9 MPLS Configuration Commands

9.1 Basic MPLS Configuration Commands

9.1.1 Command Support

Only the following switch models support MPLS:

S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H

9.1.2 authentication exclude

Function

The **authentication exclude** command configures LDP peers in a batch that a local device does not authenticate after LDP keychain or LDP MD5 is configured to authenticate all LDP peers or LDP peers in a specified group.

The **undo authentication exclude** command enables a local device to authenticate all LDP peers using LDP keychain or LDP MD5.

By default, a local device is enabled to authenticate all LDP peers using LDP keychain or LDP MD5.

Format

authentication exclude peer *peer-id*

undo authentication exclude peer *peer-id*

Parameters

Parameter	Description	Value
peer *peer-id*	Specifies the ID of an LDP peer.	This value is in dotted decimal notation.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a local device is enabled to authenticate all LDP peers using LDP keychain or LDP MD5 after LDP keychain or LDP MD5 is configured for a peer group or all LDP peers. To disable the local device from authenticating some LDP peers, run the **authentication exclude** command.

Precautions

The following commands are mutually exclusive for a specified LDP peer:

- **authentication key-chain peer** *peer-id* **name** *keychain-name*
- **md5-password** { **plain** | **cipher** } *peer-lsr-id password*

Example

# Disable a local device from authenticating an LDP peer with IP address **10.1.1.1** after LDP keychain or MD5 is configured for all LDP peers or LDP peers in a specified group.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] authentication exclude peer 10.1.1.1
```

9.1.3 authentication key-chain

Function

The **authentication key-chain** command enables Label Distribution Protocol (LDP) keychain authentication.

The **undo authentication key-chain** command disables Label Distribution Protocol (LDP) keychain authentication.

By default, LDP keychain authentication is disabled.

Format

authentication key-chain peer *peer-id* **name** *keychain-name*

undo authentication key-chain peer *peer-id*

Parameters

Parameter	Description	Value
peer *peer-id*	Specifies the ID of an LDP peer enabled with LDP keychain. The parameter is specified in the **mpls lsr-id** command.	The value is in dotted decimal notation.
name *keychain-name*	Specifies the keychain name. The keychain name is specified in the **keychain** command.	The value is an existing keychain name.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Information spoofing may occur during an LDP session. To enhance security of an LDP session, configure keychain authentication for a TCP connection over which an LDP session is created.

During keychain authentication, a group of passwords are defined to form a password string, and each password is specified with the encryption and decryption algorithms such as MD5 and SHA-1, and is configured with a validity period. When sending or receiving a packet, the system selects a valid password based on the user's configuration. Within the password validity period, the system either uses the encryption algorithm matching the password to encrypt the packet before sending it or uses the decryption algorithm matching the password to decrypt the packet before receiving it. In addition, the system automatically uses a new password after the previous one expires, preventing the password from being decrypted.

The keychain authentication password, the encryption and decryption algorithms, and password validity period that construct a keychain configuration node are configured using different commands. A keychain configuration node requires at least one password along with encryption and decryption algorithms.

To reference a keychain configuration node, specify the required peer and the node name in the MPLS-LDP view. In this manner, an LDP session is encrypted. Different peers can reference the same keychain configuration node.

Keychain authentication involves a set of passwords. It uses a new password when the previous one expires. Keychain authentication is complex to configure and is therefore recommended only for networks requiring high security.

Prerequisites

You have performed the following operations:

- Enable MPLS LDP globally using the **mpls ldp (system view)** command.
- Configure keychain authentication globally using the **keychain** command.

Precautions

- MD5 authentication and keychain authentication cannot be configured together on one peer.
- Configuring LDP keychain authentication leads to reestablishment of an LDP session and deletes the Label Switched Path (LSP) associated with the LDP session.

Example

# Configure LDP keychain authentication for the peer with an LSR ID of **10.1.1.1**. The referenced keychain name is **kc1**.

```
<HUAWEI> system-view
[HUAWEI] keychain kc1 mode absolute
[HUAWEI-keychain-kc1] quit
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] authentication key-chain peer 10.1.1.1 name kc1
```

9.1.4 authentication key-chain all

Function

The **authentication key-chain all** command enables keychain authentication in a batch for all LDP peers.

The **undo authentication key-chain all** command disables keychain authentication in a batch for all LDP peers.

By default, keychain authentication in a batch is disabled for all LDP peers. LDP keychain authentication is recommended to ensure security.

Format

authentication key-chain all name *keychain-name*

undo authentication key-chain all

Parameters

Parameter	Description	Value
name *keychain-name*	Specifies a keychain name. The keychain name is configured using the **keychain** command.	The value is a string of 1 to 47 case-insensitive characters. The string does not contain question marks or spaces. The string can contain spaces if it is enclosed with double quotation marks (").

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve LDP session security, keychain authentication can be configured for a TCP connection over which an LDP session has been established. If a great number of LDP peers are configured, run the **authentication key-chain all** command to enable keychain authentication in a batch for all LDP peers.

Prerequisites

A keychain has been configured using the **keychain** command.

Precautions

- LDP authentication configurations are prioritized in descending order: for a single peer, for a specified peer group, for all peers. Keychain and MD5 configurations of the same priority are mutually exclusive. Keychain authentication and MD5 authentication can be configured simultaneously for a specified LDP peer, for this LDP peer in a specified peer group, and for all LDP peers. The configuration with a higher priority takes effect. For example, if MD5 authentication is configured for Peer1 and then keychain authentication is configured for all LDP peers, MD5 authentication takes effect on Peer1. Keychain authentication takes effect on other peers.
- Configuring LDP keychain authentication causes the reestablishment of LDP sessions.
- After the **authentication key-chain all** command is run, the referenced keychain is applied to all LDP peers. If keychain authentication fails, an LDP session fails to be established.

Example

# Configure LDP keychain authentication for all LDP peers and use the keychain named **kc1**.

```
<HUAWEI> system-view
[HUAWEI] keychain kc1 mode absolute
[HUAWEI-keychain-kc1] key-id 1
[HUAWEI-keychain-kc1-keyid-1] algorithm sha-256
[HUAWEI-keychain-kc1-keyid-1] key-string YsHsjx_202206
[HUAWEI-keychain-kc1-keyid-1] send-time 14:30 2016-10-10 to 14:50 2016-10-10
[HUAWEI-keychain-kc1-keyid-1] receive-time 14:40 2016-10-10 to 14:50 2016-10-10
[HUAWEI-keychain-kc1-keyid-1] default send-key-id
[HUAWEI-keychain-kc1-keyid-1] quit
[HUAWEI-keychain-kc1] quit
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] authentication key-chain all name kc1
```

9.1.5 authentication key-chain peer-group

Function

The **authentication key-chain peer-group** command enables keychain authentication in a batch for a specified LDP peer group.

The **undo authentication key-chain peer-group** command disables keychain authentication in a batch for a specified LDP peer group.

By default, keychain authentication in a batch is disabled for all peer groups. LDP keychain authentication is recommended to ensure security.

Format

authentication key-chain peer-group *ip-prefix-name* **name** *keychain-name*

undo authentication key-chain peer-group

Parameters

Parameter	Description	Value
ip-prefix-name	Specifies the name of an IP prefix list. The IP prefix list name is configured using the **ip ip-prefix** command.	The value is a string of 1 to 169 case-sensitive characters, spaces not supported. The string can contain spaces if it is enclosed with double quotation marks (").
name *keychain-name*	Specifies a keychain name. The keychain name is configured using the **keychain** command.	The value is a string of 1 to 47 case-insensitive characters. The string does not contain question marks or spaces. The string can contain spaces if it is enclosed with double quotation marks (").

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To help improve LDP session security, keychain authentication can be configured for a TCP connection over which an LDP session has been established. If a great number of LDP peers are configured, run the **authentication key-chain peer-group** command to enable keychain authentication in a batch for LDP peers in a specified peer group. An IP prefix list can be specified to define the range of IP addresses in a group.

Prerequisites

The following steps have been performed:

- An IP prefix list has been configured using the **ip ip-prefix** command.
- A keychain has been configured using the **keychain** command.

Precautions

- LDP authentication configurations are prioritized in descending order: for a single peer, for a specified peer group, for all peers. Keychain and MD5 configurations of the same priority are mutually exclusive. Keychain authentication and MD5 authentication can be configured simultaneously for a specified LDP peer, for this LDP peer in a specified peer group, and for all LDP peers. The configuration with a higher priority takes effect. For example, if MD5 authentication is configured for Peer1 and then keychain authentication is configured for all LDP peers, MD5 authentication takes effect on Peer1.
- Configuring LDP keychain authentication causes the reestablishment of LDP sessions.
- After the **authentication key-chain peer-group** command is run, the referenced Keychain authentication is applied to a specified peer. If keychain authentication fails, an LDP session fails to be established.
- Before a peer group is referenced, create it. By default, a nonexistent peer group cannot be specified in this command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent peer group is specified in this command, a local device performs keychain authentication for each LDP session connected to each LDP peer.

Example

# Enable LDP keychain authentication for LDP peers with IP addresses matching the IP prefix list named **list1** in a specified peer group and use a keychain named **kc1**.

