-id 1
 mpls te commit
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 1.1.1.1 0.0.0.0
  mpls-te enable
#
return
```

- Configuration file of LSRB

```
#
 sysname LSRB
#
 vlan batch 10 20
#
 mpls lsr-id 2.2.2.2
 mpls
  mpls te
  mpls rsvp-te
```


Copyright © Huawei Technologies Co., Ltd.

```
  mpls te cspf
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
 mpls rsvp-te authentication plain 123456789
 mpls rsvp-te authentication handshake 12345678
 mpls rsvp-te authentication window-size 32
#
interface Vlanif20
 ip address 20.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port defalt vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port defalt vlan 20
#
interface LoopBack1
ip address 2.2.2.2 255.255.255.255
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
  mpls-te enable
#
return
```

- Configuration file of LSRC

```
#
 sysname LSRC
#
 vlan batch 20
#
mpls lsr-id 3.3.3.3
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
interface Vlanif20
 ip address 20.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 20.1.1.0 0.0.0.255
  network 3.3.3.3 0.0.0.0
  mpls-te enable
```

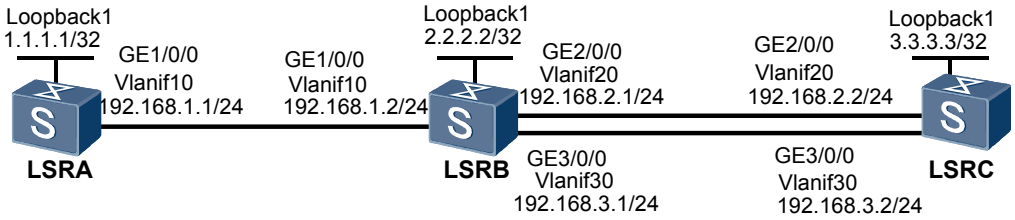

Copyright © Huawei Technologies Co., Ltd.

```
#
return
```

3.21.5 Example for Setting Attributes on the MPLS TE Tunnel

Networking Requirements

Figure 3-6 Networking diagram for setting attributes on the MPLS TE tunnel



As shown in **Figure 3-6**, the maximum link bandwidth is 100 Mbit/s and the maximum reservable bandwidth is 50 Mbit/s.

On LSRA, there are two tunnels to LSRC, namely, Tunnel 1/0/0 and Tunnel 1/0/1, both of which require the bandwidth of 40 Mbit/s. The total bandwidth (80 Mbit/s) of these two tunnels is greater than the bandwidth (50 Mbit/s) of the link between LSRA and LSRB. In addition, Tunnel 1/0/0 has a higher priority than Tunnel 1/0/0 and preemption is allowed.

The affinity property and mask is required to be used according to the administrative group property. In this manner, Tunnel 1/0/0 on LSRA uses one physical link from LSRB to LSRC and Tunnel 1/0/1 uses another physical link.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the RSVP-TE tunnel. See Configuration Roadmap in **3.21.2 Example for Configuring an RSVP-TE Tunnel**.
2. Configure the administrative group property of the outgoing interface of the tunnel on each node.
3. Configure the affinity property and mask of each tunnel according to the administrative group property and networking requirements.
4. Set the priority of each tunnel as required.

Data Preparation

To complete the configuration, you need the following data:

- OSPF process ID and OSPF area ID of each node
- Maximum bandwidth and maximum reservable bandwidth for the link along the tunnel
- Administrative group property of the link between LSRA and LSRB and administrative group property of the link between LSRB and LSRC
- Affinity property and mask of each tunnel

Copyright © Huawei Technologies Co., Ltd.

- Number of the tunnel interface, IP address, destination IP address, tunnel ID, tunnel bandwidth, tunnel priority, and signaling protocol (RSVP-TE by default)

Procedure

Step 1 Create VLANs and VLANIF interfaces, and assign IP addresses to the VLANIF interfaces.

Configure IP addresses and masks for the interfaces including loopback interfaces according to **Figure 3-6**.

The configuration details are not mentioned here.

Step 2 Configure an IGP.

Configure OSPF on all the nodes to advertise the routes of network segments and the host routes of LSR IDs.

The configuration details are not mentioned here.

Step 3 Configure basic MPLS functions, enable MPLS TE, RSVP-TE, and OSPF TE, and enable CSPF on the ingress node.

Configure basic MPLS functions and enable MPLS TE and RSVP-TE on LSRA, LSRB, and LSRC.

Take the display on LSRA as an example.

```
[LSRA] mpls lsr-id 1.1.1.1
[LSRA] mpls
[LSRA-mpls] mpls te
[LSRA-mpls] mpls rsvp-te
[LSRA-mpls] quit
[LSRA] interface vlanif 10
[LSRA-Vlanif10] mpls
[LSRA-Vlanif10] mpls te
[LSRA-Vlanif10] mpls rsvp-te
[LSRA-Vlanif10] quit
```

Enable OSPF TE on LSRA, LSRB, and LSRC. Take the display on LSRA as an example.

```
[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 of LSRB and LSRC are similar to the configuration of LSRA, and are not mentioned here.

Enable CSPF TE on LSRA that is the ingress node of the tunnel.

```
[LSRA] mpls
[LSRA-mpls] mpls te cspf
[LSRA-mpls] quit
```

Step 4 Set MPLS TE attributes of the outgoing interface of each node.

On LSRA, set the maximum link bandwidth to 100 Mbit/s and the maximum reservable bandwidth to 50 Mbit/s.

```
[LSRA] interface vlanif 10
[LSRA-Vlanif10] mpls te bandwidth max-reservable-bandwidth 50000
```

On LSRA, set the administrative group property of the link to 0x10001.

Copyright © Huawei Technologies Co., Ltd.

```
[LSRA-Vlanif10] mpls te link administrative group 10001
[LSRA-Vlanif10] quit
```

Set MPLS TE attributes of the link on LSRB.

```
[LSRB] interface vlanif 20
[LSRB-Vlanif20] mpls te bandwidth max-reservable-bandwidth 50000
[LSRB-Vlanif20] mpls te link administrative group 10101
[LSRB-Vlanif20] quit
[LSRB] interface vlanif 30
[LSRB-Vlanif30] mpls te bandwidth max-reservable-bandwidth 50000
[LSRB-Vlanif30] quit
```

After the configuration, you can view the TEDB on LSRA, including the maximum reservable bandwidth and the Color field that is the administrative group property of the link.

```
[LSRA] display mpls te cspf tedb node
Router ID: 1.1.1.1
  IGP Type: OSPF   Process Id: 1
  MPLS-TE Link Count: 1
  Link[1]:
    Interface IP Address: 192.168.1.1
    Peer  IP Address: 192.168.1.2
    Peer  Router  Id: 2.2.2.2
    Peer  OSPF  Router  Id: 2.2.2.2
    IGP Area: 0
    Link  Type: multi-access    Link Status: Active
    IGP Metric: 1               TE Metric: 1           Color: 0x10001
    Maximum Bandwidth: 100000 (kbps)
    Maximum Reservable Bandwidth: 50000 (kbps)
    Bandwidth Constraints:           Local Overbooking Multiplier:
         BC[0]:  50000      (kbps)   LOM[0]:  1
         BC[1]:  0          (kbps)   LOM[1]:  1
   BW Unreserved for Class type 0:
         [0]:    50000      (kbps),  [1]:     50000      (kbps)
         [2]:    50000      (kbps),  [3]:     50000      (kbps)
         [4]:    50000      (kbps),  [5]:     50000      (kbps)
         [6]:    50000      (kbps),  [7]:     50000      (kbps)
    BW Unreserved for Class type 1:
         [0]:    0          (kbps),  [1]:     0          (kbps)
         [2]:    0          (kbps),  [3]:     0          (kbps)
         [4]:    0          (kbps),  [5]:     0          (kbps)
         [6]:    0          (kbps),  [7]:     0          (kbps)
Router ID: 2.2.2.2
  IGP Type: OSPF   Process Id: 1
  MPLS-TE Link Count: 3
  Link[1]:
    Interface IP Address: 192.168.2.1
    Peer  IP Address: 192.168.2.2
    Peer  Router  Id: 3.3.3.3
    Peer  OSPF  Router  Id: 3.3.3.3
    IGP Area: 0
    Link  Type: multi-access    Link Status: Active
    IGP Metric: 1               TE Metric: 1           Color: 0x10101
    Maximum Bandwidth: 100000 (kbps)
    Maximum Reservable Bandwidth: 50000 (kbps)
    Bandwidth Constraints:           Local Overbooking Multiplier:
         BC[0]:  50000      (kbps)   LOM[0]:  1
         BC[1]:  0          (kbps)   LOM[1]:  1
    BW Unreserved for Class type 0:
         [0]:    50000      (kbps),  [1]:     50000      (kbps)
         [2]:    50000      (kbps),  [3]:     50000 100000     (kbps)
         [4]:    50000      (kbps),  [5]:     50000 100000     (kbps)
         [6]:    50000      (kbps),  [7]:     50000      (kbps)
    BW Unreserved for Class type 1:
         [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]:
```


Copyright © Huawei Technologies Co., Ltd.

```
    Interface IP Address: 192.168.1.2
    Peer  IP Address: 192.168.1.1
    Peer  Router  Id: 1.1.1.1
   Peer  OSPF  Router  Id: 1.1.1.1
    IGP Area: 0
    Link  Type: multi-access    Link Status: Active
    IGP Metric: 1               TE Metric: 1          Color: 0x0
    Maximum Bandwidth: 0 (kbps)
    Maximum Reservable Bandwidth: 0 (kbps)$#10$    Bandwidth Constraints:
Local Overbooking Multiplier:
         BC[0]:  0          (kbps)   LOM[0]:  1
         BC[1]:  0          (kbps)   LOM[1]:  1
   BW Unreserved for Class type 0:
         [0]:    0          (kbps),  [1]:     0          (kbps)
         [2]:    0          (kbps),  [3]:     0          (kbps)
         [4]:    0          (kbps),  [5]:     0          (kbps)
         [6]:    0          (kbps),  [7]:     0          (kbps)
    BW Unreserved for Class type 1:
         [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[3]:
    Interface IP Address: 192.168.3.1
    Peer  IP Address: 192.168.3.2
    Peer  Router  Id: 3.3.3.3
   Peer  OSPF Router  Id: 3.3.3.3
    IGP Area: 0
    Link  Type: multi-access    Link Status: Active
    IGP Metric: 1               TE Metric: 1          Color: 0x10011
    Maximum Bandwidth: 100000 (kbps)
    Maximum Reservable Bandwidth: 50000 (kbps)
    Bandwidth Constraints:          Local Overbooking Multiplier:
         BC[0]:  50000      (kbps)   LOM[0]:  1
         BC[1]:  0          (kbps)   LOM[1]:  1
    BW Unreserved for Class type 0:
         [0]:    50000      (kbps),  [1]:     50000      (kbps)
         [2]:    50000      (kbps),  [3]:     50000      (kbps)
         [4]:    50000      (kbps),  [5]:     50000      (kbps)
         [6]:    50000      (kbps),  [7]:     50000      (kbps)
    BW Unreserved for Class type 1:
         [0]:    0          (kbps),  [1]:     0          (kbps)
         [2]:    0          (kbps),  [3]:     0          (kbps)
         [4]:    0          (kbps),  [5]:     0          (kbps)
         [6]:    0          (kbps),  [7]:     0          (kbps)
Router ID: 3.3.3.3
  IGP Type: OSPF   Process Id: 1
  MPLS-TE Link Count: 2
  Link[1]:
    Interface IP Address: 192.168.2.2
    Peer  IP Address: 192.168.2.1
    Peer  Router  Id: 2.2.2.2
    Peer  OSPF  Router  Id: 2.2.2.2
    IGP Area: 0
    Link  Type: multi-access    Link Status: Active
    IGP Metric: 1               TE Metric: 1          Color: 0x0
    Maximum Bandwidth: 0 (kbps)
    Maximum Reservable Bandwidth: 0 (kbps)
    Bandwidth Constraints:          Local Overbooking Multiplier:
         BC[0]:  0          (kbps)   LOM[0]:  1
         BC[1]:  0          (kbps)   LOM[1]:  1
    BW Unreserved for Class type 0:
         [0]:    0          (kbps),  [1]:     0          (kbps)
         [2]:    0          (kbps),  [3]:     0          (kbps)
         [4]:    0          (kbps),  [5]:     0          (kbps)
         [6]:    0          (kbps),  [7]:     0          (kbps)
    BW Unreserved for Class type 1:
         [0]:    0          (kbps),  [1]:     0          (kbps)
         [2]:    0          (kbps),  [3]:     0          (kbps)
```


Copyright © Huawei Technologies Co., Ltd.

```
        [4]:    0          (kbps),  [5]:     0          (kbps)
        [6]:    0          (kbps),  [7]:     0          (kbps)
  Link[2]:
    Interface IP Address: 192.168.3.2
    Peer  IP Address: 192.168.3.1
Peer  Router  Id: 2.2.2.2
Peer  OSPF  Router  Id: 2.2.2.2
    IGP Area: 0
    Link  Type: multi-access    Link Status: Active
    IGP Metric: 1               TE Metric: 1           Color: 0x0
    Maximum Bandwidth: 0 (kbps)
    Maximum Reservable Bandwidth: 0 (kbps)
    Bandwidth Constraints:          Local Overbooking Multiplier:
        BC[0]:  0          (kbps)   LOM[0]:  1
        BC[1]:  0          (kbps)   LOM[1]:  1
   BW Unreserved for Class type 0:
        [0]:    0          (kbps),  [1]:     0          (kbps)
        [2]:    0          (kbps),  [3]:     0          (kbps)
        [4]:    0          (kbps),  [5]:     0          (kbps)
        [6]:    0          (kbps),  [7]:     0          (kbps)
    BW Unreserved for Class type 1:
        [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 Create an MPLS TE tunnel.

Create Tunnel 1/0/0 on LSRA.

```
[LSRA] interface tunnel 1/0/0
[LSRA-Tunnel1/0/0] ip address unnumbered interface loopback 1
[LSRA-Tunnel1/0/0] tunnel-protocol mpls te
[LSRA-Tunnel1/0/0] destination 3.3.3.3
[LSRA-Tunnel1/0/0] mpls te tunnel-id 100
[LSRA-Tunnel1/0/0] mpls te affinity property 10101 mask 11011
[LSRA-Tunnel1/0/0] mpls te commit
[LSRA-Tunnel1/0/0] quit
```

Here, the default setup priority and holding priority are used, that is, the lowest priority with the value of 7.

The affinity property of the tunnel is 0x10101 and the mask is 0x11011, both of which can match the administrative group property of the links along the tunnel.

After the configuration, check the status of the tunnel on LSRA:

```
[LSRA] display mpls te tunnel-interface
  Tunnel Name         :  Tunnel1/0/0
  Tunnel State Desc   :  CR-LSP is Up
  Tunnel Attributes   :
    LSP ID              :  1.1.1.1:1
    Session ID          :  100
    Admin State         :  UP                   Oper State   :  UP
    Ingress LSR ID      :  1.1.1.1              Egress LSR ID:  3.3.3.3
    Signaling Protocol  :  RSVP                 Resv Style   :  SE
    Class Type          :  CLASS 0              Tunnel BW    :  40000 kbps
    Reserved BW         :  40000 kbps
    Setup Priority      :  7                    Hold Priority:  7
    Hop Limit           :  -
    Secondary Hop Limit :  -
    BestEffort Hop Limit:  -
    Affinity Prop/Mask  :  0x10101/0x11011
    Explicit Path Name  :  -
    Secondary Affinity Prop/Mask:  0x0/0x0
    Secondary Explicit Path Name:  -
    BestEffort Affinity Prop/Mask:  0x0/0x0
    Tie-Breaking Policy :  None
    Metric Type         :  None
```


Copyright © Huawei Technologies Co., Ltd.

```
    Record Route        :  Disabled             Record Label :  Disabled
    FRR Flag            :  Disabled             BackUpBW Flag:  Not Supported
    BackUpBW Type       :  -                    BackUpBW     :  -
    Route Pinning       :  Disabled
    Reopt               :  Disabled             Reopt Freq   :  -
    Back Up Type        :  None
    Back Up LSPID       :  -
    Auto BW             :  Disabled             Auto BW Freq :  -
    Min BW              :  -                    Max BW       :  -
    Current Collected BW:  -
    Interfaces Protected:  -
    Car Policy          :  Disabled
    Tunnel  Group       :  Primary
    Primary Tunnel      :  -
    Backup  Tunnel      :  -
    IPTN    InLabel     :  -
    Group   Status      :  Up
    Oam     Status      :  Up
    Bfd Capability      :  Up
    BestEffort          :  Disabled             IsBestEffortPath:  Non-existent
```

Check the TEDB, and you can view the change of bandwidth used by the links:

```
[LSRA] display mpls te cspf tedb node
Router ID: 1.1.1.1
  IGP Type: OSPF   Process Id: 1
  MPLS-TE Link Count: 1
  Link[1]:
    Interface IP Address: 192.168.1.1
    Peer  IP Address: 192.168.1.2
    Peer  Router  Id: 2.2.2.2
    Peer  OSPF Router  Id: 2.2.2.2
    IGP Area: 0
    Link  Type: multi-access    Link Status: Active
    IGP Metric: 1               TE Metric: 1           Color: 0x10001
    Maximum Bandwidth: 100000 (kbps)
    Maximum Reservable Bandwidth: 50000 (kbps)
    Bandwidth Constraints:           Local Overbooking Multiplier:
         BC[0]:  50000      (kbps)   LOM[0]:  1
         BC[1]:  0          (kbps)   LOM[1]:  1
    BW Unreserved for Class type 0:
         [0]:    50000      (kbps),  [1]:     50000      (kbps)
         [2]:    50000      (kbps),  [3]:     50000      (kbps)
         [4]:    50000      (kbps),  [5]:     50000      (kbps)
         [6]:    50000      (kbps),  [7]:     10000      (kbps)
    BW Unreserved for Class type 1:
         [0]:    0          (kbps),  [1]:     0          (kbps)
         [2]:    0          (kbps),  [3]:     0          (kbps)
         [4]:    0          (kbps),  [5]:     0          (kbps)
         [6]:    0          (kbps),  [7]:     0          (kbps)
Router ID: 2.2.2.2
  IGP Type: OSPF   Process Id: 1
  MPLS-TE Link Count: 3
  Link[1]:
    Interface IP Address: 192.168.2.1
    Peer  IP Address: 192.168.2.2
    Peer  Router  Id: 3.3.3.3
    Peer  OSPF Router  Id: 3.3.3.3
    IGP Area: 0
    Link  Type: multi-access    Link Status: Active
    IGP Metric: 1               TE Metric: 1           Color: 0x10101
    Maximum Bandwidth: 100000 (kbps)
    Maximum Reservable Bandwidth: 50000 (kbps)
    Bandwidth Constraints:           Local Overbooking Multiplier:
         BC[0]:  50000     (kbps)   LOM[0]:  1
         BC[1]:  0          (kbps)   LOM[1]:  1
    BW Unreserved for Class type 0:
         [0]:    50000      (kbps),  [1]:     50000      (kbps)
         [2]:    50000      (kbps),  [3]:     50000      (kbps)
         [4]:    50000      (kbps),  [5]:     50000      (kbps)
```


Copyright © Huawei Technologies Co., Ltd.

```
        [6]:    50000      (kbps),  [7]:     10000      (kbps)
    BW Unreserved for Class type 1:
        [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]:
    Interface IP Address: 192.168.1.2
    Peer  IP Address: 192.168.1.1
Peer  Router  Id: 1.1.1.1
Peer  OSPF  Router  Id: 1.1.1.1
    IGP Area: 0
    Link  Type: multi-access    Link Status: Active
    IGP Metric: 1               TE Metric: 1           Color: 0x0
    Maximum Bandwidth: 0 (kbps)
    Maximum Reservable Bandwidth: 0 (kbps)
    Bandwidth Constraints:           Local Overbooking Multiplier:
        BC[0]:  0          (kbps)   LOM[0]:  1
        BC[1]:  0          (kbps)   LOM[1]:  1
    BW Unreserved for Class type 0:
        [0]:    0          (kbps),  [1]:     0          (kbps)
        [2]:    0          (kbps),  [3]:     0          (kbps)
        [4]:    0          (kbps),  [5]:     0          (kbps)
        [6]:    0          (kbps),  [7]:     0          (kbps)
    BW Unreserved for Class type 1:
        [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[3]:
    Interface IP Address: 192.168.3.1
    Peer  IP Address: 192.168.3.2
    Peer  Router  Id: 3.3.3.3
    Peer  OSPF  Router  Id: 3.3.3.3
    IGP Area: 0
    Link  Type: multi-access    Link Status: Active
    IGP Metric: 1               TE Metric: 1           Color: 0x10011
    Maximum Bandwidth: 100000 (kbps)
    Maximum Reservable Bandwidth: 50000 (kbps)
    Bandwidth Constraints:           Local Overbooking Multiplier:
        BC[0]:       (kbps)   LOM[0]:  1
        BC[1]:  0          (kbps)   LOM[1]:  1
    BW Unreserved for Class type 0:
        [0]:    50000      (kbps),  [1]:     50000      (kbps)
        [2]:    50000      (kbps),  [3]:     50000      (kbps)
        [4]:    50000      (kbps),  [5]:     50000      (kbps)
        [6]:    50000      (kbps),  [7]:     50000      (kbps)
    BW Unreserved for Class type 1:
        [0]:    0          (kbps),  [1]:     0          (kbps)
        [2]:    0          (kbps),  [3]:     0          (kbps)
        [4]:    0          (kbps),  [5]:     0          (kbps)
        [6]:    0          (kbps),  [7]:     0          (kbps)
Router ID: 3.3.3.3
  IGP Type: OSPF   Process Id: 1
  MPLS-TE Link Count: 2
  Link[1]:
    Interface IP Address: 192.168.2.2
    Peer  IP Address: 192.168.2.1
    Peer  Router  Id: 2.2.2.2
    Peer  OSPF  Router  Id: 2.2.2.2
    IGP Area: 0
    Link  Type: multi-access    Link Status: Active
    IGP Metric: 1               TE Metric: 1           Color: 0x0
    Maximum Bandwidth: 0 (kbps)
    Maximum Reservable Bandwidth: 0      (kbps)
    Bandwidth Constraints:           Local Overbooking Multiplier:
        BC[0]:  0           (kbps)   LOM[0]:  1
        BC[1]:  0          (kbps)   LOM[1]:  1
    BW Unreserved for Class type 0:
```


Copyright © Huawei Technologies Co., Ltd.

```
      [0]:    0          (kbps),  [1]:     0          (kbps)
      [2]:    0          (kbps),  [3]:     0          (kbps)
      [4]:    0          (kbps),  [5]:     0          (kbps)
      [6]:    0          (kbps),  [7]:     0          (kbps)
  BW Unreserved for Class type 1:
      [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]:
  Interface IP Address: 192.168.3.2
  Peer  IP Address: 192.168.3.1
  Peer  Router  Id: 2.2.2.2
  Peer  OSPF  Router  Id: 2.2.2.2
  IGP Area: 0
  Link  Type: multi-access    Link Status: Active
  IGP Metric: 1               TE Metric: 1           Color: 0x0
  Maximum Bandwidth: 0 (kbps)
  Maximum Reservable Bandwidth: 0 (kbps)
  Bandwidth Constraints:           Local Overbooking Multiplier:
      BC[0]:  0           (kbps)   LOM[0]:  1
      BC[1]:  0           (kbps)   LOM[1]:  1
  BW Unreserved for Class type 0:
      [0]:    0          (kbps),  [1]:     0          (kbps)
      [2]:    0          (kbps),  [3]:     0          (kbps)
      [4]:    0          (kbps),  [5]:     0          (kbps)
      [6]:    0          (kbps),  [7]:     0          (kbps)
  BW Unreserved for Class type 1:
      [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 available bandwidth from the maximum reservable bandwidth for various priorities. The display shows that the unreserved bandwidth changes for class type 7 on the outgoing interfaces on each node along the tunnel. This indicates that certain tunnels succeed in reserving 40 Mbit/s bandwidth with the priority of 7. According to bandwidth allocation , you can view the path that the tunnel takes. This indicates that the affinity property and the mask of the tunnel must match the administrative group property of the links.

You can also run the **display mpls te tunnel** command on LSRB to view the outgoing interface of the tunnel.

```
[LSRB] display mpls te tunnel
LSP-Id                    Destination          In/Out-If
1.1.1.1:100:1             3.3.3.3              Vlanif10/Vlanif20
```

Create Tunnel 1/0/1 on LSRA.

```
[LSRA] interface tunnel 1/0/1
[LSRA-Tunnel1/0/1] ip address unnumbered interface loopback 1
[LSRA-Tunnel1/0/1] tunnel-protocol mpls te
[LSRA-Tunnel1/0/1] destination 3.3.3.3
[LSRA-Tunnel1/0/1] mpls te tunnel-id 101
[LSRA-Tunnel1/0/1] mpls te affinity property 10011 mask 11101
[LSRA-Tunnel1/0/1] mpls te priority 6
[LSRA-Tunnel1/0/1] mpls te commit
[LSRA-Tunnel1/0/1] quit
```

Step 6 Verify the configuration.

After the configuration, run the **display interface Tunnel** or **display mpls te tunnel-interface** command on LSRA, and you can view the status of the tunnel on LSRA. You can view that the status of Tunnel 1/0/0 is Down. This is because the maximum reservable bandwidth of the physical link between LSRA and LSRB is insufficient, and the bandwidth of Tunnel 1/0/0 is preempted by Tunnel 1/0/1 with a higher priority.

Copyright © Huawei Technologies Co., Ltd.

Run the **display mpls te cspf tedb node** command to check the TEDB and the changes of bandwidth used on the links. It indicates that Tunnel 1/0/1 passes through VLANIF 30 of LSRB.

Or run the **display mpls te tunnel** command on LSRB, and you can view the outgoing interface of the tunnel.

```
[LSRB] display mpls te tunnel
LSP-Id                    Destination          In/Out-If
1.1.1.1:101:4             3.3.3.3              Vlanif10/Vlanif30
```

----End

Configuration Files

- Configuration file of LSRA

```
#
 sysname LSRA
#
 vlan batch 10
#
 mpls lsr-id 1.1.1.1
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
interface Vlanif10
 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 50000
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te tunnel-id 100
 mpls te affinity property 10101 mask 11011
 mpls te commit
#
interface Tunnel1/0/1
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te tunnel-id 101
 mpls te priority 6
 mpls te affinity property 10011 mask 11101
 mpls te commit
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 192.168.1.0 0.0.0.255
  mpls-te enable
#
return
```


Copyright © Huawei Technologies Co., Ltd.

- Configuration file of LSRB

```
#
 sysname LSRB
#
 vlan batch 10 20 30
#
 mpls lsr-id 2.2.2.2
 mpls
  mpls te
  mpls rsvp-te
#
interface Vlanif10
 ip address 192.168.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif20
 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 50000
 mpls rsvp-te
#
interface Vlanif30
 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 50000
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface GigabitEthernet3/0/0
 port link-type access
 port default vlan 30
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
ospf 1
 opaque-capability enable
 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
  network 192.168.3.0 0.0.0.255
  mpls-te enable
#
return
```

- Configuration file of LSRC

```
#
 sysname LSRC
#
 vlan batch 20 30
#
 mpls lsr-id 3.3.3.3
 mpls
  mpls te
  mpls rsvp-te
```


Copyright © Huawei Technologies Co., Ltd.

```
#
interface Vlanif20
 ip address 192.168.2.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif30
 ip address 192.168.3.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface GigabitEthernet3/0/0
 port link-type access
 port default vlan 30
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
ospf 1
 opaque-capability enable
 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
  mpls-te enable
#
return
```

3.21.6 Example for Configuring SRLG (TE Auto FRR)

Networking Requirements

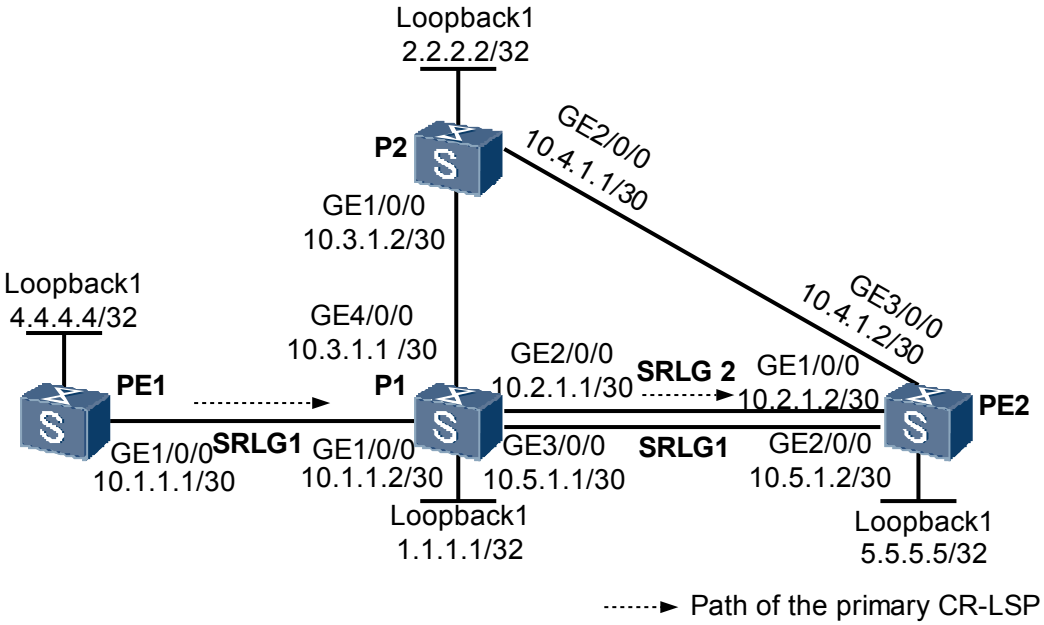
Figure 3-7 shows a networking diagram of an MPLS network. An RSVP-TE tunnel has been setup between the PE1 and PE2, the path of the tunnel is PE1 --> P1 --> PE2, and the out interface of the tunnel on P1 is GE2/0/0.

The link whose IP address is 10.2.1.0/30 and the link whose IP address is 10.5.1.0/30 are in SRLG1.

To enhance the reliability of the tunnel, TE auto FRR is required and the auto bypass tunnel's path is preferred to avoid the links that have a member in the same SRLG as the link of the primary tunnel. If SRLGs cannot be avoided, the bypass tunnel can be still set up.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-7 Networking diagram of TE Auto FRR



Switch	Interface	VLANIF interface	IP address
PE1	GigabitEthernet1/0/0	VLANIF 10	10.1.1.1/30
P1	GigabitEthernet1/0/0	VLANIF 10	10.1.1.2/30
P1	GigabitEthernet2/0/0	VLANIF 20	10.2.1.1/30
P1	GigabitEthernet3/0/0	VLANIF 30	10.5.1.1/30
P1	GigabitEthernet4/0/0	VLANIF 40	10.3.1.1/30
PE2	GigabitEthernet1/0/0	VLANIF 20	10.2.1.2/30
PE2	GigabitEthernet2/0/0	VLANIF 30	10.5.1.2/30
PE2	GigabitEthernet3/0/0	VLANIF 50	10.4.1.2/30
P2	GigabitEthernet1/0/0	VLANIF 40	10.3.1.2/30
P2	GigabitEthernet2/0/0	VLANIF 50	10.4.1.1/30

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure IP addresses and IGP on each node.
2. Enable MPLS, MPLS TE and MPLS RSVP-TE globally and on the interfaces on each node.
3. Configure IS-IS TE on each node and enable CSPF on PE1 and P1.
4. Configure SRLG numbers for the interfaces which are SRLG members.
5. Configure the SRLG path calculation mode in the system view on the PLR node.
6. Set up an RSVP-TE tunnel between PE1 and PE2, and the explicit path is PE1 --> P1 --> PE2.

Copyright © Huawei Technologies Co., Ltd.

7. Enable TE FRR on the Tunnel interface view of the ingress node and enable TE auto FRR on the out interface of the primary tunnel on PLR node.

Data Preparation

To complete the configuration, you need the following data:

- SRLG number
- SRLG path calculation mode (preferred or strict)

Procedure

Step 1 Configure VLANs that interfaces belong to.

```
<Quidway> system-view
[Quidway] sysname P1
[P1] vlan batch 10 20 30 40
[P1] interface gigabitEthernet 1/0/0
[P1-GigabitEthernet1/0/0] port hybrid pvid vlan 10
[P1-GigabitEthernet1/0/0] port hybrid untagged vlan 10
[P1-GigabitEthernet1/0/0] quit
[P1] interface gigabitEthernet 2/0/0
[P1-GigabitEthernet2/0/0] port hybrid pvid vlan 20
[P1-GigabitEthernet2/0/0] port hybrid untagged vlan 20
[P1-GigabitEthernet2/0/0] quit
[P1] interface gigabitEthernet 3/0/0
[P1-GigabitEthernet3/0/0] port hybrid pvid vlan 30
[P1-GigabitEthernet3/0/0] port hybrid untagged vlan 30
[P1-GigabitEthernet3/0/0] quit
[P1] interface gigabitEthernet 4/0/0
[P1-GigabitEthernet4/0/0] port hybrid pvid vlan 40
[P1-GigabitEthernet4/0/0] port hybrid untagged vlan 40
[P1-GigabitEthernet4/0/0] quit
```

The configurations of P2, PE1 and PE2 are similar to the configuration of P1, and are not mentioned here.

Step 2 Configure an IP address for each interface.

Configure an IP address for each interface, create loopback interfaces on nodes, and then configure the IP addresses of the loopback interfaces as MPLS LSR IDs as shown in **Figure 3-7**. For the detailed configuration, see the configuration file of this example.

The detailed configuration is not mentioned here.

Step 3 Configure an IGP.

Configure OSPF or IS-IS on each node to realize the reachability between nodes. In this example, IS-IS is configured. For the detailed configuration, see the configuration file of this example.

Step 4 Configure basic MPLS functions.

On each node, configure an LSR ID and enable MPLS in the system view. Enable MPLS in the interface view. For the detailed configuration, see the configuration file of this example.

Step 5 Configure basic MPLS TE functions.

On each node, enable MPLS-TE and MPLS RSVP-TE in the MPLS view and in the interface view. Configure the maximum bandwidth and maximum reservable bandwidth for each interface. For the detailed configuration, see the configuration file of this example.

Step 6 Configure IS-IS TE and CSPF.

Copyright © Huawei Technologies Co., Ltd.

Configure IS-IS TE on each node and CSPF on PE1 and P1. For detailed configuration, see the configuration file of this example.

Step 7 Configure SRLG

On P1, configure SRLG1 for the link whose IP address is 10.2.1.0/30 and the link whose IP address is 10.5.1.0/30.

```
[P1] interface vlanif 20
[P1-Vlanif20] mpls te srlg 1
[P1-Vlanif20] quit
[P1] interface vlanif 30
[P1-Vlanif30] mpls te srlg 1
[P1-Vlanif30] quit
```

Configure the SRLG path calculation mode on the PLR node.

```
[P1] mpls
[P1-mpls] mpls te srlg path-calculation preferred
```

Run the **display mpls te srlg** command on P1, and you can view information about the SRLG and the interfaces that belong to the SRLG.

```
[P1] display mpls te srlg all
Total SRLG supported : 512
Total SRLG configured : 2


 SRLG    1:               Vlanif20            Vlanif30
```

Run the **display mpls te link-administration srlg-information** command on P1, and you can view information about the SRLG memberships of the interfaces.

```
[P1] display mpls te link-administration srlg-information

  SRLGs on Vlanif20:
              1

  SRLGs on Vlanif30:
              1
```

Run the **display mpls te cspf tedb srlg** command on P1, and you can view TEDB information of the specified SRLG.

```
[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
```

Step 8 Configure the explicit path of the primary tunnel.

Configure the explicit path of 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] quit
```

Display information about the explicit path on PE1.

```
[PE1] display explicit-path main
Path Name : main        Path Status : Enabled
 1      10.1.1.2          Strict      Include
```


Copyright © Huawei Technologies Co., Ltd.

```
 2       10.2.1.2          Strict      Include
 3       5.5.5.5           Strict      Include
```

Step 9 Configure the tunnel interfaces for the primary tunnel.

Create a tunnel interface on PE1, specify an explicit path, and configure the tunnel bandwidth.

```
[PE1] interface tunnel 1/0/0
[PE1-Tunnel1/0/0] ip address unnumbered interface loopback 1
[PE1-Tunnel1/0/0] tunnel-protocol mpls te
[PE1-Tunnel1/0/0] destination 5.5.5.5
[PE1-Tunnel1/0/0] mpls te tunnel-id 100
[PE1-Tunnel1/0/0] mpls te path explicit-path main
[PE1-Tunnel1/0/0] mpls te commit
```

Run the **display interface tunnel 1/0/0** command on PE1, and you can view that the status of the tunnel is **UP**.

```
[PE1] display interface tunnel 1/0/0
Tunnel1/0/0 current state : UP
Line protocol current state : UP
...
```

NOTE

The output of the **display interface tunnel 1/0/0** command displays information that you needs to concern and "..." indicates that information is omitted.

Step 10 Configure TE auto FRR.

Enable TE auto FRR on the Vlanif20 of P1.

```
[P1] interface vlanif 20
[P1-Vlanif20] mpls te auto-frr link
[P1-Vlanif20] quit
```

Enable TE FRR on the Tunnel interface view of PE1.

```
[PE1] interface tunnel 1/0/0
[PE1-Tunnel1/0/0] mpls te fast-reroute
[PE1-Tunnel1/0/0] mpls te commit
```

Run the **display interface tunnel path Tunnel1/0/0** command on PE1, and you can view that the local protection is available on the out interface (10.2.1.1) of the primary tunnel on P1.

```
[PE1] display mpls te tunnel path Tunnel1/0/0
 Tunnel Interface Name : Tunnel1/0/0
 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
```

Step 11 Verify the configuration.

Run the **display mpls te tunnel name Tunnel1/0/0 verbose** command on P1, and you can view that the primary tunnel is bound with a bypass tunnel, that is Tunnel0/0/2048. The FRR next hop is 10.4.1.2.

```
[P1] display mpls te tunnel name Tunnel1/0/0 verbose
    No                    :  1
    Tunnel-Name           :  Tunnel1/0/0
    TunnelIndex           :  1          LSP Index        :  3072
    Session ID            :  100        LSP ID           :  1
    Lsr Role              :  Transit
    Ingress LSR ID        :  4.4.4.4
```


Copyright © Huawei Technologies Co., Ltd.

```
    Egress LSR ID           :  5.5.5.5
    In-Interface            :  Vlanif10
    Out-Interface           :  Vlanif20
    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
        --------------------------------
                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        :  10.4.1.2
    ReferAutoBypassHandle   :  2049
    FrrPrevTunnelTableIndex :  -            FrrNextTunnelTableIndex:  -
    Bypass Attribute(Not configured)
    Setup Priority          :  -            Hold Priority     :  -
    HopLimit                :  -            Bandwidth         :  -
    IncludeAnyGroup         :  -            ExcludeAnyGroup   :  -
    IncludeAllGroup         :  -
    Bypass Unbound Bandwidth Info(Kbit/sec)
        --------------------------------
              BFD Information
    --------------------------------
    NextSessionTunnelIndex  :  -            PrevSessionTunnelIndex:  -
    NextLspId               :  -            PrevLspId         :  -
```

Run the **display mpls te tunnel path Tunnel0/0/2048** command on the P1 to check the path of the bypass tunnel, you can view that the path of the bypass tunnel is 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
```

Run the **shutdown** command on Vlanif40 of P1.

```
[P1] interface vlanif 40
[P1-Vlanif40] shutdown
[P1-Vlanif40] return
```

Run the **display interface tunnel 1/0/0** command on PE1 and you can view that the status of the primary tunnel is **UP**.

```
[PE1] display interface tunnel 1/0/0
Tunnel1/0/0 current state : UP
Line protocol current state : UP
...
```

NOTE

The output of the **display interface tunnel 1/0/0** command displays information that needs concerns and "..." indicates that information is omitted.

Run the **display mpls te tunnel name Tunnel1/0/0 verbose** command on P1, and you can view that the primary tunnel is still bound with the Tunnel0/0/2048 and the FRR next hop is 10.5.1.2.

Copyright © Huawei Technologies Co., Ltd.

```
<P1> display mpls te tunnel name Tunnel1/0/0 verbose
    No                     :  1
    Tunnel-Name            :  Tunnel1/0/0
    TunnelIndex            :  1           LSP Index         :  2048
    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           :  Vlanif10
    Out-Interface          :  Vlanif20
    Sign-Protocol          :  RSVP TE     Resv Style        :  SE
    IncludeAnyAff          :  0x0         ExcludeAnyAff     :  0x0
    IncludeAllAff          :  0x0
    ER-Hop Table Index     :  -           AR-Hop Table Index:  5
    C-Hop Table Index      :  -
    PrevTunnelIndexInSession:  -          NextTunnelIndexInSession:  -
    PSB Handle             :  65547
    Created Time           :  2009/03/30 09:52:03
        -------------------------------
                FRR Information
    -------------------------------
    Primary LSP Info
    TE Attribute Flag      :  0x63        Protected Flag    :  0x1
    Bypass In Use          :  Not Used
    Bypass Tunnel Id       :  201359400
    BypassTunnel           :  Tunnel Index[Tunnel0/0/2048], InnerLabel[3]
    Bypass Lsp ID          :  -           FrrNextHop        :  10.5.1.2
    ReferAutoBypassHandle  :  2049
    FrrPrevTunnelTableIndex :  -          FrrNextTunnelTableIndex:  -
    Bypass Attribute(Not configured)
    Setup Priority         :  -           Hold Priority     :  -
    HopLimit               :  -           Bandwidth         :  -
    IncludeAnyGroup        :  -           ExcludeAnyGroup   :  -
    IncludeAllGroup        :  -
        -------------------------------
                BFD Information
    -------------------------------
    NextSessionTunnelIndex  :  -          PrevSessionTunnelIndex:  -
    NextLspId              :  -           PrevLspId         :  -
```

Run the **display mpls te tunnel path Tunnel0/0/2048** command on P1, you can view the path of the auto bypass tunnel.

```
[P1] display mpls te tunnel path Tunnel0/0/2048
 Tunnel Interface Name : Tunnel0/0/2048
 Lsp ID : 123.1.1.1 :2049 :2
 Hop Information
  Hop 0   10.5.1.1
  Hop 1   10.5.1.2
  Hop 2   5.5.5.5
```

You can view that the path of the auto bypass tunnel is P1-->PE2 rather than P1-->P2-->PE2. That is because that the SRLG path calculation mode is configured as **preferred**. Therefore, CSPF tries to calculate the path of the bypass tunnel to avoid the links in the same SRLG as the protected interface(s); if the calculation fails, CSPF does not take the SRLG as a constraint.