```
<HUAWEI> system-view
[HUAWEI] keychain kc1 mode absolute
[HUAWEI-keychain-kc1] key-id 1
[HUAWEI-keychain-kc1-keyid-1] algorithm sha-256
[HUAWEI-keychain-kc1-keyid-1] key-string YsHsjx_202206
[HUAWEI-keychain-kc1-keyid-1] send-time 14:30 2016-10-10 to 14:50 2016-10-10
[HUAWEI-keychain-kc1-keyid-1] receive-time 14:40 2016-10-10 to 14:50 2016-10-10
[HUAWEI-keychain-kc1-keyid-1] default send-key-id
[HUAWEI-keychain-kc1-keyid-1] quit
[HUAWEI-keychain-kc1] quit
[HUAWEI] ip ip-prefix list1 permit 10.1.1.1 32
```

```
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] authentication key-chain peer-group list1 name kc1
```

9.1.6 auto-frr lsp-trigger

Function

The **auto-frr lsp-trigger** command configures a policy for triggering LDP to establish backup LSPs based on backup routes.

The **undo auto-frr lsp-trigger** command restores the default setting.

By default, LDP uses backup routes with 32-bit addresses to establish backup LSPs.

Format

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

undo auto-frr lsp-trigger

Parameters

Parameter	Description	Value
all	Specifies all backup routes to trigger LDP to establish backup LSPs.	-
host	Specifies backup routes with 32-bit addresses to trigger LDP to establish backup LSPs.	-
ip-prefix *ip-prefix-name*	Specifies IP prefix list to trigger LDP to establish backup LSPs.	The value is an existing IP prefix list name.
none	Specifies no backup routes to trigger LDP to establish backup LSPs.	-

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an MPLS network with a backup link, if a link fault occurs, Interior Gateway Protocol (IGP) routes converge and routes related to the backup link become available. After IGP route convergence is complete, an LDP LSP over the backup link becomes available. During this process, traffic is interrupted. To prevent traffic interruption, you can configure LDP fast reroute (FRR). On the network enabled with LDP FRR, if an interface failure (detected by the interface itself or by an associated BFD session) or a primary LSP failure (detected by an associated BFD session) occurs, LDP FRR is notified of the failure and rapidly forwards traffic to a backup LSP, protecting traffic on the primary LSP. The traffic switchover is performed within 50 milliseconds, avoiding traffic interruption.

LDP FRR is classified into the following types:

- LDP manual FRR: A backup LSP is configured manually by specifying an outbound interface or a next hop. The configuration is complex but flexible because a backup LSP can be configured manually. LDP manual FRR applies to simple networks.
- Auto LDP FRR: A backup LSP is automatically created based on a specified policy. The configuration is simple and loop-free. Auto LDP FRR applies to complex and large networks.

Auto LDP FRR depends on the automatic reroute function of IGP. Auto LDP FRR is automatically enabled after IGP automatic reroute is enabled using the **frr (IS-IS)** command. To change the policy for triggering LDP to establish backup LSPs, run the **auto-frr lsp-trigger** command.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp(system view)** command in the system view.

Precautions

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

If both the **auto-frr lsp-trigger** command and the **lsp-trigger** command are run, the established backup LSPs are controlled by both the policy for triggering LDP LSP establishment and the policy for triggering backup LDP LSP establishment. For example, if the policy for triggering LDP LSP establishment is **none** and that for triggering backup LDP LSP establishment is **all**, the backup LDP LSP is established using the **none** policy.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all backup routes trigger backup LDP LSP establishment.

Example

#Configure the policy for specifying no backup routes to trigger LDP to establish backup LSPs.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] auto-frr lsp-trigger none
```

9.1.7 backoff timer

Function

The **backoff timer** command sets the initial and maximum values for an Exponential backoff timer.

The **undo backoff timer** command restores the default settings.

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

Format

backoff timer *init max*

undo backoff timer

Parameters

Parameter	Description	Value
init	Specifies the initial value of an Exponential backoff timer.	The value is an integer ranging from 5 to 2147483, in seconds.
max	Specifies the maximum value of an Exponential backoff timer.	The value is an integer ranging from 5 to 2147483, in seconds.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an LSR fails to process an LDP Initialization message or is informed that the peer LSR rejects the received LDP Initialization message, the LSR starts the Exponential backoff timer and periodically resends an LDP Initialization message to initiate an LDP session before the Exponential backoff timer expires.

When the Exponential backoff timer starts, the active role waits a period of time equal to the initial value of the Exponential backoff timer to attempt to set up an LDP session for the first time. Subsequently, the active role waits a period of time twice as long as the previous one to attempt to set up an LDP session. When the waiting period reaches the maximum value of the Exponential backoff timer, the active role waits a period of time equal to the maximum value of the Exponential backoff timer to attempt to set up an LDP session.

Run the **backoff timer** command to change the interval at which the active role attempts to set up a session.

By setting the initial value and maximum value for the Exponential backoff timer, you can flexibly control the reestablishment of sessions in different network environments.

- When a device is being upgraded, increase the initial and maximum values to set a large interval at which the active role attempts to set up a session.
- When a device that is transmitting services is prone to intermittent disconnections, reduce the initial and maximum values to set a small interval at which the active role attempts to set up a session.

NOTE

The initial value for the Exponential backoff timer cannot be smaller than 15, and the maximum value cannot be smaller than 120.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp (system view)** command.

Precautions

If a session is disconnected after the **backoff timer** command is run, the device attempts to set up a session based on the set initial and maximum values of the Exponential backoff timer.

Example

# Set the initial value to 20s and the maximum value to 160s for the Exponential backoff timer.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] backoff timer 20 160
```

9.1.8 bfd bind ldp-lsp

Function

The **bfd bind ldp-lsp** command creates a bidirectional forwarding detection (BFD) session for detecting LDP LSPs.

The **undo bfd** command deletes a specified BFD session.

By default, no BFD session is created for detecting LDP LSPs.

Format

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

undo bfd *cfg-name*

Parameters

Parameter	Description	Value
cfg-name	Specifies the name of a BFD session.	The value is a string of 1 to 15 case-insensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
peer-ip *ip-address*	Specifies the peer IP address bound to the BFD session.	The value is in dotted decimal notation.
nexthop*ip-address*	Specifies the next hop IP address of the detected LSP.	The value is in dotted decimal notation.
interface*interface-type interface-number*	Specifies the outbound interface that is bound to a BFD session. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A dynamic LSP is established using LDP on an MPLS network. It takes an interface a long period of time to detect a link fault. After a static BFD session is bound to the LDP LSP, the interface can quickly detect faults on LDP LSPs. This method applies to small networks.

Prerequisites

BFD has been enabled globally using the **bfd** command.

Precautions

- When the IP address of the outbound interface of the detected LSP is lent or borrowed, an outbound interface must be specified.

- When the LDP LSP is deleted but the LDP session exists, the BFD session is in Down state, but the configuration of the BFD session bound to the LDP session is not deleted.
- When configuring static BFD for LDP LSP on a network deployed with LDP over TE, specify **interface** *interface-type interface-number* as the tunnel interface.

Example

# Create a BFD session to detect the LDP LSP with the egress IP address being 10.2.1.1, the next hop IP address being 10.1.1.1, and the outbound interface being VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd 1to4 bind ldp-lsp peer-ip 10.2.1.1 nexthop 10.1.1.1 interface vlanif 100
[HUAWEI-bfd-lsp-session-1to4]
```

9.1.9 bfd bind static-lsp

Function

The **bfd bind static-lsp** command creates a BFD session to detect static LSPs.

The **undo bfd** command deletes a specified BFD session.

By default, no BFD session is created to detect static LSPs.

Format

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

undo bfd *cfg-name*

Parameters

Parameter	Description	Value
cfg-name	Specifies the BFD configuration name.	The value is a string of 1 to 15 case-insensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
lsp-name	Specifies the name of the static LSP bound to the BFD session.	The value is an existing static LSP name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can deploy MPLS services by manually configuring static LSPs on small networks with simple topology and stable performance. It takes an interface a long period of time to detect a link fault. After a static BFD session is bound to the LDP LSP, the interface can quickly detect faults on LDP LSPs.

Prerequisites

BFD has been enabled globally using the **bfd** command in the system view.

Precautions

- If the specified static LSP does not exist or the BFD configuration name exists, the BFD session cannot be created.
- The **commit** command must be run to make the configured BFD parameters take effect before a BFD session is created.
- When the status of the static LSP is Down, a BFD session cannot be created.

Example

# Create a BFD session to detect the static LSP named **1to4**.

```
<HUAWEI> system-view
[HUAWEI] bfd bfd1to4 bind static-lsp 1to4
[HUAWEI-bfd-lsp-session-bfd1to4]
```

9.1.10 display default-parameter mpls ldp

Function

The **display default-parameter mpls ldp** command displays the default configurations of MPLS LDP.

Format

display default-parameter mpls ldp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the default configurations of MPLS LDP, run the **display default-parameter mpls ldp** command.

Example

# Display the default configurations of MPLS LDP.

```
<HUAWEI> display default-parameter mpls ldp

 LDP Default Values:
 ---------------------------------------------------------
         Protocol version               : V1
         Graceful restart               : Off
           Neighbor liveness(sec)       : 600
           FT reconnect timer(sec)      : 300
           Recovery timer(sec)          : 300
         MTU signaling                  : On
         Label retention mode           : Liberal
         Label distribution mode        : Ordered
         Label advertisement            : DU
         Local hello-hold timer(sec)    : 15
         Remote hello-hold timer(sec)   : 45
         Keepalive-hold timer(sec)      : 45
         Backoff timer init(sec)        : 15
         Backoff timer max(sec)         : 120
         IGP-Sync delay timer(sec)      : 10
         Graceful delete                : Off
           Graceful delete timer(sec)   : 5
         Capability-announcement        : Off
         mLDP MBB Capability            : Off
           Wait-ack timer(sec)          : 10
           Switch-delay timer(ms)       : 100
         mLDP P2MP Capability           : Off
         mLDP MP2MP Capability          : Off
         Label withdraw-delay           : Off
           Withdraw-delay timer(sec)    : 5
         Send LSP down reason           : Off
         Ingress LSP Load-balance Num   : 16
         Transit LSP Load-balance Num   : 16
         Smart-policy Ingress           : Off
         Smart-policy Auto-dod-request  : Off
         Label default-route            : Off
 ---------------------------------------------------------
```

Table 9-1 Description of the **display default-parameter mpls ldp** command output

Item	Description
Protocol version	LDP version number.
Graceful restart	LDP GR capability status. ● On: LDP GR is enabled. ● Off: LDP GR is disabled. By default, LDP GR is disabled. You can configure the LDP GR capability status using the **graceful-restart** command.

Item	Description
Neighbor liveness(sec)	Value of the neighbor-liveness timer, in seconds. The default value is 600s. You can set this value using the **graceful-restart timer neighbor-liveness** command.
FT reconnect timer(sec)	Value of the reconnect timer of an LDP session, in seconds. The default value is 300s. You can set this value using the **graceful-restart timer reconnect** command.
Recovery timer(sec)	Value of the recovery timer of an LDP LSP, in seconds. The default value is 300s. You can set this value using the **graceful-restart timer recovery** command.
MTU signaling	MTU TLV status. ● On: MTU TLV is enabled. ● Off: MTU TLV is disabled. By default, MTU TLV is enabled.
Label retention mode	LDP label retention modes include: ● Liberal: free mode. ● Conservative: conservative mode. The default label retention mode is liberal.
Label distribution mode	LDP label distribution mode. Currently, only the ordered mode is supported.
Label advertisement	LDP label advertisement modes include: ● DU: downstream unsolicited mode. ● DOD: downstream on demand mode. The default label advertisement mode is DU. You can set the LDP label advertisement mode using the **mpls ldp advertisement** command.
Local hello-hold timer(sec)	Value of the local Hello hold timer, in seconds. The default value is 15s. You can set this value using the **mpls ldp timer hello-hold** command.
Remote hello-hold timer(sec)	Value of the remote Hello hold timer, in seconds. The default value is 45s. You can set this value using the **mpls ldp timer hello-hold** command.
Keepalive-hold timer(sec)	Value of the keepalive hold timer for the local and remote LDP sessions, in seconds. The default value is 45s. You can set this value using the **mpls ldp timer keepalive-hold** command.
Backoff timer init(sec)	Initial value of the Exponential backoff timer, in seconds. The default value is 15s. You can set this value using the **backoff timer** command.

Item	Description
Backoff timer max(sec)	Maximum value of the Exponential backoff timer, in seconds. The default value is 120s. You can set this value using the **backoff timer** command.
IGP-Sync delay timer(sec)	Value of the LDP-IGP association timer, in seconds. The default value is 10s. You can set this value using the **mpls ldp timer igp-sync-delay** command.
Graceful delete	Graceful deletion. This function is disabled and not supported currently.
Graceful delete timer(sec)	Value of the graceful deletion timer, in seconds. The default value is 5s.
Capability-announcement	Dynamic capability announcement function. This function is disabled and not supported currently.
mLDP MBB Capability	Whether the mLDP make-before-break capability is enabled. The default value is "Off", indicating that mLDP make-before-break is disabled.
Wait-ack timer(sec)	Time (in seconds) elapses before a local device receives a Make-before-break (MBB) ACK Notification message
Switch-delay timer(ms)	Delay time (in seconds) for switching traffic to an MBB LSP
mLDP P2MP Capability	Whether mLDP P2MP is enabled globally. The default value is "Off", indicating that mLDP P2MP is disabled globally.
mLDP MP2MP Capability	Whether mLDP multipoint-to-multipoint (MP2MP) is enabled globally. The default value is "Off", indicating that mLDP MP2MP is disabled globally.
Label withdraw-delay	Whether the label withdraw delay function is enabled. The default value is "Off", indicating that this function is disabled.
Withdraw-delay timer(sec)	Default value of the label withdraw delay timer (in seconds).
Send LSP down reason	Whether a node is enabled to report the fault cause to the ingress. The default value is "Off", indicating that the faulty node is disabled from reporting the fault cause to the ingress.
Ingress LSP Load-balance Num	Default maximum number of equal-cost LDP LSPs that can be established on the ingress.
Transit LSP Load-balance Num	Default maximum number of equal-cost LDP LSPs that can be established on a transit node.

Item	Description
Smart-policy Ingress	Whether the smart LDP ingress policy is enabled.
Smart-policy Auto-dod-request	Whether on-demand LDP request trigger is enabled.
Label default-route	Whether the device is enabled to assign a label to a default IGP route. You can set this value using the **label distribution default-route** command.

9.1.11 display default-parameter mpls management

Function

The **display default-parameter mpls management** command displays default configurations of the MPLS management module.

Format

display default-parameter mpls management

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the default configurations of MPLS management module, run the **display default-parameter mpls management** command.