----End

Configuration Files

- Configuration file of PE1

```
#
 sysname PE1
#
vlan batch 10
#
 mpls lsr-id 4.4.4.4
```


Copyright © Huawei Technologies Co., Ltd.

```
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
 explicit-path main
  next hop 10.1.1.2
  next hop 10.2.1.2
  next hop 5.5.5.5
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0004.00
 traffic-eng level-1-2
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
  mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 isis enable 1
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 5.5.5.5
 mpls te tunnel-id 100
 mpls te record-route
  mpls te path explicit-path main
 mpls te fast-reroute
 mpls te commit
#
return
```

- Configuration file of P1

```
#
 sysname P1
#
vlan batch 10 20 30 40
#
 mpls lsr-id 1.1.1.1
 mpls
  mpls te
  mpls rsvp-te
  mpls te srlg path-calculation preferred
  mpls te cspf
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0001.00
 traffic-eng level-1-2
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif20
 ip address 10.2.1.1 255.255.255.252
 isis enable 1
```


Copyright © Huawei Technologies Co., Ltd.

```
 mpls
 mpls te
 mpls te auto-frr link
 mpls te srlg 1
 mpls rsvp-te
#
interface Vlanif30
 ip address 10.5.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te srlg 1
 mpls rsvp-te
#
interface Vlanif40
 ip address 10.3.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface GigabitEthernet 3/0/0
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
interface GigabitEthernet 4/0/0
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of P2

```
#
 sysname P2
#
vlan batch 40 50
#
 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 Vlanif40
 ip address 10.3.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif50
 ip address 10.4.1.1 255.255.255.252
 isis enable 1
 mpls
```


Copyright © Huawei Technologies Co., Ltd.

```
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
vlan batch 20 30 50
#
 mpls lsr-id 5.5.5.5
 mpls
  mpls te
  mpls rsvp-te
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0006.00
 traffic-eng level-1-2
#
interface Vlanif20
 ip address 10.2.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif30
 ip address 10.5.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif50
 ip address 10.4.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 5.5.5.5 255.255.255.255
 isis enable 1
#
return
```

3.21.7 Example for Configuring SRLG (Hot-standby)

Networking Requirements

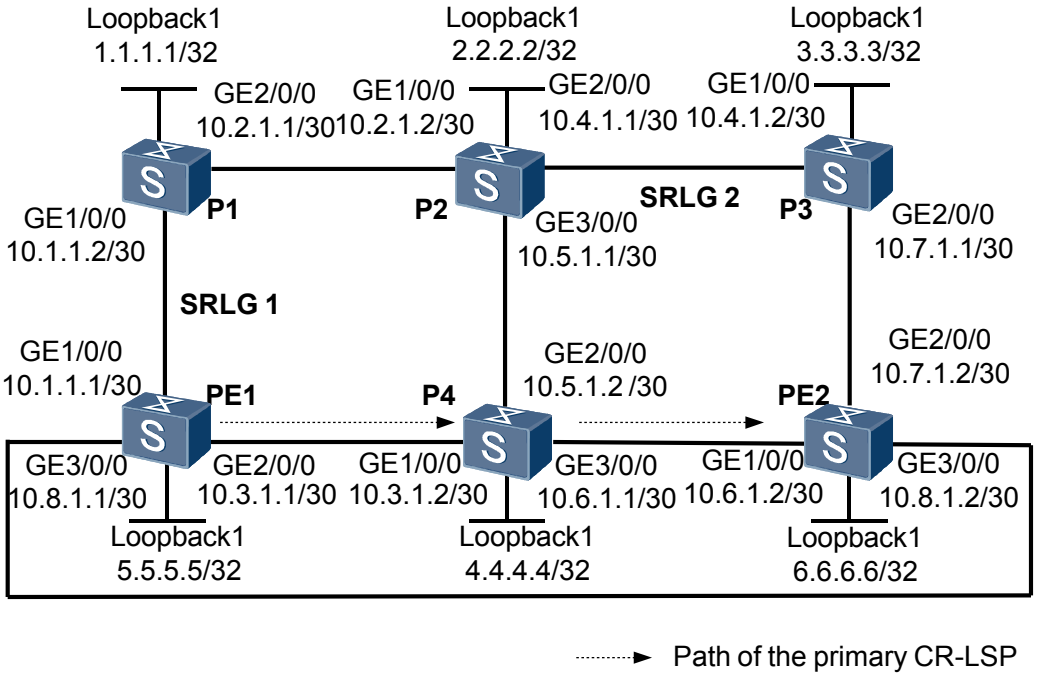
Figure 3-8 shows a networking diagram of an MPLS network. An RSVP-TE tunnel has been setup between the PE1 and PE2 and the path of the tunnel is PE1 --> P4 --> PE2.

Copyright © Huawei Technologies Co., Ltd.

The link PE1 --> P1--> P2 --> P4 and the link PE1 --> P4 are in the same SRLG (SRLG1 for example); the link P4 --> PE2 and the link P4 --> P2 --> P3 --> PE2 are in the same SLRG (take SRLG2 for example.)

To enhance the reliability of the tunnel, a hot standby CR-LSP is required and the backup tunnel's path should avoid the links that have a member in the same SRLG as the link of the primary tunnel.

Figure 3-8 Networking diagram of TE FRR



Switch	Interface	VLANIF interface	IP address
P1	GigabitEthernet1/0/0	VLANIF 10	10.1.1.2/30
P1	GigabitEthernet2/0/0	VLANIF 20	10.2.1.1/30
P2	GigabitEthernet1/0/0	VLANIF 20	10.2.1.2/30
P2	GigabitEthernet2/0/0	VLANIF 30	10.4.1.1/30
P2	GigabitEthernet3/0/0	VLANIF 40	10.5.1.1/30
P3	GigabitEthernet1/0/0	VLANIF 30	10.4.1.2/30
P3	GigabitEthernet2/0/0	VLANIF 50	10.7.1.1/30
PE2	GigabitEthernet1/0/0	VLANIF 70	10.6.1.2/30
PE2	GigabitEthernet2/0/0	VLANIF 50	10.7.1.2/30
PE2	GigabitEthernet3/0/0	VLANIF 60	10.8.1.2/30
P4	GigabitEthernet1/0/0	VLANIF 80	10.3.1.2/30
P4	GigabitEthernet2/0/0	VLANIF 40	10.5.1.2/30
P4	GigabitEthernet3/0/0	VLANIF 70	10.6.1.1/30
PE1	GigabitEthernet1/0/0	VLANIF 10	10.1.1.1/30

Copyright © Huawei Technologies Co., Ltd.

PE1	GigabitEthernet2/0/0	VLANIF 80	10.3.1.1/30
PE1	GigabitEthernet3/0/0	VLANIF 60	10.8.1.1/30

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure IP addresses and IGP on all nodes.
2. Enable MPLS, MPLS TE and MPLS RSVP-TE globally and on the interfaces on all nodes.
3. Set up an RSVP-TE tunnel between PE1 and PE2, and the explicit path is PE1 --> P1 --> PE2.
4. Configure SRLG number on the outgoing interface of the link that is in the same SRLG as the link of the primary tunnel.
5. Configure SRLG path calculation mode on the system view of the Ingress node.
6. Configure a hot-standby CR-LSP.

Data Preparation

To complete the configuration, you need the following data:

- SRLG number
- SRLG path calculation mode (preferred or strict)

Procedure

Step 1 Configure VLANs that interfaces belong to.

```
<Quidway> system-view
[Quidway] sysname P1
[P1] vlan batch 10 20
[P1] interface gigabitEthernet 1/0/0
[P1-GigabitEthernet1/0/0] port hybrid pvid vlan 10
[P1-GigabitEthernet1/0/0] port hybrid untagged vlan 10
[P1-GigabitEthernet1/0/0] quit
[P1] interface gigabitEthernet 2/0/0
[P1-GigabitEthernet2/0/0] port hybrid pvid vlan 20
[P1-GigabitEthernet2/0/0] port hybrid untagged vlan 20
[P1-GigabitEthernet2/0/0] quit
```

P2, P3, P4, PE1 and PE2 are similar to the configuration of P1, and are not mentioned here.

Step 2 Configure an IP address for each VLANIF interface.

Configure an IP address for each interface, create loopback interfaces on nodes, and then configure the IP addresses of the loopback interfaces to MPLS LSR IDs as shown in **Figure 3-8**. For detailed configuration, see the configuration file of this example.

The detailed configuration is not mentioned here.

Step 3 Configure IGP.

Configure OSPF or IS-IS on each node to realize the reachability between nodes. In this example, IS-IS is configured. For detailed configuration, see the configuration file of this example.

Copyright © Huawei Technologies Co., Ltd.

Step 4 Configure basic MPLS functions.

On each node, configure an LSR ID and enable MPLS in the system view. Enable MPLS in the interface view. For detailed configuration, see the configuration file of this example.

Step 5 Configure basic MPLS TE functions and enable MPLS RSVP-TE.

On each node, enable MPLS-TE and MPLS RSVP-TE in the system view and in the interface view. For detailed configuration, see the configuration file of this example.

Step 6 Configure IS-IS TE and CSPF.

Configure IS-IS TE on each node and CSPF on PE1. For detailed configuration, see the configuration file of this example.

Step 7 Configure the explicit path of the primary CR-LSP.

Configure the explicit path of 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] quit
```

Display information about the explicit path on PE1.

```
[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
```

Step 8 Configure the tunnel interfaces for the primary tunnel.

Create a tunnel interface on PE1, specify an explicit path, and configure the tunnel bandwidth.

```
[PE1] interface tunnel 1/0/0
[PE1-Tunnel1/0/0] ip address unnumbered interface loopback 1
[PE1-Tunnel1/0/0] tunnel-protocol mpls te
[PE1-Tunnel1/0/0] destination 6.6.6.6
[PE1-Tunnel1/0/0] mpls te tunnel-id 100
[PE1-Tunnel1/0/0] mpls te path explicit-path main
[PE1-Tunnel1/0/0] mpls te commit
```

Run the **display interface tunnel 1/0/0** command on PE1, and you can view that the status of the tunnel is **UP**.

```
[PE1] display interface tunnel 1/0/0
Tunnel1/0/0 current state : UP
Line protocol current state : UP
...
```

The output of the **display interface tunnel 1/0/0** command displays information that you need to concern and "..." indicates that information is omitted.

Step 9 Configure SRLG

Configure SRLG1 for the link PE1 --> P1 and the link PE1 --> P4.

```
[PE1] interface vlanif 10
[PE1-Vlanif10] mpls te srlg 1
[PE1-Vlanif10] quit
[PE1] interface vlanif 80
[PE1-Vlanif80] mpls te srlg 1
[PE1-Vlanif80] mpls te srlg 2
```


Copyright © Huawei Technologies Co., Ltd.

Configure SRLG2 for the link P2 --> P3.

```
[P2] interface vlanif 30
[P2-Vlanif30] mpls te srlg 2
[P2-Vlanif30] quit
```

Configure the SRLG path calculation mode on the ingress.

```
[PE1] mpls
[PE1-mpls] mpls te srlg path-calculation strict
[PE1-mpls] quit
```

Run the **display mpls te srlg** command, and you can view information about the SRLG and the interfaces that belong to that SRLG.

```
[P1] display mpls te srlg all
Total SRLG supported : 512
Total SRLG configured : 2


 SRLG    1:               Vlanif10            Vlanif20

 SRLG    2:               Vlanif20
```

Run the **display mpls te link-administration srlg-information** command, and you can view information about the memberships on the interface.

```
[PE1] display mpls te link-administration srlg-information

  SRLGs on Vlanif10:                    1

  SRLGs on Vlanif80:                    1         2
```

Run the **display mpls te cspf tedb srlg** command, and you can view TEDB information of the specified SRLG.

Take the display on PE1 as an example.

```
[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
[PE1] display mpls te cspf tedb srlg 2
Interface-Address   IGP-Type            Area
10.3.1.1            ISIS                1
10.3.1.1            ISIS                2
10.4.1.1            ISIS                1
10.4.1.1            ISIS                2
```

Step 10 Configure a hot-standby CR-LSP on the ingress.

Configure PE1.

```
[PE1] interface tunnel 1/0/0
[PE1-Tunnel1/0/0] mpls te backup hot-standby
[PE1-Tunnel1/0/0] mpls te commit
```

Run the **display mpls te hot-standby state interface tunnel 1/0/0** command on PE1, and you can view information about the hot standby.

```
[PE1] display mpls te hot-standby state interface tunnel 1/0/0
-------------------------------------------------------------
Verbose information about the Tunnel1/0/0 hot-standby state
-------------------------------------------------------------
tunnel name                           : Tunnel1/0/0
session id                            : 100
```


Copyright © Huawei Technologies Co., Ltd.

```
main LSP token                          : 0x100201a
hot-standby LSP token                   : 0x100201b
HSB switch result                       : main LSP
WTR                                        : 10s
```

Step 11 Verify the configuration.

Run the **shutdown** command on Vlanif60 of PE1.

```
[PE1] interface vlanif 60
[PE1-Vlanif60] shutdown
[PE1-Vlanif60] quit
```

Run the **display mpls te hot-standby state interface tunnel 1/0/0** command on PE1 again, and you can view that the hot-standby LSP token is 0x0. That is, the hot-standby LSP is not set up though paths are available to set up the hot-standby LSP.

```
[PE1] display mpls te hot-standby state interface tunnel 1/0/0
-------------------------------------------------------------
Verbose information about the Tunnel1/0/0 hot-standby state
-------------------------------------------------------------
tunnel name                             : Tunnel1/0/0
session id                              : 100
main LSP token                          : 0x100201c
hot-standby LSP token                   : 0x0
HSB switch result                       : main LSP
WTR                                     : 10s
```

----End

Configuration Files

- Configuration file of PE1

```
#
 sysname PE1
#
vlan batch 10 80 60
#
 mpls lsr-id 5.5.5.5
 mpls
  mpls te
  mpls rsvp-te
  mpls te srlg path-calculation strict
  mpls te cspf
#
 explicit-path main
  next hop 10.3.1.2
  next hop 10.6.1.2
  next hop 6.6.6.6
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0005.00
 traffic-eng level-1-2
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te srlg 1
 mpls rsvp-te
#
interface Vlanif80
 ip address 10.2.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
```


Copyright © Huawei Technologies Co., Ltd.

```
 mpls te srlg 1
 mpls te srlg 2
 mpls rsvp-te
#
interface Vlanif60
 ip address 10.8.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 80
 port hybrid untagged vlan 80
#
interface GigabitEthernet 3/0/0
 port hybrid pvid vlan 60
 port hybrid untagged vlan 60
#
interface LoopBack1
 ip address 5.5.5.5 255.255.255.255
 isis enable 1
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 6.6.6.6
 mpls te tunnel-id 100
 mpls te record-route
 mpls te path explicit-path main
 mpls te backup hot-standby
 mpls te commit
#
return
```

- Configuration file of P1

```
#
 sysname P1
#
vlan batch 10 20
#
 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 Vlanif10
 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 50000
 mpls rsvp-te
#
interface Vlanif20
 ip address 10.2.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
```


Copyright © Huawei Technologies Co., Ltd.

```
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of P2

```
#
 sysname P2
#
vlan batch 20 30 40
#
 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 Vlanif20
 ip address 10.2.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif30
 ip address 10.4.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te srlg 2
 mpls rsvp-te
#
interface Vlanif40
 ip address 10.5.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
interface GigabitEthernet 3/0/0
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
```


Copyright © Huawei Technologies Co., Ltd.

```
#
return
```

- Configuration file of P3

```
#
 sysname P3
#
vlan batch 30 50
#
 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 Vlanif30
 ip address 10.4.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif50
 ip address 10.7.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of P4

```
#
 sysname P4
#
vlan batch 80 40 70
#
 mpls lsr-id 4.4.4.4
 mpls
  mpls te
  mpls rsvp-te
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0004.00
 traffic-eng level-1-2
#
interface Vlanif80
 ip address 10.3.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
```


Copyright © Huawei Technologies Co., Ltd.

```
interface Vlanif40
 ip address 10.5.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif70
 ip address 10.6.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 80
 port hybrid untagged vlan 80
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface GigabitEthernet 3/0/0
 port hybrid pvid vlan 70
 port hybrid untagged vlan 70
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
vlan batch 70 50 60
#
 mpls lsr-id 6.6.6.6
 mpls
  mpls te
  mpls rsvp-te
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0006.00
 traffic-eng level-1-2
#
interface Vlanif70
 ip address 10.6.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif50
 ip address 10.7.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif60
 ip address 10.8.1.2 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
```


Copyright © Huawei Technologies Co., Ltd.

```
 port hybrid pvid vlan 70
 port hybrid untagged vlan 70
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
interface GigabitEthernet 3/0/0
 port hybrid pvid vlan 60
 port hybrid untagged vlan 60
#
interface LoopBack1
 ip address 6.6.6.6 255.255.255.255
 isis enable 1
#
Return
```

3.21.8 Example for Configuring MPLS TE FRR

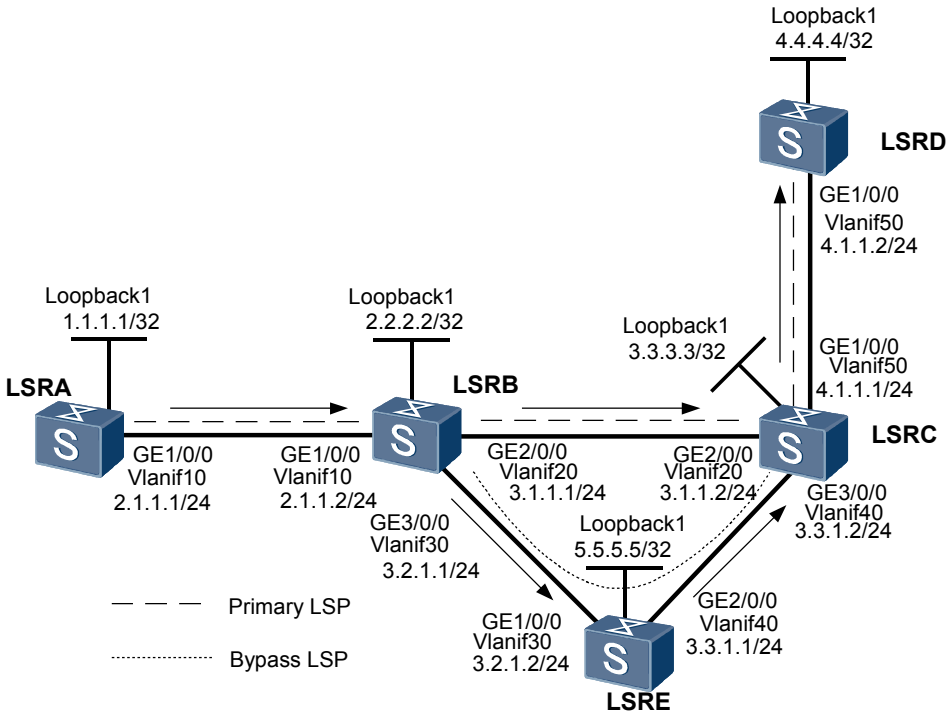
Networking Requirements

As shown in **Figure 3-9**, the primary LSP is LSRA->LSRB-> LSRC->LSRD, and the link from LSRB to LSRC requires link protection through FRR.

Establish a bypass LSP, and use the path LSRB ->LSRE-> LSRC. Here, LSRB is the PLR and LSRC is the MP.

Use the explicit path to establish the primary tunnel and the bypass tunnel of MPLS TE. RSVP-TE is used.

Figure 3-9 Networking diagram for configuring MPLS TE FRR



Copyright © Huawei Technologies Co., Ltd.

Configuration Roadmap

The configuration roadmap is as follows:

1. Set up a primary tunnel and enable FRR on the tunnel interface.
2. Configure a bypass tunnel on the ingress node of the protected link, that is, PLR, and specify the bandwidth that the bypass tunnel can protect and the interface of the protected link in the tunnel interface view.

Data Preparation

To complete the configuration, you need the following data:

- IS-IS area ID, originating system ID, and IS-IS level of each node
- Maximum bandwidth and maximum reservable bandwidth for the link along the tunnel
- Explicit paths of the primary tunnel and the bypass tunnel
- Interface names, IP addresses, destination IP addresses, tunnel IDs, signaling protocol (RSVP-TE) of the primary tunnel and the bypass tunnel
- Interface protected by the bypass tunnel

Procedure

Step 1 Create VLANs and VLANIF interfaces, and assign IP addresses to the VLANIF interfaces.

As shown in **Figure 3-9**, configure IP addresses and masks for the interfaces, including loopback interfaces. The configuration details are not mentioned here.

Step 2 Configure an IGP.

Configure IS-IS on all the nodes to advertise the host routes of the LSR IDs. The configuration details are not mentioned here.

After the configuration, run the **display ip routing-table** command on each node, and you can view that the nodes learn the routes from each other.

Step 3 Configure basic MPLS functions and enable MPLS TE, RSVP-TE, CSPF, and IS-IS TE.

Configure LSRA.

```
[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 vlanif 10
[LSRA-Vlanif10] mpls
[LSRA-Vlanif10] mpls te
[LSRA-Vlanif10] mpls rsvp-te
[LSRA-Vlanif10] quit
[LSRA] isis
[LSRA-isis-1] cost-style wide
[LSRA-isis-1] traffic-eng level-2
```


Copyright © Huawei Technologies Co., Ltd.

NOTE

The configurations on LSRB, LSRC, LSRD, and LSRE are similar to the configuration on LSRA, and are not mentioned here. CSPF needs to be enabled only on the ingress node of the primary tunnel (LSRA) and the ingress node of the bypass tunnel (LSRB); CSPF does not need to be enabled on LSRC, LSRD, and LSRE.

Step 4 Configure the MPLS TE attributes of the link.

Set the maximum link bandwidth to 100 Mbit/s and maximum reservable bandwidth to 100 Mbit/s on LSRA, LSRB, LSRC, LSRD, and LSRE.

Configure LSRA.

```
[LSRA] interface vlanif 10
[LSRA-Vlanif10] mpls te bandwidth max-reservable-bandwidth 100000
[LSRA-Vlanif10] quit
```

Configure LSRB.

```
[LSRB] interface vlanif 20
[LSRB-Vlanif20] mpls te bandwidth max-reservable-bandwidth 100000
[LSRB-Vlanif20] quit
[LSRB] interface vlanif 30
[LSRB-Vlanif30] mpls te bandwidth max-reservable-bandwidth 100000
[LSRB-Vlanif30] quit
```

Configure LSRC.

```
[LSRC] interface vlanif 50
[LSRC-Vlanif50] mpls te bandwidth max-reservable-bandwidth 100000
[LSRC-Vlanif50] quit
```

Configure LSRE.

```
[LSRE] interface vlanif 40
[LSRE-Vlanif40] mpls te bandwidth max-reservable-bandwidth 100000
[LSRE-Vlanif40] quit
```

Step 5 # Establish an MPLS TE tunnel on LSRA that is the ingress node of the primary LSP.

Configure the explicit path of the primary 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 of the primary LSP.

```
[LSRA] interface tunnel 1/0/0
[LSRA-Tunnel1/0/0] ip address unnumbered interface loopback 1
[LSRA-Tunnel1/0/0] tunnel-protocol mpls te
[LSRA-Tunnel1/0/0] destination 4.4.4.4
[LSRA-Tunnel1/0/0] mpls te tunnel-id 100
[LSRA-Tunnel1/0/0] mpls te signal-protocol rsvp-te
[LSRA-Tunnel1/0/0] mpls te path explicit-path pri-path
```

Enable FRR.

```
[LSRA-Tunnel1/0/0] mpls te fast-reroute
[LSRA-Tunnel1/0/0] mpls te commit
[LSRA-Tunnel1/0/0] quit
```

After the configuration, run the **display interface tunnel** command on LSRA, and you can view that the status of Tunnel 1/0/0 is Up.

Copyright © Huawei Technologies Co., Ltd.

```
[LSRA] display interface tunnel
Tunnel1/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time: 2008-11-16, 12:26:17
Description : HUAWEI, Quidway Series, Tunnel1/0/0 Interface
The Maximum Transmit Unit is 1500 bytes
Internet Address is unnumbered, using address of LoopBack1(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,
    300 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets output,  0 bits
    0 output error
```

Run the **display mpls te tunnel-interface** command on LSRA, and you can view detailed information about the tunnel.

```
[LSRA] display mpls te tunnel-interface
  Tunnel Name          :  Tunnel1/0/0
  Tunnel State Desc    :  CR-LSP is Up
  Tunnel Attributes    :
    LSP ID             :  1.1.1.1:1
    Session ID         :  100
    Admin State        :  UP               Oper State   :  UP
    Ingress LSR ID     :  1.1.1.1          Egress LSR ID:  4.4.4.4
    Signaling Prot     :  RSVP             Resv Style   :  SE
    Class Type         :  CLASS 0          Tunnel BW    :  0 kbps
    Reserved BW        :  50000 kbps
    Setup Priority     :  7                Hold Priority:  7
    Hop Limit          :  -
    Secondary Hop Limit :  -
    BestEffort Hop Limit:  -
    Affinity Prop/Mask  :  0x0/0x0
    Explicit Path Name  :  pri-path
    Secondary Affinity Prop/Mask:  0x0/0x0
    Secondary Explicit Path Name:  -
    BestEffort Affinity Prop/Mask:  0x0/0x0
    Tie-Breaking Policy :  None
    Metric Type        :  None
    Record Route       :  Enabled          Record Label :  Enabled
    FRR Flag           :  Enabled          BackUpBW Flag:  Not Supported
    BackUpBW Type      :  -                BackUpBW     :  -
    Route Pinning      :  Disabled
    Retry Limit        :  5                Retry Interval:  10 sec
    Reopt              :  Disabled         Reopt Freq   :  -
    Back Up Type       :  None
    Back Up LSPID      :  -
    Auto BW            :  Disabled         Auto BW Freq :  -
    Min BW             :  -                Max BW       :  -
    Current Collected BW:  -
    Interfaces Protected:  -
    Car Policy         :  Disabled
    Tunnel  Group      :  Primary
    Primary Tunnel Sum  :  -
    Primary Tunnel     :  -
    Backup  Tunnel     :  -
    IPTN    InLabel    :  -
    Group   Status     :  Up
    Oam     Status     :  Up
    Bfd Capability     :  Disable
    BestEffort         :  Disabled             IsBestEffortPath:  Non-existent
```

Step 6 Configure a bypass tunnel on LSRB that functions as the PLR.

Configure the explicit path of the bypass 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
```


Copyright © Huawei Technologies Co., Ltd.

```
[LSRB-explicit-path-by-path] next hop 3.3.3.3
[LSRB-explicit-path-by-path] quit
```

Configure the bypass tunnel.

```
[LSRB] interface tunnel 3/0/0
[LSRB-Tunnel3/0/0] ip address unnumbered interface loopback 1
[LSRB-Tunnel3/0/0] tunnel-protocol mpls te
[LSRB-Tunnel3/0/0] destination 3.3.3.3
[LSRB-Tunnel3/0/0] mpls te tunnel-id 300
[LSRB-Tunnel3/0/0] mpls te signal-protocol rsvp-te
[LSRB-Tunnel3/0/0] mpls te path explicit-path by-path
```

Configure the bandwidth that can be protected by the bypass tunnel.

```
[LSRB-Tunnel3/0/0] mpls te bypass-tunnel
```

Bind the bypass tunnel to the protected interface.

```
[LSRB-Tunnel3/0/0] mpls te protected-interface vlanif 20
[LSRB-Tunnel3/0/0] mpls te commit
[LSRB-Tunnel3/0/0] quit
```

After the configuration, run the **display interface tunnel** command on LSRB, and you can view that the status of Tunnel 3/0/0 is Up.

Run the **display mpls lsp** command on all the nodes, and you can view the LSP entry and that two LSPs pass through LSRB and LSRC.

```
[LSRA] display mpls lsp
------------------------------------------------------------------------------
                LSP Information: RSVP LSP
------------------------------------------------------------------------------
FEC                In/Out Label  In/Out IF                      Vrf Name
4.4.4.4/32         NULL/13312    -/Vlanif10

[LSRB] display mpls lsp
------------------------------------------------------------------------------
                LSP Information: RSVP LSP
------------------------------------------------------------------------------
FEC                In/Out Label  In/Out IF                      Vrf Name
4.4.4.4/32         13312/13312   Vlanif10/Vlanif20
3.3.3.3/32         NULL/13312    -/Vlanif30
[LSRC] display mpls lsp
------------------------------------------------------------------------------
                LSP Information: RSVP LSP
------------------------------------------------------------------------------
FEC                In/Out Label  In/Out IF                      Vrf Name
4.4.4.4/32         13312/3       Vlanif20/Vlanif50
3.3.3.3/32         3/NULL        Vlanif40/-
[LSRD] display mpls lsp
------------------------------------------------------------------------------
                LSP Information: RSVP LSP
------------------------------------------------------------------------------
FEC                In/Out Label  In/Out IF                      Vrf Name
4.4.4.4/32         3/NULL       Vlanif50/-
[LSRE] display mpls lsp
------------------------------------------------------------------------------
                LSP Information: RSVP LSP
------------------------------------------------------------------------------
FEC                In/Out Label  In/Out IF                      Vrf Name
3.3.3.3/32         13312/3      Vlanif30/Vlanif40
```

Run the **display mpls te tunnel** command on all the nodes, and you can view the establishment of the tunnel and that two tunnels pass through LSRB and LSRC.

```
[LSRA] display mpls te tunnel
LSP-Id                    Destination          In/Out-If
1.1.1.1:100:1             4.4.4.4              -/Vlanif10
```


Copyright © Huawei Technologies Co., Ltd.

```
[LSRB] display mpls te tunnel
LSP-Id                    Destination          In/Out-If
1.1.1.1:100:1             4.4.4.4              Vlanif10/Vlanif20
2.2.2.2:300:2             3.3.3.3              -/Vlanif30
[LSRC] display mpls te tunnel
LSP-Id                    Destination          In/Out-If
1.1.1.1:100:1             4.4.4.4              Vlanif20/Vlanif50
2.2.2.2:300:2             3.3.3.3              Vlanif40/-
[LSRD] display mpls te tunnel
LSP-Id                    Destination          In/Out-If
1.1.1.1:100:1             4.4.4.4              Vlanif50/-

[LSRE] display mpls te tunnel
LSP-Id                    Destination          In/Out-If
2.2.2.2:300:1             3.3.3.3              Vlanif20/Vlanif40
```

Run the **display mpls lsp verbose** command on LSRB, and you can view that the bypass tunnel is bound to the outgoing interface VLANIF 20 and is not in use currently.

```
[LSRB] display mpls lsp verbose
------------------------------------------------------------------------------
                 LSP Information: RSVP LSP
------------------------------------------------------------------------------
  No                  :  1
  SessionID           :  100
  IngressLsrID        :  1.1.1.1
  LocalLspID          :  1
  Tunnel-Interface    :  Tunnel1/0/0
  Fec                 :  4.4.4.4/32
  TunnelTableIndex    :  0x6
  Nexthop             :  3.1.1.2
  In-Label            :  13312
  Out-Label           :  13312
  In-Interface        :  Vlanif10
  Out-Interface       :  Vlanif20
  LspIndex            :  4104
  Token               :  0x10000
  LsrType             :  Transit
  Mpls-Mtu            :  1500
  TimeStamp           :  1265sec
  Bfd-State           :  ---

  No                  :  2
  SessionID           :  300
  IngressLsrID        :  2.2.2.2
  LocalLspID          :  2
  Tunnel-Interface    :  Tunnel3/0/0
  Fec                 :  3.3.3.3/32
  TunnelTableIndex    :  0x4
  Nexthop             :  3.2.1.2
  In-Label            :  NULL
  Out-Label           :  13313
  In-Interface        :  ----------
  Out-Interface       :  Vlanif30
  LspIndex            :  4106
  Token               :  0x10000
  LsrType             :  Ingress
  Mpls-Mtu            :  1500
  TimeStamp           :  528sec
  Bfd-State           :  ---
```

Step 7 Verify the configuration.

Make the protected outgoing interface on the PLR invalid.

```
[LSRB] interface vlanif 20
[LSRB-Vlanif20] shutdown
```

Run the **display interface tunnel 1/0/0** command on LSRA, and you can view the status of the primary LSP and that the status of the tunnel interface is still Up.

Copyright © Huawei Technologies Co., Ltd.

Run the **tracert lsp te tunnel 1/0/0** command on LSRA, and you can view the path passed by the tunnel.

```
[LSRA] tracert lsp te tunnel 1/0/0
  LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel1/0/0 , press CTRL_C to
break.
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   2.1.1.2/[13312 ]
  1     2.1.1.2            1 ms    Transit
  2     3.2.1.2            16 ms   Transit
  3     3.3.1.2            1 ms    Transit
  4     4.1.1.2            1 ms    Egress
```

The preceding information shows that services on the link are already switched to the bypass tunnel.

NOTE

After the FRR switchover, run the **display mpls te tunnel-interface** command immediately, and you can view that two CR-LSPs are in Up state. This is because FRR establishes a new LSP by using the make-before-break mechanism. The previous LSP is deleted only after the new LSP is established successfully.

Run the **display mpls lsp verbose** command on LSRB, and you can view that the bypass tunnel is used.

```
[LSRB] display mpls lsp verbose
------------------------------------------------------------------------------
                LSP Information: RSVP LSP
------------------------------------------------------------------------------
  No                  :  1
  SessionID           :  100
  IngressLsrID        :  1.1.1.1
  LocalLspID          :  1
  Tunnel-Interface    :  Tunnel1/0/0
  Fec                 :  4.4.4.4/32
  Nexthop             :  3.1.1.2
  In-Label            :  13312
  Out-Label           :  13312
  In-Interface        :  Vlanif10
  Out-Interface       :  Vlanif20
  LspIndex            :  4104
  Token               :  0x10000
  LsrType             :  Transit
  Bypass In Use       :  In Use
  Bypass Tunnel Id    :  0x0
  BypassTunnel        :  Tunnel Index[Tunnel3/0/0], InnerLabel[13312]
  Mpls-Mtu            :  1500
  TimeStamp           :  3782sec

  No                  :  2
  SessionID           :  300
  IngressLsrID        :  2.2.2.2
  LocalLspID          :  2
  Tunnel-Interface    :  Tunnel3/0/0
  Fec                 :  3.3.3.3/32
  Nexthop             :  3.2.1.2
  In-Label            :  NULL
  Out-Label           :  13313
  In-Interface        :  ----------
  Out-Interface       :  Vlanif30
  LspIndex            :  4106
  Token               :  0x10000
  LsrType             :  Ingress
  Bypass In Use       :  Not Exists
  Bypass Tunnel Id    :  0x0
  BypassTunnel        :  Tunnel Index[---]
 Mpls-Mtu            :  1500
  TimeStamp           :  1379sec
```


Copyright © Huawei Technologies Co., Ltd.

Set the scanning timer of FRR on the PLR to 5 seconds.

```
[LSRB] mpls
[LSRB-mpls] mpls te timer fast-reroute 5
[LSRB-mpls] quit
```

Re-enable the protected outgoing interface on the PLR.

```
[LSRB] intrface vlanif 20
[LSRB-Vlanif20] undo shutdown
```

Run the **display interface tunnel 1/0/0** command, and you can view the status of the primary LSP on LSRA. The tunnel interface is in Up state.

After a period of time, run the **display mpls lsp verbose** command on LSRB, and you can view that Tunnel 1/0/0 is bound to VLANIF 20 and remains unused.

----End

Configuration Files

- Configuration file of LSRA

```
#
 sysname LSRA
#
 vlan batch 10
#
 mpls lsr-id 1.1.1.1
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
 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
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 00.0005.0000.0000.0001.00
 traffic-eng level-2
#
interface Vlanif10
 ip address 2.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 isis enable 1
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 4.4.4.4
 mpls te tunnel-id 100
 mpls te record-route label
```


Copyright © Huawei Technologies Co., Ltd.

```
 mpls te path explicit-path pri-path
 mpls te fast-reroute
 mpls te commit
#
return
```

- Configuration file of LSRB

```
#
 sysname LSRB
#
 vlan batch 10 20 30
#
 mpls lsr-id 2.2.2.2
 mpls
  mpls te
  mpls te timer fast-reroute 5
  mpls rsvp-te
  mpls te cspf
#
 explicit-path by-path
  next hop 3.2.1.2
  next hop 3.3.1.2
  next hop 3.3.3.3
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 00.0005.0000.0000.0002.00
 traffic-eng level-2
#
interface Vlanif10
 ip address 2.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif20
 ip address 3.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface Vlanif30
 ip address 3.2.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface GigabitEthernet3/0/0
 port link-type access
 port default vlan 30
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
#
interface Tunnel3/0/0
```


Copyright © Huawei Technologies Co., Ltd.

```
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te tunnel-id 300
 mpls te record-route
 mpls te bypass-tunnel
 mpls te path explicit-path by-path
 mpls te protected-interface Vlanif20
 mpls te commit
#
return
```

- Configuration file of LSRC

```
#
 sysname LSRC
#
 vlan batch 20 40 50
#
 mpls lsr-id 3.3.3.3
 mpls
  mpls te
  mpls rsvp-te
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 00.0005.0000.0000.0003.00
 traffic-eng level-2
#
interface Vlanif20
 ip address 3.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif40
 ip address 3.3.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif50
 ip address 4.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 50
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface GigabitEthernet3/0/0
 port link-type access
 port default vlan 40
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of LSRD

Copyright © Huawei Technologies Co., Ltd.

```
#
 sysname LSRD
#
 vlan batch 50
#
 mpls lsr-id 4.4.4.4
 mpls
  mpls te
  mpls rsvp-te
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 00.0005.0000.0000.0004.00
 traffic-eng level-2
#
interface Vlanif50
 ip address 4.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 50
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of LSRE

```
#
 sysname LSRE
#
 vlan batch 30 40
#
 mpls lsr-id 5.5.5.5
 mpls
  mpls te
  mpls rsvp-te
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 00.0005.0000.0000.0005.00
 traffic-eng level-2
#
interface Vlanif30
 ip address 3.2.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif40
 ip address 3.3.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 30
#
interface GigabitEthernet2/0/0
```


Copyright © Huawei Technologies Co., Ltd.

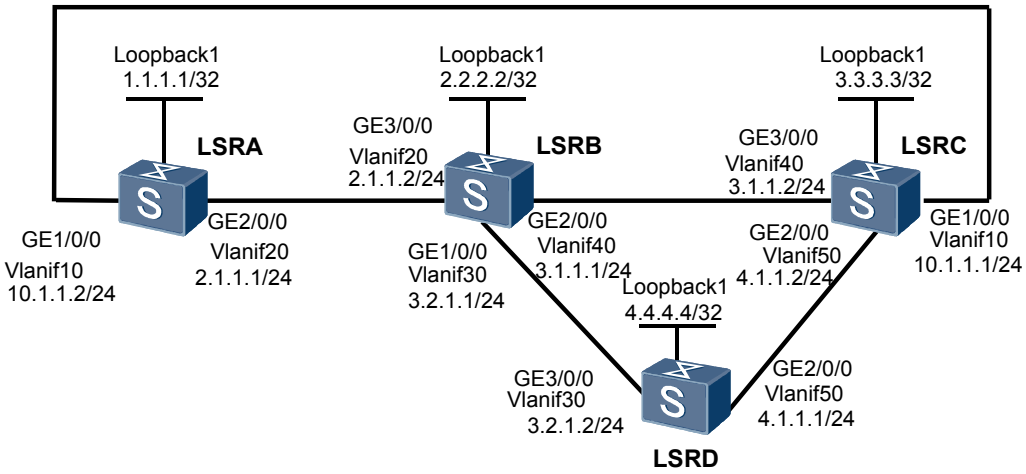
```
 port link-type access
 port default vlan 40
#
interface LoopBack1
 ip address 5.5.5.5 255.255.255.255
 isis enable 1
#
return
```

3.21.9 Example for Configuring MPLS TE Auto FRR

Networking Requirements

As shown in **Figure 3-10**, a primary tunnel is set up using the explicit path of LSRA-> LSRB->LSRC. A bypass tunnel is set up on the ingress node LSRA for node protection and a bypass tunnel is set up on the transit node LSRB for link protection, and both of them provide bandwidth protection.

Figure 3-10 Networking diagram for configuring MPLS TE auto FRR



Configuration Roadmap

The configuration roadmap is as follows:

1. Set up a primary tunnel, enable TE FRR in the tunnel interface view, and enable MPLS auto FRR in the MPLS view.
2. Specify the bandwidth that the bypass tunnel can protect and the setup priority and holding priority of the bypass tunnel.

Data Preparation

To complete the configuration, you need the following data:

- OSPF process ID and OSPF area ID of each node
- Maximum bandwidth and maximum reservable bandwidth of the link

Copyright © Huawei Technologies Co., Ltd.

- Path that the primary tunnel passes through
- Number of the primary tunnel interface, IP address, destination IP address, tunnel ID, signaling protocol (RSVP-TE), and tunnel bandwidth

Procedure

Step 1 Create VLANs and VLANIF interfaces, and assign IP addresses to the VLANIF interfaces.

As shown in **Figure 3-10**, configure IP addresses and masks for the interfaces, including loopback interfaces. The configuration details are not mentioned here.

Step 2 Configure OSPF to advertise the routes of network segments and the host routes of the LSR IDs.

Configure OSPF on all the nodes to advertise the host routes of the LSR IDs. The configuration details are not mentioned here.

After the configuration, run the **display ip routing-table** command on each node, and you can view that the nodes learn the LSR ID from each other.

Step 3 Configure basic MPLS functions and enable MPLS TE, RSVP-TE, and CSPF.

Configure LSRA.

```
[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 vlanif 20
[LSRA-Vlanif20] mpls
[LSRA-Vlanif20] mpls te
[LSRA-Vlanif20] mpls rsvp-te
[LSRA-Vlanif20] quit
[LSRA] interface vlanif 10
[LSRA-Vlanif10] mpls
[LSRA-Vlanif10] mpls te
[LSRA-Vlanif10] mpls rsvp-te
[LSRA-Vlanif10] quit
```

NOTE

The configurations on LSRB, LSRC, and LSRD are similar to the configuration on LSRA, and are not mentioned here. You need to enable CSPF only on the ingress nodes of the primary tunnel and the bypass tunnel. That is, you need to enable CSPF only on LSRA and LSRB. You do not need to enable CSPF on LSRC and LSRD.

Step 4 Configure OSPF TE.

Configure LSRA.

```
[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
```

Configure LSRB.

```
[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] quit
[LSRB-ospf-1] quit
```


Copyright © Huawei Technologies Co., Ltd.

Configure LSRC.

```
[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] quit
[LSRC-ospf-1] quit
```

Configure LSRD.

```
[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] quit
[LSRD-ospf-1] quit
```

Step 5 Configure the MPLS TE link bandwidth.

Set the maximum reservable bandwidth of the link to 10 Mbit/s and the BC1 bandwidth to 3 Mbit/s.

Configure LSRA.

```
[LSRA] interface vlanif 20
[LSRA-Vlanif20] mpls te max-reservable-bandwidth 10000 bc1 3000
```

For convenience, these configurations are used on the outgoing interfaces on the link that the primary tunnel and bypass tunnel pass through, and the details are not mentioned here.

Step 6 Configure the explicit path for the primary tunnel.

```
[LSRA] explicit-path master
[LSRA-explicit-path-master] next hop 2.1.1.2
[LSRA-explicit-path-master] next hop 3.1.1.2
```

Step 7 Enable MPLS TE auto FRR.

Configure LSRA.

```
[LSRA] mpls
[LSRA-mpls] mpls te auto-frr
```

Configure LSRB.

```
[LSRB] mpls
[LSRB-mpls] mpls te auto-frr
```

Step 8 Configure the primary tunnel.

```
[LSRA] interface tunnel2/0/0
[LSRA-Tunnel2/0/0] ip address unnumbered interface loopback1
[LSRA-Tunnel2/0/0] tunnel-protocol mpls te
[LSRA-Tunnel2/0/0] destination 3.3.3.3
[LSRA-Tunnel2/0/0] mpls te tunnel-id 200
[LSRA-Tunnel2/0/0] mpls te record-route label
[LSRA-Tunnel2/0/0] mpls te path explicit-path master
[LSRA-Tunnel2/0/0] mpls te priority 4 3
[LSRA-Tunnel2/0/0] mpls te fast-reroute bandwidth
[LSRA-Tunnel2/0/0] mpls te bypass-attributes bandwidth 200 priority 5 4
[LSRA-Tunnel2/0/0] mpls te commit
[LSRA-Tunnel2/0/0] quit
```

Step 9 Verify the configuration.

Run the **display mpls lsp verbose** command on the ingress node LSRA. You can view the LSP information about the primary tunnel and the bypass tunnel, and the primary tunnel is bound to the bypass tunnel.

Copyright © Huawei Technologies Co., Ltd.

```
[LSRA] display mpls lsp verbose
  No                   :  1
  SessionID            :  200
  IngressLsrID         :  1.1.1.1
  LocalLspID           :  1
  Tunnel-Interface     :  Tunnel2/0/0
  Fec                  :  3.3.3.3/32
  TunnelTableIndex     :  0x6
  Nexthop              :  2.1.1.2
  In-Label             :  NULL
  Out-Label            :  106497
  In-Interface         :  ----------
  Out-Interface        :  Vlanif20
  LspIndex             :  6148
  Token                :  0x10000
  LsrType              :  Ingress
  Mpls-Mtu             :  1500
  TimeStamp            :  324sec
  Bfd-State            :  ---

  No                   :  2
  SessionID            :  5097
  IngressLsrID         :  2.2.2.2
  LocalLspID           :  2
  Tunnel-Interface     :  Tunnel0/0/2048
  Fec                  :  3.3.3.3/32
  TunnelTableIndex     :  0x6
  Nexthop              :  10.1.1.1
  In-Label             :  13312
  Out-Label            :  3
  In-Interface         :  Vlanif20
  Out-Interface        :  Vlanif10
  LspIndex             :  6149
  Token                :  0x10000
  LsrType              :  Transit
  Mpls-Mtu             :  ------
  TimeStamp            :  324sec
  Bfd-State            :  ---

No                     :  3
  SessionID            :  5097
  IngressLsrID         :  1.1.1.1
  LocalLspID           :  3
  Tunnel-Interface     :  Tunnel0/0/2048
  Fec                  :  3.3.3.3/32
  TunnelTableIndex     :  0x4
  Nexthop              :  10.1.1.1
  In-Label             :  NULL
  Out-Label            :  3
  In-Interface         :  ----------
  Out-Interface        :  Vlanif20
  LspIndex             :  6150
  Token                :  0x10000
  LsrType              :  Ingress
  Mpls-Mtu             :  1500
  TimeStamp            :  324sec
  Bfd-State            :  ---
```

You can view that the primary tunnel is bound to the auto bypass tunnel, that is, Tunnel7/0/2048.

Run the **display mpls te tunnel-interface auto-bypass-tunnel** command, and you can view detailed information about the auto bypass tunnel. The bandwidth, setup priority, and holding priority of the auto bypass tunnel are the same as the bypass-attributes of the primary tunnel.

```
[LSRA] display mpls te tunnel-interface auto-bypass-tunnel Tunnel0/0/2048
Tunnel Name   :  Tunnel0/0/2048
    Tunnel State Desc  :  CR-LSP is Up
    Tunnel Attributes   :
    LSP ID  :  1.1.1.1:3
```


Copyright © Huawei Technologies Co., Ltd.

```
  Session ID    :  5097
  Admin State   :  UP
  Oper State    :  UP
  Ingress LSR ID:  1.1.1.1
  Egress LSR ID:  3.3.3.3
  Signaling Prot:  RSVP
  Resv Style    :  SE
  Class Type    :  CLASS 0
  Tunnel BW     :  200 kbps
  Reserved BW   :  200 kbps
  Setup Priority:  5
  Hold Priority:  4
  Hop Limit          :  -
  Secondary Hop Limit:  -
  BestEffort Hop Limit:  -
  Affinity Prop/Mask  :  0x0/0x0
  Explicit Path Name  :  -
  Secondary Affinity Prop/Mask:  0x0/0x0
  Secondary Explicit Path Name:  -
  BestEffort Affinity Prop/Mask:  0x0/0x0
  Tie-Breaking Policy :  None
  Metric Type   :  None
  Record Route  :  Enabled
  Record Label :  Disabled
  FRR Flag:  Disabled
  BackUpBW Flag:  Not Supported
  BackUpBW Type :  -
  BackUpBW      :  -
  Route Pinning :  Disabled
  Retry Limit   :  5
  Retry Interval:  10 sec
  Reopt   :  Disabled
   Reopt Freq   :  -
  Back Up Type  :  None
  Back Up LSPID :  -
  Auto BW       :  Disabled
  Auto BW Freq  :  -
  Min BW  :  -   Max BW :  -
  Current Collected BW:  -
  Interfaces Protected:  GE2/0/0
  Excluded IP Address :  2.1.1.1, 2.2.2.2, 3.1.1.2
  Car Policy    :  Disabled
  Tunnel  Group :  Primary
  Primary Tunnel:  -
  Backup  Tunnel:  -
  IPTN    InLabel     :  -
  Group   Status:  Up
  Oam     Status:  -
  Bfd Capability      :  None
  BestEffort          :  Disabled
      IsBestEffortPath:  Non-existent
```

You can view that the auto bypass tunnel protects the primary tunnel through VLANIF 20 rather than through other three interfaces on the primary tunnel. The bandwidth of the auto bypass tunnel is 200 kbit/s, and its setup priority and the holding priority is 5 and 4 respectively.

Run the **display mpls te tunnel path** command on LSRA, and you can view the path information about the primary tunnel and the auto bypass tunnel, and node protection and bandwidth protection are provided for the outgoing interface on the primary tunnel.

```
[LSRA] display mpls te tunnel path
Tunnel Interface Name : Tunnel2/0/0
 Lsp ID : 1.1.1.1 :200:1
 Hop Information
  Hop 0   2.1.1.1 Local-Protection available | bandwidth | node
  Hop 1   2.1.1.2  Label 106497
  Hop 2   2.2.2.2
  Hop 3   3.1.1.1 Local-Protection available | bandwidth
  Hop 4   3.1.1.2  Label 3
```


Copyright © Huawei Technologies Co., Ltd.

```
  Hop 5   3.3.3.3

Tunnel Interface Name : Tunnel2/0/2048
 Lsp ID : 2.2.2.2 :5097 :2
 Hop Information
  Hop 0   2.2.2.2
  Hop 1   2.1.1.2
  Hop 2   2.1.1.1
  Hop 3   1.1.1.1
  Hop 4   10.1.1.2
  Hop 5   10.1.1.1
  Hop 6   3.3.3.3

 Tunnel Interface Name : Tunnel0/0/2048
 Lsp ID : 1.1.1.1 :5097:3
 Hop Information
  Hop 0   10.1.1.2
  Hop 1   10.1.1.1
  Hop 2   3.3.3.3
```

----End

Configuration Files

- Configuration file of LSRA

```
#
 sysname LSRA
#
 vlan batch 10 20
#
 mpls lsr-id 1.1.1.1
 mpls
  mpls te
  mpls te auto-frr
  mpls rsvp-te
  mpls te cspf
#
 explicit-path master
  next hop 2.1.1.2
  next hop 3.1.1.2
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 10000 bc1 3000
 mpls rsvp-te
#
interface Vlanif20
 ip address 2.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 10000 bc1 3000
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
interface Tunnel2/0/0
 ip address unnumbered interface LoopBack1
```


Copyright © Huawei Technologies Co., Ltd.

```
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te tunnel-id 200
 mpls te record-route label
 mpls te path explicit-path master
 mpls te priority 4 3
 mpls te fast-reroute bandwidth
 mpls te bypass-attributes bandwidth 200 priority 5 4
 mpls te commit
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  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
  mpls-te enable
#
return
```

- Configuration file of LSRB

```
#
 sysname LSRB
#
 vlan batch 20 30 40
#
 mpls lsr-id 2.2.2.2
 mpls
  mpls te
  mpls te auto-frr
  mpls rsvp-te
  mpls te cspf
#
interface Vlanif20
 ip address 2.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif30
 ip address 3.2.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 10000 bc1 3000
 mpls rsvp-te
#
interface Vlanif40
 ip address 3.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 10000 bc1 3000
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 30
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 40
#
interface GigabitEthernet3/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
ospf 1
 opaque-capability enable
```


Copyright © Huawei Technologies Co., Ltd.

```
 area 0.0.0.0
  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
  mpls-te enable
#
return
```

- Configuration file of LSRC

```
#
 sysname LSRC
#
 vlan batch 10 40 50
#
 mpls lsr-id 3.3.3.3
 mpls
  mpls te
  mpls rsvp-te
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif40
 ip address 3.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif50
 ip address 4.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 50
#
interface GigabitEthernet3/0/0
 port link-type access
 port default vlan 40
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  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
  mpls-te enable
#
return
```

- Configuration file of LSRD

```
#
 sysname LSRD
#
 vlan batch 30 50
#
```


Copyright © Huawei Technologies Co., Ltd.

```
 mpls lsr-id 4.4.4.4
 mpls
  mpls te
  mpls rsvp-te
#
interface Vlanif30
 ip address 3.2.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif50
 ip address 4.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 10000 bc1 3000
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 50
#
interface GigabitEthernet3/0/0
 port link-type access
 port default vlan 30
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  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
  mpls-te enable
#
return
```

3.21.10 Example for Configuring RSVP Key Authentication (RSVP-TE FRR)

Networking Requirements

As shown in **Figure 3-11**, the primary tunnel is along the path LSR A -> LSR B -> LSR C -> LSR D, and FRR is required on the link between LSR B and LSR C for protection.

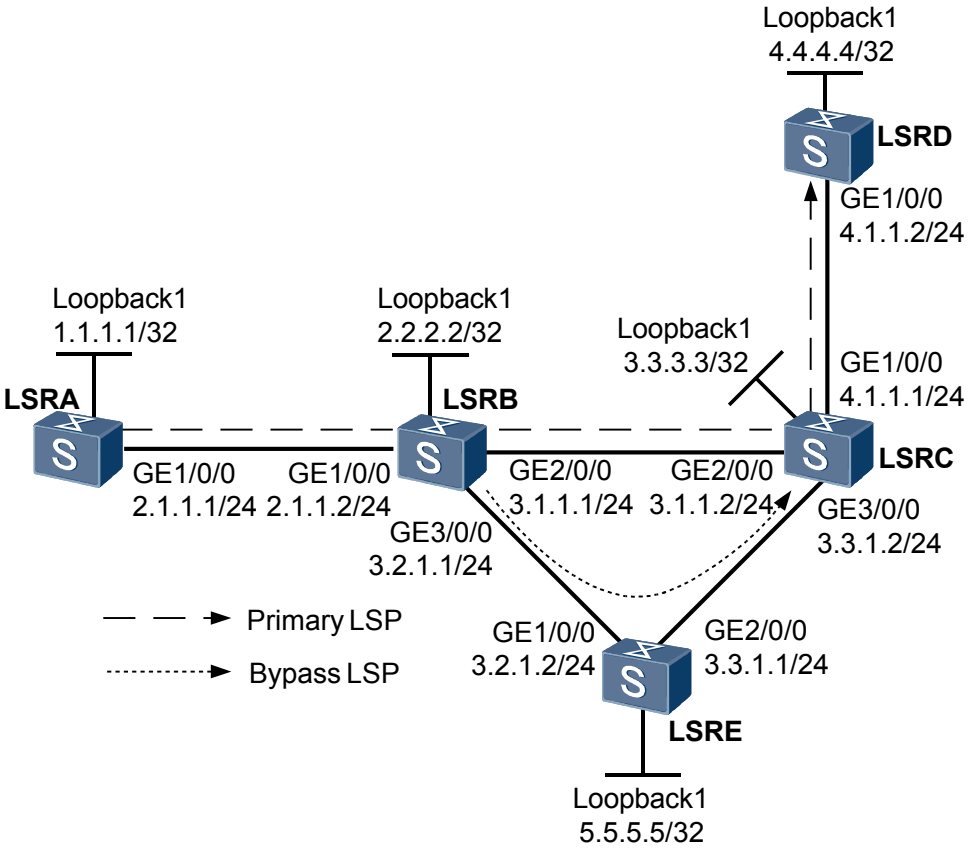
A bypass tunnel is set up along the path LSR B -> LSR E -> LSR C. LSR B functions as the PLR and LSR C functions as the MP.

The primary and bypass MPLS TE tunnels are set up by using explicit paths. RSVP-TE is used as the signaling protocol.

The RSVP authentication needs to be configured on LSR B and LSR C. In this example, LSR B and LSR C are configured as neighboring nodes by using their LSR IDs. Then, the RSVP key authentication is enabled, achieving higher reliability.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-11 Networking diagram of the MPLS TE FRR-based RSVP key authentication



Switch	Interface	VLANIF interface	IP address
LSRA	GigabitEthernet1/0/0	VLANIF 10	2.1.1.1/24
LSRB	GigabitEthernet1/0/0	VLANIF 10	2.1.1.2/24
LSRB	GigabitEthernet2/0/0	VLANIF 20	3.1.1.1/24
LSRB	GigabitEthernet3/0/0	VLANIF 30	3.2.1.1/24
LSRC	GigabitEthernet1/0/0	VLANIF 50	4.1.1.1/24
LSRC	GigabitEthernet2/0/0	VLANIF 20	3.1.1.2/24
LSRC	GigabitEthernet3/0/0	VLANIF 40	3.3.1.2/24
LSRD	GigabitEthernet1/0/0	VLANIF 50	4.1.1.2/24
LSRE	GigabitEthernet1/0/0	VLANIF 30	3.2.1.2/24
LSRE	GigabitEthernet2/0/0	VLANIF 40	3.3.1.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure MPLS TE FRR according to **Example for Configuring MPLS TE FRR**.

Copyright © Huawei Technologies Co., Ltd.

2. Configure the RSVP key authentication on LSR B and LSR C of the tunnel, preventing forged Resv messages from illegally requesting for network resources.

Data Preparation

To complete the configuration, you need the following data:

- MPLS LSR ID of each router
- Local password and key for the RSVP authentication
- Data listed in "Data Preparation" of **Example for Configuring MPLS TE FRR**

Procedure

Step 1 Configure MPLS TE FRR.

Configure the primary tunnel and bypass tunnel according to **Example for Configuring MPLS TE FRR** and then bind the two tunnels.

Step 2 Configure the RSVP key authentication on LSR B and LSR C to enhance security of packet transmission. In addition, to check whether the RSVP key authentication is successfully configured, configure the RSVP-TE handshake function and set a local password.

Configure the RSVP key authentication on LSR B.

```
[LSRB] mpls rsvp-te peer 3.3.3.3
[LSRB-mpls-rsvp-te-peer-3.3.3.3] mpls rsvp-te authentication plain huawei
[LSRB-mpls-rsvp-te-peer-3.3.3.3] mpls rsvp-te authentication handshake beijingHW
```

Configure the RSVP key authentication on LSR C.

```
[LSRC] mpls rsvp-te peer 2.2.2.2
[LSRC-mpls-rsvp-te-peer-2.2.2.2] mpls rsvp-te authentication plain huawei
[LSRC-mpls-rsvp-te-peer-2.2.2.2] mpls rsvp-te authentication handshake beijingHW
```

Step 3 Verify the configuration.

Run the **display mpls rsvp-te statistics global** command on LSR B. You can view the status of the RSVP key authentication. If the command output shows that the values of the SendChallengeMsgCounter field, RecChallengeMsgCounter field, SendResponseMsgCounter field, and RecResponseMsgCounter field are not zero, this indicates that the PLR and the MP successfully shake hands with each other and the authentication is configured successfully.

```
<LSRB> display mpls rsvp-te statistics global
 LSR ID: 2.2.2.2                      LSP Count: 2
 PSB Count: 1                         RSB Count: 1
 RFSB Count: 0

Total Statistics Information:
 PSB CleanupTimeOutCounter: 0         RSB CleanupTimeOutCounter: 0
 SendPacketCounter: 104               RecPacketCounter: 216
 SendCreatePathCounter: 7             RecCreatePathCounter: 57
 SendRefreshPathCounter: 48           RecRefreshPathCounter: 28
 SendCreateResvCounter: 4             RecCreateResvCounter: 4
 SendRefreshResvCounter: 26           RecRefreshResvCounter: 49
 SendResvConfCounter: 0               RecResvConfCounter: 0
 SendHelloCounter: 0                  RecHelloCounter: 0
 SendAckCounter: 0                    RecAckCounter: 0
 SendPathErrCounter: 1                RecPathErrCounter: 0
 SendResvErrCounter: 0                RecResvErrCounter: 0
 SendPathTearCounter: 0               RecPathTearCounter: 1
 SendResvTearCounter: 1               RecResvTearCounter: 1
 SendSrefreshCounter: 0               RecSrefreshCounter: 0
```


Copyright © Huawei Technologies Co., Ltd.

```
 SendAckMsgCounter: 0                RecAckMsgCounter: 0
 SendChallengeMsgCounter: 1          RecChallengeMsgCounter: 1
 SendResponseMsgCounter: 1           RecResponseMsgCounter: 1
 SendErrMsgCounter: 1                RecErrMsgCounter: 0
 ResourceReqFaultCounter: 0
 Bfd neighbor count: 1               Bfd session count: 0
```

Shut down the protected outgoing interface on the PLR.

```
[LSRB] interface vlanif 20
[LSRB-Vlanif20] shutdown
```

Run the **display interface tunnel 1/0/0** command on LSR A to view the status of the primary tunnel. You can view that the tunnel interface is Up.

Run the **tracert lsp te tunnel 1/0/0** command on LSR A. You can view the path by which the tunnel passes.

```
[LSRA] tracert lsp te tunnel 1/0/0
  LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel1/0/0 , press CTRL_C to
break.
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   2.1.1.2/[13312 ]
  1     2.1.1.2            1 ms    Transit   3.2.1.2/[13312 13312 ]
  2     3.2.1.2            16 ms   Transit   3.3.1.2/[3 ]
  3     3.3.1.2            1 ms    Transit   4.1.1.2/[3 ]
  4     4.1.1.2            1 ms    Egress
```

The command output shows that traffic is switched to the bypass tunnel.

Run the command on LSR B. You can view that the bypass tunnel is working.

Run the **display mpls rsvp-te peer** command. You can view whether the bypass tunnel is successfully set up.

```
[LSRB] display mpls rsvp-te peer
Remote Node id Neighbor
 Neighbor Addr:  -----
 SrcInstance: 0xDAC29CB4              NbrSrcInstance: 0x0
 PSB Count: 1                         RSB Count: 0
 Hello Type Sent: NONE
 SRefresh Enable: NO
 Last valid seq # rcvd: NULL

Interface: Vlanif10
 Neighbor Addr: 2.1.1.1
 SrcInstance: 0xDAC29CB4              NbrSrcInstance: 0x0
 PSB Count: 1                        RSB Count: 0
 Hello Type Sent: NONE
 SRefresh Enable: NO
 Last valid seq # rcvd: NULL

Interface: Vlanif20
 Neighbor Addr: 3.1.1.2
 SrcInstance: 0xDAC29CB4              NbrSrcInstance: 0x0
 PSB Count: 0                         RSB Count: 0
 Hello Type Sent: NONE
 SRefresh Enable: NO
 Last valid seq # rcvd: NULL

Interface: Vlanif30
 Neighbor Addr: 3.2.1.2
 SrcInstance: 0xDAC29CB4              NbrSrcInstance: 0x0
 PSB Count: 0                         RSB Count: 1
 Hello Type Sent: NONE
 SRefresh Enable: NO
 Last valid seq # rcvd: NULL
```


Copyright © Huawei Technologies Co., Ltd.

The command output shows that the number of RSBs on Vlanif30 of LSR B is not zero. This indicates that the RSVP key authentication is successful on LSR B and its neighbor LSR E, and the resources are successfully reserved.

----End

Configuration Files

- Configuration file of LSR A

```
#
 sysname LSRA
#
vlan batch 10
#
 mpls lsr-id 1.1.1.1
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
 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
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 00.0005.0000.0000.0001.00
 traffic-eng level-2
#
interface Vlanif10
 ip address 2.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 isis enable 1
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 4.4.4.4
mpls te record-route label
 mpls te path explicit-path pri-path
mpls te tunnel-id 100
mpls te fast-reroute
 mpls te commit
#
return
```

- Configuration file of LSR B

```
#
sysname LSRB
#
vlan batch 10 20 30
#
#
 mpls lsr-id 2.2.2.2
```


Copyright © Huawei Technologies Co., Ltd.

```
 mpls
  mpls te
  mpls te timer fast-reroute 5
  mpls rsvp-te
  mpls te cspf
#
 explicit-path by-path
  next hop 3.2.1.2
  next hop 3.3.1.2
  next hop 3.3.3.3
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 00.0005.0000.0000.0002.00
 traffic-eng level-2
#
interface Vlanif10
 ip address 2.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif20
 ip address 3.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif30
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface GigabitEthernet 3/0/0
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
interface Tunnel3/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te tunnel-id 300
 mpls te record-route
  mpls te path explicit-path by-path
 mpls te protected-interface Vlanif20
 mpls te commit
mpls rsvp-te peer 3.3.3.3
 mpls rsvp-te authentication plain huawei
 mpls rsvp-te authentication handshake beijingHW
#
return
```

- Configuration file of LSR C

```
#
```


Copyright © Huawei Technologies Co., Ltd.

```
 sysname LSRC
#
vlan batch 50 20 40
#
 mpls lsr-id 3.3.3.3
 mpls
  mpls te
  mpls rsvp-te
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 00.0005.0000.0000.0003.00
 traffic-eng level-2
#
interface Vlanif50
 ip address 4.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif20
 ip address 3.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif40
 ip address 3.3.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface GigabitEthernet 3/0/0
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 isis enable 1
mpls rsvp-te peer 2.2.2.2
 mpls rsvp-te authentication plain huawei
 mpls rsvp-te authentication handshake beijingHW
#
return
```

- Configuration file of LSR D

```
#
 sysname LSRD
#
vlan batch 50
#
 mpls lsr-id 4.4.4.4
 mpls
  mpls te
  mpls rsvp-te
#
isis 1
 is-level level-2
```


Copyright © Huawei Technologies Co., Ltd.

```
 cost-style wide
 network-entity 00.0005.0000.0000.0004.00
 traffic-eng level-2
#
interface Vlanif50
 ip address 4.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of LSR E

```
#
 sysname LSRE
#
vlan batch 30 40
#
 mpls lsr-id 5.5.5.5
 mpls
  mpls te
  mpls rsvp-te
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 00.0005.0000.0000.0005.00
 traffic-eng level-2
#
interface Vlanif30
 clock master
 ip address 3.2.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif40
 clock master
 ip address 3.3.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface LoopBack1
 ip address 5.5.5.5 255.255.255.255
 isis enable 1
#
return
```


Copyright © Huawei Technologies Co., Ltd.

3.21.11 Example for Configuring RSVP-TE Summary Refresh (RSVP-TE FRR)

Networking Requirements

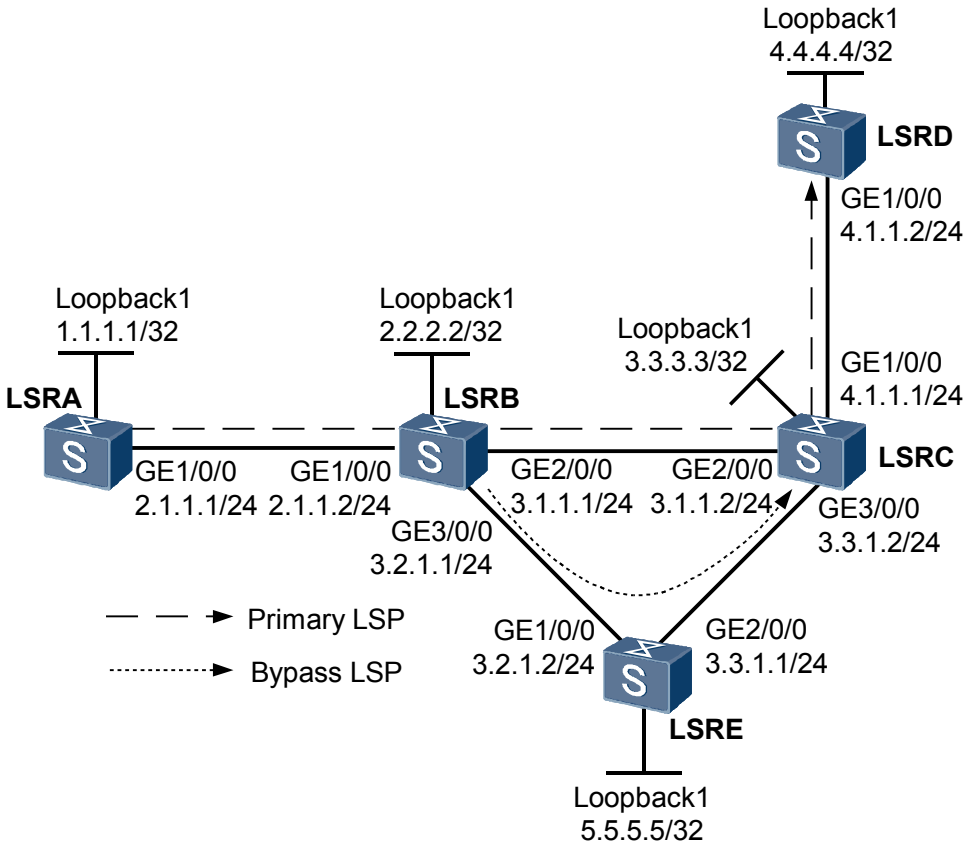
As shown in **Figure 3-12**, the primary tunnel is along the path LSR A -> LSR B -> LSR C -> LSR D, and the link between LSR B and LSR C requires FRR for protection. In addition, the summary refresh (Srefresh) function need to be configured on LSR B and LSR C.

A bypass tunnel is set up along the path LSR B -> LSR E -> LSR C.LSR B functions as the PLR and LSR C functions as the MP.

The primary and bypass MPLS TE tunnels are set up by using explicit paths. RSVP-TE is used as the signaling protocol.

The Srefresh function needs to be configured on LSR B and LSR C. In addition, the RSVP key authentication is configured in the MPLS view. This helps the Srefresh function to achieve higher reliability.

Figure 3-12 Networking diagram of the MPLS TE FRR-based Srefresh function



Switch	Interface	VLANIF interface	IP address
LSRA	GigabitEthernet1/0/0	VLANIF 10	2.1.1.1/24
LSRB	GigabitEthernet1/0/0	VLANIF 10	2.1.1.2/24
LSRB	GigabitEthernet2/0/0	VLANIF 20	3.1.1.1/24

Copyright © Huawei Technologies Co., Ltd.

LSRB	GigabitEthernet3/0/0	VLANIF 30	3.2.1.1/24
LSRC	GigabitEthernet1/0/0	VLANIF 50	4.1.1.1/24
LSRC	GigabitEthernet2/0/0	VLANIF 20	3.1.1.2/24
LSRC	GigabitEthernet3/0/0	VLANIF 40	3.3.1.2/24
LSRD	GigabitEthernet1/0/0	VLANIF 50	4.1.1.2/24
LSRE	GigabitEthernet1/0/0	VLANIF 30	3.2.1.2/24
LSRE	GigabitEthernet2/0/0	VLANIF 40	3.3.1.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure MPLS TE FRR according to **Example for Configuring MPLS TE FRR**.
2. Configure the Srefresh function on the PLR and MP along a tunnel to enhance transmission reliability of RSVP messages and improve resource usage.

Data Preparation

To complete the configuration, you need the following data:

Data listed in "Data Preparation" of **Example for Configuring MPLS TE FRR**

Procedure

Step 1 Configure MPLS TE FRR.

You can configure the primary and bypass MPLS TE tunnels according to **Example for Configuring MPLS TE FRR**, and then bind the two tunnels.

Step 2 Configure the Srefresh function on LSR B functioning as the PLR and LSR C functioning as the MP.

Configure the Srefresh function on LSR B.

```
[LSRB] mpls
[LSRB-mpls] mpls rsvp-te srefresh
[LSRB-mpls] quit
```

Configure the Srefresh function on LSR C.

```
[LSRC] mpls
[LSRC-mpls] mpls rsvp-te srefresh
[LSRC-mpls] quit
```

Step 3 Verify the configuration.

Run the **display mpls rsvp-te statistics global** command on LSR B. You can view the status of the Srefresh function. If the command output shows that the values of the SendSrefreshCounter field, RecSrefreshCounter field, SendAckMsgCounter field, and RecAckMsgCounter field are not zero, this indicates that the Srefresh packets are successfully transmitted.

```
[LSRB] display mpls rsvp-te statistics global
 LSR ID: 2.2.2.2                      LSP Count: 2
```


Copyright © Huawei Technologies Co., Ltd.

```
 PSB Count: 1                          RSB Count: 1
 RFSB Count: 0

Total Statistics Information:
 PSB CleanupTimeOutCounter: 0          RSB CleanupTimeOutCounter: 0
 SendPacketCounter: 104                RecPacketCounter: 216
 SendCreatePathCounter: 7              RecCreatePathCounter: 57
 SendRefreshPathCounter: 48            RecRefreshPathCounter: 28
 SendCreateResvCounter: 4              RecCreateResvCounter: 4
 SendRefreshResvCounter: 26            RecRefreshResvCounter: 49
 SendResvConfCounter: 0                RecResvConfCounter: 0
 SendHelloCounter: 0                   RecHelloCounter: 0
 SendAckCounter: 0                     RecAckCounter: 0
 SendPathErrCounter: 1                 RecPathErrCounter: 0
 SendResvErrCounter: 0                 RecResvErrCounter: 0
 SendPathTearCounter: 0                RecPathTearCounter: 1
 SendResvTearCounter: 1                RecResvTearCounter: 1
 SendSrefreshCounter: 1                RecSrefreshCounter: 6
 SendAckMsgCounter: 6                  RecAckMsgCounter: 16
 SendChallengeMsgCounter: 0            RecChallengeMsgCounter: 0
 SendResponseMsgCounter: 0             RecResponseMsgCounter: 0
 SendErrMsgCounter: 1                  RecErrMsgCounter: 0
 ResourceReqFaultCounter: 0
 Bfd neighbor count: 1                 Bfd session count: 0
```

Shut down the protected outgoing interface Vlanif20.

```
[LSRB] interface vlanif 20
[LSRB-Vlanif20] shutdown
```

Run the **display interface tunnel 1/0/0** command on LSR A to view the status of the primary tunnel. You can view that the tunnel interface is Up.

Run the **tracert lsp te tunnel 1/0/0** command on LSR A. You can view the path by which the tunnel passes.

```
[LSRA] tracert lsp te tunnel 1/0/0
  LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel1/0/0 , press CTRL_C to
break.
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   2.1.1.2/[13312 ]
  1     2.1.1.2            1 ms    Transit   3.2.1.2/[13312 13312 ]
  2     3.2.1.2            16 ms   Transit   3.3.1.2/[3 ]
  3     3.3.1.2            1 ms    Transit   4.1.1.2/[3 ]
  4     4.1.1.2            1 ms    Egress
```

The command output shows that traffic is switched to the bypass tunnel.

Run the command on LSR B. You can view that the bypass tunnel is working.

```
[LSRB] display mpls te tunnel name tunnel1/0/0 verbose
    No                      :  1
    Tunnel-Name             :  Tunnel1/0/0
    TunnelIndex             :  1           LSP Index         :  4098
    Session ID              :  100         LSP ID            :  1
    Lsr Role                :  Transit
    Ingress LSR ID          :  1.1.1.1
    Egress LSR ID           :  4.4.4.4
    In-Interface            :  Vlanif10
    Out-Interface           :  Vlanif20
    Sign-Protocol           :  RSVP TE     Resv Style        :  SE
    IncludeAnyAff           :  0x0         ExcludeAnyAff     :  0x0
    IncludeAllAff           :  0x0
    ER-Hop Table Index      :  3           AR-Hop Table Index:  12
    C-Hop Table Index       :  50
    PrevTunnelIndexInSession:  -           NextTunnelIndexInSession:  -
    PSB Handle              :  66000
    Created Time            :  2009/01/12 10:09:10
    -------------------------------
```


Copyright © Huawei Technologies Co., Ltd.

```
          DS-TE Information
--------------------------------
Bandwidth Reserved Flag :  Unreserved
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       :  0x63        Protected Flag    :  0x1
Bypass In Use           :  In Use
Bypass Tunnel Id        :  67141670
BypassTunnel            :  Tunnel Index[Tunnel3/0/0], InnerLabel[1024]
Bypass Lsp ID           :  9           FrrNextHop        :  3.3.1.2
ReferAutoBypassHandle   :  -
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 rsvp-te statistics global** command. You can view statistics of the Srefresh function.

```
[LSRB]display mpls rsvp-te statistics global
 LSR ID: 2.2.2.2                      LSP Count: 2
 PSB Count: 2                         RSB Count: 2
 RFSB Count: 1

Total Statistics Information:
 PSB CleanupTimeOutCounter: 0         RSB CleanupTimeOutCounter: 0
 SendPacketCounter: 28                RecPacketCounter: 61
 SendCreatePathCounter: 3             RecCreatePathCounter: 18
 SendRefreshPathCounter: 9            RecRefreshPathCounter: 6
 SendCreateResvCounter: 3             RecCreateResvCounter: 2
 SendRefreshResvCounter: 4            RecRefreshResvCounter: 10
 SendResvConfCounter: 0               RecResvConfCounter: 0
 SendHelloCounter: 0                  RecHelloCounter: 0
 SendAckCounter: 0                    RecAckCounter: 0
 SendPathErrCounter: 1                RecPathErrCounter: 0
 SendResvErrCounter: 0                RecResvErrCounter: 0
 SendPathTearCounter: 0               RecPathTearCounter: 0
 SendResvTearCounter: 0               RecResvTearCounter: 0
 SendSrefreshCounter: 14              RecSrefreshCounter: 8
 SendAckMsgCounter: 8                 RecAckMsgCounter: 18
 SendChallengeMsgCounter: 0           RecChallengeMsgCounter: 0
 SendResponseMsgCounter: 0            RecResponseMsgCounter: 0
 SendErrMsgCounter: 0                 RecErrMsgCounter: 0
 ResourceReqFaultCounter: 0
 Bfd neighbor count: 2                Bfd session count: 0
```

----End

Copyright © Huawei Technologies Co., Ltd.

Configuration Files

- Configuration file of LSR A

```
#
 sysname LSRA
#
vlan batch 10
#
 mpls lsr-id 1.1.1.1
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
 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
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 00.0005.0000.0000.0001.00
 traffic-eng level-2
#
interface Vlanif10
 ip address 2.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 isis enable 1
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 4.4.4.4
mpls te record-route label
 mpls te path explicit-path pri-path
mpls te tunnel-id 100
mpls te fast-reroute
 mpls te commit
#
return
```

- Configuration file of LSR B

```
#
sysname LSRB
#
vlan batch 10 20 30
#
 mpls lsr-id 2.2.2.2
 mpls
  mpls te
  mpls te timer fast-reroute 5
  mpls rsvp-te
  mpls te cspf
  mpls rsvp-te srefresh
#
 explicit-path by-path
  next hop 3.2.1.2
```


Copyright © Huawei Technologies Co., Ltd.

```
  next hop 3.1.1.2
  next hop 3.3.3.3
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 00.0005.0000.0000.0002.00
 traffic-eng level-2
#
interface Vlanif10
 ip address 2.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif20
 ip address 3.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif30
 ip address 3.2.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface GigabitEthernet 3/0/0
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
#
interface Tunnel3/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te tunnel-id 300
 mpls te record-route
  mpls te path explicit-path by-path
  mpls te bypass-tunnel
 mpls te protected-interface Vlanif20
 mpls te commit
#
return
```

- Configuration file of LSR C

```
#
 sysname LSRC
#
vlan batch 50 20 40
#
 mpls lsr-id 3.3.3.3
 mpls
  mpls te
  mpls rsvp-te
  mpls rsvp-te srefresh
```


Copyright © Huawei Technologies Co., Ltd.

```
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 00.0005.0000.0000.0003.00
 traffic-eng level-2
#
interface Vlanif50
 ip address 4.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif20
 ip address 3.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif40
 ip address 3.3.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface GigabitEthernet 3/0/0
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of LSR D

```
#
 sysname LSRD
#
vlan batch 50
#
 mpls lsr-id 4.4.4.4
 mpls
  mpls te
  mpls rsvp-te
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 00.0005.0000.0000.0004.00
 traffic-eng level-2
#
interface Vlanif50
 ip address 4.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
```


Copyright © Huawei Technologies Co., Ltd.

```
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of LSR E

```
#
 sysname LSRE
#
vlan batch 30 40
#
 mpls lsr-id 5.5.5.5
 mpls
  mpls te
  mpls rsvp-te
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 00.0005.0000.0000.0005.00
 traffic-eng level-2
#
interface Vlanif30
 clock master
 ip address 3.2.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif40
 clock master
 ip address 3.3.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface LoopBack1
 ip address 5.5.5.5 255.255.255.255
 isis enable 1
#
return
```

3.21.12 Example for Configuring Board Removing Protection

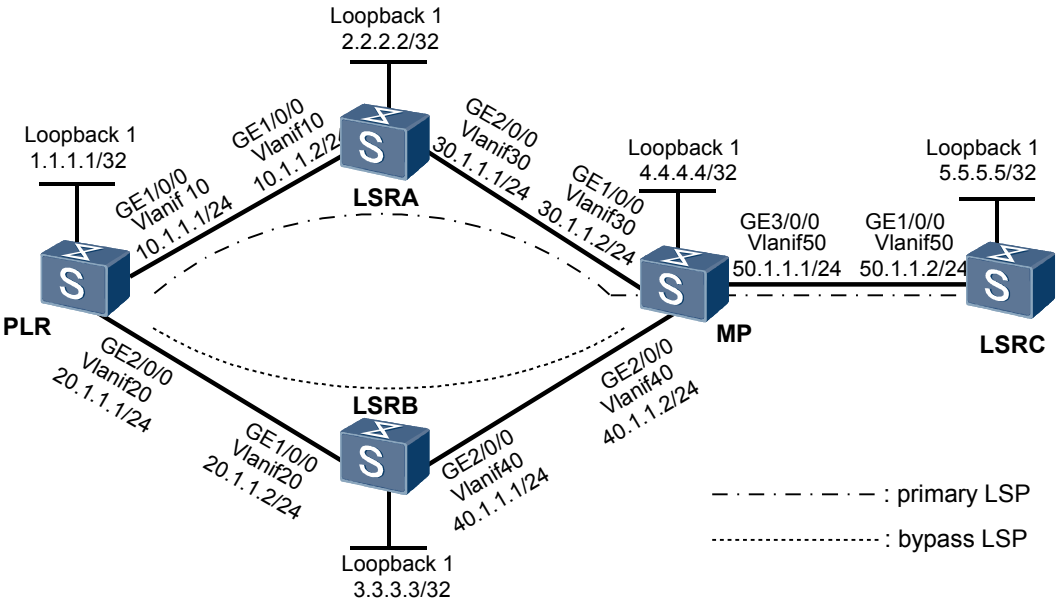
Networking Requirements

Figure 3-13 shows the networking diagram of MPLS TE FRR. The primary tunnel is along PLR-LSRA-MP->LSRC, and its bypass tunnel is along PLR-> LSRB->MP. It is required that the TE traffic of the primary tunnel be switched to the bypass tunnel after the LPU where GE 1/0/0 of the PLR is located is removed, and the traffic be switched back to the primary tunnel after the removed LPU is re-installed.

Copyright © Huawei Technologies Co., Ltd.

Both the PLR and the MP are switches.

Figure 3-13 Networking diagram for configuring MPLS TE FRR



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the tunnel interfaces of the primary tunnel and the bypass tunnel of the PLR on the main control board.
2. Specify the explicit paths of the primary tunnel and the bypass tunnel when you configure MPLS TE FRR. The explicit paths of the primary tunnel and the bypass tunnel must pass through different LPUs of the PLR; otherwise, board removing protection cannot be implemented.

Data Preparation

To complete the configuration, you need the following data:

- Slot number of the main control board on the PLR
- Tunnel interfaces of the primary tunnel and the bypass tunnel
- Outgoing interfaces of the primary tunnel and the bypass tunnel on the PLR
- Explicit paths of the primary tunnel and the bypass tunnel

Procedure

Step 1 Create VLANs and VLANIF interfaces, and assign IP addresses to the VLANIF interfaces.

As shown in **Figure 3-13**, configure IP addresses and masks for the interfaces, including loopback interfaces. The configuration details are not mentioned here.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Configure OSPF to advertise the routes of network segments and the host routes of the LSR IDs.

Configure OSPF on all the nodes to advertise the host routes of the LSR IDs. The configuration details are not mentioned here.

After the configuration, run the **display ip routing-table** command on each node, and you can view that the nodes learn the LSR ID from each other.

Step 3 Configure basic MPLS functions and enable MPLS TE and RSVP-TE.

Configure the PLR.