Example

# Display the default configurations of the MPLS management module.

```
<HUAWEI> display default-parameter mpls management

 Global Information:
 --------------------------------------------------------------
         BFD detect-multiplier        : 3
         BFD min-tx-interval(ms)      : 1000
         BFD min-rx-interval(ms)      : 1000
         Label advertisement mode     : Implicit null
         LSP trigger mode             : Host
         LDP LSP number threshold-alarm upper limit  : 80
         LDP LSP number threshold-alarm lower limit  : 75
```

```
  BGP LSP number threshold-alarm upper limit  : 80
  BGP LSP number threshold-alarm lower limit  : 75
  BGP V6 LSP number threshold-alarm upper limit  : 80
  BGP V6 LSP number threshold-alarm lower limit  : 75
  Dynamic Label number threshold-alarm upper limit  : 80
  Dynamic Label number threshold-alarm lower limit  : 70
  RSVP LSP number threshold-alarm upper limit  : 80
  RSVP LSP number threshold-alarm lower limit  : 75
  Total LSP number threshold-alarm upper limit  : 80
  Total LSP number threshold-alarm lower limit  : 75
  Total CR LSP number threshold-alarm upper limit  : 80
  Total CR LSP number threshold-alarm lower limit  : 75
  Ingress LDP LSP number threshold-alarm upper limit  : 80
  Ingress LDP LSP number threshold-alarm lower limit  : 75
  Transit LDP LSP number threshold-alarm upper limit  : 80
  Transit LDP LSP number threshold-alarm lower limit  : 75
  Egress LDP LSP number threshold-alarm upper limit  : 80
  Egress LDP LSP number threshold-alarm lower limit  : 75
  Ingress BGP LSP number threshold-alarm upper limit  : 80
  Ingress BGP LSP number threshold-alarm lower limit  : 75
  Egress BGP LSP number threshold-alarm upper limit  : 80
  Egress BGP LSP number threshold-alarm lower limit  : 75
  Egress BGP V6 LSP number threshold-alarm upper limit  : 80
  Egress BGP V6 LSP number threshold-alarm lower limit  : 75
  Ingress RSVP LSP number threshold-alarm upper limit  : 80
  Ingress RSVP LSP number threshold-alarm lower limit  : 75
  Transit RSVP LSP number threshold-alarm upper limit  : 80
  Transit RSVP LSP number threshold-alarm lower limit  : 75
  Egress RSVP LSP number threshold-alarm upper limit  : 80
  Egress RSVP LSP number threshold-alarm lower limit  : 75
  Total ingress LSP number threshold-alarm upper limit  : 80
  Total ingress LSP number threshold-alarm lower limit  : 75
  Total transit LSP number threshold-alarm upper limit  : 80
  Total transit LSP number threshold-alarm lower limit  : 75
  Total egress LSP number threshold-alarm upper limit  : 80
  Total egress LSP number threshold-alarm lower limit  : 75
  Total ingress CR LSP number threshold-alarm upper limit  : 80
  Total ingress CR LSP number threshold-alarm lower limit  : 75
  Total transit CR LSP number threshold-alarm upper limit  : 80
  Total transit CR LSP number threshold-alarm lower limit  : 75
  Total egress CR LSP number threshold-alarm upper limit  : 80
  Total egress CR LSP number threshold-alarm lower limit  : 75
  Auto bypass tunnel interface number threshold-alarm upper limit  : 80
  Auto bypass tunnel interface number threshold-alarm lower limit  : 75
  P2MP auto tunnel interface number threshold-alarm upper limit  : 80
  P2MP auto tunnel interface number threshold-alarm lower limit  : 75
  TE dynamic bfd number threshold-alarm upper limit  : 80
  TE dynamic bfd number threshold-alarm lower limit  : 75
  LDP dynamic bfd number threshold-alarm upper limit  : 80
  LDP dynamic bfd number threshold-alarm lower limit  : 75
  Total MLDP tree number threshold-alarm upper limit  : 80
  Total MLDP tree number threshold-alarm lower limit  : 75
  Total MLDP branch number threshold-alarm upper limit  : 80
  Total MLDP branch number threshold-alarm lower limit  : 75
  Total LDP remote adjacency number threshold-alarm upper limit  : 80
  Total LDP remote adjacency number threshold-alarm lower limit  : 75
  Total LDP local adjacency number threshold-alarm upper limit  : 80
  Total LDP local adjacency number threshold-alarm lower limit  : 75
  Total CSPF node number threshold-alarm upper limit  : 80
  Total CSPF node number threshold-alarm lower limit  : 75
  Total CSPF link number threshold-alarm upper limit  : 80
  Total CSPF link number threshold-alarm lower limit  : 75
  Total CSPF network-lsa number threshold-alarm upper limit  : 80
  Total CSPF network-lsa number threshold-alarm lower limit  : 75
  Total CSPF SRLG number threshold-alarm upper limit  : 80
  Total CSPF SRLG number threshold-alarm lower limit  : 75
  RSVP peer number threshold-alarm upper limit  : 80
  RSVP peer number threshold-alarm lower limit  : 75
--------------------------------------------------------------
```

Table 9-2 Description of the display default-parameter mpls management command output

Item	Description
BFD detect-multiplier	BFD detection multiplier. The default value is 3. You can set this value using the **mpls bfd** command.
BFD min-tx-interval(ms)	Interval for sending BFD packets. You can set this value using the **mpls bfd** command.
BFD min-rx-interval(ms)	Interval for receiving BFD packets. You can set this value using the **mpls bfd** command.
Label advertisement mode	Mode in which the egress node assigns labels to the penultimate hop. ● Implicit null: The egress node assigns an implicit empty label to the penultimate hop. The value of the label is 3. ● Explicit null: The egress node assigns an explicit empty label to the penultimate hop. The value of the label is 0. ● Non null: The egress node assigns a label to the penultimate hop properly. The value of the label is not smaller than 16. By default, the implicit null mode is used. You can set the label advertisement mode using the **label advertise** command.
LSP trigger mode	Policy for triggering LSP setup. ● All: All static routes and IGP routing entries trigger the setup of LSPs. ● Host: The IP route of the 32-bit address host triggers the setup of LSPs. ● Ip-prefix: Only FECs that match entries in the IP address prefix list trigger the setup of LSPs. ● None: The setup of LSPs is not triggered. The default trigger policy is **Host**. You can set the LSP trigger mode using the **lsp-trigger** command.
LDP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for LDP LSPs. You can set the LSP trigger mode using the **mpls ldp-lsp-number threshold-alarm** command.
LDP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for LDP LSPs. You can set the LSP trigger mode using the **mpls ldp-lsp-number threshold-alarm** command.
BGP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for BGP LSPs. You can set the LSP trigger mode using the **mpls bgp-lsp-number threshold-alarm** command.

Item	Description
BGP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for BGP LSPs. You can set the LSP trigger mode using the **mpls bgp-lsp-number threshold-alarm** command.
BGP V6 LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for BGP IPv6 LSPs. You can set the LSP trigger mode using the **mpls bgpv6-lsp-number threshold-alarm** command.
BGP V6 LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for BGP IPv6 LSPs. You can set the LSP trigger mode using the **mpls bgpv6-lsp-number threshold-alarm** command.
Dynamic Label number threshold-alarm upper limit	Upper limit of the alarm threshold for dynamic label usage. You can set the LSP trigger mode using the **mpls dynamic-label-number threshold-alarm** command.
Dynamic Label number threshold-alarm lower limit	Lower limit of the alarm threshold for dynamic label usage. You can set the LSP trigger mode using the **mpls dynamic-label-number threshold-alarm** command.
RSVP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for RSVP LSPs. You can set the LSP trigger mode using the **mpls rsvp-lsp-number threshold-alarm** command.
RSVP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for RSVP LSPs. You can set the LSP trigger mode using the **mpls rsvp-lsp-number threshold-alarm** command.
Total LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total LSPs. You can set the LSP trigger mode using the **mpls total-lsp-number threshold-alarm** command.
Total LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total LSPs. You can set the LSP trigger mode using the **mpls total-lsp-number threshold-alarm** command.
Total CR LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total CR-LSPs. You can set the LSP trigger mode using the **mpls total-crlsp-number threshold-alarm** command.
Total CR LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total CR-LSPs. You can set the LSP trigger mode using the **mpls total-crlsp-number threshold-alarm** command.
Ingress LDP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for ingress LDP LSP

Item	Description
Ingress LDP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for ingress LDP LSP
Transit LDP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for transit LDP LSP
Transit LDP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for transit LDP LSP
Egress LDP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for egress LDP LSP
Egress LDP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for egress LDP LSP
Ingress BGP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for ingress BGP LSP
Ingress BGP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for ingress BGP LSP
Egress BGP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for egress BGP LSP
Egress BGP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for egress BGP LSP
Egress BGP V6 LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for egress BGP V6 LSP
Egress BGP V6 LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for egress BGP V6 LSP
Ingress RSVP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for ingress RSVP LSP
Ingress RSVP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for ingress RSVP LSP

Item	Description
Transit RSVP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for transit RSVP LSP
Transit RSVP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for transit RSVP LSP
Egress RSVP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for egress RSVP LSP
Egress RSVP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for egress RSVP LSP
Total ingress LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total ingress LSP
Total ingress LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total ingress LSP
Total transit LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total transit LSP
Total transit LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total transit LSP
Total egress LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total egress LSP
Total egress LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total egress LSP
Total ingress CR LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total ingress CR-LSP
Total ingress CR LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total ingress CR-LSP
Total transit CR LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total transit CR-LSP