```
[PLR] mpls lsr-id 1.1.1.1
[PLR] mpls
[PLR-mpls] mpls te
[PLR-mpls] mpls rsvp-te
[PLR-mpls] quit
[PLR] interface vlanif 10
[PLR-Vlanif10] mpls
[PLR-Vlanif10] mpls te
[PLR-Vlanif10] mpls rsvp-te
[PLR-Vlanif10] quit
[PLR] interface vlanif 20
[PLR-Vlanif20] mpls
[PLR-Vlanif20] mpls te
[PLR-Vlanif20] mpls rsvp-te
[PLR-Vlanif20] quit
```

NOTE

The configurations on LSRA, LSRB, MP, and LSRC are similar to the configuration on the PLR, and are not mentioned here.

Step 4 Configure OSPF TE and enable CSPF on the ingress node of the tunnel.

Configure OSPF TE.

```
[PLR] ospf
[PLR-ospf-1] opaque-capability enable
[PLR-ospf-1] area 0
[PLR-ospf-1-area-0.0.0.0] mpls-te enable
[PLR-ospf-1-area-0.0.0.0] quit
[PLR-ospf-1] quit
```

NOTE

The configurations on LSRB, LSRC, and LSRD are similar to the configuration on the PLR, and are not mentioned here.

Enable CSPF on the ingress node of the primary tunnel.

```
[PLR] mpls
[PLR-mpls] mpls te cspf
```

Step 5 Configure the bandwidth for the interfaces on the link.

Set the maximum reservable bandwidth of the link to 10 Mbit/s, the BC0 bandwidth to 10 Mbit/s, and the BC1 bandwidth to 3 Mbit/s.

Configure the PLR.

```
[PLR] interface vlanif 10
[PLR-Vlanif10] mpls te bandwidth max-reservable-bandwidth 10000 bc1 3000
[PLR-Vlanif10] quit
[PLR] interface vlanif 20
[PLR-Vlanif20] mpls te bandwidth max-reservable-bandwidth 10000 bc1 3000
[PLR-Vlanif20] quit
```


Copyright © Huawei Technologies Co., Ltd.

Configure link bandwidth on all the outgoing interfaces of the link along the primary tunnel and the bypass tunnel, and the details are not mentioned here.

Step 6 Configure the primary tunnel.

Configure the explicit path for the primary tunnel on the PLR.

```
[PLR] explicit-path master
[PLR-explicit-path-master] next hop 10.1.1.2
[PLR-explicit-path-master] next hop 30.1.1.2
[PLR-explicit-path-master] next hop 50.1.1.2
[PLR-explicit-path-master] next hop 5.5.5.5
[PLR-explicit-path-master] quit
```

Configure the tunnel interface of the primary tunnel.

```
[PLR] interface tunnel0/0/1
[PLR-Tunnel0/0/1] ip address unnumbered interface loopback1
[PLR-Tunnel0/0/1] tunnel-protocol mpls te
[PLR-Tunnel0/0/1] destination 5.5.5.5
[PLR-Tunnel0/0/1] mpls te tunnel-id 100
[PLR-Tunnel0/0/1] mpls te signal-protocol rsvp-te
[PLR-Tunnel0/0/1] mpls te path explicit-path master
```

Enable TE FRR.

```
[PLR-Tunnel0/0/1] mpls te fast-reroute
[PLR-Tunnel0/0/1] mpls te commit
[PLR-Tunnel0/0/1] quit
```

After the configuration, run the **display interface tunnel** command on the PLR, and you can view that the status of Tunnel 1/0/1 is Up.

```
[PLR] display interface tunnel 0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : UP
Description : HUAWEI, Quidway Series, Tunnel0/0/1 Interface
The Maximum Transmit Unit is 1500 bytes
Internet Address is unnumbered, using address of LoopBack1(1.1.1.1/32)
Encapsulation is TUNNEL, loopback not set
Tunnel destination 5.5.5.5
Tunnel up/down statistics 1
Tunnel protocol/transport MPLS/MPLS, ILM is available,
    300 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets output,  0 bits
    0 output error
```

Step 7 Configure the bypass tunnel.

Configure the explicit path for the bypass tunnel on the PLR.

```
[PLR] explicit-path by-path
[PLR-explicit-path-by-path] next hop 20.1.1.2
[PLR-explicit-path-by-path] next hop 40.1.1.2
[PLR-explicit-path-by-path] next hop 4.4.4.4
```

Configure the tunnel interface of the bypass tunnel.

```
[PLR] interface tunnel 0/0/2
[PLR-Tunnel0/0/2] ip address unnumbered interface loopback 1
[PLR-Tunnel0/0/2] tunnel-protocol mpls te
[PLR-Tunnel0/0/2] destination 4.4.4.4
[PLR-Tunnel0/0/2] mpls te tunnel-id 200
[PLR-Tunnel0/0/2] mpls te signal-protocol rsvp-te
[PLR-Tunnel0/0/2] mpls te path explicit-path by-path
[PLR-Tunnel0/0/2] mpls te bypass-tunnel bandwidth 400
```

Specify the interface protected by the bypass tunnel.

Copyright © Huawei Technologies Co., Ltd.

```
[PLR-Tunnel0/0/2] mpls te protected-interface vlanif 10
[PLR-Tunnel0/0/2] mpls te commit
```

After the configuration, run the **display interface tunnel** command on the PLR, and you can view that the status of Tunnel 0/0/2 is Up.

```
<PLR> display interface tunnel 0/0/2
Tunnel0/0/2 current state : UP
Line protocol current state : UP
Description : HUAWEI, Quidway Series, Tunnel0/0/2 Interface
The Maximum Transmit Unit is 1500 bytes
Internet Address is unnumbered, using address of LoopBack1(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,
    300 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets output,  0 bits
    0 output error
```

Step 8 Verify the configuration.

Run the **tracert lsp te tunnel** command on the PLR, and you can view that the TE traffic is transmitted through the primary tunnel.

```
<PLR> tracert lsp te tunnel 0/0/1
  LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel0/0/1 , press CTRL_C to
break.
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   10.1.1.2/[13312 ]
  1     10.1.1.2           50 ms   Transit   30.1.1.2/[13312 ]
  2     30.1.1.2           40 ms   Transit   50.1.1.2/[3 ]
  3     5.5.5.5            70 ms   Egress
```

After the LPU where the outgoing interface of the primary tunnel (GE 1/0/0) is located is removed, run the **display interface tunnel** command, and you can view that the tunnel interface of the primary tunnel remains Up.

Run the **display mpls te tunnel stale-interface** and **display mpls te tunnel stale-interface** *interface-index* **verbose** commands on the PLR, and you can view that the outgoing interface of the primary tunnel is in Stale state.

```
<PLR> display mpls stale-interface
Stale-interface       Status    TE Attri   LSP Count  CRLSP Count  Effective MTU
0x018000106            Up         Dis         0           1              -

<PLR> display mpls te tunnel stale-interface 18000106 verbose
No             : 1
LSP-Id         : 1.1.1.1:100:1
Tunnel-Name    : Tunnel0/0/1
Destination    : 5.5.5.5
In-Interface   : 0x18000186
Out-Interface  : 0x18000106
Tunnel BW      : 400 kbps
Class Type     : bc0
Ingress LSR-Id : 1.1.1.1
Egress LSR-Id  : 5.5.5.5
Setup-Priority : 7
Hold-Priority  : 7
Sign-Protocol  : RSVP TE
Resv Style     : SE
IncludeAnyAff  : 0x0
ExcludeAnyAff  : 0x0
IncludeAllAff  : 0x0
Created Time   : 2007/10/18 18:35:38
```

Run the **display mpls te tunnel path** command on the PLR, and you can view that the path of the primary tunnel passes through LSRB.

Copyright © Huawei Technologies Co., Ltd.

```
<PLR> display mpls te tunnel path Tunnel0/0/1
 Tunnel Interface Name : Tunnel0/0/1
 Lsp ID : 1.1.1.1 :100 :1
 Hop Information
  Hop 0   20.1.1.1
  Hop 1   20.1.1.2
  Hop 2   3.3.3.3
  Hop 3   40.1.1.1
  Hop 4   40.1.1.2
  Hop 5   4.4.4.4
  Hop 3   50.1.1.1
  Hop 4   50.1.1.2
  Hop 5   5.5.5.5
```

Run the **tracert lsp te tunnel** command on the PLR, and you can view that the TE traffic is transmitted through the bypass tunnel.

```
<PLR> tracert lsp te tunnel 0/0/1
  LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel0/0/1 , press CTRL_C to
break.
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   20.1.1.2/[13312 13312 ]
  1     20.1.1.2           50 ms   Transit   40.1.1.2/[3 ]
  2     40.1.1.2           50 ms   Transit
  3     5.5.5.5            60 ms   Egress
```

After the removed LPU where the outgoing interface of the primary tunnel is located is re-installed, run the **tracert lsp te tunnel** command, and you can view that the traffic is switched back to the primary tunnel.

```
<PLR> tracert lsp te tunnel 0/0/1
  LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel6/0/0 , press CTRL_C to
break.
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   10.1.1.2/[13312 ]
  1     10.1.1.2           40 ms   Transit   30.1.1.2/[13312 ]
  2     30.1.1.2           50 ms   Transit   50.1.1.2/[3 ]
  3     5.5.5.5            60 ms   Egress
```

----End

Configuration Files

- Configuration file of the PLR

```
#
 sysname PLR
#
 vlan batch 10 20
#
 mpls lsr-id 1.1.1.1
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
 explicit-path master
  next hop 10.1.1.2
  next hop 30.1.1.2
  next hop 50.1.1.2
  next hop 5.5.5.5
#
 explicit-path by-path
  next hop 20.1.1.2
  next hop 40.1.1.2
  next hop 4.4.4.4
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
```


Copyright © Huawei Technologies Co., Ltd.

```
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 10000 bc1 3000
 mpls rsvp-te
#
interface Vlanif20
 ip address 20.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 10000 bc1 3000
 mpls rsvp-te
#
interface GigabitEhernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEhernet2/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
interface Tunnel0/0/1
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 5.5.5.5
 mpls te tunnel-id 100
 mpls te path explicit-path master
 mpls te fast-reroute
 mpls te commit
#
interface Tunnel0/0/2
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 4.4.4.4
 mpls te tunnel-id 200
 mpls te record-route
 mpls te path explicit-path by-path
 mpls te bypass-tunnel bandwidth 400
 mpls te protected-interface Vlanif10
 mpls te commit
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 10.1.1.0 0.0.0.3
  network 20.1.1.0 0.0.0.3
  network 1.1.1.1 0.0.0.0
  mpls-te enable
#
return
```

- Configuration file of LSRA

```
#
 sysname LSRA
#
 vlan batch 10 30
#
 mpls lsr-id 2.2.2.2
 mpls
  mpls te
  mpls rsvp-te
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
```


Copyright © Huawei Technologies Co., Ltd.

```
interface Vlanif30
 ip address 30.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 10000 bc1 3000
 mpls rsvp-te
#
interface GigabitEhernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEhernet2/0/0
 port link-type access
 port default vlan 30
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 10.1.1.0 0.0.0.3
  network 30.1.1.0 0.0.0.3
  network 2.2.2.2 0.0.0.0
  mpls-te enable
#
return
```

- Configuration file of LSRB

```
#
 sysname LSRB
#
 vlan batch 20 40
#
 mpls lsr-id 3.3.3.3
 mpls
  mpls te
  mpls rsvp-te
#
interface Vlanif20
 ip address 20.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif40
 ip address 40.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 10000 bc1 3000
 mpls rsvp-te
#
interface GigabitEhernet1/0/0
 port link-type access
 port default vlan 20
#
interface GigabitEhernet2/0/0
 port link-type access
 port default vlan 40
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 20.1.1.0 0.0.0.3
  network 30.1.1.0 0.0.0.3
  network 3.3.3.3 0.0.0.0
  mpls-te enable
```


Copyright © Huawei Technologies Co., Ltd.

```
#
return
```

- Configuration file of the MP

```
#
 sysname MP
#
 vlan batch 30 40 50
#
 mpls lsr-id 4.4.4.4
 mpls
  mpls te
  mpls rsvp-te
#
interface Vlanif30
 ip address 30.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif40
 ip address 40.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif50
 ip address 50.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 10000 bc1 3000
 mpls rsvp-te
#
interface GigabitEhernet1/0/0
 port default vlan 30
#
interface GigabitEhernet2/0/0
 port link-type access
 port default vlan 40
#
interface GigabitEhernet3/0/0
 port link-type access
 port default vlan 50
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 30.1.1.0 0.0.0.3
  network 40.1.1.0 0.0.0.3
  network 50.1.1.0 0.0.0.3
  network 4.4.4.4 0.0.0.0
  mpls-te enable
#
return
```

- Configuration file of LSRC

```
#
 sysname LSRC
#
 vlan batch 50
#
 mpls lsr-id 5.5.5.5
 mpls
  mpls te
  mpls rsvp-te
#
interface Vlanif50
```


Copyright © Huawei Technologies Co., Ltd.

```
 ip address 50.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEhernet1/0/0
 port link-type access
 port default vlan 50
#
interface LoopBack1
 ip address 5.5.5.5 255.255.255.255
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 50.1.1.0 0.0.0.3
  network 5.5.5.5 0.0.0.0
  mpls-te enable
#
return
```

3.21.13 Example for Configuring CR-LSP Hot Standby

Networking Requirements

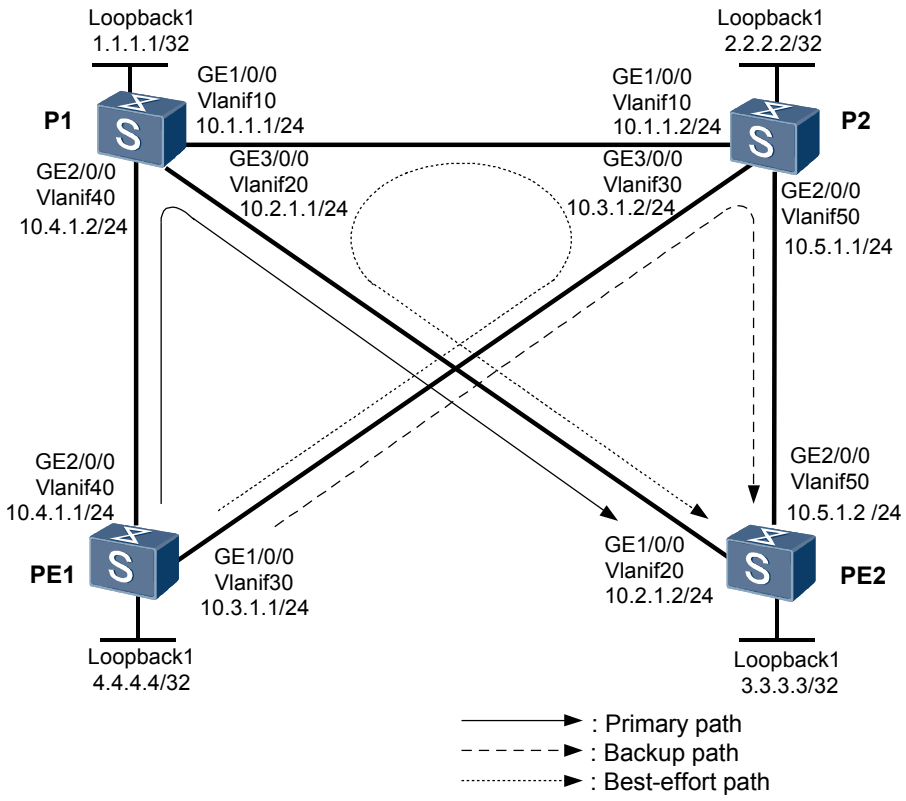
Figure 3-14 shows an MPLS VPN. P and PE devices are S9300s. A TE tunnel with PE1 as the ingress node and PE2 as the egress node needs to be established on PE1. CR-LSP hot standby and best-effort path also need to be configured.

- 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 faulty primary CR-LSP is recovered, the traffic can be switched back to the primary CR-LSP after 15 seconds. If both the primary and backup CR-LSPs fail, traffic can be switched to the best-effort path.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-14 Networking diagram for configuring CR-LSP hot standby



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an IP address for each interface and enable an IGP on each node to implement interworking.
2. Configure MPLS and basic MPLS TE functions.
3. Configure explicit paths for the primary and backup CR-LSPs on PE1.
4. Create the tunnel interface with PE2 as the egress node on PE1 and specify the explicit path; enable hot standby and configure the best-effort path; set the WTR time to 15 seconds.

Data Preparation

To complete the configuration, you need the following data:

- Type of an IGP and data required for configuring an IGP
- MPLS LSR ID
- Bandwidth attributes of links along the tunnel
- Tunnel interface number and bandwidth occupied by the tunnel
- Explicit paths of the primary CR-LSP and the backup CR-LSP

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Create VLANs and VLANIF interfaces, and assign IP addresses to the VLANIF interfaces.

As shown in **Figure 3-14**, configure an IP address for each interface, create loopback interfaces on the nodes, and then configure the IP addresses of the loopback interfaces as MPLS LSR IDs. For detailed configuration, see the configuration files in this example.

Step 2 Configure an IGP.

Configure OSPF or IS-IS on each node to implement interworking between the nodes. In this example, IS-IS is configured. For detailed configuration, see the configuration files in this example.

Step 3 Configure basic MPLS functions.

On each node, enable MPLS TE and MPLS RSVP-TE in the MPLS view and in the view of the physical interface. Set the maximum MPLS TE bandwidth and maximum reservable bandwidth for each interface to 100 Mbit/s and 100 Mbit/s respectively. For detailed configuration, see the configuration files in this example.

Step 4 Configure IS-IS TE and CSPF.

Configure IS-IS TE on each node and configure CSPF on PE1. For the configuration procedure, see **3.4 Configuring an RSVP-TE Tunnel**.

Step 5 Configure the explicit paths for the primary CR-LSP and the backup 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 10.4.1.2
[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 the explicit path for the backup 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] quit
```

View information about the explicit paths on PE1.

```
[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 6 Configure the tunnel interface.

```
[PE1] interface tunnel 1/0/0
[PE1-Tunnel1/0/0] ip address unnumbered interface loopback 1
[PE1-Tunnel1/0/0] tunnel-protocol mpls te
[PE1-Tunnel1/0/0] destination 3.3.3.3
[PE1-Tunnel1/0/0] mpls te tunnel-id 100
[PE1-Tunnel1/0/0] mpls te path explicit-path main
```


Copyright © Huawei Technologies Co., Ltd.

Configure hot standby on the tunnel interface, set the WTR time to 15 seconds, specify the backup explicit path, and configure the best-effort path.

```
[PE1-Tunnel1/0/0] mpls te backup hot-standby wtr 15
[PE1-Tunnel1/0/0] mpls te path explicit-path backup secondary
[PE1-Tunnel1/0/0] mpls te backup ordinary best-effort
[PE1-Tunnel1/0/0] mpls te commit
[PE1-Tunnel1/0/0] quit
```

After the configuration, run the **display mpls te tunnel-interface tunnel 1/0/0** command on PE1, and you can find that the primary CR-LSP and the backup CR-LSP are established.

```
[PE1] display mpls te tunnel-interface tunnel 1/0/0
  Tunnel Name         :  Tunnel1/0/0
  Tunnel State Desc   :  Primary CR-LSP Up and HotBackup CR-LSP Up
  Tunnel Attributes   :
    LSP ID              :  4.4.4.4:2
    Session ID          :  100
    Admin State         :  UP               Oper State   :  UP
    Ingress LSR ID      :  4.4.4.4          Egress LSR ID:  3.3.3.3
    Signaling Prot      :  RSVP             Resv Style   :  SE
    Class Type          :  CLASS 0          Tunnel BW    :  10000 kbps
    Reserved BW         :  50000 kbps
    Setup Priority      :  7                Hold Priority:  7
    Hop Limit           :  -
    Secondary Hop Limit :  -
    BestEffort Hop Limit:  -
    Affinity Prop/Mask  :  0x0/0x0
    Explicit Path Name  :  -
    Secondary Affinity Prop/Mask:  0x0/0x0
    Secondary Explicit Path Name:  -
    BestEffort Affinity Prop/Mask:  0x0/0x0
    Tie-Breaking Policy :  None
    Metric Type         :  None
    Record Route        :  Enabled          Record Label :  Disabled
    FRR Flag            :  Disabled         BackUpBW Flag:  Not Supported
    BackUpBW Type       :  -                BackUpBW     :  -
    Route Pinning       :  Disabled
    Reopt               :  Disabled         Reopt Freq   :  -
    Back Up Type        :  HotStandBy
    Back Up LSPID       :  4.4.4.4:32770
    Auto BW             :  Disabled         Auto BW Freq :  -
    Min BW              :  -                Max BW       :  -
    Current Collected BW:  -
    Interfaces Protected:  -
    Car Policy          :  Disabled
    Tunnel  Group       :  Primary
    Primary Tunnel      :  -
    Backup  Tunnel      :  -
    IPTN    InLabel     :  -
    Group   Status      :  Up
    Oam     Status      :  Up
    Bfd Capability      :  None
    BestEffort          :  Enabled              IsBestEffortPath:  Non-existent
```

Step 7 Verify the configuration.

Connect two interfaces, namely, Port 1 and Port 2 on a tester, to PE1 and PE2 respectively. On Port 1, send MPLS traffic to Port 2. After the cable of GE 2/0/0 on PE1 or P1 is removed, the fault recovers at the millisecond level. Run the **display mpls te hot-standby state interface tunnel 1/0/0** command on PE1, and you can find that traffic is switched to the backup CR-LSP.

```
[PE1] display mpls te hot-standby state interface tunnel 1/0/0
-------------------------------------------------------------
Verbose information about the Tunnel1/0/0 hot-standby state
-------------------------------------------------------------
tunnel name                          : Tunnel1/0/0
session id                           : 100
```


Copyright © Huawei Technologies Co., Ltd.

```
main LSP token                          : 0x0
hot-standby LSP token                   : 0x100201b
HSB switch result                       : hot-standby LSP
WTR                                     : 15s
```

After installing the cable into GE 2/0/0, you can view that traffic is switched back to the primary CR-LSP after 15 minutes.

If you remove the cable from GE 2/0/0 on PE1 or P1 and then remove the cable from GE 2/0/0 on PE2 and P2, the tunnel interface changes from Down to Up and traffic is switched to the best-effort path.

```
[PE1] display mpls te tunnel-interface tunnel 1/0/0

  Tunnel Name         :  Tunnel1/0/0
  Tunnel State Desc   :  Backup CR-LSP In use and Primary CR-LSP setting Up
  Tunnel Attributes   :
    LSP ID             :  4.4.4.4:3
    Session ID         :  100
    Admin State        :  UP                   Oper State   :  UP
    Ingress LSR ID     :  4.4.4.4              Egress LSR ID:  3.3.3.3
    Signaling Protocol :  RSVP                 Resv Style   :  SE
    Class Type         :  CLASS 0              Tunnel BW    :  100000 kbps
    Reserved BW        :  50000 kbps
    Setup Priority     :  7                    Hold Priority:  7
    Hop Limit          :  -
    Secondary Hop Limit :  -
    BestEffort Hop Limit:  -
    Affinity Prop/Mask  :  0x0/0x0
    Explicit Path Name  :  main
    Secondary Affinity Prop/Mask:  0x0/0x0
    Secondary Explicit Path Name:  backup
    BestEffort Affinity Prop/Mask:  0x0/0x0
    Tie-Breaking Policy :  None
    Metric Type        :  None
    Record Route       :  Enabled              Record Label :  Disabled
    FRR Flag           :  Disabled             BackUpBW Flag:  Not Supported
    BackUpBW Type      :  -                    BackUpBW     :  -
    Route Pinning      :  Disabled
    Retry Limit        :  5                    Retry Interval:  10 sec
    Reopt              :  Disabled             Reopt Freq   :  -
    Back Up Type       :  HotStandBy
    Back Up LSPID      :  4.4.4.4:32776
    Auto BW            :  Disabled             Auto BW Freq :  -
    Min BW             :  -                    Max BW       :  -
    Current Collected BW:  -
    Interfaces Protected:  -
    Car Policy         :  Disabled
    Tunnel  Group      :  Primary
    Primary Tunnel Sum  :  -
    Primary Tunnel     :  -
    Backup  Tunnel     :  -
    IPTN    InLabel    :  -
    Group   Status     :  Up
    Oam     Status     :  Up
    Bfd Capability     :  None
    BestEffort         :  Enabled              IsBestEffortPath:  Up

[PE1] display mpls te tunnel path
 Tunnel Interface Name : Tunnel1/0/0
 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
```


Copyright © Huawei Technologies Co., Ltd.

```
Hop 7   10.2.1.2
Hop 8   3.3.3.3
```

----End

Configuration Files

- Configuration file of PE1

```
#
 sysname PE1
#
 vlan batch 30 40
#
 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 Vlanif30
 ip address 10.3.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface Vlanif40
 ip address 10.4.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 30
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 40
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 isis enable 1
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te tunnel-id 100
 mpls te record-route
```


Copyright © Huawei Technologies Co., Ltd.

```
 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
#
return
```

- Configuration file of P1

```
#
 sysname P1
#
 vlan batch 10 20 40
#
 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 Vlanif10
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif20
 ip address 10.2.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface Vlanif40
 ip address 10.4.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 40
#
interface GigabitEthernet3/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of P2

```
#
 sysname P2
#
 vlan batch 10 30 50
#
```


Copyright © Huawei Technologies Co., Ltd.

```
 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 Vlanif10
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface Vlanif30
 ip address 10.3.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif50
 ip address 10.5.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 50
#
interface GigabitEthernet3/0/0
 port link-type access
 port default vlan 30
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
 vlan batch 20 50
#
 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 Vlanif20
 ip address 10.2.1.2 255.255.255.0
 isis enable 1
```


Copyright © Huawei Technologies Co., Ltd.

```
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif50
 ip address 10.5.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 20
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 50
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 isis enable 1
#
return
```

3.21.14 Example for Configuring Synchronization of the Bypass Tunnel and the Backup CR-LSP

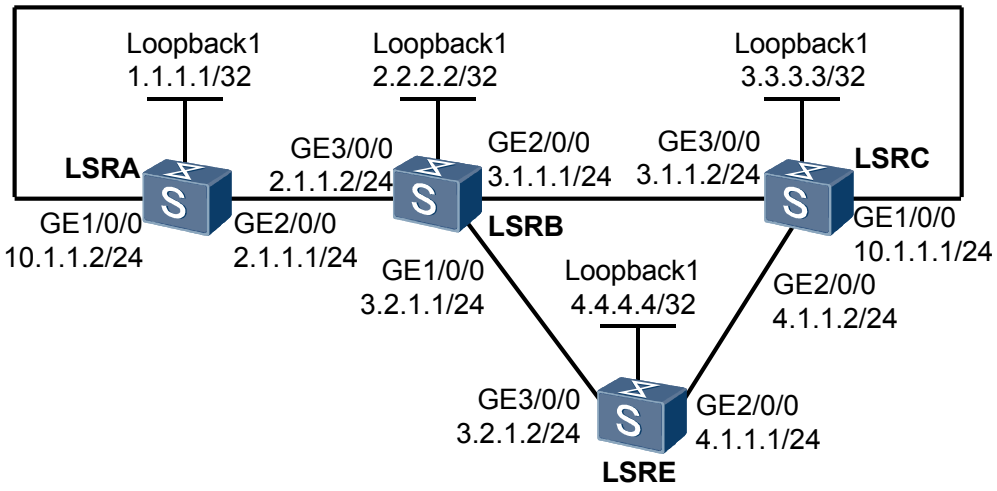
Networking Requirements

As shown in **Figure 3-15**, a primary tunnel is set up by using the explicit path LSR A --> LSR B --> LSR C. A TE FRR bypass tunnel is set up on the transit LSR B along the path LSR B --> LSR E --> LSR C; an ordinary CR-LSP is set up on the ingress LSR A along the path LSR A --> LSR C.

After the link between LSR B and LSR C is faulty, the system starts the TE FRR bypass tunnel (that is, the primary CR-LSP is in FRR-in-use state) and tries to restore the primary CR-LSP. At the same time, the system tries to set up the backup CR-LSP.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-15 Networking diagram of configuring synchronization of the bypass tunnel and the backup CR-LSP



Switch	Interface	VLANIF interface	IP address
LSRA	GigabitEthernet1/0/0	VLANIF 10	10.1.1.2/24
LSRA	GigabitEthernet2/0/0	VLANIF 20	2.1.1.1/24
LSRB	GigabitEthernet1/0/0	VLANIF 40	3.2.1.1/24
LSRB	GigabitEthernet2/0/0	VLANIF 30	3.1.1.1/24
LSRB	GigabitEthernet3/0/0	VLANIF 20	2.1.1.2/24
LSRC	GigabitEthernet1/0/0	VLANIF 10	10.1.1.1/24
LSRC	GigabitEthernet2/0/0	VLANIF 50	4.1.1.2/24
LSRC	GigabitEthernet3/0/0	VLANIF 30	3.1.1.2/24
LSRE	GigabitEthernet2/0/0	VLANIF 50	4.1.1.1/24
LSRE	GigabitEthernet3/0/0	VLANIF 40	3.2.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. On the ingress LSR A, set up a primary tunnel destined for LSR C.
2. On the transit LSR B, set up a TE FRR bypass tunnel along the path LSR B --> LSR E --> LSR C to protect the link between LSR B and LSR C.
3. On the ingress LSR A, set up an ordinary CR-LSP along the path LSR A --> LSR C.
4. Configure synchronization of the bypass tunnel and the backup CR-LSP in the tunnel interface view.

Data Preparation

To complete the configuration, you need the following data:

Copyright © Huawei Technologies Co., Ltd.

- An IGP and its parameters
- Explicit paths of the primary CR-LSP and the backup CR-LSP
- TE FRR protection mode and the protected links or nodes
- Name and IP address of the primary tunnel interface, destination address, tunnel ID, tunnel signaling protocol (RSVP-TE)

Procedure

Step 1 Configure the IP address for each interface.

Configure the IP address and mask for each interface including each Loopback interface as shown in **Figure 3-15**. The detailed configuration is omitted here.

Step 2 Enable an IGP.

Enable OSPF or IS-IS on each LSR to ensure connectivity between routers. In this example, OSPF is used as IGP. For the detailed configuration, see the configuration files in this example.

Step 3 Configure the basic MPLS function.

On each LSR, configure an LSR ID and enable MPLS in the system view and in the interface view. For the detailed configuration, see the configuration files in this example.

Step 4 Configure the basic MPLS TE functions.

On each LSR, enable MPLS-TE and MPLS RSVP-TE in the MPLS view and in the interface view of the link. For the detailed configuration, see the configuration files in this example.

Step 5 Enable OSPF TE and configure the CSPF.

Enable OSPF TE on each LSR and configure the CSPF on LSR A and LSR B. For the detailed configuration, see **Configuring the RSVP-TE Tunnel**.

Step 6 Configure the explicit paths of the primary and backup CR-LSPs.

Configure the explicit path of the primary CR-LSP on LSR A.

```
[LSRA] explicit-path master
[LSRA-explicit-path-master] next hop 2.1.1.2
[LSRA-explicit-path-master] next hop 3.1.1.2
```

Configure the explicit path of the backup CR-LSP on LSR A.

```
[LSRA] explicit-path backup
[LSRA-explicit-path-backup] next hop 10.1.1.1
```

Step 7 Configure the tunnel interface.

Create a tunnel interface on LSR A, specify an explicit path of the primary tunnel.

```
[LSRA] interface tunnel2/0/0
[LSRA-Tunnel2/0/0] ip address unnumbered interface loopback1
[LSRA-Tunnel2/0/0] tunnel-protocol mpls te
[LSRA-Tunnel2/0/0] destination 3.3.3.3
[LSRA-Tunnel2/0/0] mpls te tunnel-id 200
[LSRA-Tunnel2/0/0] mpls te record-route label
[LSRA-Tunnel2/0/0] mpls te path explicit-path master
[LSRA-Tunnel2/0/0] mpls te commit
[LSRA-Tunnel2/0/0] quit
```

Step 8 Enable TE Auto FRR and configure link protection.

Configure LSR A.

Copyright © Huawei Technologies Co., Ltd.

```
[LSRA] interface tunnel2/0/0
[LSRA-Tunnel2/0/0] mpls te fast-reroute
[LSRA-Tunnel2/0/0] mpls te commit
[LSRA-Tunnel2/0/0] quit
```

Configure LSR B.

```
[LSRB] interface gigabitethernet 2/0/0
[LSRB-GigabitEthernet2/0/0] mpls te auto-frr
[LSRB-GigabitEthernet2/0/0] quit
```

After the configurations, run the **display mpls te tunnel path lsp-id 1.1.1.1 1 1** command on LSR A, and you can view that the bypass tunnel is set up successfully.

```
[LSRA] display mpls te tunnel path lsp-id 1.1.1.1 1 1
 Tunnel Interface Name : Tunnel2/0/0
 Lsp ID : 1.1.1.1 :1 :1
 Hop Information
  Hop 0   2.1.1.1
  Hop 1   2.1.1.2  Label 11264
  Hop 2   2.2.2.2  Label 11264
  Hop 3   3.1.1.1 Local-Protection available
  Hop 4   3.1.1.2  Label 3
  Hop 5   3.3.3.3  Label 3
```

Step 9 Configure an ordinary CR-LSP and specify its explicit path.

Configure LSR A.

```
[LSRA] interface tunnel2/0/0
[LSRA-Tunnel2/0/0] mpls te backup ordinary
[LSRA-Tunnel2/0/0] mpls te path explicit-path backup secondary
[LSRA-Tunnel2/0/0] mpls te commit
[LSRA-Tunnel2/0/0] quit
```

Step 10 Configure synchronization of the bypass tunnel and the backup CR-LSP on the ingress LSR A of the primary CR-LSP.

Configure LSR A.

```
[LSRA] interface tunnel2/0/0
[LSRA-Tunnel2/0/0] mpls te backup frr-in-use
[LSRA-Tunnel2/0/0] mpls te commit
[LSRA-Tunnel2/0/0] quit
```

Run the **display mpls te tunnel-interface tunnel2/0/0** command on the ingress LSR A, and you can view information about the primary CR-LSP.

```
[LSRA] display mpls te tunnel-interface tunnel2/0/0
    Tunnel Name       :  Tunnel2/0/0
    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
    Tie-Breaking Policy :  None                 Metric Type  :  None
    Car Policy          :  Disabled             Bfd Cap      :  None
    BypassBW Flag       :  Not Supported
    BypassBW Type       :  -                    Bypass BW    :  -
    Retry Limit         :  5                    Retry Int    :  10 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
```


Copyright © Huawei Technologies Co., Ltd.

```
    Primary Tunnel      :  -                    Pri Tunn Sum :  -
    Backup Tunnel       :  -
    Group Status        :  Up                   Oam Status   :  Up
    IPTN InLabel        :  -
    BackUp Type         :  Ordinary             BestEffort   :  Disabled
    Secondary HopLimit  :  -
    BestEffort HopLimit :  -
    Secondary Explicit Path Name:  backup
    Secondary Affinity Prop/Mask:  0xf0/0xff
    BestEffort Affinity Prop/Mask:  0x0/0x0

    Primary LSP ID      :  1.1.1.1:2
    Setup Priority      :  7                    Hold Priority:  7
    Affinity Prop/Mask  :  0x0/0x0              Resv Style   :  SE
    CT0 Bandwidth(Kbit/sec) :  0          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(kbps):  -
    Explicit Path Name  :  master               Hop Limit    :  -
    Record Route        :  Enabled              Record Label :  Enabled
    Route Pinning       :  Disabled
    FRR Flag            :  Enabled
    IdleTime Remain     :  -
```

Step 11 Verify the configuration.

Invalidate the outgoing interface that is protected on LSR B.

```
[LSRB] interface vlanif 30
[LSRB-Vlanif30] shutdown
```

Configure the affinity property of the tunnel on LSR A.

```
[LSRA] interface tunnel2/0/0
[LSRA-Tunnel2/0/0] mpls te affinity property f0 mask ff secondary
[LSRA-Tunnel2/0/0] mpls te commit
[LSRA-Tunnel2/0/0] quit
```

Run the **display mpls te tunnel-interface** command on the ingress LSR A, and you can view that the tunnel status is "Primary CR-LSP UP and Ordinary CR-LSP setting Up." That is, the primary is in FRR-in-use state and the ordinary CR-LSP is being set up.

```
[LSRA] display mpls te tunnel-interface
    Tunnel Name       :  Tunnel2/0/0
    Tunnel State Desc :  Primary CR-LSP UP and Ordinary CR-LSP setting 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
    Tie-Breaking Policy :  None                 Metric Type  :  None
    Car Policy          :  Disabled             Bfd Cap      :  None
    BypassBW Flag       :  Not Supported
    BypassBW Type       :  -                    Bypass BW    :  -
    Retry Limit         :  5                    Retry Int    :  10 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         :  Ordinary             BestEffort   :  Disabled
```


Copyright © Huawei Technologies Co., Ltd.

```
    Secondary HopLimit  :  -
    BestEffort HopLimit :  -
    Secondary Explicit Path Name:  -
    Secondary Affinity Prop/Mask:  0xf0/0xff
    BestEffort Affinity Prop/Mask:  0x0/0x0

    Primary LSP ID      :  1.1.1.1:2
    Setup Priority      :  7                    Hold Priority:  7
    Affinity Prop/Mask  :  0x0/0x0              Resv Style   :  SE
    CT0 Bandwidth(Kbit/sec) :  0          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(kbps):  -
    Explicit Path Name  :  master               Hop Limit    :  -
    Record Route        :  Enabled              Record Label :  Enabled
    Route Pinning       :  Disabled
    FRR Flag            :  Enabled
    IdleTime Remain     :  -

    Modify LSP ID       :  1.1.1.1:4
    Setup Priority      :  7                    Hold Priority:  7
    Affinity Prop/Mask  :  0x0/0x0              Resv Style   :  SE
    CT0 Bandwidth(Kbit/sec) :  0          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(kbps):  -
    Explicit Path Name  :  master               Hop Limit    :  -
    Record Route        :  Enabled              Record Label :  Enabled
    Route Pinning       :  Disabled
    FRR Flag            :  Enabled
    IdleTime Remain     :  -
```

After about 10 seconds, run the **display mpls te tunnel-interface** command on LSR A, and you can view that the tunnel status is "Modifying CR-LSP is setting up." That is, the primary CR-LSP is being restored.

```
[LSRA] display mpls te tunnel-interface
Tunnel Name       :  Tunnel2/0/0
    Tunnel State Desc :  Modifying CR-LSP is setting 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
    Tie-Breaking Policy :  None                 Metric Type  :  None
    Car Policy          :  Disabled             Bfd Cap      :  None
    BypassBW Flag       :  Not Supported
    BypassBW Type       :  -                    Bypass BW    :  -
    Retry Limit         :  5                    Retry Int    :  10 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         :  Ordinary             BestEffort   :  Disabled
    Secondary HopLimit  :  -
    BestEffort HopLimit :  -
    Secondary Explicit Path Name:  -
    Secondary Affinity Prop/Mask:  0xf0/0xff
    BestEffort Affinity Prop/Mask:  0x0/0x0
```


Copyright © Huawei Technologies Co., Ltd.

```
Primary LSP ID      :  1.1.1.1:2
Setup Priority      :  7                    Hold Priority:  7
Affinity Prop/Mask  :  0x0/0x0              Resv Style   :  SE
CT0 Bandwidth(Kbit/sec) :  0          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(kbps):  -
Explicit Path Name  :  master               Hop Limit    :  -
Record Route        :  Enabled              Record Label :  Enabled
Route Pinning       :  Disabled
FRR Flag            :  Enabled
IdleTime Remain     :  -

Modify LSP ID       :  1.1.1.1:4
Setup Priority      :  7                    Hold Priority:  7
Affinity Prop/Mask  :  0x0/0x0              Resv Style   :  SE
CT0 Bandwidth(Kbit/sec) :  0          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(kbps):  -
Explicit Path Name  :  master               Hop Limit    :  -
Record Route        :  Enabled              Record Label :  Enabled
Route Pinning       :  Disabled
FRR Flag            :  Enabled
IdleTime Remain     :  -
```

When the primary CR-LSP is faulty (that is, the primary CR-LSP is in FRR-in-use state), the system starts the TE FRR bypass tunnel and tries to restore the primary CR-LSP. At the same time, the system tries to set up a backup CR-LSP.

----End

Configuration Files

- Configuration file of LSR A

```
#
 sysname LSRA
#
vlan batch 10 20
#
 mpls lsr-id 1.1.1.1
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
 explicit-path master
  next hop 2.1.1.2
  next hop 3.1.1.2
#
 explicit-path backup
  next hop 10.1.1.2
#
interface Vlanif20
 ip address 2.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
```


Copyright © Huawei Technologies Co., Ltd.

```
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface Tunnel2/0/0
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te tunnel-id 1
 mpls te record-route label
 mpls te path explicit-path master
 mpls te path explicit-path backup secondary
 mpls te affinity property f0 mask ff secondary
 mpls te fast-reroute
 mpls te backup ordinary
 mpls te backup frr-in-use
 mpls te commit
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 2.1.1.0 0.0.0.255
  mpls-te enable
#
return
```

- Configuration file of LSR B

```
#
 sysname LSRB
#
vlan batch 40 30 20
#
 mpls lsr-id 2.2.2.2
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
interface Vlanif20
 ip address 2.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif40
 ip address 3.2.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif30
 ip address 3.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te auto-frr link
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface GigabitEthernet 2/0/0
```


Copyright © Huawei Technologies Co., Ltd.

```
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
interface GigabitEthernet 3/0/0
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 2.1.1.0 0.0.0.255
  network 3.1.1.0 0.0.0.255
  network 3.2.1.0 0.0.0.255
  mpls-te enable
#
return
```

- Configuration file of LSR C

```
#
 sysname LSRC
#
vlan batch 10 50 30
#
 mpls lsr-id 3.3.3.3
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
interface Vlanif50
  ip address 4.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif30
 ip address 3.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
interface GigabitEthernet 3/0/0
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
```


Copyright © Huawei Technologies Co., Ltd.

```
  network 3.1.1.0 0.0.0.255
  network 4.1.1.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
  mpls-te enable
#
return
```

- Configuration file of LSR E

```
#
 sysname LSRE
#
vlan batch 50 40
#
 mpls lsr-id 4.4.4.4
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
interface Vlanif50
 ip address 4.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif40
 ip address 3.2.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
interface GigabitEthernet 3/0/0
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 3.2.1.0 0.0.0.255
  network 4.1.1.0 0.0.0.255
  mpls-te enable
#
return
```

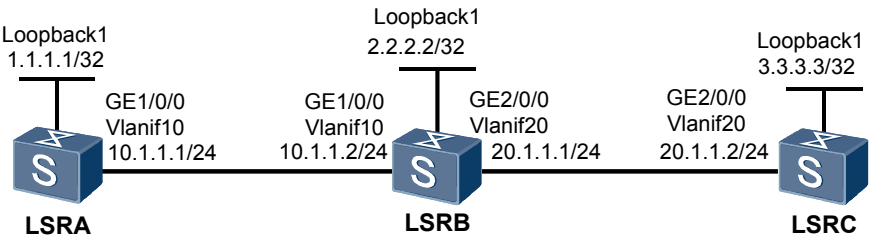
3.21.15 Example for Configuring RSVP GR

Networking Requirements

As shown in **Figure 3-16**, LSRA, S9300-B, and LSRC are configured with dual main control boards. Three switches learn routes from each other through the IS-IS protocol, and then use the RSVP protocol to set up a TE tunnel from S9300-A to LSRC. RSVP GR is required to ensure that MPLS forwarding is continuous when the switchover between the main control board and the LPU occurs on LSRA, LSRB, or LSRC.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-16 Networking diagram for configuring RSVP GR



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the IP addresses for the interfaces of the devices and the address of the loopback interface that is used as the LSR ID.
2. Configure the IS-IS protocol to implement interworking and enable IS-IS TE.
3. Set the LSR ID.
4. Enable global MPLS, MPLS TE, and MPLS RSVP-TE.
5. Enable MPLS, MPLS TE, and MPLS RSVP-TE on each interface, and configure bandwidth attributes of the MPLS TE link.
6. On the ingress node LSRA, enable CSPF and create a tunnel interface, and specify the IP address, tunneling protocol, destination IP address, tunnel ID, and dynamic signaling protocol RSVP-TE.
7. Enable IS-IS GR on each node.
8. Enable RSVP GR on each node.

Data Preparation

To complete the configuration, you need the following data:

- IP address of each interface on each node
- IS-IS NET and IS-IS level that each node belongs to
- LSR ID of each node
- Bandwidth attributes of links along the tunnel
- Tunnel interface number of the ingress node, tunnel ID, and tunnel bandwidth

Procedure

Step 1 Create VLANs and VLANIF interfaces, and assign IP addresses to the VLANIF interfaces.

Configure IP addresses as shown in **Figure 3-16** and create loopback interfaces on the nodes. For detailed configuration, see the configuration files in this example.

Step 2 Configure basic IS-IS functions.

Configure LSRA.

```
[LSRA] isis 1
[LSRA-isis-1] network-entity 00.0005.0000.0000.0001.00
```


Copyright © Huawei Technologies Co., Ltd.

```
[LSRA-isis-1] is-level level-2
[LSRA-isis-1] quit
[LSRA] interface vlanif 10
[LSRA-Vlanif10] isis enable 1
[LSRA-Vlanif10] quit
[LSRA] interface loopback 1
[LSRA-LoopBack1] isis enable 1
[LSRA-LoopBack1] quit
```

Configure LSRB.

```
[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 vlanif 10
[LSRB-Vlanif10] isis enable 1
[LSRB-Vlanif10] quit
[LSRB] interface vlanif 20
[LSRB-Vlanif20] isis enable 1
[LSRB-Vlanif20] quit
[LSRB] interface loopback 1
[LSRB-LoopBack1] isis enable 1
[LSRB-LoopBack1] quit
```

Configure LSRC.

```
[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 vlanif 20
[LSRC-Vlanif20] isis enable 1
[LSRC-Vlanif20] quit
[LSRC] interface loopback 1
[LSRC-LoopBack1] isis enable 1
[LSRC-LoopBack1] quit
```

After the configuration, run the **display ip routing-table** command on each node, and you can view that the nodes learn the routes from each other.

Step 3 Configure basic MPLS functions, enable MPLS TE, RSVP-TE, and CSPF, and configure bandwidth attributes of the link.

Configure LSRA.

```
[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 vlanif 10
[LSRA-Vlanif10] mpls
[LSRA-Vlanif10] mpls te
[LSRA-Vlanif10] mpls rsvp-te
[LSRA-Vlanif10] mpls te bandwidth max-reservable-bandwidth 100000
[LSRA-Vlanif10] quit
```

Configure LSRB.

```
[LSRB] mpls lsr-id 2.2.2.2
[LSRB] mpls
[LSRB-mpls] mpls te
[LSRB-mpls] mpls rsvp-te
[LSRB-mpls] quit
[LSRB] interface vlanif 10
[LSRB-Vlanif10] mpls
[LSRB-Vlanif10] mpls te
```


Copyright © Huawei Technologies Co., Ltd.

```
[LSRB-Vlanif10] mpls rsvp-te
[LSRB-Vlanif10] quit
[LSRB] interface vlanif 20
[LSRB-Vlanif20] mpls
[LSRB-Vlanif20] mpls te
[LSRB-Vlanif20] mpls rsvp-te
[LSRB-Vlanif20] mpls te bandwidth max-reservable-bandwidth 100000
[LSRB-Vlanif20] quit
```

Configure LSRC.

```
[LSRC] mpls lsr-id 3.3.3.3
[LSRC] mpls
[LSRC-mpls] mpls te
[LSRC-mpls] mpls rsvp-te
[LSRC-mpls] quit
[LSRC] interface vlanif 20
[LSRC-Vlanif20] mpls
[LSRC-Vlanif20] mpls te
[LSRC-Vlanif20] mpls rsvp-te
[LSRC-Vlanif20] quit
```

Step 4 Configure IS-IS TE and enable IS-IS GR.

Configure LSRA.

```
[LSRA] isis 1
[LSRA-isis-1] cost-style wide
[LSRA-isis-1] is-name LSRA
[LSRA-isis-1] traffic-eng level-2
[LSRA-isis-1] graceful-restart
[LSRA-isis-1] quit
```

Configure LSRB.

```
[LSRB] isis 1
[LSRB-isis-1] cost-style wide
[LSRB-isis-1] is-name LSRB
[LSRB-isis-1] traffic-eng level-2
[LSRB-isis-1] graceful-restart
[LSRB-isis-1] quit
```

Configure LSRC.

```
[LSRC] isis 1
[LSRC-isis-1] cost-style wide
[LSRC-isis-1] is-name LSRC
[LSRC-isis-1] traffic-eng level-2
[LSRC-isis-1] graceful-restart
[LSRC-isis-1] quit
```

Step 5 Configure the MPLS TE tunnel.

Create an MPLS TE tunnel on LSRA.

```
[LSRA] interface tunnel 1/0/0
[LSRA-Tunnel1/0/0] ip address unnumbered interface loopback 1
[LSRA-Tunnel1/0/0] tunnel-protocol mpls te
[LSRA-Tunnel1/0/0] destination 3.3.3.3
[LSRA-Tunnel1/0/0] mpls te tunnel-id 100
[LSRA-Tunnel1/0/0] mpls te signal-protocol rsvp-te
[LSRA-Tunnel1/0/0] mpls te commit
[LSRA-Tunnel1/0/0] quit
```

After the configuration, run the **display interface tunnel** command on LSRA, and you can view that the status of the tunnel interface is Up.

```
[LSRA] display interface tunnel
Tunnel1/0/0 current state : UP
Line protocol current state : UP
```


Copyright © Huawei Technologies Co., Ltd.

```
Description : HUAWEI, Quidway Series, Tunnel1/0/0 Interface
The Maximum Transmit Unit is 1500 bytes
Internet Address is unnumbered, using address of LoopBack1(1.1.1.9/32)
Encapsulation is TUNNEL, loopback not set
Tunnel destination 3.3.3.3
Tunnel up/down statistics 1
Tunnel protocol/transport MPLS/MPLS, ILM is available,
    300 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets output,  0 bits
    0 output error
```

Step 6 Enable RSVP GR.

Configure LSRA.

```
[LSRA] mpls
[LSRA-mpls] mpls rsvp-te hello
[LSRA-mpls] mpls rsvp-te hello full-gr
[LSRA-mpls] quit
[LSRA] interface vlanif 10
[LSRA-Vlanif10] mpls rsvp-te hello
```

Configure LSRB.

```
[LSRB] mpls
[LSRB-mpls] mpls rsvp-te hello
[LSRB-mpls] mpls rsvp-te hello full-gr
[LSRB-mpls] quit
[LSRB] interface vlanif 10
[LSRB-Vlanif10] mpls rsvp-te hello
[LSRB] interface vlanif 20
[LSRB-Vlanif20] mpls rsvp-te hello
```

Configure LSRC.

```
[LSRC] mpls
[LSRC-mpls] mpls rsvp-te hello
[LSRC-mpls] mpls rsvp-te hello full-gr
[LSRC-mpls] quit
[LSRC] interface vlanif 20
[LSRC-Vlanif20] mpls rsvp-te hello
```

Step 7 Verify the configuration.

After the configuration, run the **display mpls rsvp-te graceful-restart** command on LSRB, and you can view the local GR status, restart time, and recovery time.

```
[LSRB] display mpls rsvp-te graceful-restart
Display Mpls Rsvp te graceful restart information
 LSR ID: 2.2.2.2
 Graceful-Restart Capability:    GR-Self GR-Support
 Restart Time:  90060 Milli Second
 Recovery Time: 0 Milli Second
 GR Status:  Restart time Not going on
 Number of Restarting neighbors: 2
 Received Gr Path message count: 2
 Send Gr Path message count: 0
 Received RecoveryPath message count: 2
 Send RecoveryPath message count: 0.
```

Run the **display mpls rsvp-te graceful-restart peer** command on LSRB, and you can view the GR status of the neighboring node.

```
[LSRB] display mpls rsvp-te graceful-restart peer
Neighbor on Interface Vlanif10
 Neighbor Addr: 10.1.1.1
 SrcInstance: 47860                    NbrSrcInstance: 49409
 Neighbor Capability:
                     Can Do Self GR
```


Copyright © Huawei Technologies Co., Ltd.

```
                    Can Support GR
GR Status:          Normal
Restart Time:  90060 Milli Second
Recovery Time: 0 Milli Second
Stored GR message number: 0
```

----End

Configuration Files

- Configuration file of LSRA

```
#
 sysname LSRA
#
 vlan batch 10
#
 mpls lsr-id 1.1.1.1
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
  mpls rsvp-te hello
  mpls rsvp-te hello full-gr
#
isis 1
 graceful-restart
 is-level level-2
 cost-style wide
 is-name LSRA
 network-entity 00.0005.0000.0000.0001.00
 traffic-eng level-2
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
 mpls rsvp-te hello
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 isis enable 1
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te tunnel-id 100
 mpls te commit
#
return
```

- Configuration file of LSRB

```
#
 sysname LSRB
#
 vlan batch 10 20
#
 mpls lsr-id 2.2.2.2
 mpls
  mpls te
  mpls rsvp-te
```


Copyright © Huawei Technologies Co., Ltd.

```
  mpls rsvp-te hello
  mpls rsvp-te hello full-gr
#
isis 1
 graceful-restart
 is-level level-2
 cost-style wide
 is-name LSRB
 network-entity 00.0005.0000.0000.0002.00
 traffic-eng level-2
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
 mpls rsvp-te hello
#
interface Vlanif20
ip address 20.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
 mpls rsvp-te hello
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of LSRC

```
#
 sysname LSRC
#
 vlan batch 20
#
 mpls lsr-id 3.3.3.3
 mpls
  mpls te
  mpls rsvp-te
  mpls rsvp-te hello
  mpls rsvp-te hello full-gr
#
isis 1
 graceful-restart
 is-level level-2
 cost-style wide
 is-name LSRC
 network-entity 00.0005.0000.0000.0003.00
 traffic-eng level-2
#
interface Vlanif20
 ip address 20.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
 mpls rsvp-te hello
```


Copyright © Huawei Technologies Co., Ltd.

```
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 isis enable 1
#
return
```

3.21.16 Example for Configuring Static BFD for CR-LSPs

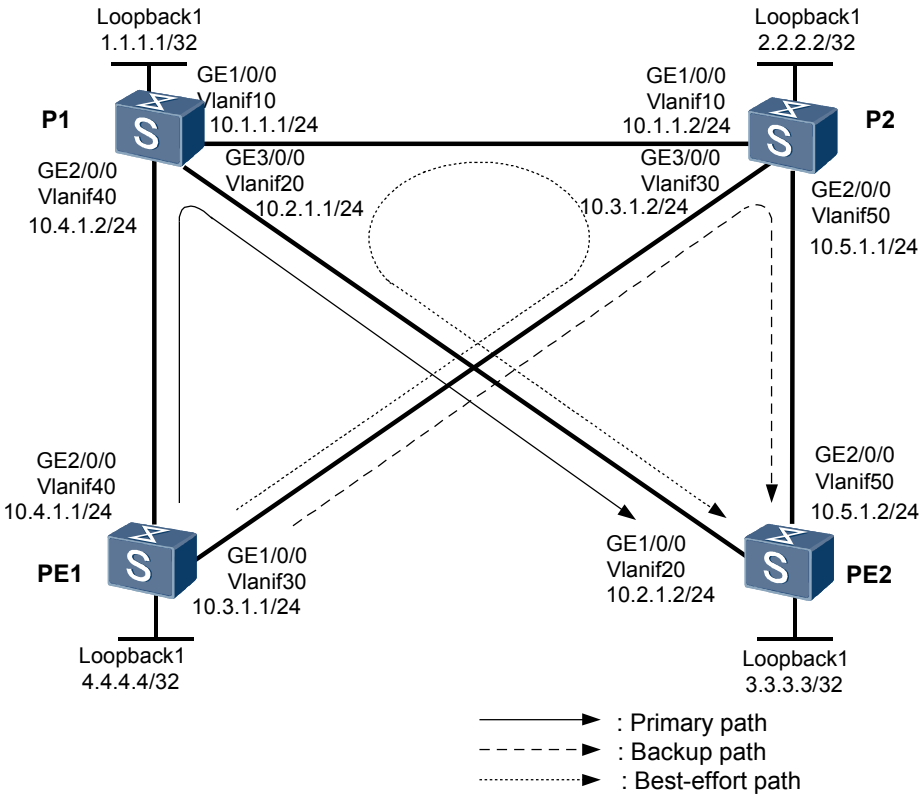
Networking Requirements

Figure 3-17 shows a network where CR-LSP hot standby is configured. A TE tunnel is established between PE1 and PE2. The tunnel is enabled with hot standby and configured with the best-effort path. If the primary CR-LSP fails, traffic is switched to the backup CR-LSP. After the faulty primary CR-LSP is recovered, the traffic is switched back to the primary CR-LSP after 15 seconds. If both the primary and backup CR-LSPs fail, traffic is switched to the best-effort path.

You are required to create two static BFD sessions to detect the primary and backup CR-LSPs. After the configuration, the following should be achieved:

- If the primary CR-LSP fails, traffic is rapidly switched to the backup CR-LSP.
- After the primary CR-LSP is recovered in less than 15 seconds, traffic is switched back to the primary CR-LSP if the backup CR-LSP fails.

Figure 3-17 Networking diagram for configuring CR-LSP hot standby



Copyright © Huawei Technologies Co., Ltd.

P to PE devices are the switches in this example.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure CR-LSP hot standby according to **3.21.13 Example for Configuring CR-LSP Hot Standby**.
2. On PE1, create two BFD sessions and bind the two sessions to the primary CR-LSP and the backup CR-LSP; on PE2, create 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:

- BFD configuration name, local discriminator, and remote discriminator
- Minimum intervals for receiving and sending BFD packets
- Local detection multiplier of BFD
- For other data, see **3.21.13 Example for Configuring CR-LSP Hot Standby**.

Procedure

Step 1 Configure CR-LSP hot standby.

Configure the primary CR-LSP, backup CR-LSP, and best-effort path according to **3.21.13 Example for Configuring CR-LSP Hot Standby**.

Step 2 Configure BFD for CR-LSPs.

Create BFD sessions between PE1 and PE2 to detect faults on the primary CR-LSP and the backup CR-LSP. Bind the BFD sessions on PE1 to the primary CR-LSP and the backup CR-LSP respectively; bind the BFD session on PE2 to the IP link. Set the minimum intervals for sending and receiving BFD packets to 100 milliseconds and the local detection multiplier of BFD to 3.

Configure PE1.

```
[PE1] bfd
[PE1-bfd] quit
[PE1] bfd mainlsptope2 bind mpls-te interface tunnel1/0/0 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] detect-multiplier 3
[PE1-bfd-lsp-session-mainlsptope2] process-pst
[PE1-bfd-lsp-session-mainlsptope2] commit
[PE1-bfd-lsp-session-mainlsptope2] quit
[PE1] bfd backuplsptope2 bind mpls-te interface tunnel1/0/0 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] detect-multiplier 3
[PE1-bfd-lsp-session-backuplsptope2] process-pst
[PE1-bfd-lsp-session-backuplsptope2] commit
[PE1-bfd-lsp-session-backuplsptope2] quit
```


Copyright © Huawei Technologies Co., Ltd.

Configure PE2.

```
[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] detect-multiplier 3
[PE2-bfd-lsp-session-mainlsptope2] commit
[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] detect-multiplier 3
[PE2-bfd-lsp-session-backuplsptope2] commit
[PE2-bfd-lsp-session-backuplsptope2] quit
```

After the configuration, run the **display bfd session discriminator** *local-discriminator-value* command on PE1 and PE2, and you can find that the status of the BFD sessions is Up.

Take the display on PE1 as an example:

```
[PE1] display bfd session discriminator 413
--------------------------------------------------------------------------------
Local  Remote PeerIpAddr      InterfaceName                 State     Type
--------------------------------------------------------------------------------
413    314    3.3.3.3         Tunnel1/0/0                   Up        S_TE_LSP
--------------------------------------------------------------------------------

[PE1] display bfd session discriminator 423
--------------------------------------------------------------------------------
Local  Remote PeerIpAddr      InterfaceName                 State     Type
--------------------------------------------------------------------------------
423    324    3.3.3.3         Tunnel1/0/0                   Up        S_TE_LSP
--------------------------------------------------------------------------------
```

Step 3 Verify the configuration.

Connect two interfaces, namely, Port 1 and Port 2 on a tester, to PE1 and PE2 respectively. On Port 1, send MPLS traffic to Port 2. After the cable of GE 2/0/0 on PE1 or P1 is removed, the fault recovers at the millisecond level.

After installing the cable into GE 2/0/0 and then removing the cable from GE 1/0/0 on PE1 in 15 seconds, you can find that the fault recovers at the millisecond level.

----End

Configuration Files

- Configuration file of PE1

```
#
 sysname PE1
#
 vlan batch 30 40
#
 bfd
#
 mpls lsr-id 4.4.4.4
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
```


Copyright © Huawei Technologies Co., Ltd.

```
#
 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 Vlanif30
 ip address 10.3.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface Vlanif40
 ip address 10.4.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 30
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 40
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 isis enable 1
#
interface Tunnel1/0/0
 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 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 Tunnel1/0/0 te-lsp backup
 discriminator local 423
 discriminator remote 324
 min-tx-interval 100
 min-rx-interval 100
 process-pst
 commit
#
bfd mainlsptope2 bind mpls-te interface Tunnel1/0/0 te-lsp
 discriminator local 413
 discriminator remote 314
 min-tx-interval 100
 min-rx-interval 100
```


Copyright © Huawei Technologies Co., Ltd.

```
 process-pst
 commit
#
return
```

- Configuration file of P1

```
#
 sysname P1
#
 vlan batch 10 20 40
#
 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 Vlanif10
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif20
 ip address 10.2.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface Vlanif40
 ip address 10.4.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 40
#
interface GigabitEthernet3/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of P2

```
#
 sysname P2
#
 vlan batch 10 30 50
#
 mpls lsr-id 2.2.2.2
 mpls
  mpls te
```


Copyright © Huawei Technologies Co., Ltd.

```
  mpls rsvp-te
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0002.00
 traffic-eng level-1-2
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface Vlanif30
 ip address 10.3.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif50
 ip address 10.5.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 50
#
interface GigabitEthernet3/0/0
 port link-type access
 port default vlan 30
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
 vlan batch 20 50
#
 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 Vlanif20
 ip address 10.2.1.2 255.255.255.0
 isis enable 1
 mpls
```


Copyright © Huawei Technologies Co., Ltd.

```
 mpls te
 mpls rsvp-te
#
interface Vlanif50
 ip address 10.5.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 20
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 50
#
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
 commit
#
bfd mainlsptope2 bind peer-ip 4.4.4.4
 discriminator local 314
 discriminator remote 413
 min-tx-interval 100
 min-rx-interval 100
 commit
#
return
```

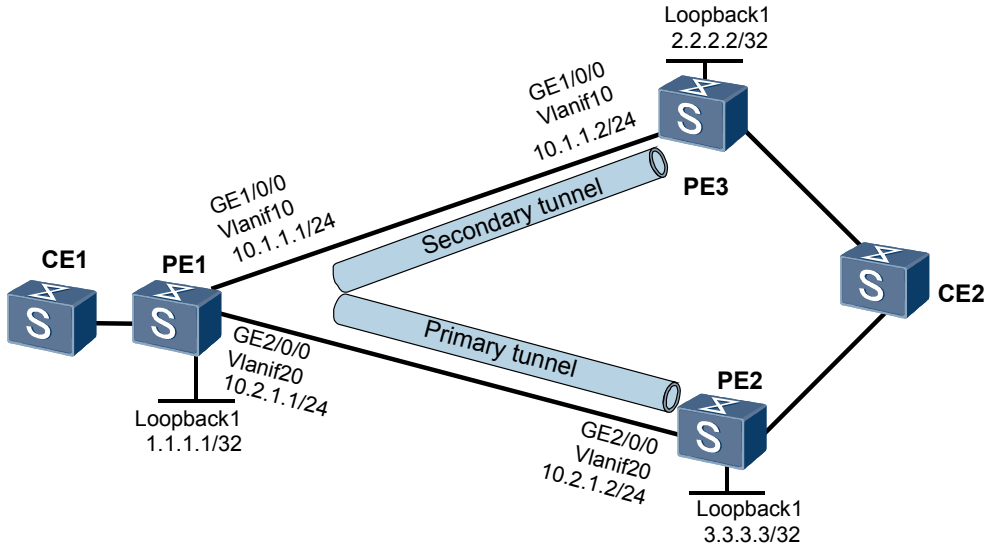
3.21.17 Example for Configuring Static BFD for TE Tunnels

Networking Requirements

Figure 3-18 shows an MPLS network where PE and CE devices are switches. PE1 is configured with VPN FRR and the MPLS TE tunnel. The primary path of VPN FRR is PE1->PE2; the backup path of VPN FRR is PE1->PE3. Normally, VPN traffic is transmitted over the primary path. If the primary path fails, VPN traffic switches to the backup path. You are required to configure BFD for TE tunnels to detect faults on the TE tunnel over the primary path and enable VPN to rapidly detect the faults. Therefore, traffic can be switched between the primary path and backup path in case of faults, and fault recovery is shortened.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-18 Networking diagram for configuring static BFD for TE tunnels



NOTE

For ease of description, the IP addresses of the interfaces connecting the PEs and the CEs are not described in **Figure 3-18**.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic MPLS functions, and establish bi-directional TE tunnels between PE1 and PE2, and between PE1 and PE3.
2. Configure VPN FRR.
3. Enable global BFD on PE1, PE2, and PE3.
4. Configure a BFD session on PE1 to detect faults on the TE tunnel over the primary path.
5. Configure a BFD session on PE2 and PE3 and specify the TE tunnel as the BFD backward tunnel.

Data Preparation

To complete the configuration, you need the following data:

- Type of an IGP and data required for configuring an IGP
- BGP AS number and interfaces of BGP sessions
- MPLS LSR ID
- Maximum bandwidth and maximum reservable bandwidth for the link of the outgoing interface 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

Copyright © Huawei Technologies Co., Ltd.

- Data required for configuring VPN FRR such as the names of the IP prefix and the routing policy
- BFD configuration name, local discriminator, and remote discriminator

Procedure

Step 1 Create VLANs and VLANIF interfaces, and assign IP addresses to the VLANIF interfaces.

Configure an IP address for each interface according to the networking diagram, create loopback interfaces on nodes, and then configure the IP addresses of the loopback interfaces as MPLS LSR IDs. For detailed configuration, see the configuration files in this example.

Step 2 Configure an IGP.

Configure OSPF or IS-IS on each node to implement interworking between PE1 and PE2, and between PE1 and PE3. OSPF is configured in this example. For detailed configuration, see the configuration file of this example.

Step 3 Configure basic MPLS functions.

On each node, configure an LSR ID and enable MPLS in the system view and enable MPLS on each physical interface. For detailed configuration, see the configuration files in this example.

Step 4 Configure basic MPLS TE functions.

On each node, enable MPLS TE and MPLS RSVP-TE in the MPLS view and in the view of the physical interface. Set the maximum MPLS TE bandwidth and maximum reservable bandwidth for each interface to 100 Mbit/s and 100 Mbit/s respectively. For detailed configuration, see the configuration files in this example.

Step 5 Configure OSPF TE and CSPF.

Configure OSPF TE on each node and configure CSPF on PE1. For the configuration procedure, see **3.4 Configuring an RSVP-TE Tunnel**.

Step 6 Configure tunnel interfaces.

Configure explicit paths on PE1, PE2, and PE3. For PE1, two explicit paths must be created.

Configure PE1.

```
<PE1>system-view
[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] quit
```

Configure PE2.

```
<PE2>system-view
[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] quit
```

Configure PE3.

```
<PE3> system-view
[PE3] explicit-path tope1
```


Copyright © Huawei Technologies Co., Ltd.

```
[PE3-explicit-path-tope1] next hop 10.1.1.1
[PE3-explicit-path-tope1] next hop 1.1.1.1
[PE3-explicit-path-tope1] quit
```

Create tunnel interfaces on PE1, PE2, and PE3, configure explicit paths, and set the 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 2/0/0
[PE1-Tunnel2/0/0] ip address unnumbered interface loopback 1
[PE1-Tunnel2/0/0] tunnel-protocol mpls te
[PE1-Tunnel2/0/0] destination 3.3.3.3
[PE1-Tunnel2/0/0] mpls te tunnel-id 200
[PE1-Tunnel2/0/0] mpls te path explicit-path tope2
[PE1-Tunnel2/0/0] mpls te bandwidth bc0 10000
[PE1-Tunnel2/0/0] mpls te reserved-for-binding
[PE1-Tunnel2/0/0] mpls te commit
[PE1-Tunnel2/0/0] quit
[PE1] interface tunnel 1/0/0
[PE1-Tunnel1/0/0] ip address unnumbered interface loopback 1
[PE1-Tunnel1/0/0] tunnel-protocol mpls te
[PE1-Tunnel1/0/0] destination 2.2.2.2
[PE1-Tunnel1/0/0] mpls te tunnel-id 100
[PE1-Tunnel1/0/0] mpls te path explicit-path tope3
[PE1-Tunnel1/0/0] mpls te reserved-for-binding
[PE1-Tunnel1/0/0] mpls te commit
[PE1-Tunnel1/0/0] quit
```

Configure PE2.

```
[PE2] interface tunnel 2/0/0
[PE2-Tunnel2/0/0] ip address unnumbered interface loopback 1
[PE2-Tunnel2/0/0] tunnel-protocol mpls te
[PE2-Tunnel2/0/0] destination 1.1.1.1
[PE2-Tunnel2/0/0] mpls te tunnel-id 200
[PE2-Tunnel2/0/0] mpls te path explicit-path tope1
[PE2-Tunnel2/0/0] mpls te bandwidth bc0 10000
[PE2-Tunnel2/0/0] mpls te reserved-for-binding
[PE2-Tunnel2/0/0] mpls te commit
[PE2-Tunnel2/0/0] quit
```

Configure PE3.

```
[PE3] interface tunnel 1/0/0
[PE3-Tunnel1/0/0] ip address unnumbered interface loopback 1
[PE3-Tunnel1/0/0] tunnel-protocol mpls te
[PE3-Tunnel1/0/0] destination 1.1.1.1
[PE3-Tunnel1/0/0] mpls te tunnel-id 100
[PE3-Tunnel1/0/0] mpls te path explicit-path tope1
[PE3-Tunnel1/0/0] mpls te reserved-for-binding
[PE3-Tunnel1/0/0] mpls te commit
[PE3-Tunnel1/0/0] quit
```

After the configuration, run the **display mpls-te tunnel-interface tunnel** *interface-number* command on the PEs, and you can find that the status of Tunnel 1/0/0 and Tunnel 2/0/0 on PE1, Tunnel 2/0/0 on PE2, and Tunnel 1/0/0 on PE3 is displayed as **CR-LSP is Up**.

Step 7 Configure VPN FRR.

Create VPN instances on PE1, PE2, and PE3 respectively. Set all VPN instance names to **vpn1**, RDs to 100:1, 100:2, and 100:3 respectively, and all RTs to 100:1. Connect the CEs to the PEs. The configuration details are not mentioned here.

Establish MP IBGP peer relationships 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,

Copyright © Huawei Technologies Co., Ltd.

PE2, and PE3 is used as the interface for creating BGP sessions. The configuration details are not mentioned here.

Configure tunnel policies for PE1, PE2, and PE3 and bind 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 2/0/0
[PE1-tunnel-policy-policy1] tunnel binding destination 2.2.2.2 te tunnel 1/0/0
[PE1-tunnel-policy-policy1] quit
[PE1] ip vpn-instance vpn1
[PE1-ip-vpn-instance-vpn1] tnl-policy policy1
[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 2/0/0
[PE2-tunnel-policy-policy1] quit
[PE2] ip vpn-instance vpn1
[PE2-ip-vpn-instance-vpn1] tnl-policy policy1
[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 1/0/0
[PE3-tunnel-policy-policy1] quit
[PE3] ip vpn-instance vpn1
[PE3-ip-vpn-instance-vpn1] tnl-policy policy1
[PE3-ip-vpn-instance-vpn1] quit
```

Configure VPN FRR on PE1.

```
[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] quit
```

After the configuration, the CEs can communicate, and traffic flows through PE1 and PE2. After the cable of any interface connecting PE1 and PE2 is removed, or Switch fails, or PE2 fails, VPN traffic is switched to the backup path PE1->PE3. Time taken in fault recovery is close to the IGP convergence time.

Step 8 Configure BFD for TE tunnels.

Configure a BFD session on PE1 to detect faults on the TE tunnel over the primary path. Set the minimum intervals for sending and receiving BFD packets and the local detection multiplier of BFD.

```
[PE1] bfd
[PE1-bfd] quit
[PE1] bfd test bind mpls-te interface tunnel2/0/0
[PE1-bfd-lsp-session-test] discriminator local 12
[PE1-bfd-lsp-session-test] discriminator remote 21
[PE1-bfd-lsp-session-test] min-tx-interval 100
[PE1-bfd-lsp-session-test] min-rx-interval 100
[PE1-bfd-lsp-session-test] detect-multiplier 3
[PE1-bfd-lsp-session-test] process-pst
[PE1-bfd-lsp-session-test] commit
```


Copyright © Huawei Technologies Co., Ltd.

Configure a BFD session on PE2 and specify the TE tunnel as the backward tunnel. Set the minimum intervals for sending and receiving BFD packets and the local detection multiplier of BFD.

```
[PE2] bfd
[PE2-bfd] quit
[PE2] bfd test bind mpls-te interface tunnel2/0/0
[PE2-bfd-lsp-session-test] discriminator local 21
[PE2-bfd-lsp-session-test] discriminator remote 12
[PE2-bfd-lsp-session-test] min-tx-interval 100
[PE2-bfd-lsp-session-test] min-rx-interval 100
[PE2-bfd-lsp-session-test] detect-multiplier 3
[PE2-bfd-lsp-session-test] commit
```

After the configuration, run the **display bfd session** { **all** | **discriminator** *discr-value* | **mpls-te** | [**slot** *slot-id*] [**verbose**] command on PE1 and PE2, and you can view that the status of the BFD sessions is Up.

Step 9 Verify the configuration.

Connect two interfaces, namely, Port 1 and Port 2 on a tester, to CE1 and CE2 respectively. Send traffic from Port 1 to Port 2, and you can find that a fault can be recovered at the millisecond level when the cable of any interface between PE1 and PE2 is removed.

----End

Configuration Files

NOTE

The configuration files of CE1 and CE2 are not mentioned here. The configurations related to the CE accessing the PE are also not mentioned.

- Configuration file of PE1

```
#
 sysname PE1
#
 vlan batch 10 20
#
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 Vlanif10
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls te
```


Copyright © Huawei Technologies Co., Ltd.

```
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface Vlanif20
 ip address 10.2.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 2.2.2.2
 mpls te tunnel-id 100
 mpls te bandwidth bc0 10000
 mpls te path explicit-path tope3
 mpls te reserved-for-binding
 mpls te commit
#
interface Tunnel2/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te tunnel-id 200
 mpls te path explicit-path tope2
 mpls te reserved-for-binding
 mpls te 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
```


Copyright © Huawei Technologies Co., Ltd.

```
 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 Tunnel2/0/0
 tunnel binding destination 2.2.2.2 te Tunnel1/0/0
#
bfd test bind mpls-te interface Tunnel2/0/0
 discriminator local 12
 discriminator remote 21
 min-tx-interval 100
 min-rx-interval 100
 process-pst
 commit
#
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
 vlan batch 20
#
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 Vlanif20
 ip address 10.2.1.2 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
interface Tunnel2/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 1.1.1.1
 mpls te tunnel-id 200
 mpls te bandwidth bc0 10000
 mpls te path explicit-path tope1
 mpls te reserved-for-binding
 mpls te commit
#
bgp 100
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 connect-interface LoopBack1
 #
```


Copyright © Huawei Technologies Co., Ltd.

```
 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 Tunnel2/0/0
#
bfd test bind mpls-te interface Tunnel2/0/0
 discriminator local 21
 discriminator remote 12
 min-tx-interval 100
 min-rx-interval 100
 commit
#
return
```

- Configuration file of PE3

```
#
 sysname PE3
#
 vlan batch 10
#
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 Vlanif10
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 1.1.1.1
```


Copyright © Huawei Technologies Co., Ltd.

```
 mpls te tunnel-id 100
 mpls te path explicit-path tope1
 mpls te reserved-for-binding
 mpls te 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 Tunnel1/0/0
#
return
```

3.21.18 Example for Configuring Dynamic BFD for CR-LSPs

Networking Requirements

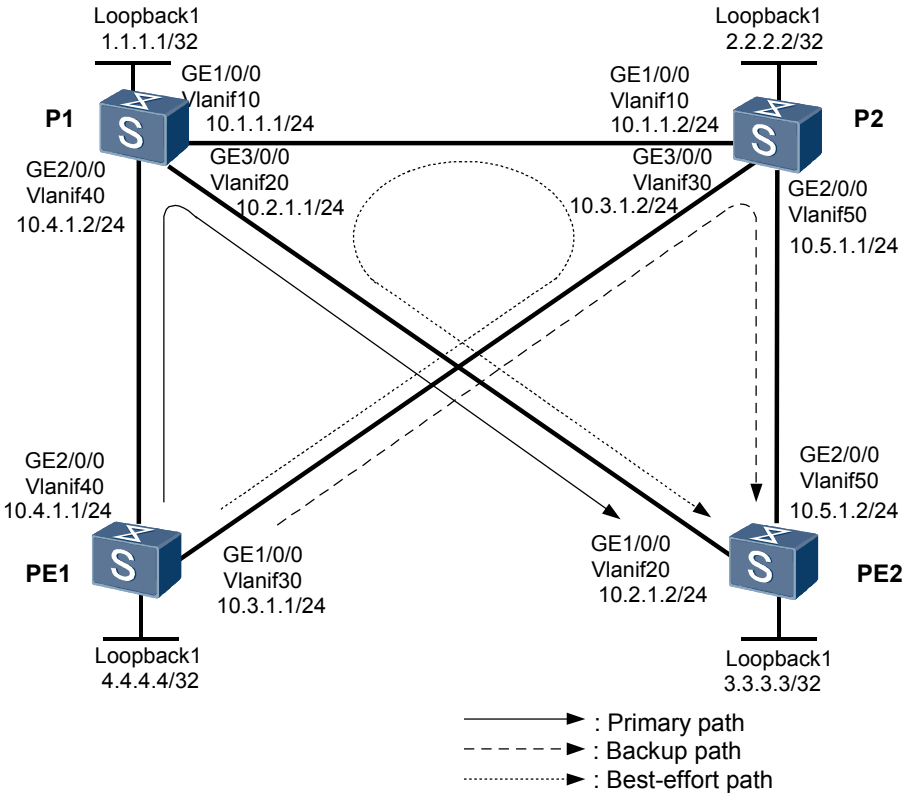
Figure 3-19 shows a network where CR-LSP hot standby is configured. A TE tunnel is established between PE1 and PE2. The tunnel is enabled with hot standby and configured with the best-effort path. If the primary CR-LSP fails, traffic is switched to the backup CR-LSP. After the faulty primary CR-LSP is recovered, the traffic is switched back to the primary CR-LSP after 15 seconds. If both the primary and backup CR-LSPs fail, traffic is switched to the best-effort path.

You are required to configure dynamic BFD for CR-LSPs to detect faults on the primary and backup CR-LSPs. After the configuration, the following should be achieved:

- If the primary CR-LSP fails, traffic is rapidly switched to the backup CR-LSP.
- After the primary CR-LSP is recovered in less than 15 seconds, traffic is switched back to the primary CR-LSP if the backup CR-LSP fails.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-19 Networking diagram for configuring CR-LSP hot standby



NOTE

Compared with static BFD, dynamic BFD is configured easier. In addition, by using dynamic BFD, the number of BFD sessions to be created is reduced. That is, the number of BFD packets transmitted on a network is reduced and less network resources is occupied. This is because only one BFD session is created on a tunnel interface when you use dynamic BFD.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure CR-LSP hot standby according to **3.21.13 Example for Configuring CR-LSP Hot Standby**.
2. Enable BFD on the ingress node of the tunnel; configure MPLS TE BFD; set the minimum intervals for sending and receiving BFD packets and the local detection multiplier of BFD.
3. Enable the capability of passively creating BFD sessions on the egress node.

Data Preparation

To complete the configuration, you need the following data:

- Minimum intervals for sending and receiving BFD packets on the ingress node (The default values are specified in the license.)
- Local detection multiplier of BFD on the ingress node (The default value is specified in the license.)

Copyright © Huawei Technologies Co., Ltd.

- For other data, see **3.21.13 Example for Configuring CR-LSP Hot Standby**.

Procedure

Step 1 Configure CR-LSP hot standby.

Configure the primary CR-LSP, backup CR-LSP, and best-effort path according to **3.21.13 Example for Configuring CR-LSP Hot Standby**.

Step 2 Enable BFD on the ingress node of the tunnel and configure MPLS TE BFD.

Enable MPLS TE BFD on the tunnel interface on PE1. Set the minimum intervals for sending and receiving BFD packets to 100 milliseconds and the local detection multiplier of BFD to 3.

```
<PE1> system-view
[PE1] bfd
[PE1-bfd] quit
[PE1] interface tunnel 1/0/0
[PE1-Tunnel1/0/0] mpls te bfd enable
[PE1-Tunenl1/0/0] mpls te bfd min-tx-interval 100 min-rx-interval 100 detect-
multiplier 3
[PE1-Tunenl1/0/0] mpls te commit
```

Step 3 Enable the capability of passively creating BFD sessions on the egress node of the tunnel.

```
<PE2> system-view
[PE2] bfd
[PE2-bfd] mpls-passive
[PE2-bfd] quit
```

After the configuration, run the **display bfd session discriminator** *local-discriminator-value* command on PE1 and PE2, and you can find that the status of the BFD sessions is Up.

```
[PE1] display bfd se mpls-te interface Tunnel 1/0/0 te-lsp
--------------------------------------------------------------------------------
Local  Remote PeerIpAddr      InterfaceName                 State     Type
--------------------------------------------------------------------------------
8208   8217   3.3.3.3         Tunnel1/0/0                   Up        D_TE_LSP
--------------------------------------------------------------------------------
     Total UP/DOWN Session Number : 1/0
```

Step 4 Verify the configuration.