Item	Description
Total transit CR LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total transit CR-LSP
Total egress CR LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total egress CR-LSP
Total egress CR LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total egress CR-LSP
Auto bypass tunnel interface number threshold-alarm upper limit	Upper limit of the alarm threshold for auto bypass tunnel interface
Auto bypass tunnel interface number threshold-alarm lower limit	Lower limit of the alarm threshold for auto bypass tunnel interface
P2MP auto tunnel interface number threshold-alarm upper limit	Upper limit of the alarm threshold for P2MP auto tunnel interface
P2MP auto tunnel interface number threshold-alarm lower limit	Lower limit of the alarm threshold for P2MP auto tunnel interface
TE dynamic bfd number threshold-alarm upper limit	Upper limit of the alarm threshold for TE dynamic bfd
TE dynamic bfd number threshold-alarm lower limit	Lower limit of the alarm threshold for TE dynamic bfd
LDP dynamic bfd number threshold-alarm upper limit	Upper limit of the alarm threshold for LDP dynamic bfd
LDP dynamic bfd number threshold-alarm lower limit	Lower limit of the alarm threshold for LDP dynamic bfd
Total MLDP tree number threshold-alarm upper limit	Upper limit of the alarm threshold for total MLDP tree

Item	Description
Total MLDP tree number threshold-alarm lower limit	Lower limit of the alarm threshold for total MLDP tree
Total MLDP branch number threshold-alarm upper limit	Upper limit of the alarm threshold for total MLDP branch
Total MLDP branch number threshold-alarm lower limit	Lower limit of the alarm threshold for total MLDP branch
Total LDP remote adjacency number threshold-alarm upper limit	Upper limit of the alarm threshold for total LDP remote adjacency
Total LDP remote adjacency number threshold-alarm lower limit	Lower limit of the alarm threshold for total LDP remote adjacency
Total LDP local adjacency number threshold-alarm upper limit	Upper limit of the alarm threshold for total LDP local adjacency
Total LDP local adjacency number threshold-alarm lower limit	Lower limit of the alarm threshold for total LDP local adjacency
Total CSPF node number threshold-alarm upper limit	Upper limit of the alarm threshold for total CSPF node
Total CSPF node number threshold-alarm lower limit	Lower limit of the alarm threshold for total CSPF node
Total CSPF link number threshold-alarm upper limit	Upper limit of the alarm threshold for total CSPF link
Total CSPF link number threshold-alarm lower limit	Lower limit of the alarm threshold for total CSPF link
Total CSPF network-lsa number threshold-alarm upper limit	Upper limit of the alarm threshold for total CSPF network-lsa
Total CSPF network-lsa number threshold-alarm lower limit	Lower limit of the alarm threshold for total CSPF network-lsa

Item	Description
Total CSPF SRLG number threshold-alarm upper limit	Upper limit of the alarm threshold for total CSPF SRLG
Total CSPF SRLG number threshold-alarm lower limit	Lower limit of the alarm threshold for total CSPF SRLG
RSVP peer number threshold-alarm upper limit	Upper limit of the alarm threshold for RSVP peer
RSVP peer number threshold-alarm lower limit	Lower limit of the alarm threshold for RSVP peer

9.1.12 display isis ldp-sync interface

Function

The **display isis ldp-sync interface** command displays information about LDP and IS-IS synchronization on an interface.

Format

display isis [*process-id* | **vpn-instance** *vpn-instance-name*] **ldp-sync interface**

Parameters

Parameter	Description	Value
process-id	Specifies the IS-IS process ID.	The value is an integer ranging from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the VPN instance name.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

For all the interfaces that are enabled with LDP and IS-IS synchronization, run the **display isis ldp-sync** command to view information about LDP and IS-IS synchronization.

Example

# Display information about LDP and IS-IS synchronization on an interface.

```
<HUAWEI> display isis ldp-sync interface

               Ldp Sync interface information for ISIS(1)
               ------------------------------------------
Interface    HoldDownTimer    HoldMaxCostTimer   LDP State   Sync State
Vlanif100     10               10                Down        Init
```

Table 9-3 Description of the display isis ldp-sync interface command output

Item	Description
Interface	Interface connected to neighbors.
HoldDownTimer	Interval during which the interface waits for the LDP session establishment and does not create the IS-IS neighbor relationship. The default value is 10 seconds. You can set this value using the **isis timer ldp-sync hold-down** command.
HoldMaxCostTimer	Interval for IS-IS to notify the local device of the maximum metric in the link state PDU (LSP). The default value is 10 seconds. You can set this value using the **isis timer ldp-sync hold-max-cost** command. **NOTE** If the value of this field is **infinite**, IS-IS permanently notifies the local device of the maximum metric in the LSP before an LDP session is established.
LDP State	LDP session status, which can be: ● Up: The LDP session is normal. ● Down: The LDP session is disconnected. ● GR: The LDP session is in GR state. If the interface is maintaining the session before GR, the LDP status is displayed as GR state during GR.

Item	Description
Sync State	Status of synchronization between LDP and IS-IS: ● Sync-Achieved: The creation of an LDP session and establishment of the IS-IS neighbor relationship are synchronized. ● HoldDown: indicates the state in which the interface waits to create an LDP session without creating the IS-IS neighbor relationship. ● HoldMaxCost: indicates the state in which IS-IS advertises the maximum metric in LSPs sent by the local device. ● Init: indicates the initial state.

9.1.13 display lspv configuration

Function

The **display lspv configuration** command displays the current configuration of LSPV tracert.

Format

display lspv configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display lspv configuration** command to check the current LSPV configurations.

Example

# Display the current configuration of LSPV tracert.

```
<HUAWEI> display lspv configuration
lspv packet filter 2100
undo lspv mpls-lsp-ping echo enable
```

Table 9-4 Description of the **display lspv configuration** command output

Item	Description
lspv packet filter 2100	Filters the LSPV tracert packet with the specific source address according to ACL 2100. To configure the filtering of the LSPV tracert packet with the specific source address, run the **lspv packet-filter** command.
undo lspv mpls-lsp-ping echo enable	Disables the response to MPLS Ping packets. To configure a device to respond to MPLS Echo Request packets, run the **lspv mpls-lsp-ping echo enable** command.

9.1.14 display lspv statistics

Function

The **display lspv statistics** command displays LSPV statistics.

Format

display lspv statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

In MPLS network management, the **ping lsp** or **tracert lsp** command can be used for LSP detection.

If the LSP detection fails, you can run the **display lspv statistics** command to view statistics about MPLS packets sent and received on the local device. If the number of MPLS packets that the local device sends is the same as the number of MPLS packets that the local device receives, but the ping or trace operation fails, the detection failure is caused by the fault of the local device, not the LSP.

Precautions

Before running the **display lspv statistics** command to collect LSPV statistics, run the **reset lspv statistics** command to clear the existing statistics.

Example

# Display LSPV statistics on the device.

```
<HUAWEI> display lspv statistics
Total sent: 0 packet(s)
Total received: 0 packet(s)
MPLS echo request sent: 0 packet(s), received: 0 packet(s)
MPLS echo reply sent: 0 packet(s), received: 0 packet(s)
---------------------------------------------------------------------
Statistics base on ReturnCode:
0 - No return code,1 - Malformed echo request received,2 - One or more
of the TLVs was not understood,3 - Replying router is an egress for
the FEC at stack-depth, 4 - Replying router has no mapping for the FEC
at stack-depth,5 - Downstream Mapping Mismatch, 6 - Upstream Interface
Index Unknown, 7 - Reserved, 8 - Label switched at stack-depth,9 -
Label switched but no MPLS forwarding at stack-depth,10 - Mapping for
this FEC is not the given label at stack-depth,11 - No label entry at
stack-depth,12 - Protocol not associated with interface at FEC
stack-epth,13 - Premature termination of ping due to label stack
shrinking to a single label.:
---------------------------------------------------------------------
Value      SendNum      RecvNum       Value      SendNum      RecvNum
   0          0           0           1          0          0
   2          0           0           3          0          0
   4          0           0           5          0          0
   6          0           0           7          0          0
   8          0           0           9          0          0
  10          0           0          11          0          0
  12          0           0          13          0          0
---------------------------------------------------------------------
```

Table 9-5 Description of the **display lspv statistics** command output

Item	Description
Total sent	Total number of sent MPLS Echo Request and MPLS Echo Reply packets
Total received	Total number of received MPLS Echo Request and MPLS Echo Reply packets
MPLS echo request sent, received	Number of sent and received MPLS Echo Request packets
MPLS echo reply sent, received	Number of sent and received MPLS Echo Reply packets

Item	Description
Statistics base on ReturnCode	Statistics base on ReturnCode: ● 0: No return code ● 1: Malformed echo request received ● 2: One or more of the TLVs was not understood ● 3: Replying router is an egress for the FEC at stack-depth ● 4: Replying router has no mapping for the FEC at stack-depth ● 5: Downstream Mapping Mismatch ● 6: Upstream Interface Index Unknown ● 7: Reserved ● 8: Label switched at stack-depth ● 9: Label switched but no MPLS forwarding at stack-depth ● 10: Mapping for this FEC is not the given label at stack-depth ● 11: No label entry at stack-depth ● 12: Protocol not associated with interface at FEC stack-epth ● 13: Premature termination of ping due to label stack shrinking to a single label
Value	The value of ReturnCode in sent or received LSP verification packets.
SendNum	Number of sent packets with this ReturnCode.
RecvNum	Number of received packets with this ReturnCode.