Connect two interfaces, namely, Port 1 and Port 2 on a tester, to PE1 and PE2 respectively. On Port 1, send MPLS traffic to Port 2. After the cable of GE 2/0/0 on PE1 or P1 is removed, the fault recovers at the millisecond level.

After installing the cable into GE 2/0/0 and then removing the cable from GE 1/0/0 on PE1 in 15 seconds, you can find that the fault recovers at the millisecond level.

----End

Configuration Files

- Configuration file of PE1

```
#
 sysname PE1
#
 vlan batch 30 40
#
bfd
#
 mpls lsr-id 4.4.4.4
 mpls
  mpls te
```


Copyright © Huawei Technologies Co., Ltd.

```
  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 Vlanif30
 ip address 10.3.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface Vlanif40
 ip address 10.4.1.1 255.255.255.252
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 30
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 40
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 isis enable 1
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te tunnel-id 100
 mpls te bfd enable
 mpls te record-route
 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 bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier 3
 mpls te commit
#
return
```

- Configuration file of P1

```
#
 sysname P1
#
 vlan batch 10 20 40
#
 mpls lsr-id 1.1.1.1
 mpls
```


Copyright © Huawei Technologies Co., Ltd.

```
  mpls te
  mpls rsvp-te
#
isis 1
 cost-style wide
 network-entity 10.0000.0000.0001.00
 traffic-eng level-1-2
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif20
 ip address 10.2.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface Vlanif40
 ip address 10.4.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 40
#
interface GigabitEthernet3/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of P2

```
#
 sysname P2
#
 vlan batch 10 30 50
#
 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 Vlanif10
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
```


Copyright © Huawei Technologies Co., Ltd.

```
 mpls rsvp-te
#
interface Vlanif30
 ip address 10.3.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif50
 ip address 10.5.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 50
#
interface GigabitEthernet3/0/0
 port link-type access
 port default vlan 30
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
 bfd
 mpls-passive
#
 vlan batch 20 50
#
 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 Vlanif10
 ip address 10.2.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif50
 ip address 10.5.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
```


Copyright © Huawei Technologies Co., Ltd.

```
 port default vlan 20
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 50
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 isis enable 1
#
return
```

3.21.19 Example for Configuring Dynamic BFD for RSVP

Networking Requirements

Figure 3-20 shows an MPLS network where P and PE devices are switches. An MPLS TE tunnel is established between PE1 and PE2. TE FRR with P1 as the PLR and PE1 as the MP is configured. The primary CR-LSP is PE1->P1->Switch->P2->PE2; the backup CR-LSP is P1->P3->PE2. In addition, each node is configured with RSVP GR.

P1 cannot determine whether a fault occurs on the link or its neighbor is performing RSVP GR; therefore, P1 cannot determine whether to perform TE FRR switchover in either of the following situations:

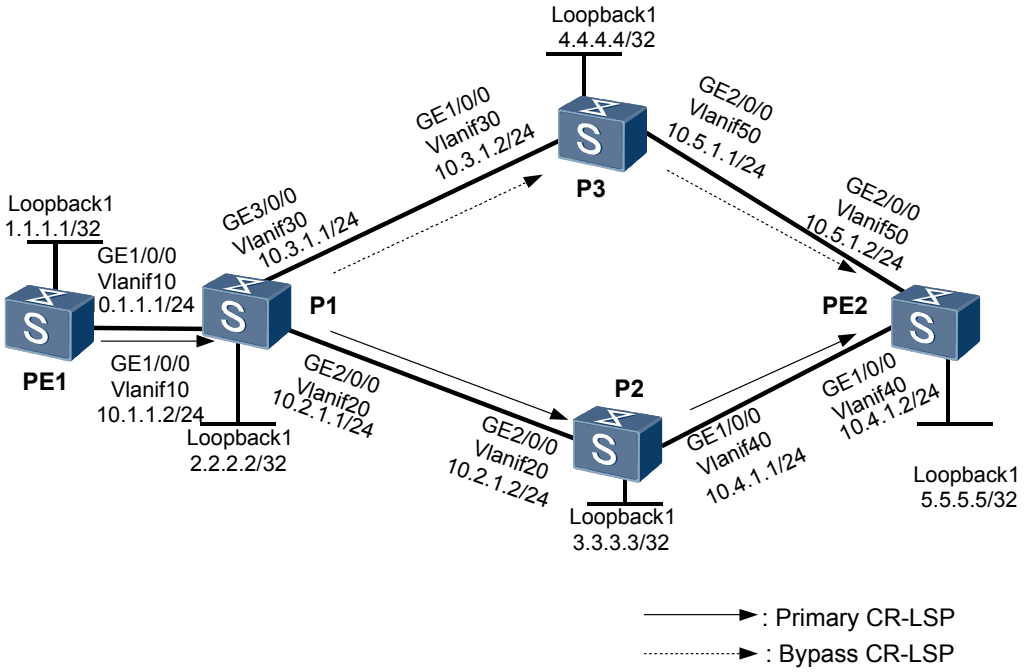
- P2 is performing RSVP GR.
- The link between P1 and P2 fails.

By default, the interval for sending Hello packets of RSVP is 3 seconds; the interval for declaring that a neighbor is Down is three times as long as the interval for sending Hello packets. That is, a node can detect a fault on an RSVP neighbor at the second level. BFD, however, can detect a fault at the millisecond level.

If BFD for RSVP is used on the network, P1 can rapidly detect the fault and perform TE FRR after the link between P1 and P2 fails.

Copyright © Huawei Technologies Co., Ltd.

Figure 3-20 Networking diagram for configuring dynamic BFD for RSVP



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an IP address for each interface and enable an IGP on each node to implement interworking. Enable IGP GR. To support RSVP GR, IGP GR needs to be configured.
2. Configure basic MPLS and MPLS TE functions.
3. Configure explicit paths for the primary CR-LSP and the backup CR-LSP.
4. Create a TE primary tunnel interface and enable TE FRR on PE1, and configure the bypass tunnel on P1.
5. Configure RSVP GR on all LSRs and establish Hello sessions between P1 and PE2.

   NOTE

   On a network where TE FRR is configured, you need to create a Hello session between a PLR and an MP of the bypass tunnel if you want to configure RSVP GR. Otherwise, after traffic is switched to the bypass tunnel because the primary tunnel fails, the primary tunnel turns Down if the PLR or MP performs RSVP GR.
6. Configure BFD for RSVP on P1 and P2.

Data Preparation

To complete the configuration, you need the following data:

- Type of an IGP and data required for configuring an IGP
- MPLS LSR ID
- Bandwidth attributes of the outgoing interfaces of the links along the tunnel

Copyright © Huawei Technologies Co., Ltd.

- Primary tunnel interface number, bandwidth occupied by the primary tunnel, and explicit path
- Bypass tunnel interface number, bandwidth occupied by the bypass tunnel, and explicit path
- Interfaces to be protected by the bypass tunnel
- Minimum intervals for sending and receiving BFD packets (The default values are specified in the license.)
- Local detection multiplier of BFD (The default value is specified in the license.)

Procedure

Step 1 Create VLANs and VLANIF interfaces, and assign IP addresses to the VLANIF interfaces.

Configure an IP address for each interface according to the networking diagram, create loopback interfaces on nodes, and then configure the IP addresses of the loopback interfaces as MPLS LSR IDs. For detailed configuration, see the configuration files in this example.

Step 2 Configure an IGP and IGP GR.

Configure OSPF or IS-IS on each node to implement interworking between nodes and configure IGP GR to support RSVP GR. In this example, OSPF is used. For detailed configuration, see the configuration files in this example.

Step 3 Configure basic MPLS functions.

On each node, configure an LSR ID and enable MPLS in the system view and enable MPLS on each physical interface. For detailed configuration, see the configuration files in this example.

Step 4 Configure basic MPLS TE functions.

On each node, enable MPLS TE and MPLS RSVP-TE in the MPLS view and in the view of the physical interface. Set the maximum bandwidth and the maximum reservable bandwidth of the link on each outgoing interface along the tunnel to 100 Mbit/s. For detailed configuration, see the configuration files in this example.

Step 5 Configure OSPF TE and CSPF.

Configure OSPF TE on each node and CSPF on PE1 and P1. For the configuration procedure, see **3.21.2 Example for Configuring an RSVP-TE Tunnel**.

Step 6 Configure the primary tunnel.

Configure an explicit path for the primary tunnel on PE1.

```
<PE1> system-view
[PE1] explicit-path tope2
[PE1-explicit-path-tope2] next hop 10.1.1.2
[PE1-explicit-path-tope2] next hop 10.2.1.2
[PE1-explicit-path-tope2] next hop 10.4.1.2
[PE1-explicit-path-tope2] next hop 5.5.5.5
[PE1-explicit-path-tope2] quit
```

Create a tunnel interface on PE1, specify an explicit path, set the tunnel bandwidth to 10 Mbit/s, and enable TE FRR.

```
[PE1] interface tunnel 1/0/0
[PE1-Tunnel1/0/0] ip address unnumbered interface loopback 1
[PE1-Tunnel1/0/0] tunnel-protocol mpls te
[PE1-Tunnel1/0/0] destination 5.5.5.5
[PE1-Tunnel1/0/0] mpls te tunnel-id 100
```


Copyright © Huawei Technologies Co., Ltd.

```
[PE1-Tunnel1/0/0] mpls te path explicit-path tope2
[PE1-Tunnel1/0/0] mpls te fast-reroute
[PE1-Tunnel1/0/0] mpls te commit
[PE1-Tunnel1/0/0] quit
```

After the configuration, run the **display mpls-te tunnel-interface tunnel** *interface-number* command on PE1, and you can find that the status of Tunnel 1/0/0 on PE1 is displayed as **CR-LSP is Up**.

Step 7 Configure the bypass tunnel.

Configure the explicit path for the bypass tunnel on P1.

```
<P1> system-view
[P1] explicit-path tope2
[P1-explicit-path-tope2] next hop 10.3.1.2
[P1-explicit-path-tope2] next hop 10.5.1.2
[P1-explicit-path-tope2] next hop 5.5.5.5
[P1-explicit-path-tope2] quit
```

Configure the tunnel interface of the bypass tunnel on P1. Specify an explicit path for the bypass tunne1, set the tunnel bandwidth to 20 Mbit/s and the protected bandwidth to 10 Mbit/s, and specify the physical interface to be protected by the bypass tunnel.

```
[P1] interface tunnel 3/0/0
[P1-Tunnel3/0/0] ip address unnumbered interface loopback 1
[P1-Tunnel3/0/0] tunnel-protocol mpls te
[P1-Tunnel3/0/0] destination 5.5.5.5
[P1-Tunnel3/0/0] mpls te tunnel-id 300
[P1-Tunnel3/0/0] mpls te path explicit-path tope2
[P1-Tunnel3/0/0] mpls te bandwidth bc0 20000
[P1-Tunnel3/0/0] mpls te bypass-tunnel bandwidth bc0 10000
[P1-Tunnel3/0/0] mpls te protected-interface vlanif 20
[P1-Tunnel3/0/0] mpls te commit
[P1-Tunnel3/0/0] quit
```

Step 8 Configure RSVP GR on all LSRs and establish Hello sessions between P1 and PE2.

Configure PE1.

```
[PE1] mpls
[PE1-mpls] mpls rsvp-te hello
[PE1-mpls] mpls rsvp-te hello full-gr
[PE1-mpls] quit
[PE1] interface vlanif 10
[PE1-Vlanif10] mpls rsvp-te hello
```

Configure P1.

```
[P1] mpls
[P1-mpls] mpls rsvp-te hello
[P1-mpls] mpls rsvp-te hello full-gr
[P1-mpls] mpls rsvp-te hello nodeid-session 5.5.5.5
[P1-mpls] quit
[P1] interface vlanif 10
[P1-Vlanif10] mpls rsvp-te hello
[P1-Vlanif10] quit
[P1] interface vlanif 20
[P1-Vlanif20] mpls rsvp-te hello
[P1-Vlanif20] quit
[P1] interface vlanif 30
[P1-Vlanif30] mpls rsvp-te hello
[P1-Vlanif30] quit
```

Configure P2.

```
[P2] mpls
[P2-mpls] mpls rsvp-te hello
```


Copyright © Huawei Technologies Co., Ltd.

```
[P2-mpls] mpls rsvp-te hello full-gr
[P2-mpls] quit
[P2] vlanif 40
[P2-Vlanif40] mpls rsvp-te hello
[P2-Vlanif40] quit
[P2] interface vlanif 20
[P2-Vlanif20] mpls rsvp-te hello
[P2-Vlanif20] quit
```

Configure P3.

```
[P3] mpls
[P3-mpls] mpls rsvp-te hello
[P3-mpls] mpls rsvp-te hello full-gr
[P3-mpls] quit
[P3] interface vlanif 30
[P3-Vlanif30] mpls rsvp-te hello
[P3-Vlanif30] quit
[P3] interface vlanif 50
[P3-Vlanif50] mpls rsvp-te hello
[P3-Vlanif50] quit
```

Configure PE2.

```
[PE2] mpls
[PE2-mpls] mpls rsvp-te hello
[PE2-mpls] mpls rsvp-te hello full-gr
[PE2-mpls] mpls rsvp-te hello nodeid-session 2.2.2.2
[PE2-mpls] quit
[PE2] interface vlanif 40
[PE2-Vlanif40] mpls rsvp-te hello
[PE2-Vlanif40] quit
[PE2] interface vlanif 50
[PE2-Vlanif50] mpls rsvp-te hello
[PE2-Vlanif50] quit
```

Step 9 Configure BFD for RSVP.

Enable BFD for RSVP on VLANIF 20 on P1 and P2, and set the minimum interval for sending and receiving BFD packets and the local detection multiplier of BFD.

Configure P1.

```
[P1] bfd
[P1-bfd] quit
[P1] interface  vlanif 20
[P1-Vlanif20] mpls rsvp-te bfd enable
[P1-Vlanif20] mpls rsvp-te bfd min-tx-interval 100 min-rx-interval 100 detect-
multiplier 3
[P1-Vlanif20] quit
```

Configure P2.

```
[P2] bfd
[P2-bfd] quit
[P2] interface vlanif 20
[P2-Vlanif20] mpls rsvp-te bfd enable
[P2-Vlanif20] mpls rsvp-te bfd min-tx-interval 100 min-rx-interval 100 detect-
multiplier 3
[P2-Vlanif2] quit
```

After the configuration, run the **display mpls rsvp-te bfd session** { **all** | **interface** *interface-name* | **peer** *ip-addr* } command on PE1 and PE2, and you can view that the status of the BFD sessions is Up.

Step 10 Verify the configuration.

Copyright © Huawei Technologies Co., Ltd.

Connect two interfaces, namely, Port 1 and Port 2 on a tester, to PE1 and PE2 respectively. On Port 1, send MPLS traffic to Port 2. After the cable of any interface on P1 and P2 is removed, you can find that the fault recovers at the millisecond level.

----End

Configuration Files

- Configuration file of PE1

```
#
 sysname PE1
#
 vlan batch 10
#
 mpls lsr-id 1.1.1.1
 mpls
  mpls te
  mpls rsvp-te
  mpls rsvp-te hello
  mpls rsvp-te hello full-gr
  mpls te cspf
#
 explicit-path tope2
  next hop 10.1.1.2
  next hop 10.2.1.2
  next hop 10.4.1.2
  next hop 5.5.5.5
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
 mpls rsvp-te hello
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 5.5.5.5
 mpls te tunnel-id 100
 mpls te bandwidth bc0 10000
 mpls te path explicit-path tope2
 mpls te fast-reroute
 mpls te commit
#
ospf 1
 opaque-capability enable
 graceful-restart
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 1.1.1.1 0.0.0.0
  mpls-te enable
#
return
```

- Configuration file of P1

```
#
 sysname P1
#
```


Copyright © Huawei Technologies Co., Ltd.

```
 vlan batch 10 20 30
#
 bfd
#
 mpls lsr-id 2.2.2.2
 mpls
  mpls te
  mpls rsvp-te
  mpls rsvp-te hello
  mpls rsvp-te hello full-gr
  mpls rsvp-te hello nodeid-session 5.5.5.5
  mpls te cspf
#
 explicit-path tope2
  next hop 10.3.1.2
  next hop 10.5.1.2
  next hop 5.5.5.5
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
 mpls rsvp-te hello
#
interface Vlanif20
 ip address 10.2.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
 mpls rsvp-te hello
 mpls rsvp-te bfd enable
 mpls rsvp-te bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier 3
#
interface Vlanif30
 ip address 10.3.1.1 255.255.255.0
 mpls
 mpls te
  mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
 mpls rsvp-te hello
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface GigabitEthernet3/0/0
 port link-type access
 port default vlan 30
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
interface Tunnel3/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 5.5.5.5
 mpls te tunnel-id 300
 mpls te bandwidth bc0 20000
 mpls te path explicit-path tope2
 mpls te bypass-tunnel bandwidth bc0 10000
 mpls te protected-interface Vlanif20
 mpls te commit
#
```


Copyright © Huawei Technologies Co., Ltd.

```
ospf 1
 opaque-capability enable
 graceful-restart
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.2.1.0 0.0.0.255
  network 10.3.1.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
  mpls-te enable
#
return
```

- Configuration file of P2

```
#
 sysname P2
#
 vlan batch 20 40
#
 bfd
#
 mpls lsr-id 3.3.3.3
 mpls
  mpls te
  mpls rsvp-te
  mpls rsvp-te hello
  mpls rsvp-te hello full-gr
#
interface Vlanif20
 ip address 10.2.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
 mpls rsvp-te hello
 mpls rsvp-te bfd enable
 mpls rsvp-te bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier 3
#
interface Vlanif40
 ip address 10.4.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
 mpls rsvp-te hello
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 40
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
ospf 1
 opaque-capability enable
 graceful-restart
 area 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.4.1.0 0.0.0.255
  network 3.3.3.3 0.0.0.0
  mpls-te enable
#
return
```

- Configuration file of P3

```
#
 sysname P3
#
```


Copyright © Huawei Technologies Co., Ltd.

```
 vlan batch 30 50
#
 mpls lsr-id 4.4.4.4
 mpls
  mpls te
  mpls rsvp-te
  mpls rsvp-te hello
  mpls rsvp-te hello full-gr
#
interface Vlanif30
 ip address 10.3.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
 mpls rsvp-te hello
#
interface  Vlanif50
 ip address 10.5.1.1 255.255.255.0
 mpls
 mpls te
 mpls te bandwidth max-reservable-bandwidth 100000
 mpls rsvp-te
 mpls rsvp-te hello
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 30
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 50
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
#
ospf 1
 opaque-capability enable
 graceful-restart
 area 0.0.0.0
  network 10.3.1.0 0.0.0.255
  network 10.5.1.0 0.0.0.255
  network 4.4.4.4 0.0.0.0
  mpls-te enable
#
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
 mpls lsr-id 5.5.5.5
 mpls
  mpls te
  mpls rsvp-te
  mpls rsvp-te hello
  mpls rsvp-te hello full-gr
  mpls rsvp-te hello nodeid-session 2.2.2.2
#
interface Vlanif40
 ip address 10.4.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
 mpls rsvp-te hello
#
interface Vlanif50
 ip address 10.5.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
```


Copyright © Huawei Technologies Co., Ltd.

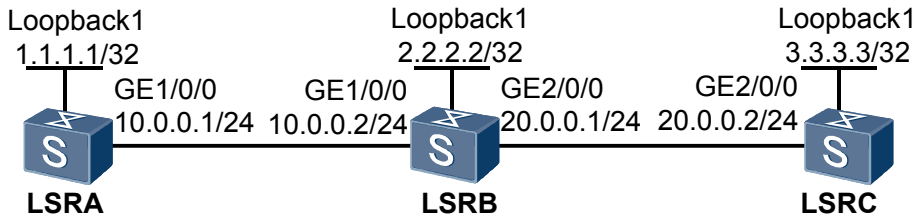
```
 mpls rsvp-te hello
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 40
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 50
#
interface LoopBack1
 ip address 5.5.5.5 255.255.255.255
#
ospf 1
 opaque-capability enable
 graceful-restart
 area 0.0.0.0
  network 10.4.1.0 0.0.0.255
  network 10.5.1.0 0.0.0.255
  network 5.5.5.5 0.0.0.0
  mpls-te enable
#
return
```

3.21.20 Example for Advertising MPLS LSR IDs to Multiple OSPF Areas

Networking Requirements

As shown in **Figure 3-21**, OSPF runs on LSRA, LSRB, and LSRC. LSRA and LSRB reside in Area 0; LSRB and LSRC reside in Area 1; LSRB is an ABR. It is required that a tunnel be set up on LSRA and LSRC separately destined for LSRB and IGP shortcut be enabled on LSRA and LSRC so that the routes on LSRA and LSRC to LSRB use the tunnel interfaces as the outbound interfaces.

Figure 3-21 Networking for configuring inter-area tunnels



Switch	Interface	VLANIF interface	IP address
LSRA	GigabitEthernet1/0/0	VLANIF 10	10.0.0.1/24
LSRB	GigabitEthernet1/0/0	VLANIF 10	10.0.0.2/24
LSRB	GigabitEthernet2/0/0	VLANIF 20	20.0.0.1/24
LSRC	GigabitEthernet2/0/0	VLANIF 20	20.0.0.2/24

Configuration Roadmap

The configuration roadmap is as follows:

Copyright © Huawei Technologies Co., Ltd.

1. Configure an IP address for each interface on the LSRs and the loopback interface address used as the LSR ID, and configure OSPF to advertise the network segments connected to the interfaces on the LSRs and host routes of LSR IDs.
2. Configure the LSR ID of each LSR and enable MPLS, MPLS TE and MPLS RSVP-TE on each LSR and interface.
3. Set up a tunnel on LSRA and LSRC respectively destined for LSRB and enable IGP shortcut on LSRA and LSRC.
4. Run the **advertise mpls-lsr-id** command on LSRB so that the host route 2.2.2.2, as an inter-area route, is advertised to both Area 0 and Area 1.

Data Preparation

To complete the configuration, you need the following data:

- OSPF process ID and area ID of each LSR
- Interface number, IP address, destination address, and tunnel ID of each tunnel interface on LSRA and LSRC

Procedure

Step 1 Configure VLANs that interfaces belong to.

```
<Quidway> system-view
[Quidway] sysname LSRA
[LSRA] vlan batch 10
[LSRA] interface gigabitEthernet 1/0/0
[LSRA-GigabitEthernet1/0/0] port hybrid pvid vlan 10
[LSRA-GigabitEthernet1/0/0] port hybrid untagged vlan 10
[LSRA-GigabitEthernet1/0/0] quit
```

The configurations of LSRB and LSRC are similar to the configuration of LSRA, and are not mentioned here.

Step 2 Configure an IP address for each VLANIF interface on the LSRs and configure OSPF.

Configure an IP address and a mask for each interface and configure OSPF so that all LSRs can interconnect with each other.

The configuration details are not mentioned here.

Step 3 Configure basic MPLS functions and enable MPLS TE, MPLS RSVP-TE.

Configure LSRA.

```
[LSRA] mpls lsr-id 1.1.1.1
[LSRA] mpls
[LSRA-mpls] mpls te
[LSRA-mpls] mpls rsvp-te
[LSRA-mpls] quit
[LSRA] interface vlanif 10
[LSRA-Vlanif10] ospf network-type p2p
[LSRA-Vlanif10] mpls
[LSRA-Vlanif10] mpls te
[LSRA-Vlanif10] quit
```

The configurations of LSRB and LSRC are similar to the configuration of LSRA, and are not mentioned here.

Step 4 Configure MPLS TE tunnels and IGP shortcut.

Copyright © Huawei Technologies Co., Ltd.

Set up an MPLS TE tunnel from LSRA to LSRB and configure IGP shortcut. The OSPF cost of the tunnel is smaller than that of the physical link.

```
[LSRA] interface tunnel 1/0/0
[LSRA-Tunnel1/0/0] ip address unnumbered interface loopback 1
[LSRA-Tunnel1/0/0] tunnel-protocol mpls te
[LSRA-Tunnel1/0/0] destination 2.2.2.2
[LSRA-Tunnel1/0/0] mpls te tunnel-id 100
[LSRA-Tunnel1/0/0] mpls te igp shortcut ospf
[LSRA-Tunnel1/0/0] mpls te igp metric absolute 1
[LSRA-Tunnel1/0/0] mpls te commit
[LSRA-Tunnel1/0/0] quit
```

Set up an MPLS TE tunnel from LSRC to LSRB and configure IGP shortcut. The OSPF cost of the tunnel is smaller than that of the physical link.

```
[LSRC] interface tunnel 2/0/0
[LSRC-Tunnel2/0/0] ip address unnumbered interface loopback 1
[LSRC-Tunnel2/0/0] tunnel-protocol mpls te
[LSRC-Tunnel2/0/0] destination 2.2.2.2
[LSRC-Tunnel2/0/0] mpls te tunnel-id 200
[LSRC-Tunnel2/0/0] mpls te igp shortcut ospf
[LSRC-Tunnel2/0/0] mpls te igp metric absolute 1
[LSRC-Tunnel2/0/0] mpls te commit
[LSRC-Tunnel2/0/0] quit
```

After the configurations are complete, run the **display interface tunnel** command on LSRA. You can view that the tunnel interface is Up.

Run the **display mpls te tunnel** command on LSRA and LSRC. You can view information about each MPLS TE tunnel.

```
<LSRA> display mpls te tunnel
LSP-Id                      Destination          In/Out-If
1.1.1.1:100:1               2.2.2.2              -/Vlanif10

<LSRC> display mpls te tunnel
LSP-Id                      Destination          In/Out-If
3.3.3.3:200:1               2.2.2.2              -/Vlanif20
```

Step 5 Configure the ABR, that is, LSRB to advertise the MPLS LSR IDs to multiple OSPF areas.

```
[LSRB] ospf 1
[LSRB-ospf-1] advertise mpls-lsr-id
```

Step 6 Verify the configuration.

Run the **display ospf peer brief** command on LSRB. You can view that a neighbor in Area 0 and Area 1 respectively exists, and the neighbors are in the Full state.

```
[LSRB] display ospf peer brief

          OSPF Process 1 with Router ID 2.2.2.2
                    Peer Statistic Informations
--------------------------------------------------------------------------
Area Id          Interface                  Neighbor id         State
0.0.0.0          Vlanif10                  1.1.1.1             Full
0.0.0.1          Vlanif10                  3.3.3.3             Full
--------------------------------------------------------------------------
```

Run the **display ip routing-table 2.2.2.2** command on LSRA. You can view in the routing table that the outbound interface of the route to 2.2.2.2 is the tunnel interface.

```
<LSRA> display ip routing-table 2.2.2.2
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
```


Copyright © Huawei Technologies Co., Ltd.

```
Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface

        2.2.2.2/32  OSPF   10   1         D     1.1.1.1         Tunnel1/0/0

<LSRC> display ip routing-table 2.2.2.2
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : Public
Summary Count : 1
Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface

        2.2.2.2/32  OSPF   10   1         D     3.3.3.3         Tunnel2/0/0
```

----End

Configuration Files

- Configuration file of LSRA

```
#
 sysname LSRA
#
vlan batch 10
#
 mpls lsr-id 1.1.1.1
 mpls
  mpls te
  mpls rsvp-te
#
interface Vlanif10
 ip address 10.0.0.1 255.255.255.0
 ospf cost 10
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 2.2.2.2
 mpls te tunnel-id 100
 mpls te igp shortcut ospf
 mpls te igp metric absolute 1
 mpls te commit
#
ospf 1 router-id 1.1.1.1
 opaque-capability enable
 enable traffic-adjustment
 area 0.0.0.0
  network 10.0.0.0 0.0.0.255
  network 1.1.1.1 0.0.0.0
  mpls-te enable
#
return
```

- Configuration file of LSRB

```
#
 sysname LSRB
#
vlan batch 10 20
#
 mpls lsr-id 2.2.2.2
```


Copyright © Huawei Technologies Co., Ltd.

```
 mpls
  mpls te
  mpls rsvp-te
#
interface Vlanif10
  ip address 10.0.0.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif20
  ip address 20.0.0.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
ospf 1 router-id 2.2.2.2
 opaque-capability enable
 enable traffic-adjustment
 advertise mpls-lsr-id
 area 0.0.0.0
  network 10.0.0.0 0.0.0.255
  mpls-te enable
 area 0.0.0.1
  network 20.0.0.0 0.0.0.255
  mpls-te enable
#
return
```

- Configuration file of LSRC

```
#
 sysname LSRC
#
vlan batch 20
#
 mpls lsr-id 3.3.3.3
 mpls
  mpls te
  mpls rsvp-te
#
interface Vlanif20
 ip address 20.0.0.2 255.255.255.0
 ospf cost 10
 mpls
 mpls te
 mpls rsvp-te
#
interface NULL0
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface Tunnel2/0/0
 ip address unnumbered interface LoopBack0
 tunnel-protocol mpls te
```


Copyright © Huawei Technologies Co., Ltd.

```
 destination 2.2.2.2
 mpls te tunnel-id 200
 mpls te igp shortcut ospf
 mpls te igp metric absolute 1
 mpls te commit
#
ospf 1 router-id 3.3.3.3
 opaque-capability enable
 enable traffic-adjustment
 area 0.0.0.1
  network 20.0.0.0 0.0.0.255
  network 3.3.3.3 0.0.0.0
  mpls-te enable
#
return
```

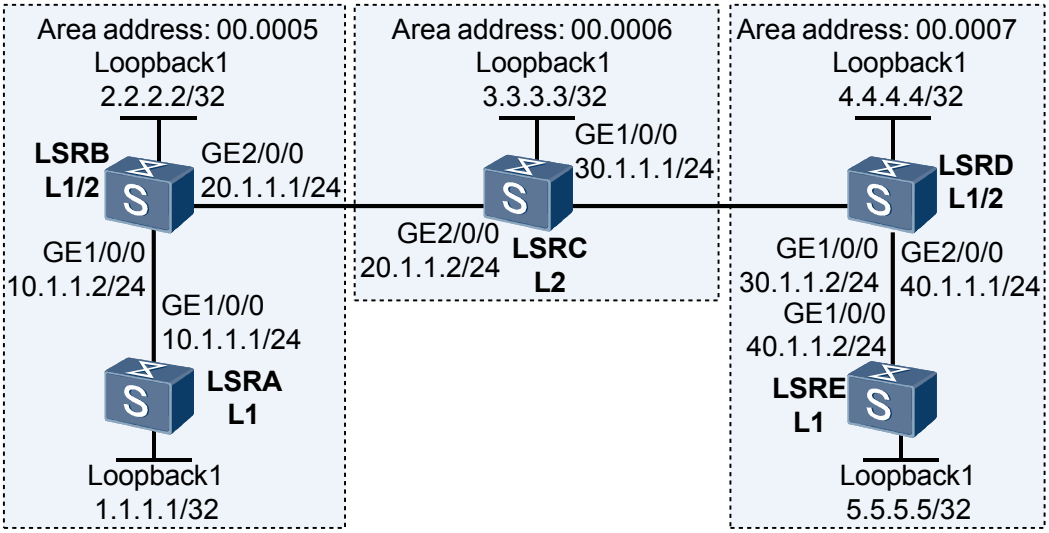
3.21.21 Example for Configuring Inter-Area Tunnel

Networking Requirements

As shown in **Figure 3-22**,

- IS-IS is run on LSR A, LSR B, LSR C, LSR D, and LSR E.
  - LSR A and LSR E are Level-1 devices.
  - LSR B and LSR D are Level-1-2 devices.
  - LSR C is Level-2 devices.

Figure 3-22 Networking diagram of configuring Inter-Area Tunnel



Device	Interface	VLANIF interface	IP address
LSRA	GigabitEthernet1/0/0	VLANIF 10	10.1.1.1/24
LSRB	GigabitEthernet1/0/0	VLANIF 10	10.1.1.2/24
LSRB	GigabitEthernet2/0/0	VLANIF 20	20.1.1.1/24
LSRC	GigabitEthernet1/0/0	VLANIF 30	30.1.1.1/24
LSRC	GigabitEthernet2/0/0	VLANIF 20	20.1.1.2/24

Copyright © Huawei Technologies Co., Ltd.

LSRD	GigabitEthernet1/0/0	VLANIF 30	30.1.1.2/24
LSRD	GigabitEthernet2/0/0	VLANIF 40	40.1.1.1/24
LSRE	GigabitEthernet1/0/0	VLANIF 40	40.1.1.2/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure IP addresses for interfaces on each LSR, configure loopback address as the LSR ID.
2. Enable globally the IS-IS protocol, configure the network entity title and change the Cost type to enable IS-IS TE.
3. Configure the loose explicit path including ABR (LSR B, LSR C, and LSR D).
4. Enable MPLS RSVP-TE.
5. Establish the tunnel interface on the ingress, specify the IP address of the tunnel, the tunnel protocol, the destination address, the tunnel ID and the RSVP-TE protocol.

Data Preparation

To complete the configuration, you need the following data.

- IS-IS area ID of each LSR, originating system ID, and IS-IS level
- Name of the tunnel interface, IP address, destination address, tunnel ID, tunnel signalling protocol (RSVP-TE), and tunnel bandwidth

Procedure

Step 1 Configure VLANs that interfaces belong to.

```
<Quidway> system-view
[Quidway] sysname LSRA
[LSRA] vlan batch 10 20
[LSRA] interface gigabitEthernet 1/0/0
[LSRA-GigabitEthernet1/0/0] port hybrid pvid vlan 10
[LSRA-GigabitEthernet1/0/0] port hybrid untagged vlan 10
[LSRA-GigabitEthernet1/0/0] quit
```

The configurations of LSRB, LSRC, LSRD and LSRE are similar to the configuration of LSRA, and are not mentioned here.

Step 2 Configure an IP address for each interface.

The IP address and mask on each interface including the loopback interface are configured as shown in **Figure 3-22**.

The detailed configuration is not mentioned here.

Step 3 Configure the IS-IS protocol to advertise routes.

Configure LSR A.

```
[LSRA] isis 1
[LSRA-isis-1] network-entity 00.0005.0000.0000.0001.00
[LSRA-isis-1] is-level level-1
```


Copyright © Huawei Technologies Co., Ltd.

```
[LSRA-isis-1] quit
[LSRA] interface vlanif 10
[LSRA-Vlanif10] isis enable 1
[LSRA-Vlanif10] quit
[LSRA] interface loopback 1
[LSRA-LoopBack1] isis enable 1
[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 vlanif 10
[LSRB-Vlanif10] isis enable 1
[LSRB-Vlanif10] quit
[LSRB] interface vlanif 20
[LSRB-Vlanif20] isis enable 1
[LSRB-Vlanif20] quit
[LSRB] interface loopback 1
[LSRB-LoopBack1] isis enable 1
[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 vlanif 30
[LSRC-Vlanif30] isis enable 1
[LSRC-Vlanif30] quit
[LSRC] interface vlanif 20
[LSRC-Vlanif20] isis enable 1
[LSRC-Vlanif20] quit
[LSRC] interface loopback 1
[LSRC-LoopBack1] isis enable 1
[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 vlanif 30
[LSRD-Vlanif30] isis enable 1
[LSRD-Vlanif30] quit
[LSRD] interface vlanif 40
[LSRD-Vlanif40] isis enable 1
[LSRD-Vlanif40] quit
[LSRD] interface loopback 1
[LSRD-LoopBack1] isis enable 1
[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 vlanif 40
[LSRE-Vlanif40] isis enable 1
[LSRE-Vlanif40] quit
[LSRE] interface loopback 1
[LSRE-LoopBack1] isis enable 1
[LSRE-LoopBack1] quit
```


Copyright © Huawei Technologies Co., Ltd.

After the configuration, run the **display ip routing-table** command on each LSR, and you can view that LSRs learn routes from each other.

Take the display on LSR A as an example.

```
[LSRA] display ip routing-table
Route Flags: R - relied, D - download to fib
------------------------------------------------------------------------------
Routing Tables: 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      Vlanif10
        3.3.3.3/32  ISIS   15   20          D  10.1.1.2      Vlanif10
        4.4.4.4/32  ISIS   15   30          D  10.1.1.2      Vlanif10
        5.5.5.5/32  ISIS   15   40          D  10.1.1.2      Vlanif10
       10.1.1.0/24  Direct 0    0           D  10.1.1.1      Vlanif10
       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      Vlanif10
       30.1.1.0/24  ISIS   15   30          D  10.1.1.2      Vlanif10
       40.1.1.0/24  ISIS   15   40          D  10.1.1.2      Vlanif10
      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 4 Configure basic MPLS functions, enable MPLS TE, RSVP-TE and enable CSPF on the ingress of the 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 vlanif 10
[LSRA-Vlanif10] mpls
[LSRA-Vlanif10] mpls te
[LSRA-Vlanif10] mpls rsvp-te
[LSRA-Vlanif10] 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 vlanif 10
[LSRB-Vlanif10] mpls
[LSRB-Vlanif10] mpls te
[LSRB-Vlanif10] mpls rsvp-te
[LSRB-Vlanif10] quit
[LSRB] interface vlanif 20
[LSRB-Vlanif20] mpls
[LSRB-Vlanif20] mpls te
[LSRB-Vlanif20] mpls rsvp-te
[LSRB-Vlanif20] 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
```


Copyright © Huawei Technologies Co., Ltd.

```
[LSRC] interface vlanif 30
[LSRC-Vlanif30] mpls
[LSRC-Vlanif30] mpls te
[LSRC-Vlanif30] mpls rsvp-te
[LSRC-Vlanif30] quit
[LSRC] interface vlanif 20
[LSRC-Vlanif20] mpls
[LSRC-Vlanif20] mpls te
[LSRC-Vlanif20] mpls rsvp-te
[LSRC-Vlanif20] 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 vlanif 30
[LSRD-Vlanif30] mpls
[LSRD-Vlanif30] mpls te
[LSRD-Vlanif30] mpls rsvp-te
[LSRD-Vlanif30] quit
[LSRD] interface vlanif 40
[LSRD-Vlanif40] mpls
[LSRD-Vlanif40] mpls te
[LSRD-Vlanif40] mpls rsvp-te
[LSRD-Vlanif40] 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 vlanif 40
[LSRE-Vlanif40] mpls
[LSRE-Vlanif40] mpls te
[LSRE-Vlanif40] mpls rsvp-te
[LSRE-Vlanif40] quit
```

Step 5 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] quit
```

Configure LSR B.

```
[LSRB] isis 1
[LSRB-isis-1] cost-style wide
[LSRB-isis-1] traffic-eng level-1-2
[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] quit
```

Configure LSR D.

```
[LSRD] isis 1
[LSRD-isis-1] cost-style wide
[LSRD-isis-1] traffic-eng level-1-2
```


Copyright © Huawei Technologies Co., Ltd.

```
[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] quit
```

Step 6 Configure the 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
```

Step 7 Configure MPLS TE tunnel.

Configure the MPLS TE tunnel on LSR A.

```
[LSRA] interface tunnel 1/0/0
[LSRA-Tunnel1/0/0] ip address unnumbered interface loopback 1
[LSRA-Tunnel1/0/0] tunnel-protocol mpls te
[LSRA-Tunnel1/0/0] destination 5.5.5.5
[LSRA-Tunnel1/0/0] mpls te tunnel-id 100
[LSRA-Tunnel1/0/0] mpls te signal-protocol rsvp-te
[LSRA-Tunnel1/0/0] mpls te path explicit-path atoe
[LSRA-Tunnel1/0/0] mpls te commit
[LSRA-Tunnel1/0/0] quit
```

Step 8 Verify the configuration.

After the configuration, run the **display interface tunnel** command on LSR A, and you can view that the status of the tunnel interface is Up.

```
[LSRA] display interface Tunnel
Tunnel1/0/0 current state : UP
Line protocol current state : UP
Last up time: 2009/01/10 10:36:20
Description : HUAWEI, Quidway Series, Tunnel1/0/0 Interface, Route Port
Route Port,The Maximum Transmit Unit is 1500 bytes
Internet Address is unnumbered, using address of LoopBack1(1.1.1.9/32)
Encapsulation is TUNNEL, loopback not set
Tunnel destination 5.5.5.5
Tunnel up/down statistics 1
Tunnel protocol/transport MPLS/MPLS, ILM is available,
primary tunnel id is 0x40804bb9, secondary tunnel id is 0x0
    300 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets output,  0 bits
    0 output error
```

Run the **display mpls te tunnel-interface** command on LSR A to display information about the tunnel.

```
[LSRA] display mpls te tunnel-interface
```

----End

Configuration Files

- Configuration file of LSR A

```
#
 sysname LSRA
#
vlan batch 10
#
 mpls lsr-id 1.1.1.1
```


Copyright © Huawei Technologies Co., Ltd.

```
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
 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
#
isis 1
 is-level level-1
 cost-style wide
 network-entity 00.0005.0000.0000.0001.00
 traffic-eng level-1
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
 isis enable 1
#
interface Tunnel1/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 5.5.5.5
 mpls te tunnel-id 100
mpls te path explicit-path atoe
 mpls te commit
#
return
```

- Configuration file of LSR B

```
#
 sysname LSRB
#
vlan batch 10 20
#
 mpls lsr-id 2.2.2.2
 mpls
  mpls te
  mpls rsvp-te
#
isis 1
 is-level level-1-2
 cost-style wide
import-route isis level-2 into level-1
 network-entity 00.0005.0000.0000.0002.00
 traffic-eng level-1-2
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif20
 clock master
 ip address 20.1.1.1 255.255.255.0
```


Copyright © Huawei Technologies Co., Ltd.

```
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet 2/0/0
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of LSR C

```
#
 sysname LSRC
#
vlan batch 30 20
#
 mpls lsr-id 3.3.3.3
 mpls
  mpls te
  mpls rsvp-te
#
isis 1
 is-level level-2
 cost-style wide
 network-entity 00.0006.0000.0000.0003.00
 traffic-eng level-2
#
interface Vlanif30
 ip address 30.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif20
 ip address 20.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of LSR D

```
#
 sysname LSRD
#
vlan batch 30 40
#
```


Copyright © Huawei Technologies Co., Ltd.

```
 mpls lsr-id 4.4.4.4
 mpls
  mpls te
  mpls rsvp-te
#
isis 1
 is-level level-1-2
 cost-style wide
 network-entity 00.0007.0000.0000.0004.00
import-route isis level-2 into level-1
 traffic-eng level-1-2
#
interface Vlanif30
 ip address 30.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif40
 ip address 40.1.1.1 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
 isis enable 1
#
return
```

- Configuration file of LSR E

```
#
 sysname LSRE
#
vlan batch 40
#
 mpls lsr-id 5.5.5.5
 mpls
  mpls te
  mpls rsvp-te
#
isis 1
 is-level level-1
 cost-style wide
 network-entity 00.0005.0000.0000.0005.00
 traffic-eng level-1
#
interface Vlanif40
 ip address 40.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet 1/0/0
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface LoopBack1
 ip address 5.5.5.5 255.255.255.255
```


Copyright © Huawei Technologies Co., Ltd.

```
 isis enable 1
#
return
```


Copyright © Huawei Technologies Co., Ltd.

4 MPLS OAM Configuration

About This Chapter

This chapter describes the principles of Multiprotocol Label Switching Operation, Administration and Maintenance (MPLS OAM), procedures of configuring protection switching and remote advertisement of the link status, and provides configuration examples.

Copyright © Huawei Technologies Co., Ltd.

4.1 MPLS OAM Overview

MPLS OAM can effectively detect, identify, and locate faults on the MPLS user plane.

The Operation Administration & Maintenance (OAM) is a effective method of reducing the cost of network maintenance. The MPLS OAM mechanism is used on the MPLS layer.

MPLS OAM mechanism is independent of the upper and lower layers and provides the following functions:

- Detecting, identifying, and locatingfaults on the MPLS user plane.
- Performing protection switching in the case of link or node failure to shorten the defect duration and improves the availability.

For details about requirements for OAM functionality for MPLS networks, refer to the ITU-T Recommendation Y.1710. For details about OAM mechanism for MPLS networks, refer to the ITU-T Recommendation Y.1711.

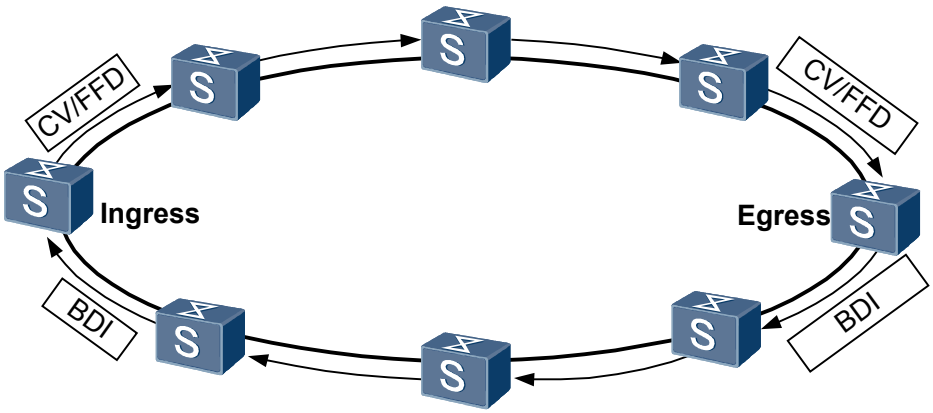
4.2 MPLS OAM Features Supported by the S9300

MPLS OAM provides functions such as connectivity detection, fault detection, and protection switching.

Basic MPLS OAM Detection

The basic detection function of MPLS OAM refers to the detection on the connectivity of an LSP.

Figure 4-1 Schematic diagram of MPLS OAM connectivity detection



As shown in **Figure 4-1**, procedures of MPLS OAM connectivity detection are as follows:

1. The ingress sends a CV or an FFD detection packet to the egress along the LSP to be detected.
2. The egress judges whether the received packet is correct by comparing the packet type, frequency, and TTSI in the received packet with expected values recorded on the egress.

Copyright © Huawei Technologies Co., Ltd.

It counts the number of the correct packets and the error packets received within a certain period, and thus monitors the LSP connectivity.

3. When the egress detects a defect on the LSP, it analyzes the defect type and sends a Backward Defect Indication (BDI) () packet carrying the defect information to the ingress through the backward tunnel. This enables the ingress to know the defect status in real time. If a protection group has been configured in the correct manner, the corresponding switching is triggered.

Backward Tunnel

When configuring the basic OAM detection function, bind a backward tunnel to the detected LSP.

A backward tunnel is an LSP with its ingress and egress being converse to the ingress and egress of the detected LSP. It also can be a non-MPLS path connected to the ingress and egress of the detected LSP.

There are three types of backward tunnels:

- Private backward LSP
- Shared backward LSP
- A non-MPLS backward path

NOTE

At current, only LSPs can function as backward tunnels on the S9300l.

Auto-protocol Function of MPLS OAM

The ITU-T Y.1710 protocol has the following drawbacks:

- If the OAM function on the LSP ingress starts later than that on the LSP egress, or the egress is enabled with the OAM function but the ingress is not, the egress generates a Loss of Connectivity Verification defect (dLOCV) alarm.
- If the OAM function is disabled on the ingress whereas is enabled on the egress, the egress generates a dLOCV alarm .
- To modify the type of the detection packet or the frequency at which detection packets are sent, you must disable the OAM function on the egress and the ingress separately.
- OAM parameters need to be configured separately on the ingress and egress. This may cause the detection packet type and the frequency at which detection packets are sent to be different on the ingress and egress.

The S9300 uses the OAM auto-protocol to solve problems existing in the ITU-T Y.1710.

The OAM auto-protocol is configured on the egress. It provides functions of initial packet triggering and dynamic enabling or disabling.

Protection Switching

In protection switching, a protection tunnel (backup tunnel) is set up for the working tunnel (primary tunnel). A working tunnel and a protection tunnel compose a protection group. When the working tunnel fails, the data flow switches to the protection tunnel; thus improving the network reliability.

The difference between protection switching and CR-LSP backup are as follows:

Copyright © Huawei Technologies Co., Ltd.

- Protection switching uses one tunnel to protect another tunnel. Attributes of every tunnel in the tunnel protection group are independent. For example, the protection tunnel with the bandwidth being 10 Mbit/s can protect the working tunnel that requires 100 Mbit/s bandwidth protection.
- CR-LSP backup has the primary and backup CR-LSPs in the same tunnel group. The backup CR-LSP protects the primary CR-LSP. Except for TE FRR, attributes of the primary and backup CR-LSPs, such as the bandwidth, setup priority, and holding priority, are identical.

Protection Mode

The S9300 supports the following protection switching modes:

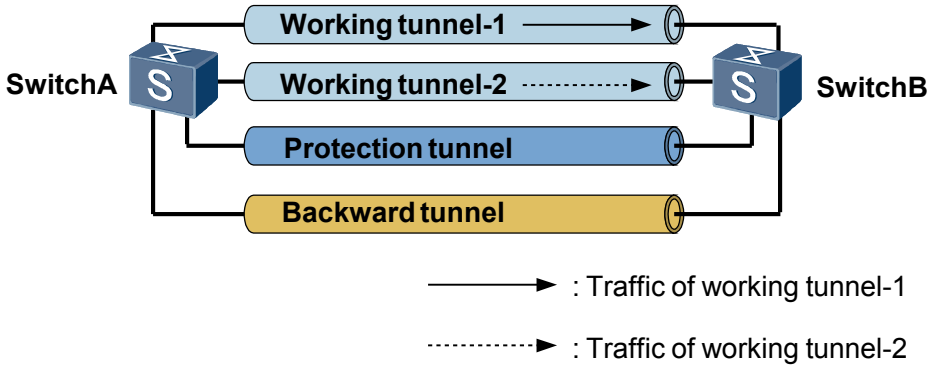
- 1:1 protection

  One working tunnel and one protection tunnel exist between the ingress and the egress.
  - Data is generally forwarded through the working tunnel.
  - When the working tunnel fails, the ingress performs protection switching and switches the data flow to the protection tunnel for transmission.
- N:1 protection

  As shown in **Figure 4-2**, one tunnel provides protection for several working tunnels.

  This mode is applicable to a mesh network for saving bandwidth.

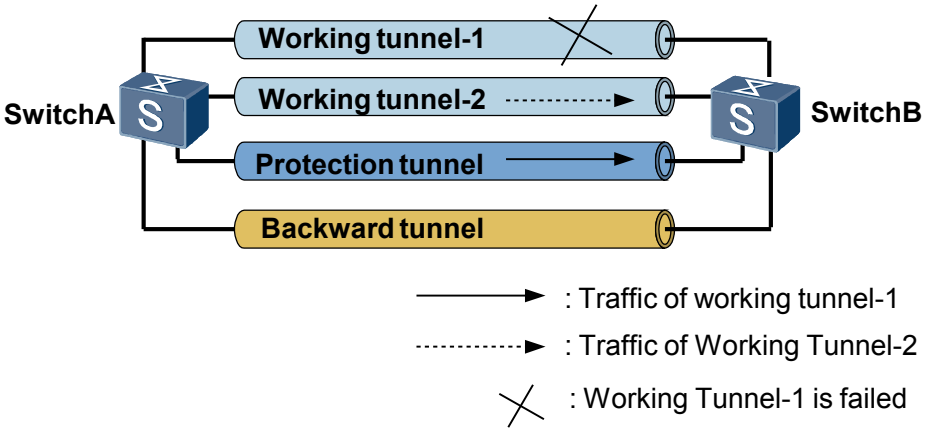
Figure 4-2 N:1 protection mode



As shown in **Figure 4-3**, when one of the working tunnels fails, its traffic switches to the shared protection tunnel.

Huawei Proprietary and Confidential
Copyright © Huawei Technologies Co., Ltd.

Figure 4-3 N:1 protection mode - working tunnel fails



4.3 Configuring Basic MPLS OAM Functions of LSP

MPLS OAM is configured on the ingress and egress of an LSP to detect connectivity of the LSP. MPLS OAM can also detect the connectivity of a TE LSP.

4.3.1 Establishing the Configuration Task

MPLS OAM can detect an ordinary LSP and a TE LSP. Before configuring MPLS OAM, you need to create an LSP. The following sections describe the applicable environment, pre-configuration tasks, data preparation, and configuration procedure of configuring MPLS OAM detection.

Applicable Environment

The S9300 provides MPLS OAM to detect the connectivity of an RSVP-TE LSP, a static CR-LSP, and a static LSP.

To implement MPLS OAM functions, you need to create a backward LSP for bearing BDI packets. The type of the backward LSP can be different from that of the tested LSP, but the backward LSP must be bound to a TE tunnel.

Pre-configuration Tasks

Before configuring basic MPLS OAM functions, complete the following tasks:

- Configuring basic MPLS functions
- Creating a forward LSP, the LSP to be detected by OAM and is bound to the TE tunnel
- Creating a backward LSP

NOTE

If the forward LSP is static and the backward LSP is dynamic, and the backward LSP is in the shared mode, you must specify **lsrid** *ingress-lsr-id* and **tunnel-id** *tunnel-id* when running the **static-lsp egress** command or the **static-cr-lsp egress** command to create a forward LSP. For creating the LSP bound to a TE tunnel, refer to the chapter "MPLS TE Configuration."

Copyright © Huawei Technologies Co., Ltd.

Data Preparation

To configure basic MPLS OAM functions, you need the following data.

No.	Data
1	Ingress: Number of tunnel interfaces bound to the detected LSP
2	(Optional) Ingress: backward tunnel ● If a static LSP or a static CR-LSP acts as the backward tunnel, the name of the static LSP or the static CR-LSP is required. ● If a dynamic LSP (RSVP-TE LSP) acts as the backward tunnel, the LSP ID and tunnel ID are required .
3	Egress: Number of the tunnel interface that is bound to the backward LSP and the protection mode
4	Egress: detected LSP ● If a static LSP or a static CR-LSP is to be detected, the name of the LSP, LSR ID, and tunnel ID are required. ● If a dynamic LSP (RSVP-TE LSP) is to be detected, the LSR ID and the tunnel ID are required.
5	(Optional) MPLS OAM parameters ● Parameters for the ingress: detection type, frequency at which FFD packets are sent, and priority of the detection packet. ● Parameters for the egress: detection type, frequency at which FFD packets are sent, status of the auto-protocol (enabled or disabled), timeout period of the auto-protocol, and frequency at which BDI packets are sent.

NOTE

- The backward LSP must be specified on the egress; otherwise, BDI packets cannot be correctly sent to the source end.
- If a shared backward LSP is used, you do not need to specify the backward LSP on the ingress.

4.3.2 Configuring MPLS OAM on the Ingress

When configuring OAM on the ingress of an LSP, you can configure a backward tunnel as required.

Context

Do as follows on the ingress of the LSP:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Copyright © Huawei Technologies Co., Ltd.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Step 3 Run:

```
mpls oam
```

MPLS OAM is enabled globally.

By default, MPLS OAM is disabled globally.

Step 4 Run:

```
quit
```

Return to the system view.

Step 5 Configure MPLS OAM parameters for the ingress.

If the PHP function is not configured when a backward LSP is set up, you must specify the backward LSP when configuring parameters for the MPLS OAM ingress.

- If no backward LSP is specified, run:

  ```
  mpls oam ingress tunnel tunnel-number [ type { cv | ffd frequency ffd-fre } ]
  [ backward-lsp share ] [ packet-priority priority ]
  ```

  NOTE

  Parameters of the backward LSP depend on the configuration of the egress.

- If a backward LSP is specified, run:

  ```
  mpls oam ingress tunnel tunnel-number [ type { cv | ffd frequency ffd-fre } ]
  backward-lsp { lsp-name lsp-name | lsr-id rev-ingress-lsr-id tunnel-id rev-
  tunnel-id }  [ packet-priority priority ]
  ```

  If the backward LSP is a static LSP or a static CR-LSP, you cannot configure it in private mode.

  If **lsrid** *ingress-lsr-id* and **tunnel-id** *tunnel-id* are specified when you run the **static-lsp egress** *lsp-name* **incoming-interface** *interface-type interface-number* **in-label** *in-label* [**lsrid** *ingress-lsr-id* **tunnel-id** *tunnel-id*] command or the **static-cr-lsp egress** *lsp-name* **incoming-interface** *interface-type interface-number* **in-label** *in-label* [**lsrid** *ingress-lsr-id* **tunnel-id** *tunnel-id*] command to create a backward LSP, you can use these two parametersspecify parameters in this step; otherwise, you can specifyonly the parameter **lsp-name** *lsp-name*.

  By default, the type of the detection packet is CV. The frequency at which CV packets are sent is one second. The priority of the detection packet is 0, the lowest priority.

Step 6 Run:

```
mpls oam ingress enable { all | tunnel tunnel-number }
```

OAM is enabled on the ingress.

----End

4.3.3 Configuring MPLS OAM on the Egress

When configuring OAM on the egress of an LSP, you need to enable or disable the OAM auto protocol. By default, the OAM auto protocol is enabled.

Copyright © Huawei Technologies Co., Ltd.

Context

Do as follows on the egress of the LSP:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mpls
```

The MPLS view is displayed.

Step 3 Run:

```
mpls oam
```

MPLS OAM is enabled globally.

Step 4 Run:

```
quit
```

Return to the system view.

Step 5 Configure OAM parameters for the egress.

- Run:

  mpls oam egress { **lsp-name** *lsp-name* | **lsr-id** *ingress-lsr-id* **tunnel-id** *tunnel-id* } [**auto-protocol** [**overtime** *over-time*]] [**backward-lsp tunnel** *tunnel-number* [**private** | **share**] [**bdi-frequency** { **detect-freq** | **per-second** }]]

  The auto-protocol extension of OAM is enabled.

- Run:

  mpls oam egress { **lsp-name** *lsp-name* | **lsr-id** *ingress-lsr-id* **tunnel-id** *tunnel-id* } **type** { **cv** | **ffd frequency** *ffd-fre* } [**backward-lsp tunnel** *tunnel-number* [**private** | **share**] [**bdi-frequency** { **detect-freq** | **per-second** }]]

  OAM parameters is configured for the egress when the auto-protocol extension of OAM is disabled.

If **lsrid** *ingress-lsr-id* and **tunnel-id** *tunnel-id* are specified when you run the **static-lsp egress** *lsp-name* **incoming-interface** *interface-type interface-number* **in-label** *in-label* [**lsrid** *ingress-lsr-id* **tunnel-id** *tunnel-id*] command or the **static-cr-lsp egress** *lsp-name* **incoming-interface** *interface-type interface-number* **in-label** *in-label* [**lsrid** *ingress-lsr-id* **tunnel-id** *tunnel-id*] command to create a forward tunnel, you can use these two parameters in this step; otherwise, you can specify only the parameter **lsp-name** *lsp-name*.

By default, the auto-protocol function of OAM is enabled. The timeout period for the first packet to wait for response is five minutes.

By default, the backward LSP is in the shared mode. When the backward LSP is a static LSP or a CR-LSP, it is in the private mode.

By default, the frequency at which BDI packets are sent through the backward LSP is **detect-freq**.

Copyright © Huawei Technologies Co., Ltd.

NOTE

If a shared backward LSP is used to enable the OAM auto-protocol extension in Step 5, Step 6 is not necessary. When the egress receives the first CV/FFD packet, it automatically records the packet type and the frequency at which CV/FFD packets are sent, and starts to detect the connectivity.

Step 6 Run:

```
mpls oam egress enable { all | lsp-name lsp-name | lsr-id ingress-lsr-id tunnel-id tunnel-id }
```

OAM is enabled on the egress.

----End

4.3.4 Checking the Configuration

After the configuration, you can use display commands on the ingress and egress of an LSP to view information about the LSP, OAM detection, and OAM backward LSP.

Prerequisite

The configurations of basic MPLS OAM functions are complete.

Procedure

- Run **display mpls oam ingress** { **all** | **tunnel** *interface-number* } [**verbose**] command to view MPLS OAM information on the ingress.
- Run **display mpls oam egress** { **all** | **lsp-name** *lsp-name* | **lsr-id** *ingress-lsr-id* **tunnel-id** *tunnel-id* } [**verbose**] command to view MPLS OAM information on the egress.

----End

Example

If the configurations succeed, run the commands mentioned above and you can view the following results:

- Basic information about the LSP, including the tunnel name, LSP type, LSP ingress LSR ID, and LSP tunnel ID
- Basic information about OAM, including the tunnel name, TTSI, packet type, and frequency
- OAM detection information, including the packet type, frequency at which detection packets are sent, detection status, and defect status. If the link works properly, the detection status is Start and the defect status is non-defect
- Information about backward LSP, including the sharing mode and configurations of the backward LSP

4.4 Configuring MPLS OAM Protection Switching of LSP

MPLS OAM protection switching enables a tunnel to protect one or more tunnels. The tunnel under protection is a working tunnel, and the tunnel providing protection is a protection tunnel. When a protection tunnel protects one working tunnel, it indicates that tunnel protection is in 1:1 mode.

Copyright © Huawei Technologies Co., Ltd.

4.4.1 Establishing the Configuration Task

MPLS OAM protection switching is a high-reliability technology applicable to tunnel protection. After one or more working tunnels and a protection tunnel are configured, the protection tunnel can protect the working tunnel(s), which improves reliability of the working tunnel(s). The following sections describe the applicable environment, pre-configuration tasks, data preparation, and configuration procedure of configuring MPLS OAM protection switching.

Applicable Environment

If the tunnel requires high availability, you can configure the MPLS OAM protection switching to protect the tunnel.

MPLS OAM protection switching enables one tunnel to protect one or multiple tunnels. The tunnel under protection is a working tunnel, and the tunnel providing protection is a protection tunnel. A working tunnel and a protection tunnel compose a protection group.

One protection tunnel can protect one or more working tunnels. The protection mechanism in which one protection tunnel protects only one working tunnel is called 1:1 protection; one protection tunnel protects two or more working tunnel is called N:1 protection. "N" indicates the number of the working tunnels in the same protection group. Working tunnels in the same protection group use the same ingress and egress.

The S9300 supports 1:1 protection and N:1 protection.

- Working tunnel and protection tunnel

  Attributes of every tunnel in the tunnel protection group are not related. For example, the protection tunnel with the bandwidth being 50 Mbit/s can protect the working tunnel with the bandwidth being 100 Mbit/s.

  You can configure TE FRR on the working tunnel in the protection group to provide dual protection for the working tunnel. The protection tunnel cannot serve as the TE FRR primary tunnel to be protected by other tunnels. In addition, the protection tunnel cannot be enabled with TE FRR.

- Protection switching trigger mechanism

  The S9300 complies the following switch request criteria to initiate (or prevent) a protection switching.

Table 4-1 Switch Request Criteria

Switch Request	Order of Priority	Description
Clear	Highest	Clears all switching requests initiated through commands, including forced switching and manual switching. Traffic switching is not performed in the case of signal failure.
Signal Fail	↑	Automatically triggers the protection switching between the working tunnel and the protection tunnel in the case of a signal failure.

Copyright © Huawei Technologies Co., Ltd.

Switch Request	Order of Priority	Description
Manual Switch	↑	Switches traffic from the working tunnel to the protection tunnel only when the protection tunnel functions properly or switches traffic from the protection tunnel to the working tunnel only when the working tunnel functions properly.
Wait To Restore	↑	Switches traffic from the protection tunnel to the working tunnel after the working tunnel recovers for a certain period specified by the wait-to-restore (WTR) timer.
No Request	Lowest	Indicates that there is no switching request.

Pre-configuration Tasks

Before configuring MPLS OAM protection switching, complete the following tasks:

- Creating the working tunnel and protection tunnel
- **Configuring basic MPLS OAM functions**

Data Preparation

To configure MPLS OAM protection switching, you need the following data.

No.	Data
1	Number of the working tunnel in the protection group **NOTE** The maximum number of working tunnels in a protection group is equal to or smaller than 16 depending on the License.
2	Tunnel ID of the protection tunnel in the protection group
3	Parameters for the protection group, such as the hold off time, revertive mode, and WTR time

4.4.2 Configuring a Tunnel Protection Group

You can configure a tunnel protection group for the primary tunnel on the ingress of a tunnel. In addition, you can configure the switchback delay time and the switchback mode. The switchback mode can be classified into the revertive mode and non-revertive mode. By default, revertive mode is used. In revertive mode, you can set the switchback delay time .

Copyright © Huawei Technologies Co., Ltd.

Context

Do as follows on the ingress of the tunnel:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The tunnel interface view is displayed.

Step 3 Run:

```
mpls te protection tunnel tunnel-id [ holdoff holdoff-time ] [ mode { non-revertive | revertive [ wtr wtr-time ] } ]
```

The working tunnel is added to the protection group.

Note the following parameters or concepts before perform this step:

- The *tunnel-id* indicates the tunnel ID of the protection tunnel.
- The hold-off time indicates the time between declaration of signal failure and the initialization of the protection switching algorithm. The hold-off time ranges from 0 to 100. By default, the hold-off time is 0. *holdoff-time* specifies the number of steps for the hold-off time. The value of each step is 100, in milliseconds.

  NOTE

  Multiplying 100 milliseconds by *holdoff-time*, you can get the hold-off time.
- Non-revertive mode indicates that traffic does not switch back to the working tunnel even though the working tunnel recovers.
- Revertive mode indicates that traffic switches back to the working tunnel when the working tunnel recovers.

  By default, the protection group is in revertive mode.
- Wait to Restore time (WTR time) indicates the time to be waited before traffic switching. The WTR time ranges from 0 to 30 minutes. The default value is 12. The parameter *wtr-time* indicates the number of steps. The value of each step is 30, in seconds.

  NOTE

  Multiplying 30 seconds by *wtr-time*, you can get the value of WTR time.

NOTE

If the number of the working tunnels in the same protection group is N, perform Step 2 and Step 3 for N times by using different *tunnel-number*.

Step 4 Run:

```
mpls te commit
```

The current configuration of the tunnel protection group is committed.

----End

Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

Configurations described in this section are also applicable in modifying the configuration of the tunnel protection group.

Besides configuring a tunnel protection group to protect the working tunnel, you can configure TE FRR on the working tunnel in the protection group to provide dual protection for the working tunnel. The protection tunnel cannot serve as the working tunnel to be protected by other tunnels. In addition, the protection tunnel cannot be enabled with TE FRR.

4.4.3 (Optional) Configuring the Protection Switching Trigger Mechanism

After configuring a tunnel protection group, you can configure a trigger mechanism of protection switching to force traffic to switch to the primary LSP or the backup LSP. Alternatively, you can perform switchover manually.

Context

Pay attention to the **switch request criteria** before configuring the protection switching trigger mechanism.

Do as follows on the ingress of the tunnel protection group as required:

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface tunnel tunnel-number
```

The tunnel interface view is displayed.

Step 3 Select one of the following protection switching trigger methods as required:

- To switch traffic to the working tunnel, run:

  ```
  mpls te protect-switch manual protect-lsp
  ```

- To switch traffic to the protection tunnel, run:

  ```
  mpls te protect-switch manual work-lsp
  ```

- To cancel the configuration of the protection switching trigger mechanism, run:

  ```
  mpls te protect-switch  clear
  ```

Step 4 Run:

```
mpls te commit
```

The current configuration is committed.

----End

4.4.4 Checking the Configuration

After the configurations, you can use the display commands to view information about the tunnel protection group and tunnel bindings.

Copyright © Huawei Technologies Co., Ltd.

Prerequisite

The configurations of the MPLS OAM protection switching function are complete.

Procedure

- Run **display mpls te protection tunnel** { **all** | *tunnel-id* | **interface tunnel** *interface-number* } [**verbose**] command to check information about a tunnel protection group.
- Run **display mpls te protection binding protect-tunnel** { *tunnel-id* | **interface tunnel** *interface-number* } command to check the protection relationship of the tunnel.

----End

Example

After the configuration succeeds, run the preceding commands to view information about the protection group.

4.5 Maintaining MPLS OAM

You can use display commands to monitor MPLS OAM and the tunnel protection group.

4.5.1 Monitoring the Running of MPLS OAM

You can use display commands to view the MPLS OAM operation status including the status of OAM-enabled LSPs on the ingress and egress.

Context

In routine maintenance, you can run the following commands in any view to check the MPLS OAM operation status.

Procedure

- Run the **display mpls oam egress** { **all** | **lsp-name** *lsp-name* | **lsr-id** *ingress-lsr-id* **tunnel-id** *tunnel-id* } [**verbose**] command to view information about the current status and configuration of the OAM-enabled LSP on the egress.
- Run the **display mpls oam ingress** { **all** | **tunnel** *tunnel-number* } [**verbose**] command to view information about the MPLS OAM parameters and status of the LSP on the ingress.
- Run the **display mpls oam oam-index** *index-value* command to view information about parameters and status of MPLS OAM.

----End

4.5.2 Monitoring the Running of Protection Group

You can use display commands to view the operation of a tunnel protection group and information about tunnels in the tunnel protection group.

Context

In routine maintenance, you can run the following commands in any view to check the operating status of the protection group.

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Run the **display mpls te protection tunnel** { **all** | *tunnel-id* | **interface tunnel** *interface-number* } [**verbose**] command to view information about the tunnel protection group.
- Run the **display mpls te protection binding protect-tunnel** { *tunnel-id* | **interface tunnel** *interface-number* } command to view information about tunnels in the tunnel protection group.

----End

4.5.3 Debugging the Tunnel Protection Group

When a tunnel protection group fails, you can use debugging commands to debug the tunnel protection group.

Context

CAUTION

Debugging affects the performance of the system. After debugging, run the **undo debugging all** command to disable it immediately.

When a defect occurs, run the following debugging command in the user view to debug MPLS OAM and locate the defect.

For the procedure of enabling the debugging, refer to the *Quidway S9300 Terabit Routing Switch Configuration Guide - Device Management*. For the description of the debugging command, refer to the *Quidway S9300 Terabit Routing Switch - Debugging Reference*.

Procedure

- Run the **debugging mpls te protect-switch** { **all** | **error** | **inter** | **process** | **timer** } command to enable the debugging of the OAM function.

----End

4.5.4 Debugging MPLS OAM

When an MPLS OAM fault occurs, you can use debugging commands to debug MPLS OAM.

Context

CAUTION

Debugging affects the performance of the system. After debugging, run the **undo debugging all** command to disable it immediately.

When a defect occurs in a tunnel protection group, run the following debugging command in the user view to debug the tunnel protection group and locate the fault.

Copyright © Huawei Technologies Co., Ltd.

For the procedure of enabling the debugging, refer to the *Quidway S9300 Terabit Routing Switch Configuration Guide - Device Management*. For the description of the debugging command, refer to the *Quidway S9300 Terabit Routing Switch - Debugging Reference*.

Procedure

- Run the **debugging mpls oam** { **all** | **bdi** | **cv** | **decode** | **defect-detect** | **error** | **fdi** | **ffd** | **fsm** | **hsb** | **main** | **packet** | **process** | **timer** } command to enable the debugging of the protection switching function.

----End

4.6 Configuration Examples

This section provides several configuration examples of MPLS OAM.

4.6.1 Example for Configuring MPLS OAM to Detect the Connectivity of the Static LSP

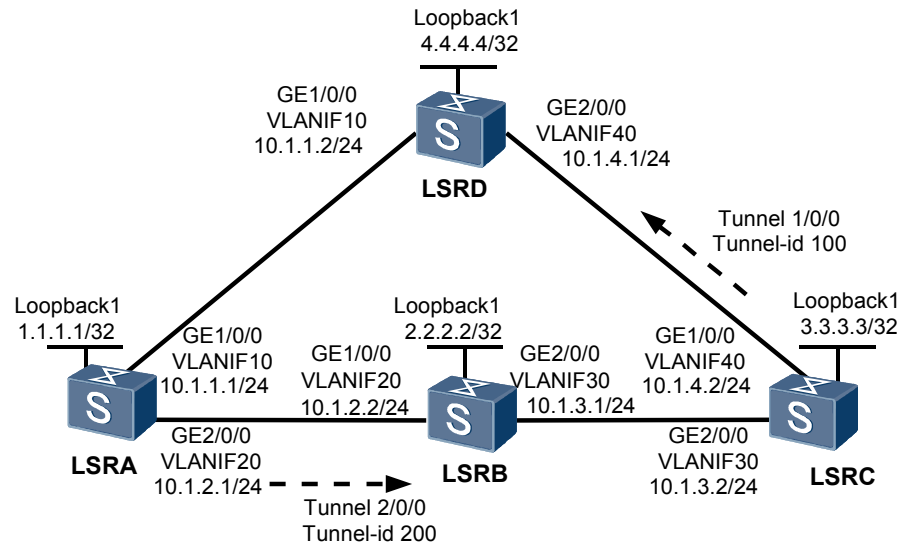
After the MPLS OAM function is configured, you can detect the connectivity of a static LSP and obtain the type of link defect.

Networking Requirements

On an MPLS network shown in **Figure 4-4**, a static LSP is set up along LSRA->LSRB->LSRC.

It is required that MPLS OAM be used to detect the connectivity of the static LSP. Egress node LSRC can notify the defect to the ingress node LSRA when a connectivity defect occurs.

Figure 4-4 Networking diagram for configuring basic MPLS OAM functions



Device	Interface	VLANIF interface	IP address

Copyright © Huawei Technologies Co., Ltd.

LSRA	GE1/0/0	VLANIF10	10.1.1.1/24
LSRA	GE2/0/0	VLANIF20	10.1.2.1/24
LSRB	GE1/0/0	VLANIF20	10.1.2.2/24
LSRB	GE2/0/0	VLANIF30	10.1.3.1/24
LSRC	GE1/0/0	VLANIF40	10.1.4.2/24
LSRC	GE2/0/0	VLANIF30	10.1.3.2/24
LSRD	GE1/0/0	VLANIF10	10.1.1.2/24
LSRD	GE2/0/0	VLANIF40	10.1.4.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Create a TE tunnel that is based on the static LSP between LSRA and LSRC.
2. Create a static CR-LSP along LSRC->LSRD->LSRA as the backward tunnel to notify the ingress node of the defect.
3. Set OAM parameters on ingress node LSRA and enable MPLS OAM.
4. Set OAM parameters on egress node LSRC and enable the MPLS OAM auto protocol.

Data Preparation

To complete the configuration, you need the following data:

- IP address of the interface on each node, name of each tunnel interface, and tunnel ID
- Type of detection packets
- Mode of the backward tunnel

Procedure

Step 1 Create VLANs and VLANIF interfaces, and assign IP addresses to the VLANIF interfaces, and configure routing protocols for the VLANIF interfaces.

Configure IP addresses and masks for the interfaces including loopback interfaces according to **Figure 4-4**.

Configure OSPF on all the nodes and advertise the routes on the loopback interfaces. The configuration details are not mentioned here.

After the configuration, LSRs can ping each other. Run the **display ip routing-table** command on each LSR, and you can view the routing entries to the LSRs.

Take the display on LSRA as an example:

```
<LSRA> display ip routing-table
Route Flags: R - relied, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 14        Routes : 15
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
```


Copyright © Huawei Technologies Co., Ltd.

```
      1.1.1.1/32    Direct 0    0         D    127.0.0.1       InLoopBack1
      2.2.2.2/32    OSPF   10   2         D    10.1.2.2        Vlanif20
      3.3.3.3/32    OSPF   10   3         D    10.1.1.2        Vlanif10
                    OSPF   10   3         D    10.1.2.2        Vlanif20
      4.4.4.4/32    OSPF   10   2         D    10.1.1.2        Vlanif10
     10.1.1.0/24    Direct 0    0         D    10.1.1.1        Vlanif10
     10.1.1.1/32    Direct 0    0         D    127.0.0.1       InLoopBack1
     10.1.1.2/32    Direct 0    0         D    10.1.1.2        Vlanif10
     10.1.2.0/24    Direct 0    0         D    10.1.2.1        Vlanif20
     10.1.2.1/32    Direct 0    0         D    127.0.0.1       InLoopBack1
     10.1.2.2/32    Direct 0    0         D    10.1.2.2        Vlanif20
     10.1.3.0/24    OSPF   10   2         D    10.1.2.2        Vlanif20
     10.1.4.0/24    OSPF   10   2         D    10.1.1.2        Vlanif10
    127.0.0.0/8     Direct 0    0         D    127.0.0.1       InLoopBack1
    127.0.0.1/32    Direct 0    0         D    127.0.0.1       InLoopBack1
```

Step 2 Set up a static LSP to be detected.

Configure basic MPLS functions and enable MPLS TE on LSRA.

```
<LSRA> system-view
[LSRA] mpls lsr-id 1.1.1.1
[LSRA] mpls
[LSRA-mpls] mpls te
[LSRA-mpls] quit
[LSRA] interface vlanif 10
[LSRA-Vlanif10] mpls
[LSRA-Vlanif10] mpls te
[LSRA-Vlanif10] quit
[LSRA] interface vlanif 20
[LSRA-Vlanif20] mpls
[LSRA-Vlanif200] mpls te
[LSRA-Vlanif20] quit
```

The configurations on LSRB, LSRC, and LSRD are similar to the configuration on LSRA, and are not mentioned here.

On LSRA, configure a static LSP (MPLS TE tunnel) destined for LSRC.

```
<LSRA> system-view
[LSRA] interface tunnel 2/0/0
[LSRA-tunnel2/0/0] ip address unnumbered interface loopback 1
[LSRA-tunnel2/0/0] tunnel-protocol mpls te
[LSRA-tunnel2/0/0] destination 3.3.3.3
[LSRA-tunnel2/0/0] mpls te tunnel-id 200
[LSRA-tunnel2/0/0] mpls te signal-protocol static
[LSRA-tunnel2/0/0] mpls te commit
[LSRA-tunnel2/0/0] quit
```

Configure LSRA as the ingress node of the static LSP and use the TE tunnel.

```
[LSRA] static-lsp ingress tunnel-interface tunnel 2/0/0 destination 3.3.3.3 nexthop
10.1.2.2 out-label 20
```

Configure LSRB as the transit node of the static LSP.

```
<LSRB> system-view
[LSRB] static-lsp transit oamlsp incoming-interface vlanif 20 in-label 20 nexthop
10.1.3.2 out-label 30
```

Configure LSRC as the egress node of the static LSP and specify **lsr-id** and **tunnel-id**.

```
<LSRC> system-view
[LSRC] static-lsp egress oamlsp incoming-interface vlanif 30 in-label 30 lsrid
1.1.1.1 tunnel-id 200
```

After the configuration, run the **display mpls te tunnel-interface** command on LSRA. You can view that the TE tunnel is Up and uses the static signaling protocol. Note the following information:

Copyright © Huawei Technologies Co., Ltd.

```
<LSRA> display mpls te tunnel-interface
  tunnel Name         :  tunnel2/0/0
  tunnel State Desc   :  CR-LSP is Up
  tunnel Attributes   :
    LSP ID              :  1.1.1.1:1
    Session ID          :  200
    Admin State         :  UP                   Oper State   :  UP
    Ingress LSR ID      :  1.1.1.1              Egress LSR ID:  3.3.3.3
    Signaling Prot      :  STATIC
```

Run the **display mpls static-lsp** command on LSRA, and you can view that the static LSP corresponding to Tunnel 2/0/0 is Up.

```
<LSRA> display mpls static-lsp
TOTAL          : 1       STATIC LSP(S)
UP             : 1       STATIC LSP(S)
DOWN           : 0       STATIC LSP(S)
Name            FEC           I/O Label  I/O If                    Stat
tunnel2/0/0     3.3.3.3/32    NULL/20    -/Vlanif20                Up
```

Step 3 Set up a backward tunnel.

On LSRC, configure a static LSP (MPLS TE tunnel) destined for LSRA.

```
<LSRC> system-view
[LSRC] interface tunnel1/0/0
[LSRC-tunnel1/0/0] ip address unnumbered interface loopback 1
[LSRC-tunnel1/0/0] tunnel-protocol mpls te
[LSRC-tunnel1/0/0] destination 1.1.1.1
[LSRC-tunnel1/0/0] mpls te tunnel-id 100
[LSRC-tunnel1/0/0] mpls te signal-protocol cr-static
[LSRC-tunnel1/0/0] mpls te commit
[LSRC-tunnel1/0/0] quit
```

Configure LSRC as the ingress node of the static CR-LSP.

```
[LSRC] static-cr-lsp ingress tunnel-interface tunnel1/0/0 destination 1.1.1.1
nexthop 10.1.4.1 out-label 70
```

Configure LSRD as the transit node of the static CR-LSP.

```
<LSRD> system-view
[LSRD] static-cr-lsp transit tunnel1/0/0 incoming-interface vlanif 40 in-label 70
nexthop 10.1.1.1 out-label 80
```

Configure LSRA as the egress node of the static LSP and specify **lsr-id** and **tunnel-id**.

```
<LSRA> system-view
[LSRA] static-cr-lsp egress tunnel1/0/0 incoming-interface vlanif 10 in-label 80
lsrid 3.3.3.3 tunnel-id 100
```

After the configuration, run the **display mpls te tunnel-interface** command on LSRC. You can view that the backward TE tunnel is Up. Note the following information:

```
<LSRC> display mpls te tunnel-interface
  tunnel Name         :  tunnel1/0/0
  tunnel State Desc   : CR-LSP is Up
  tunnel Attributes   :
  LSP ID              :  3.3.3.3:1
    Session ID          :  100
    Admin State         :  UP                   Oper State   :  UP
    Ingress LSR ID      :  3.3.3.3              Egress LSR ID:  1.1.1.1
    Signaling Prot      :  STATIC-CR
```

Run the **display mpls static-cr-lsp** command on LSRC, and you can view that the static CR-LSP is Up.

```
<LSRC> display mpls static-cr-lsp
TOTAL          : 1     STATIC CRLSP(S)
```


Copyright © Huawei Technologies Co., Ltd.

```
UP             : 1     STATIC CRLSP(S)
DOWN           : 0     STATIC CRLSP(S)
Name            FEC            I/O Label  I/O If                    Stat
tunnel1/0/0     1.1.1.1/32     NULL/70    -/Vlanif40                Up
```

Step 4 Configure MPLS OAM functions.

On LSRA, configure MPLS OAM functions on the ingress node. Use the default configurations, that is, send CV packets. The parameters of the backward tunnel depend on the configuration on the egress node.

```
<LSRA> system-view
[LSRA] mpls
[LSRA-mpls] mpls oam
[LSRA-mpls] quit
[LSRA] mpls oam ingress tunnel2/0/0 backward-lsp lsr-id 3.3.3.3 tunnel-id 100
[LSRA] mpls oam ingress enable all
```

On LSRC, configure MPLS OAM functions on the egress node.

```
<LSRC> system-view
[LSRC] mpls
[LSRC-mpls] mpls oam
[LSRC-mpls] quit
```

Enable the MPLS OAM auto protocol on the egress node. Detect the LSP named **oamlsp**. The backward LSP that is configured on tunnel 0/0/1 is in private mode.

```
[LSRC] mpls oam egress lsp-name oamlsp auto-protocol backward-lsp tunnel 1/0/0
private
```

After the MPLS OAM auto protocol is configured on the egress node, the egress node starts OAM when receiving the first correct detection packet.

After the previous configuration, check the MPLS OAM parameters and status of the LSP on ingress node LSRA and on egress node LSRC. You can view that the ingress and egress nodes are in normal detection state and no defects occur.

```
<LSRA> display mpls oam ingress all verbose
------------------------------------------------------------------------------
Verbose information about the NO.1 oam at the ingress
------------------------------------------------------------------------------
lsp basic information:                oam basic information:
-----------------------------------   -----------------------------------
tunnel-name         : tunnel2/0/0     Oam-Index               : 256
Lsp signal status   : Up               Oam select board        : 1
Lsp establish type  : Static lsp       Enable-state            : Manual enable
Lsp ingress lsr-id  : 1.1.1.1          Ttsi/lsr-id             : 1.1.1.1
Lsp tnl-id/Lsp-id   : 200/1            Ttsi/tunnel-id          : 200
oam detect information:               oam backward information:
-----------------------------------   -----------------------------------
Type                : CV               Share attribute     : Private
Frequency           : 1 s              Lsp-name            : tunnel1/0/0
Detect-state        : Start            Lsp ingress lsr-id  : 3.3.3.3
Defect-state        : Non-defect       Lsp tnl-id/lsp id   : 100/1
Available-state     : Available        Lsp-inLabel         : 80
Unavailable time (s): 0                Lsp signal status   : Up
------------------------------------------------------------------------------
Total Oam Num:                    1
Total Start Oam Num:              1
Total Defect Oam Num:             0
Total Unavaliable Oam Num:        0

<LSRC> display mpls oam egress all verbose
------------------------------------------------------------------------------
Verbose information about the NO.1 oam at the egress
------------------------------------------------------------------------------
lsp basic information:                oam basic information:
```


Copyright © Huawei Technologies Co., Ltd.