9.1.15 display mpls bfd session

Function

The **display mpls bfd session** command displays information about BFD sessions for MPLS.

Format

display mpls bfd session [**fec** *fec-address* | **monitor** | **nexthop** *ip-address* | **outgoing-interface** *interface-type interface-number* | **statistics** | **verbose**]

display mpls bfd session protocol ldp [**fec** *fec-address* [**verbose**]]

display mpls bfd session protocol { **cr-static** | **rsvp-te** } [**lsp-id** *ingress-lsr-id session-id lsp-id* [**verbose**]]

display mpls bfd session protocol bgp [**fec** *fec-address* [**verbose**]]

Parameters

Parameter	Description	Value
fec *fec-address*	Displays information about the BFD session of a specified FEC.	The value is in dotted decimal notation.
monitor	Displays monitoring information of BFD sessions.	-
nexthop *ip-address*	Displays information about the BFD session of a specified next hop.	The value is in dotted decimal notation.
outgoing-interface *interface-type interface-number*	Displays information about the BFD session of the LSP with a specified outbound interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
protocol	Indicates the type of the protocol.	-
cr-static	Displays information about the BFD session for static CR-LSP.	-
ldp	Displays information about the BFD session for LDP.	-
rsvp-te	Displays information about the BFD session for RSVP-TE.	-
statistics	Displays statistics about BFD sessions such as the total number of BFD sessions.	-
verbose	Displays detailed information about BFD sessions.	-
lsp-id *ingress-lsr-id*	Specifies the LSR ID of the ingress.	The value is in dotted decimal notation.
session-id	Specifies the ID of a session.	The value is an integer ranging from 0 to 65535.
lsp-id	Specifies the LSP ID.	The value is an integer ranging from 0 to 65535.
bgp	Displays information about BFD sessions for BGP.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display mpls bfd session** command to view information about a BFD session and the LSP detected by BFD, including the destination address and outbound interface of the LSP, the local discriminator of the BFD session, and the status of an MPLS BFD session.

Example

# Display information about the BFD session.

```
<HUAWEI> display mpls bfd session
-----------------------------------------------------------------------------
              BFD Information: LDP  LSP
-----------------------------------------------------------------------------
FEC           DISC  OUT-IF      NEXTHOP       TUNNEL        STATE
3.3.3.3       8     VLANIF100   10.1.1.2      Tunnel1       Up
```

Table 9-6 Description of the display mpls bfd session command output

Item	Description
FEC	Forwarding equivalence class.
DISC	Local discriminator of a BFD session.
OUT-IF	Outbound interface.
NEXTHOP	IP address of the next hop.
TUNNEL	Name of a tunnel.
STATE	Status of an MPLS BFD session. ● Up ● Down

# Display detailed information about a BFD session with the specified protocol type and LSP ID.

```
<HUAWEI> display mpls bfd session protocol rsvp-te lsp-id 3.3.3.3 3 1 verbose
--------------------------------------------------------------------
              BFD Information: TE TUNNEL
--------------------------------------------------------------------
 No                    :  1
 LspIndex              :  6157
 Protocol              :  RSVP-TE
 Tunnel-Interface      :  Tunnel1
 Fec                   :  2.2.2.2
 Nexthop               :  10.2.3.2
```

```
Out-Interface             :  Vlanif100
Bfd-Discriminator         :  8195
TEMIB Tunn Table Index    :  3
SessionTunnelID           :  3
LocalLspId                :  1
PrevSessionTunnelID       :  -
NextSessionTunnelID       :  12
ActTx                     :  2200
ActRx                     :  2200
ActMulti                  :  -
Bfd-State                 :  Down
Time                      :  2559 sec
```

Table 9-7 Description of the display mpls bfd session protocol rsvp-te lsp-id 3.3.3.3 3 1 verbose command output

Item	Description
No	Serial number.
LspIndex	Index number of an LSP.
Protocol	Protocol type.
Tunnel-Interface	Name of a tunnel interface.
Fec	Forwarding equivalence class.
Nexthop	IP address of the next hop.
Out-Interface	Name of an outbound interface.
Bfd-Discriminator	Local discriminator of a BFD session.
TEMIB Tunn Table Index	Index of the tunnel entry to which an LSP corresponds.
SessionTunnelID	BFD session ID.
LocalLspId	ID of a local LSP.
PrevSessionTunnelID	Tunnel ID mapping the previous LSP to which a BFD session is bound.
NextSessionTunnelID	Tunnel ID mapping the next LSP to which a BFD session is bound.
ActTx	Actual interval for sending BFD packets, in milliseconds.
ActRx	Actual interval for receiving BFD packets, in milliseconds.
ActMulti	Actual local detection multiple of a BFD session.
Bfd-State	Status of the BFD session. ● Up ● Down

Item	Description
Time	Period from the time when the BFD session is created or updated till now, in seconds.

# Display BFD session statistics.

```
<HUAWEI> display mpls bfd session statistics
Lsp Type       sess num   Tx        Rx        Mult      Trig-type
LDP LSP        0          1000      1000      3         NONE
BGP LSP        0          1000      1000      3         NONE
STATIC CRLSP   0          1000      1000      3         -
RSVP           0          1000      1000      3         -
TOTAL          0
```

Table 9-8 Description of the **display mpls bfd session statistics** command output

Item	Description
Lsp Type	LSP type.
sess num	Number of BFD sessions monitoring the LSP.
Tx	Effective minimum interval (in ms) at which BFD packets are sent.
Rx	Effective minimum interval (in ms) at which BFD packets are received.
Mult	Effective BFD detection multiplier.
Trig-type	BFD session establishment policy: ● HOST: BFD sessions are established using host addresses. ● IP-PREFIX: BFD sessions are established using an IP address prefix list. ● FEC-LIST: BFD sessions are established using a FEC list. ● NONE: No policy for establishing BFD sessions is configured. ● -: N/A

# Display BFD session monitoring information.

```
<HUAWEI> display mpls bfd session monitor

LDP BFD TRIGGER INFO:
  Trig-Type  : None
  OutIfIndex : Invalid
  NextHop    : Invalid

LDP BFD SCAN INFO:
  Cur BackGround Oper  : Off
  Cur Scan Index       : Invalid
  First Bfd Scan Index : Invalid
  Scan Again           : No
  License Lim Reached  : No
  License Lim Scn Agn  : No
  BackGround Status    : Suspended/Off
  Current Scan Node    : -

BGP BFD SCAN INFO:
  Cur BackGround Oper  : Off
  Cur Scan Index       : Invalid
  Scan Again           : No
  License Lim Reached  : No
  BackGround Status    : Suspended/Off

TE BFD SCAN INFO:
  Cur BackGround Oper  : Off
  Cur Scan Index       : 0
  First Bfd Scan Index : 0
  Scan Again           : No
  License Lim Reached  : No
  License Lim Scn Agn  : No
  BackGround Status    : Suspended/Off

CAPABILITY :
  Bfd Capability     : Disable
  Ldp Bfd Capability : Disable
  Bgp Bfd Capability : Disable
  Te Bfd Capability  : Disable
  Bfd Session Full   : Not-full
  Bfd Clearing       : No


BFD FOR LSP PAF LICENSE INFORMATION:
Lsp Type  Min-Val   Max-Val   Avail-Val Created
LDP LSP   0         1024      1024      0
BGP LSP   0         1024      1024      0
TE LSP    0         2048      256       0 + 0 (RSVP + CRSTATIC)
```

Table 9-9 Description of the **display mpls bfd session monitor** command output

Item	Description
Trig-Type	BFD session establishment policy: ● HOST: BFD sessions are established using host addresses. ● IP-PREFIX: BFD sessions are established using an IP address prefix list. ● FEC-LIST: BFD sessions are established using a FEC list. ● NONE: No policy for establishing BFD sessions is configured. ● -: N/A
OutIfIndex	Index of a BFD session outbound interface.
NextHop	Next-hop IP address of a BFD session.

Item	Description
Cur BackGround Oper	Background operation: ● Create ● Delete ● Update ● Off
Cur Scan Index	Scanned BFD session index. "Invalid" indicates that no BFD session is established.
First Bfd Scan Index	First scanned BFD session index. "Invalid" indicates that no BFD session is established.
Scan Again	Whether a device scans BFD sessions again: ● Yes ● No
License Lim Reached	Whether the number of established BFD sessions reaches the upper limit specified in the license file: ● Yes ● No
License Lim Scn Agn	Whether the switch needs to check the threshold-crossing event about establishment BFD sessions: ● Yes ● No
BackGround Status	Background status: ● Running ● Suspended/Off
Current Scan Node	Name of a node that is being scanned.
Bfd Capability	Whether MPLS BFD is enabled: ● Enable ● Disable
Ldp Bfd Capability	Whether BFD for LDP is enabled: ● Enable ● Disable
Bgp Bfd Capability	Whether BFD for BGP tunnel is enabled: ● Enable ● Disable
Te Bfd Capability	Whether BFD for Traffic Engineering (TE) is enabled: ● Enable ● Disable

Item	Description
Bfd Session Full	Whether the number of created BFD sessions reaches the upper limit: - Full: The number of created BFD sessions reached the upper limit. - Not-full: The number of created BFD sessions is lower than the upper limit.
Bfd Clearing	Whether BFD is disabled globally: - Yes - No
Lsp Type	LSP type
Min-Val	Minimum number of supported LSPs specified in the license file.
Max-Val	Maximum number of supported LSPs specified in the license file.
Avail-Val	Average number of supported LSPs specified in the license file.
Created	Number of established LSPs.

9.1.16 display mpls graceful-restart

Function

The **display mpls graceful-restart** command displays graceful restart (GR) information about all protocols related to MPLS.

Format

display mpls graceful-restart

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When MPLS is used together with other protocols, run the **display mpls graceful-restart** command to view GR information about protocols related to MPLS, including the GR status, GR start time, and GR type.

Example

# Display GR information related to all protocols.

```
<HUAWEI> display mpls graceful-restart
Protocol     GR state     GR start time          GR type
LDP          Normal       -                      -
CRLDP        Normal       -                      -
RSVP         Normal       -                      -
BGP          Normal       -                      -
L3VPN        Normal       -                      -
STATIC       Normal       -                      -
CRSTATIC     Normal       -                      -
BGP IPV6     Normal       -                      -
STATIC HA    Normal       -                      -
L3VPN IPV6   Normal       -                      -
STATIC TP    Normal       -                      -
```

Table 9-10 Description of the display mpls graceful-restart command output

Item	Description
Protocol	Protocol type: LDP, CRLDP, RSVP, BGP, L3VPN, STATIC, CRSTATIC, BGP IPV6, STATIC HA, L3VPN IPV6, and STATIC TP.
GR state	GR status of a protocol: ● Restarting: The protocol is in the GR process. ● Normal: The protocol is not in the GR process.
GR start time	Time when the GR process starts When the GR process does not start, a hyphen (-) is displayed.
GR type	GR type: ● System restart: indicates the system GR. ● Protocol restart: indicates the protocol GR. When the GR process does not start, a hyphen (-) is displayed.

9.1.17 display mpls interface

Function

The **display mpls interface** command displays information about all MPLS-enabled interfaces.

Format

display mpls interface [*interface-type interface-number*] [**verbose**]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-
verbose	Displays detailed information about the interface enabled with MPLS.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After enabling MPLS functions, run the **display mpls interface** command to view information about the interface enabled with MPLS.

Example

# Display information about all MPLS-enabled interfaces.

```
<HUAWEI> display mpls interface
Interface            Status   TE Attr   LSP Count  CRLSP Count Effective MTU
Vlanif100              Up       Dis       2          0           1500
```

Table 9-11 Description of the display mpls interface command output

Item	Description
Interface	The interface enabled with MPLS.
Status	Interface status: ● Up ● Down
TE Attr	Status of the TE attributes on an interface: ● Dis: MPLS TE is disabled on the interface. ● En: MPLS TE is enabled on the interface.
LSP Count	Number of LSPs established on an interface.
CRLSP Count	Number of CR-LSPs established on an interface.

Item	Description
Effective MTU	MPLS MTU used during data forwarding: ● If the MPLS MTU is not set, the interface MTU takes effect. ● If the MPLS MTU is set, the smaller one between the MPLS MTU and the interface MTU takes effect. To set the MPLS MTU, run the **mpls mtu** command. To set the interface MTU, run the **mtu** command.

# Display detailed information about a specified MPLS-enabled interface.

```
<HUAWEI> display mpls interface vlanif 100 verbose
No                   :  1
Interface            :  Vlanif100
Status               :  Up
TE Attribute         :  Disable
Static LSPCount      :  0
Static CR-LSPCount   :  0
LDP LSPCount         :  0
RSVP LSPCount        :  0
MPLS MTU             :  -
Interface MTU        :  1500
Effective MTU        :  1500
TE FRR               :  Disable
Interface Index      :  0xd1
```

Table 9-12 Description of the display mpls interface verbose command output

Item	Description
No	Serial number.
Interface	The interface enabled with MPLS.
Status	Interface status: ● Up ● Down
TE Attribute	Status of the TE attributes on the interface: ● Disable: MPLS TE is disabled on the interface. ● Enable: MPLS TE is enabled on the interface.
Static LSPCount	Number of static LSPs established on the interface.
Static CR-LSPCount	Number of static CR-LSPs established on the interface.
LDP LSPCount	Number of LDP LSPs created on the interface.
RSVP LSPCount	Number of RSVP-TE LSPs established on the interface.
MPLS MTU	MPLS MTU value configured using the **mpls mtu** command. When no MPLS MTU is set, a hyphen (-) is displayed.

Item	Description
Interface MTU	MTU value configured on an interface. To set the interface MTU, run the **mtu** command.
Effective MTU	MPLS MTU used during data forwarding: ● If no MPLS MTU is set, the interface MTU takes effect. ● If the MPLS MTU is set, the smaller one between the MPLS MTU and the interface MTU takes effect. To set the MPLS MTU, run the **mpls mtu** command. To set the interface MTU, run the **mtu** command.
TE FRR	Whether the TE FRR is enabled or disabled on the interface: ● Disable: No bypass tunnel is set up in manual FRR mode to protect the interface. ● Enable: A bypass tunnel is set up in manual FRR mode to protect the interface.
Interface Index	Interface index value.

9.1.18 display mpls label static available

Function

The **display mpls label static available** command displays information about labels available for transmitting static services.

Format

display mpls label static available [[**label-from** *label-index*] **label-number** *label-number*]

Parameters

Parameter	Description	Value
label-from *label-index*	Specifies the start label value.	The value is an integer ranging from 16 to 1023.
label-number *label-number*	Specifies the number of the required labels.	The value is an integer ranging from 1 to 1008.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

By default, the system reserves separate label spaces for dynamic and static services, allowing labels for dynamic and static services to be stored in separate spaces.

Before specifying a label for static services, ensure that the specified label is available. You can run the **display mpls label static available** command to view labels for static services.

In the command output, a hyphen is used to specify a range. For example, labels 1000, 1001, and 1002 are displayed as 1000-1002.

Follow-up Procedure

Labels displayed in the command output can be allocated for static services.

Example

# Display information about labels available for transmitting static services.

```
<HUAWEI> display mpls label static available
16-1023
```

9.1.19 display mpls label-stack ilm inlabel

Function

The **display mpls label-stack ilm inlabel** command displays information about the label stack for packets with a specified incoming label.

Format

display mpls label-stack ilm inlabel *in-label*

Parameters

Parameter	Description	Value
in-label	Specifies the incoming label for the packets about which label-stack information is to be displayed.	The value is an integer ranging from 16 to 1048575.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to query information about the outgoing label stack for packets based on the incoming label. The supported public network tunnels include static LSP tunnels, LDP LSPs, dynamic TE tunnels, and static TE tunnels. This command cannot be used in the following situations:

- Tunnels overlap.
- Tunnels load-balance traffic.
- The primary and secondary SPE egresses are used.
- Routes recurse to a ring network.
- Layer 3 labels are used.

Example

# Display the outgoing label, outbound interface, and tunnel type in the packets with the incoming label value of 1028.

```
<HUAWEI> display mpls label-stack ilm inlabel 1028
Label-stack  : 1
Level        : 1
Type         : LDP
Label        : 1025
OutInterface : Vlanif111
```

Table 9-13 Description of the **display mpls label-stack ilm inlabel** command output

Item	Description
Label-stack	Number of label stacks
Level	Number of labels
Type	Tunnel type
Label	Value of the outgoing label
OutInterface	Outbound interface

9.1.20 display mpls last-info lsp-down

Function

The **display mpls last-info lsp-down** command displays information about LSPs in Down state.