```
----------------------------------   ----------------------------------
Lsp name            : oamlsp         Oam-Index           : 256
Lsp signal status   : Up             Oam select board    : 1
Lsp establish type  : Static lsp     Enable-state        : --
Lsp incoming Label  : 30             Auto-protocol       : Enable
Lsp ingress lsr-id  : 1.1.1.1        Auto-overtime (s)   : 300
Lsp tnl-id/lsp-id   : 200/1          Ttsi/lsr-id         : 1.1.1.1
Lsp Incoming-int      Vlanif40       Ttsi/tunnel-id      : 200

oam detect information:              oam backward information:
----------------------------------   ----------------------------------
Type                : CV             tunnel name         : tunnel1/0/0
Frequency           : 1 s            Share attribute     : Private
Detect-state        : Start          Lsp signal status   : Up
Defect-state        : Non-defect     Bdi-frequency       : Detect frequency
Available-state     : Available
Unavailable time (s): 0
--------------------------------------------------------------------------
Total Oam Num:                   1
Total Start Oam Num:             1
Total Defect Oam Num:            0
Total Unavaliable Oam Num:       0
```

Step 5 Verify the configuration.

Run the **shutdown** command on VLANIF30 of LSRB and simulate a defect on the link.

```
<LSRB> system-view
[LSRB] interface vlanif 30
[LSRB-Vlanif30] shutdown
```

Run the **display mpls oam egress all verbose** command on LSRC, and you can view that LSRC detects the defect with the status as dLocv.

```
<LSRC> display mpls oam egress all verbose
--------------------------------------------------------------------------
Verbose information about the NO.1 oam at the egress
--------------------------------------------------------------------------

lsp basic information:               oam basic information:
----------------------------------   ----------------------------------
Lsp name            : oamlsp         Oam-Index           : 256
Lsp signal status   : Up             Oam select board    : 1
Lsp establish type  : Static lsp     Enable-state        : --
Lsp incoming Label  : 30             Auto-protocol       : Enable
Lsp ingress lsr-id  : 1.1.1.1        Auto-overtime (s)   : 300
Lsp tnl-id/lsp-id   : 200/1          Ttsi/lsr-id         : 1.1.1.1
Lsp Incoming-int      Vlanif30       Ttsi/tunnel-id      : 200

oam detect information:               oam backward information:
----------------------------------   ----------------------------------
Type                : CV             tunnel name         : tunnel1/0/0
Frequency           : 1 s            Share attribute     : Private
Detect-state        : Stop           Lsp signal status   : Up
Defect-type         : dEgressDown           Bdi-frequency       : Detect frequency
Available-state     : Available
Unavailable time (s): 0
--------------------------------------------------------------------------
Total Oam Num:                   1
Total Start Oam Num:             1
Total Defect Oam Num:            1
Total Unavaliable Oam Num:       1
```

----End

Configuration Files

- Configuration file of LSRA

Copyright © Huawei Technologies Co., Ltd.

```
#
 sysname LSRA
#
 vlan batch 10 20
#
 mpls lsr-id 1.1.1.1
 mpls
  mpls te
  mpls oam
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls te
#
interface Vlanif20
 ip address 10.1.2.1 255.255.255.0
 mpls
 mpls te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
interface tunnel2/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 3.3.3.3
 mpls te signal-protocol static
 mpls te tunnel-id 200
 mpls te commit
#
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
  network 10.1.2.0 0.0.0.255
#
 static-lsp ingress tunnel-interface  tunnel2/0/0 destination 3.3.3.3 nexthop
10.1.2.2 out-label 20
 static-cr-lsp egress tunnel1/0/0 incoming-interface Vlanif10 in-label 80
lsrid 3.3.3.3 tunnel-id 100
#
 mpls oam ingress tunnel2/0/0 backward-lsp lsr-id 3.3.3.3 tunnel-id 100
 mpls oam ingress enable tunnel2/0/0
#
return
```

- Configuration file of LSRB

```
#
 sysname LSRB
#
 vlan batch 20 30
#
 mpls lsr-id 2.2.2.2
 mpls
  mpls te
#
interface Vlanif20
 ip address 10.1.2.2 255.255.255.0
 mpls
 mpls te
#
```


Copyright © Huawei Technologies Co., Ltd.

```
interface Vlanif30
 ip address 10.1.3.1 255.255.255.0
 mpls
 mpls te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 20
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 30
#
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 10.1.2.0 0.0.0.255
  network 10.1.3.0 0.0.0.255
#
 static-lsp transit oamlsp incoming-interface vlanif20 in-label 20 nexthop
10.1.3.2 out-label 30
#
return
```

- Configuration file of LSRC

```
#
 sysname LSRC
#
 vlan batch 30 40
#
 mpls lsr-id 3.3.3.3
 mpls
  mpls te
  mpls oam
#
interface Vlanif30
 ip address 10.1.3.2 255.255.255.0
 mpls
 mpls te
#
interface Vlanif40
 ip address 10.1.4.2 255.255.255.0
 mpls
 mpls te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 40
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 30
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
interface tunnel1/0/0
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 1.1.1.1
 mpls te signal-protocol cr-static
 mpls te tunnel-id 100
 mpls te commit
#
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
```


Copyright © Huawei Technologies Co., Ltd.

```
  network 10.1.3.0 0.0.0.255
  network 10.1.4.0 0.0.0.255
#
 static-lsp egress oam lsp incoming-interface vlanif30 in-label 30 lsrid
1.1.1.1 tunnel-id 200
 static-cr-lsp ingress tunnel1/0/0 destination 1.1.1.1 nexthop 10.1.4.1 out-
label 70 bandwidth bc0 0
#
 mpls oam egress lsp-name oamlsp backward-lsp tunnel1/0/0 private
#
return
```

- Configuration file of LSRD

```
#
 sysname LSRD
#
 vlan batch 10 40
#
 mpls lsr-id 4.4.4.4
 mpls
  mpls te
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls te
#
interface Vlanif40
 ip address 10.1.4.1 255.255.255.0
 mpls
 mpls te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 40
#
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 10.1.1.0 0.0.0.255
  network 10.1.4.0 0.0.0.255
#
 static-cr-lsp transit tunnel1/0/0 incoming-interface vlanif40 in-label 70
nexthop 10.1.1.1 out-label 80 bandwidth bc0 0
#
return
```

4.6.2 Example for Configuring MPLS OAM Protection Switching

After the MPLS OAM protection switching function is configured, the interrupted services can be restored quickly if the working tunnel is faulty.

Networking Requirements

On an MPLS network shown in **Figure 4-5**, there are three bidirectional LSPs bound to three tunnel interfaces, namely, Tunnel 1/0/10, Tunnel 1/0/11, and Tunnel 1/0/12, from PE1 to PE2. Tunnel 1/0/10 and Tunnel 1/0/11 function as working tunnels; Tunnel 1/0/12 functions as the protection tunnel.

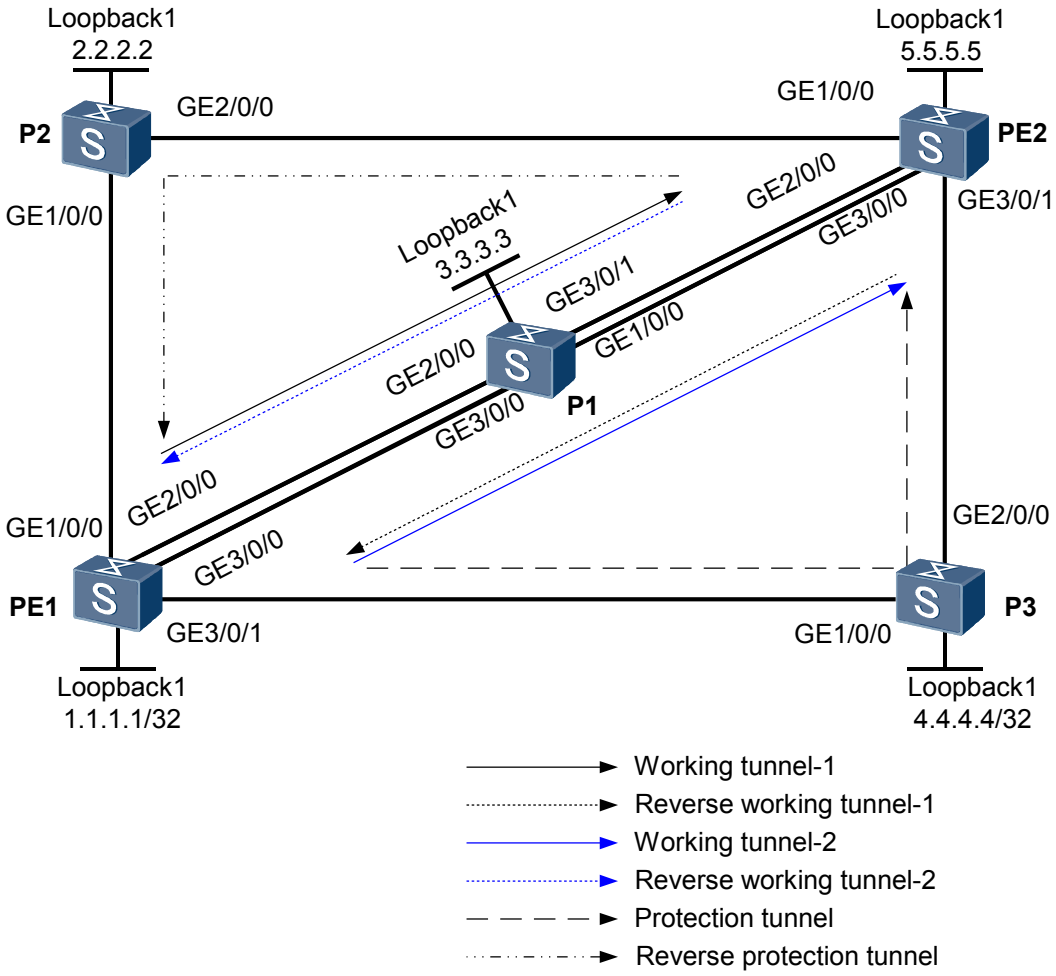
Copyright © Huawei Technologies Co., Ltd.

It is required that MPLS OAM protection switching be configured. Tunnel 1/0/12 protects Tunnel 1/0/10 and Tunnel 1/0/11. When one of the working tunnels fails, the traffic on the faulty working tunnel is switched to the protection tunnel.

NOTE

P to PE devices are the S9300s.

Figure 4-5 Networking diagram of configuring MPLS OAM protection group



Switch	Interface	VLANIF interface	IP address
PE1	GE1/0/0	VLANIF10	10.1.1.1/24
PE1	GE2/0/0	VLANIF20	10.1.2.1/24
PE1	GE3/0/0	VLANIF30	10.1.3.1/24
PE1	GE3/0/1	VLANIF40	10.1.4.1/24

Copyright © Huawei Technologies Co., Ltd.

Switch	Interface	VLANIF interface	IP address
P1	GE1/0/0	VLANIF80	10.1.8.1/24
P1	GE2/0/0	VLANIF20	10.1.2.2/24
P1	GE3/0/0	VLANIF30	10.1.3.2/24
P1	GE3/0/1	VLANIF70	10.1.7.2/24
P2	GE1/0/0	VLANIF10	10.1.1.2/24
P2	GE2/0/0	VLANIF50	10.1.5.2/24
P3	GE1/0/0	VLANIF40	10.1.4.2/24
P3	GE2/0/0	VLANIF60	10.1.6.2/24
PE2	GE1/0/0	VLANIF50	10.1.5.1/24
PE2	GE2/0/0	VLANIF70	10.1.7.1/24
PE2	GE3/0/0	VLANIF80	10.1.8.2/24
PE2	GE3/0/1	VLANIF60	10.1.6.1/24

Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and VLANIF interfaces on the nodes, assign IP addresses to the VLANIF interfaces, and configure OSPF on the VLANIF interfaces.
2. Enable MPLS, MPLS TE, and MPLS OAM on the nodes.
3. Create three TE tunnel interfaces, that is, Tunnel 1/0/10, Tunnel 1/0/11, and Tunnel 1/0/12, on PE1 and PE2, two of which function as working tunnels and the third one functions as the protection tunnel.
4. Configure two static CR-LSPs on PE1 and bind the two static CR-LSPs to Tunnel1/0/10 and Tunnel1/0/12 respectively.
5. On PE1, configure an RSVP-TE tunnel to PE2.
6. On PE2, configure three static CR-LSP as the backward LSPs to PE1 and bind the three static CR-LSPs to Tunnel 1/0/10, Tunnel 1/0/11, and Tunnel 1/0/12 respectively.
7. Set MPLS OAM parameters and enable MPLS OAM to detect bidirectional LSPs.

Data Preparation

To complete the configuration, you need the following data:

Copyright © Huawei Technologies Co., Ltd.

- IP address of the interface on each node, name of the tunnel interface, and tunnel ID
- Type of MPLS OAM detection packets
- Parameters of the protection group including delay in protection switching, revertive mode, and WTR time

Procedure

Step 1 Create VLANs and VLANIF interfaces on the nodes, assign IP addresses to the VLANIF interfaces, and configure OSPF on the VLANIF interfaces.

Configure IP addresses and masks for the interfaces, including loopback interfaces.

Configure OSPF on all the nodes and advertise the routes on the loopback interfaces. The configuration details are not mentioned here. For details on the interfaces and IP addresses of the nodes, see **Figure 4-5**.

After the configuration, LSRs can ping each other. Run the **display ip routing-table** command on each LSR, and you can view the routing entries to the LSRs.

Step 2 Enable MPLS and MPLS TE globally and on the physical interfaces.

The configuration details are not mentioned here.

Step 3 Configure tunnel interfaces.

On PE1 and PE2, configure Tunnel 1/0/10 and Tunnel 1/0/11 as working tunnels and Tunnel 1/0/12 as the protection tunnel. Tunnel 1/0/12 protects both Tunnel 1/0/10 and Tunnel 1/0/11. RSVP-TE is used on Tunnel1/0/11 and cr-static is used on Tunnel 1/0/10 and Tunnel 1/0/11.

Configure PE1.

```
<PE1> system-view
[PE1] interface tunnel1/0/10
[PE1-Tunnel1/0/10] description Working tunnel-1 to PE2
[PE1-Tunnel1/0/10] ip address unnumbered interface loopback 1
[PE1-Tunnel1/0/10] tunnel-protocol mpls te
[PE1-Tunnel1/0/10] destination 5.5.5.5
[PE1-Tunnel1/0/10] mpls te signal-protocol cr-static
[PE1-Tunnel1/0/10] mpls te tunnel-id 100
[PE1-Tunnel1/0/10] mpls te commit
[PE1-Tunnel1/0/10] quit
[PE1] interface tunnel1/0/11
[PE1-Tunnel1/0/11] description Working tunnel-2 to PE2
[PE1-Tunnel1/0/11] ip address unnumbered interface loopback 1
[PE1-Tunnel1/0/11] tunnel-protocol mpls te
[PE1-Tunnel1/0/11] destination 5.5.5.5
[PE1-Tunnel1/0/11] mpls te signal-protocol rsvp-te
[PE1-Tunnel1/0/11] mpls te tunnel-id 101
[PE1-Tunnel1/0/11] mpls te commit
[PE1-Tunnel1/0/11] quit
[PE1] interface tunnel1/0/12
[PE1-Tunnel1/0/12] description Protection tunnel to PE2
[PE1-Tunnel1/0/12] ip address unnumbered interface loopback 1
[PE1-Tunnel1/0/12] tunnel-protocol mpls te
[PE1-Tunnel1/0/12] destination 5.5.5.5
[PE1-Tunnel1/0/12] mpls te signal-protocol cr-static
[PE1-Tunnel1/0/12] mpls te tunnel-id 102
[PE1-Tunnel1/0/12] mpls te commit
[PE1-Tunnel1/0/12] quit
```

Configure PE2.

```
<PE2> system-view
[PE2] interface tunnel1/0/10
```


Copyright © Huawei Technologies Co., Ltd.

```
[PE2-Tunnel1/0/10] description Working tunnel-1 to PE1
[PE2-Tunnel1/0/10] ip address unnumbered interface loopback 1
[PE2-Tunnel1/0/10] tunnel-protocol mpls te
[PE2-Tunnel1/0/10] destination 1.1.1.1
[PE2-Tunnel1/0/10] mpls te signal-protocol cr-static
[PE2-Tunnel1/0/10] mpls te tunnel-id 100
[PE2-Tunnel1/0/10] mpls te commit
[PE2-Tunnel1/0/10] quit
[PE2] interface tunnel1/0/11
[PE2-Tunnel1/0/11] description Working tunnel-2 to PE1
[PE2-Tunnel1/0/11] ip address unnumbered interface loopback 1
[PE2-Tunnel1/0/11] tunnel-protocol mpls te
[PE2-Tunnel1/0/11] destination 1.1.1.1
[PE2-Tunnel1/0/11] mpls te signal-protocol rsvp-te
[PE2-Tunnel1/0/11] mpls te tunnel-id 101
[PE2-Tunnel1/0/11] mpls te commit
[PE2-Tunnel1/0/11] quit
[PE2] interface tunnel1/0/12
[PE2-Tunnel1/0/12] description Protection tunnel to PE1
[PE2-Tunnel1/0/12] ip address unnumbered interface loopback 1
[PE2-Tunnel1/0/12] tunnel-protocol mpls te
[PE2-Tunnel1/0/12] destination 1.1.1.1
[PE2-Tunnel1/0/12] mpls te signal-protocol cr-static
[PE2-Tunnel1/0/12] mpls te tunnel-id 102
[PE2-Tunnel1/0/12] mpls te commit
[PE2-Tunnel1/0/12] quit
```

Step 4 Configure two static CR-LSPs from PE1 to PE2, and bind them to the tunnel interfaces on PE1.

Configure PE1.

```
[PE1] static-cr-lsp ingress Tunnel1/0/10 destination 5.5.5.5 nexthop 10.1.2.2 out-
label 19
[PE1] static-cr-lsp ingress Tunnel1/0/12 destination 5.5.5.5 nexthop 10.1.4.2 out-
label 30
```

Configure P1.

```
<P1> system-view
[P1] static-cr-lsp transit PE1toPE2-2 incoming-interface vlanif 20 in-label 19
nexthop 10.1.7.1 out-label 21
```

Configure P3.

```
<P3> system-view
[P3] static-cr-lsp transit PE1toPE2-3 incoming-interface vlanif 40 in-label 30
nexthop 10.1.6.1 out-label 31
```

Configure PE2.

```
<PE2> system-view
[PE2] static-cr-lsp egress PE1toPE2-2 incoming-interface vlanif 70 in-label 21
lsrid 1.1.1.1 tunnel-id 100
[PE2] static-cr-lsp egress PE1toPE2-3 incoming-interface vlanif 60 in-label 31
lsrid 1.1.1.1 tunnel-id 102
```

After the configuration, run the **display mpls te tunnel** command on PE1 and PE2, and you can view the created TE tunnel.

Take the display on PE1 as an example.

```
[PE1] display mpls te tunnel
LSP-Id                Destination     In/Out-If
1.1.1.1:102:1        5.5.5.5         -/Vlanif40
1.1.1.1:100:1        5.5.5.5         -/Vlanif20
```

Step 5 Configure an RSVP-TE tunnel.

Configure PE1.

Copyright © Huawei Technologies Co., Ltd.

```
[PE1] mpls
[PE1-mpls] mpls rsvp-te
[PE1-mpls] mpls te cspf
[PE1-mpls] quit
[PE1] interface vlanif 30
[PE1-Vlanif30] mpls rsvp-te
[PE1-Vlanif30] quit
[PE1] ospf 1
[PE1-ospf-1] opaque-capability enable
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] mpls-te enable
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

Configure P1.

```
[P1] mpls
[P1-mpls] mpls rsvp-te
[P1-mpls] mpls te cspf
[P1-mpls] quit
[P1] interface vlanif 30
[P1-Vlanif30] mpls rsvp-te
[P1-Vlanif30] quit
[P1] interface vlanif 80
[P1-Vlanif80] mpls rsvp-te
[P1-Vlanif80] quit
[P1] ospf 1
[P1-ospf-1] opaque-capability enable
[P1-ospf-1] area 0
[P1-ospf-1-area-0.0.0.0] mpls-te enable
[P1-ospf-1-area-0.0.0.0] quit
[P1-ospf-1] quit
```

Configure PE2.

```
[PE2] mpls
[PE2-mpls] mpls rsvp-te
[PE2-mpls] mpls te cspf
[PE2-mpls] quit
[PE2] interface vlanif 80
[PE2-Vlanif80] mpls rsvp-te
[PE2-Vlanif80] quit
[PE2] ospf 1
[PE2-ospf-1] opaque-capability enable
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] mpls-te enable
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

Run the **display mpls te tunnel-interface tunnel1/0/11** command on PE1, and you can view information about Tunnel1/0/11.

```
[PE1] display mpls te tunnel-interface tunnel1/0/11
  Tunnel Name         :  Tunnel1/0/11
  Tunnel State Desc   :  CR-LSP is Up
  Tunnel Attributes   :
    LSP ID              :  1.1.1.1:0
    Session ID          :  101
    Admin State         :  UP               Oper State   :  UP
    Ingress LSR ID      :  1.1.1.1          Egress LSR ID:  5.5.5.5
    Signaling Prot      :  RSVP             Resv Style   :  SE
```

NOTE

The **display mpls te tunnel-interface tunnel1/0/11** command displays the information that needs to be noted. Information marked in "..." is omitted.

Step 6 Configure three static CR-LSPs from PE2 to PE1, and bind them to the tunnel interfaces.

Configure PE2.

Copyright © Huawei Technologies Co., Ltd.

```
[PE2] static-cr-lsp ingress Tunnel1/0/10 destination 1.1.1.1 nexthop 10.1.7.2 out-
label 21
[PE2] static-cr-lsp ingress Tunnel1/0/11 destination 1.1.1.1 nexthop 10.1.8.2 out-
label 21
[PE2] static-cr-lsp ingress Tunnel1/0/12 destination 1.1.1.1 nexthop 10.1.5.2 out-
label 31
```

Configure P1.

```
[P1] static-cr-lsp transit PE2toPE1-2 incoming-interface vlanif 70 in-label 21
nexthop 10.1.2.1 out-label 19
[P1] static-cr-lsp transit PE2toPE1-1 incoming-interface vlanif30 in-label 21
nexthop 10.1.3.1 out-label 20
```

Configure P2.

```
<P2> system-view
[P2] static-cr-lsp transit PE2toPE1-3 incoming-interface vlanif 50 in-label 31
nexthop 10.1.1.1 out-label 30
```

Configure PE1.

```
[PE1] static-cr-lsp egress PE2toPE1-2 incoming-interface vlanif 20 in-label 19
lsrid 5.5.5.5 tunnel-id 100
[PE1] static-cr-lsp egress PE2toPE1-1 incoming-interface vlanif 30 in-label 20
lsrid 5.5.5.5 tunnel-id 101
[PE1] static-cr-lsp egress PE2toPE1-3 incoming-interface vlanif 10 in-label 30
lsrid 5.5.5.5 tunnel-id 102
```

Step 7 Enable MPLS OAM and configure MPLS OAM to detect the LSP.

Configure PE1.

```
[PE1] mpls
[PE1-mpls] mpls oam
[PE1-mpls] quit
[PE1] mpls oam ingress Tunnel1/0/10
[PE1] mpls oam ingress Tunnel1/0/11
[PE1] mpls oam ingress Tunnel1/0/12
[PE1] mpls oam ingress enable all
[PE1] mpls oam egress lsp-name PE2toPE1-1
[PE1] mpls oam egress lsp-name PE2toPE1-2
[PE1] mpls oam egress lsp-name PE2toPE1-3
[PE1] mpls oam egress enable all
```

Configure PE2.

```
[PE2] mpls
[PE2-mpls] mpls oam
[PE2-mpls] quit
[PE2] mpls oam ingress Tunnel1/0/10
[PE2] mpls oam ingress Tunnel1/0/11
[PE2] mpls oam ingress Tunnel1/0/12
[PE2] mpls oam ingress enable all
[PE2] mpls oam egress lsr-id 1.1.1.1 tunnel-id 101
[PE2] mpls oam egress lsp-name PE1toPE2-2
[PE2] mpls oam egress lsp-name PE1toPE2-3
[PE2] mpls oam egress enable all
```

After the configuration, run the **display mpls oam ingress all verbose** command to check the MPLS OAM parameters and the status of the LSP, and you can view that the detected LSP is in **Non-defect** state.

Take the display on PE1 as an example.

```
[PE1] display mpls oam ingress all verbose

--------------------------------------------------------------------------------
```


Copyright © Huawei Technologies Co., Ltd.

```
Verbose information about NO.1 oam at the ingress
--------------------------------------------------------------------------------


lsp basic information:                   oam basic information:
----------------------------------------  ----------------------------------------
Tunnel-name         : Tunnel1/0/10        Oam-Index           : 512
Lsp signal status   : Up                  Oam select board    : 2
Lsp establish type  : Static lsp          Enable-state        : Manual disable
Lsp ingress lsr-id  : 1.1.1.1             Ttsi/lsr-id         : 1.1.1.1
Lsp tnl-id/Lsp-id   : 100/1              Ttsi/tunnel-id      : 100

oam detect information:                  oam backward information:
----------------------------------------  ----------------------------------------
Type                : CV                  Share attribute     : Share
Frequency           : 1 s                 Lsp-name            : --
Detect-state        : Start               Lsp ingress lsr-id  : --
Defect-state        : Non-defect          Lsp tnl-id/lsp id   : --/--
Available-state     : Available           Lsp-inLabel         : --
Unavailable time (s): 0                   Lsp signal status   : --

--------------------------------------------------------------------------------

Verbose information about NO.2 oam at the ingress
--------------------------------------------------------------------------------


lsp basic information:                   oam basic information:
----------------------------------------  ----------------------------------------
Tunnel-name         : Tunnel1/0/11        Oam-Index           : 513
Lsp signal status   : Up                  Oam select board    : 3
Lsp establish type  : RSVP-TE             Enable-state        : Manual disable
Lsp ingress lsr-id  : 1.1.1.1             Ttsi/lsr-id         : 1.1.1.1
Lsp tnl-id/Lsp-id   : 101/1              Ttsi/tunnel-id      : 101

oam detect information:                  oam backward information:
----------------------------------------  ----------------------------------------
Type                : CV                  Share attribute     : Share
Frequency           : 1 s                 Lsp-name            : --
Detect-state        : Start               Lsp ingress lsr-id  : --
Defect-type         : Non-defect          Lsp tnl-id/lsp id   : --/--
Available-state     : Available           Lsp-inLabel         : --
Unavailable time (s): 0                   Lsp signal status   : --

--------------------------------------------------------------------------------

Verbose information about NO.3 oam at the ingress
--------------------------------------------------------------------------------


lsp basic information:                   oam basic information:
----------------------------------------  ----------------------------------------
Tunnel-name         : Tunnel1/0/12        Oam-Index           : 514
Lsp signal status   : Up                  Oam select board    : 4
Lsp establish type  : Static lsp          Enable-state        : Manual disable
Lsp ingress lsr-id  : 1.1.1.1             Ttsi/lsr-id         : 1.1.1.1
Lsp tnl-id/Lsp-id   : 102/1              Ttsi/tunnel-id      : 102

oam detect information:                  oam backward information:
----------------------------------------  ----------------------------------------
Type                : CV                  Share attribute     : Share
Frequency           : 1 s                 Lsp-name            : --
Detect-state        : Start               Lsp ingress lsr-id  : --
Defect-type         : Non-defect          Lsp tnl-id/lsp id   : --/--
Available-state     : Available           Lsp-inLabel         : --
Unavailable time (s): 0                   Lsp signal status   : --

--------------------------------------------------------------------------------
```


Copyright © Huawei Technologies Co., Ltd.

```
Total Oam Num:                   3
Total Start Oam Num:             3
Total Defect Oam Num:            0
Total Unavailable Oam Num:       0
```

Step 8 Configure the protection group.

On PE1, configure Tunnel 1/0/10 and Tunnel 1/0/11 as working tunnels and Tunnel 1/0/12 as the protection tunnel, use the revertive mode, and set WTR time to 2 minutes.

```
[PE1] interface tunnel 1/0/10
[PE1-Tunnel1/0/10] mpls te protection tunnel 12 mode revertive wtr 4
[PE1-Tunnel1/0/10] mpls te commit
[PE1-Tunnel1/0/10] quit
[PE1] interface tunnel 1/0/11
[PE1-Tunnel1/0/11] mpls te protection tunnel 12 mode revertive wtr 4
[PE1-Tunnel1/0/11] mpls te commit
[PE1-Tunnel1/0/11] quit
```

After this step, run the **display mpls te protection tunnel all** commands on PE devices, and you can view that all tunnels are in **Non-defect** state and the working tunnels forward traffic.

Take the display on PE1 as an example.

```
[PE1] display mpls te protection tunnel all
------------------------------------------------------------------------------
No. Work-tunnel status  /id  Protect-tunnel status /id    Switch-Result
------------------------------------------------------------------------------
1          non-defect   /100       non-defect     /102    work-tunnel
2          non-defect   /101       non-defect     /102    work-tunnel
```

Run the **display mpls te protection binding protect-tunnel** commands on PE devices, and you can view that Tunnel 1/0/12 protects Tunnel 1/0/10 and Tunnel 1/0/10.

Take the display on PE1 as an example.

```
[PE1] display mpls te protection binding protect-tunnel 12
------------------------------------------------------------------------------
Binding information of( tunnel id:  102 )
------------------------------------------------------------------------------
    Protect-tunnel id                    :102
    Protect-tunnel name                  :Tunnel1/0/12
    Maximum number of bound work-tunnels :8
    Currently bound work-tunnels         :Total( 2 )
                                         :Tunnel1/0/10
                                         :Tunnel1/0/11
```

Step 9 Verify the configuration.

Run the **display mpls te protection tunnel interface tunnel** *interface-number* **verbose** commands on PE devices, and you can view detailed information about the protection group. Take the display of Tunnel 1/0/10 on PE1 as an example.

```
[PE1] display mpls te protection tunnel interface tunnel 1/0/10 verbose
------------------------------------------------------------------
Verbose information about the  1th proteciton-group
------------------------------------------------------------------
Work-tunnel id                          : 100
Protect-tunnel id                       : 102
Work-tunnel name                        : Tunnel1/0/10
Protect-tunnel name                     : Tunnel1/0/12
Work-tunnel reverse-lsp name            : PE2toPE1-1
Protect-tunnel reverse-lsp name         : PE2toPE1-3
switch result                           : work-tunnel
work-tunnel defect state                : non-defect
protect-tunnel defect state             : non-defect
work-tunnel reverse-lsp defect state    : non-defect
protect-tunnel reverse-lsp defect state : non-defect
HoldOff                                 : 0ms
```


Copyright © Huawei Technologies Co., Ltd.

```
WTR                                     : 120s
Mode                                    : revertive
```

Run the **mpls te protect-switch manual work-lsp** command on Tunnel 1/0/10 of PE1 to manually trigger protection switching.

```
[PE1] interface tunnel1/0/10
[PE1] mpls te protect-switch manual work-lsp
```

Run the **display mpls te protection tunnel all** command on PE1, and you can view that the "Switch-Result" field on Tunnel 1/0/10 is displayed as **protect-tunnel**.

```
[PE1] display mpls te protection tunnel all
------------------------------------------------------------------------------
No. Work-tunnel status  /id  Protect-tunnel status /id      Switch-Result
------------------------------------------------------------------------------
1          non-defect   /100       non-defect     /102   protect-tunnel
2          non-defect   /101       non-defect     /102      work-tunnel
```

Run the **shutdown** command on VLANIF 40 of PE1 to simulate defects on a physical link of the protection tunnel.

```
[PE1] interface vlanif 40
[PE1-Vlanif40] shutdown
[PE1-Vlanif400] quit
```

Run the **display mpls te protection tunnel all** command on PE1, and you can view that the "Protect-tunnel status" field on Tunnel 1/0/10 is displayed as **in-defect** and the "Switch-Result" field is displayed as **work-tunnel**.

```
[PE1] display mpls te protection tunnel all
------------------------------------------------------------------------------
No. Work-tunnel status  /id  Protect-tunnel status /id    Switch-Result
------------------------------------------------------------------------------
1          non-defect   /100        in-defect     /102    work-tunnel
2          non-defect   /101       non-defect     /102    work-tunnel
```

NOTE

When no defects occur on all the tunnels, and the **mpls te protect-switch manual work-lsp** command is used in the tunnel interface view of the working tunnel, the traffic is switched to the protection tunnel. In this case, if the link of the protection tunnel fails, the traffic then is switched back to the working tunnel and the **mpls te protect-switch manual work-lsp** command in the tunnel interface view of the working tunnel is deleted. This is because the link defect triggers the switching request in Signaling Failure node and Signaling Failure takes precedence over Manual Switch.

----End

Configuration Files

- Configuration file of PE1

```
#
 sysname PE1
#
 vlan batch 10 20 30 40
#
 mpls lsr-id 1.1.1.1
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
  mpls oam
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls te
```


Copyright © Huawei Technologies Co., Ltd.

```
#
interface Vlanif20
 ip address 10.1.2.1 255.255.255.0
 mpls
 mpls te
#
interface Vlanif30
 ip address 10.1.3.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif40
 ip address 10.1.4.1 255.255.255.0
 mpls
 mpls te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface GigabitEthernet3/0/0
 port link-type access
 port default vlan 30
#
interface GigabitEthernet4/0/0
 port link-type access
 port default vlan 40
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
interface Tunnel1/0/10
 description Working tunnel-1 to PE2
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 5.5.5.5
 mpls te signal-protocol cr-static
 mpls te tunnel-id 100
 mpls te protection tunnel 12 mode revertive wtr 4
 mpls te commit
#
interface Tunnel1/0/11
 description Working tunnel-2 to PE2
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 5.5.5.5
 mpls te tunnel-id 101
 mpls te protection tunnel 12 mode revertive wtr 4
 mpls te commit
#
interface Tunnel1/0/12
 description Protection tunnel to PE2
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 5.5.5.5
 mpls te signal-protocol cr-static
 mpls te tunnel-id 102
 mpls te commit
#
ospf 100
 opaque-capability enable
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 10.1.1.0 0.0.0.255
```


Copyright © Huawei Technologies Co., Ltd.

```
  network 10.1.2.0 0.0.0.255
  network 10.1.3.0 0.0.0.255
  network 10.1.4.0 0.0.0.255
  mpls-te enable
#
 static-cr-lsp ingress Tunnel1/0/10 destination 5.5.5.5 nexthop 10.1.2.2 out-
label 19
 static-cr-lsp ingress Tunnel1/0/12 destination 5.5.5.5 nexthop 10.1.4.2 out-
label 30
 static-cr-lsp egress PE2toPE1-2 incoming-interface vlanif20 in-label 19 lsrid
1.1.1.1 tunnel-id 100
 static-cr-lsp egress PE2toPE1-1 incoming-interface vlanif30 in-label 20 lsrid
1.1.1.1 tunnel-id 101
 static-cr-lsp egress PE2toPE1-3 incoming-interface vlanif10 in-label 30 lsrid
1.1.1.1 tunnel-id 102
#
 mpls oam ingress Tunnel1/0/10
 mpls oam ingress Tunnel1/0/11
 mpls oam ingress Tunnel1/0/12
 mpls oam ingress enable all
 mpls oam egress lsp-name PE2toPE1-1
 mpls oam egress lsp-name PE2toPE1-2
 mpls oam egress lsp-name PE2toPE1-3
 mpls oam egress enable all
#
return
```

- Configuration file of P2

```
#
 sysname P2
#
 vlan batch 10 50
#
 mpls lsr-id 2.2.2.2
 mpls
  mpls te
#
interface Vlanif10
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls te
#
interface Vlanif50
 ip address 10.1.5.2 255.255.255.0
 mpls
 mpls te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 50
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
ospf 100
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.5.0 0.0.0.255
#
 static-cr-lsp transit PE2toPE1-3 incoming-interface vlanif 50 in-label 31
nexthop 10.1.1.1 out-label 30
#
return
```

- Configuration file of P1

Copyright © Huawei Technologies Co., Ltd.

```
#
 sysname P1
#
 vlan batch 20 30 70 80
#
 mpls lsr-id 3.3.3.3
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
#
interface Vlanif20
 ip address 10.1.2.2 255.255.255.0
 mpls
 mpls te
#
interface Vlanif30
 ip address 10.1.3.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif70
 ip address 10.1.7.2 255.255.255.0
 mpls
 mpls te
#
interface Vlanif80
 ip address 10.1.8.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 80
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 20
#
interface GigabitEthernet3/0/0
 port link-type access
 port default vlan 30
#
interface GigabitEthernet4/0/0
 port link-type access
 port default vlan 70
#
interface LoopBack1
 ip address 3.3.3.3 255.255.255.255
#
ospf 100
 opaque-capability enable
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 10.1.3.0 0.0.0.255
  network 10.1.7.0 0.0.0.255
  network 10.1.8.0 0.0.0.255
  mpls-te enable
#
 static-cr-lsp transit PE1toPE2-2 incoming-interface vlanif20 in-label 19
nexthop 10.1.7.1 out-label 21
 static-cr-lsp transit PE2toPE1-2 incoming-interface vlanif70 in-label 21
nexthop 10.1.2.1 out-label 19
 static-cr-lsp transit PE2toPE1-1 incoming-interface vlanif80 in-label 21
nexthop 10.1.3.1 out-label 20
```


Copyright © Huawei Technologies Co., Ltd.

```
#
return
```

- Configuration file of P3

```
#
 sysname P3
#
 vlan batch 40 60
#
 mpls lsr-id 4.4.4.4
 mpls
  mpls te
#
interface Vlanif40
 ip address 10.1.4.2 255.255.255.0
 mpls
 mpls te
#
interface Vlanif60
 ip address 10.1.6.2 255.255.255.0
 mpls
 mpls te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 40
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 60
#
interface LoopBack1
 ip address 4.4.4.4 255.255.255.255
#
ospf 100
 area 0.0.0.0
  network 4.4.4.4 0.0.0.0
  network 10.1.4.0 0.0.0.255
  network 10.1.6.0 0.0.0.255
#
 static-cr-lsp transit PE1toPE2-3 incoming-interface vlanif40 in-label 30
nexthop 10.1.6.1 out-label 31
#
return
```

- Configuration file of PE2

```
#
 sysname PE2
#
 vlan batch 50 60 70 80
#
 mpls lsr-id 5.5.5.5
 mpls
  mpls te
  mpls rsvp-te
  mpls te cspf
  mpls oam
#
interface Vlanif50
 ip address 10.1.5.1 255.255.255.0
 mpls
 mpls te
#
interface Vlanif60
 ip address 10.1.6.1 255.255.255.0
 mpls
 mpls te
#
interface Vlanif70
 ip address 10.1.7.1 255.255.255.0
```


Copyright © Huawei Technologies Co., Ltd.

```
 mpls
 mpls te
#
interface Vlanif80
 ip address 10.1.8.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet1/0/0
 port link-type access
 port default vlan 50
#
interface GigabitEthernet2/0/0
 port link-type access
 port default vlan 70
#
interface GigabitEthernet3/0/0
 port link-type access
 port default vlan 80
#
interface GigabitEthernet4/0/0
 port link-type access
 port default vlan 60
#
interface LoopBack1
 ip address 5.5.5.5 255.255.255.255
#
interface Tunnel1/0/10
 description Working tunnel-1 to PE1
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 1.1.1.1
 mpls te signal-protocol static
 mpls te tunnel-id 100
 mpls te protection tunnel 12 mode revertive wtr 4
 mpls te commit
#
interface Tunnel1/0/11
 description Working tunnel-2 to PE1
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 1.1.1.1
 mpls te signal-protocol static
 mpls te tunnel-id 101
 mpls te protection tunnel 12 mode revertive wtr 4
 mpls te commit
#
interface Tunnel1/0/12
 description Protection tunnel to PE1
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 1.1.1.1
 mpls te signal-protocol static
 mpls te tunnel-id 102
 mpls te commit
#
ospf 100
 opaque-capability enable
 area 0.0.0.0
  network 5.5.5.5 0.0.0.0
  network 10.1.5.0 0.0.0.255
  network 10.1.6.0 0.0.0.255
  network 10.1.7.0 0.0.0.255
  network 10.1.8.0 0.0.0.255
  mpls-te enable
#
 static-cr-lsp ingress Tunnel1/0/10 destination 1.1.1.1 nexthop 10.1.7.2 out-
label 21
```


Copyright © Huawei Technologies Co., Ltd.

```
 static-cr-lsp ingress Tunnel1/0/11 destination 1.1.1.1 nexthop 10.1.8.2 out-
label 21
 static-cr-lsp ingress Tunnel1/0/12 destination 1.1.1.1 nexthop 10.1.5.2 out-
label 31
 static-cr-lsp egress PE1toPE2-2 incoming-interface vlanif70 in-label 21 lsrid
1.1.1.1 tunnel-id 100
 static-cr-lsp egress PE1toPE2-3 incoming-interface vlanif60 in-label 31 lsrid
1.1.1.1 tunnel-id 102
#
 mpls oam ingress Tunnel1/0/10
 mpls oam ingress Tunnel1/0/11
 mpls oam ingress Tunnel1/0/12
 mpls oam ingress enable all
 mpls oam egress lsr-id 1.1.1.1 tunnel-id 101
 mpls oam egress lsp-name PE1toPE2-2
 mpls oam egress lsp-name PE1toPE2-3
 mpls oam egress enable all
#
return
```


Copyright © Huawei Technologies Co., Ltd.