Format

display mpls last-info lsp-down [**protocol ldp**] [**verbose**]

Parameters

Parameter	Description	Value
protocol ldp	Displays information about LSPs in Down state.	-
verbose	Displays detailed information about LDP LSPs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If LSPs fail and enter the Down state, run the **display mpls last-info lsp-down** command to view the faults that cause the latest 64 LSPs to go Down.

Example

# Display brief information about LDP LSPs that just enter the Down state.

```
<HUAWEI> display mpls last-info lsp-down
-------------------------------------------------------------------------------
                LDP LSP Information: Host Address
-------------------------------------------------------------------------------
FEC              In/Out Label  Out Interface      Down Reason
10.12.12.12/32     1029/3        vlanif10          route changed
10.12.12.12/32     NULL/3         vlanif10          route changed
10.11.11.11/32     1034/3        vlanif10          cannot recovery from GR
10.11.11.11/32     NULL/3         vlanif10          cannot recovery from GR
10.11.11.11/32     1033/3        vlanif10          DS lost
10.11.11.11/32     NULL/3         vlanif10          DS lost
```

Table 9-14 Description of the display mpls last-info lsp-down command output

Item	Description
FEC	Forwarding equivalence class.
In/Out Label	Values of the incoming and outgoing labels.
Out Interface	Outbound interface.

Item	Description
Down Reason	LSPs go Down due to the following causes: ● route changed: A route was changed. ● adjacency changed: An adjacency was changed. ● cannot recovery from GR: The LDP LSP failed to be reestablished during GR. ● recv release msg: A Release message was received. ● recv withdraw msg: A Withdraw message was received. ● US lost: The session with the upstream node went Down. ● DS lost: The session with the downstream node went Down. ● policy changed: The policy to establish LSPs was changed (Generally, configurations of the policy was changed). ● reach paf limit: PAF resources are insufficient. ● GR aging: The LSP aged after GR. ● others

# Display detailed information about LDP LSPs that just enter the Down state.

```
<HUAWEI> display mpls last-info lsp-down protocol ldp verbose
-------------------------------------------------------------------------------
              LDP LSP Information: Host Address
-------------------------------------------------------------------------------
 No                 :  1
 VrfIndex           :
 Fec                :  10.1.1.1/32
 Nexthop            :  127.0.0.1
 In-Label           :  3
 Out-Label          :  NULL
 Out-Interface      :  vlanif13
 LspIndex           :  6144
 Token              :  0x0
 LsrType            :  Egress
 Outgoing token     :  0x0
 Label Operation    :  POP
 Down Time          :  2011/11/08 16:39:59+00:00
 Exist time         :  14sec
 Down Reason        :  policy changed

 No                 :  2
 VrfIndex           :
 Fec                :  10.2.2.2/32
 Nexthop            :  10.1.2.2
 In-Label           :  NULL
 Out-Label          :  3
 Out-Interface      :  vlanif13
 LspIndex           :  6146
 Token              :  0x1
 LsrType            :  Ingress
 Outgoing token     :  0x0
 Label Operation    :  PUSH
```

```
Down Time          :  2011/11/08 16:51:26+00:00
Exist time         :  5sec
Down Reason        :  route changed
```

Table 9-15 Description of the display mpls last-info lsp-down protocol ldp verbose command output

Item	Description
No	Record No.
VrfIndex	Index of a VRF instance.
Fec	Forwarding equivalence class.
Nexthop	Next hop IP address.
In-Label	Value of the incoming label.
Out-Label	Value of the outgoing label.
Out-Interface	Outbound interface.
LspIndex	Index of an LSP.
Token	Token value, in the hexadecimal format.
LsrType	Type of an LSR on an LSP, which can be ingress, transit, or egress.
Outgoing token	Outgoing token value, in the hexadecimal format.
Label Operation	Label operation, which can be PUSH, POP, SWAP, or SWAPPUSH.
Down Time	Time when an LSP goes Down.
Exist time	Existing period of an LDP LSP, in seconds.

Item	Description
Down Reason	LSPs go Down due to the following causes: ● route changed: A route was changed. ● adjacency changed: An adjacency was changed. ● cannot recovery from GR: The LDP LSP failed to be reestablished during GR. ● recv release msg: A Release message was received. ● recv withdraw msg: A Withdraw message was received. ● US lost: The session with the upstream node went Down. ● DS lost: The session with the downstream node went Down. ● policy changed: The policy to establish LSPs was changed (Generally, configurations of the policy was changed). ● reach paf limit: PAF resources are insufficient. ● GR aging: The LSP aged after GR. ● others

9.1.21 display mpls ldp

Function

The **display mpls ldp** command displays global LDP configurations.

Format

display mpls ldp [**all**] [**verbose**]

Parameters

Parameter	Description	Value
all	Displays all LDP information.	-
verbose	Displays detailed information about the LDP protocol and the LSR.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After global MPLS is enabled, run the **display mpls ldp** command to view LDP configurations, including configurations of the GR timer, label distribution, and label management.

Prerequisites

MPLS has been enabled globally using the **mpls** command, and MPLS LDP has been enabled globally using the **mpls ldp** command.

Example

# Display global LDP configurations.

```
<HUAWEI> display mpls ldp

                         LDP Global Information
 ------------------------------------------------------------------------------
 Protocol Version        : V1             Neighbor Liveness    : 600 Sec
 Graceful Restart        : Off            FT Reconnect Timer   : 300 Sec
 MTU Signaling           : On             Recovery Timer       : 300 Sec
 Capability-Announcement : On             Longest-match        : Off
 mLDP P2MP Capability    : Off            mLDP MBB Capability  : Off
 mLDP MP2MP Capability   : Off

                         LDP Instance Information
 ------------------------------------------------------------------------------
 Instance ID             : 0              VPN-Instance         :
 Instance Status         : Active         LSR ID               : 10.1.1.1
 Loop Detection          : Off            Path Vector Limit    : 32
 Label Distribution Mode : Ordered
 Label Retention Mode    : Liberal(DU)/Conservative(DOD)
 Instance Deleting State : No             Instance Resetting State : No
 Graceful-Delete         : Off            Graceful-Delete Timer : 5 Sec
 ------------------------------------------------------------------------------
```

Table 9-16 Description of the display mpls ldp command output

Item	Description
LDP Global Information	Global LDP information.
Protocol Version	LDP protocol version.
Neighbor Liveness	Timeout period of the GR Neighbor-liveness timer. To set the timeout period of the GR Neighbor-liveness timer, run the **graceful-restart timer neighbor-liveness** command.

Item	Description
Graceful Restart	Whether LDP is enabled with GR: ● On: GR is enabled. ● Off: GR is disabled. To enable LDP GR, run the **graceful-restart** command.
FT Reconnect Timer	Timeout period of the GR reconnect timer. To set the timeout period of the GR reconnect timer, run the **graceful-restart timer reconnect** command.
MTU Signaling	Whether the MTU signaling is enabled: ● On: The private MTU TLV is sent. ● Off: The MTU TLV is not supported. ● On(apply-tlv): The MTU TLV is sent according to RFC 3988. To set the MTU signaling, run the **mtu-signalling** command.
Recovery Timer	Timeout period of the GR Recovery timer. To set the timeout period of the GR Recovery timer, run the **graceful-restart timer recovery** command.
Capability-Announcement	Status of the LDP dynamic capability announcement function: ● On: LDP dynamic capability announcement is enabled. ● Off: LDP dynamic capability announcement is disabled. **NOTE** The switch does not support this parameter.
Longest-match	Status of LDP extension for inter-area LSP: ● On: LDP extension for inter-area LSP is enabled. ● Off: LDP extension for inter-area LSP is disabled. To set the status of LDP extension for inter-area LSP, run the **longest-match** command.
mLDP P2MP Capability	Whether mLDP P2MP is globally enabled: ● On: mLDP P2MP is enabled globally. ● Off: mLDP P2MP is disabled globally. **NOTE** The switch does not support this parameter.

Item	Description
mLDP MBB Capability	Whether the mLDP make-before-break capability is enabled: ● On: mLDP make-before-break is enabled. ● Off: mLDP make-before-break is disabled. **NOTE** The switch does not support this parameter.
mLDP MP2MP Capability	Whether multipoint extensions for LDP (mLDP) multipoint-to-multipoint (MP2MP) is globally enabled: ● On: mLDP MP2MP is enabled globally. ● Off: mLDP MP2MP is disabled globally. **NOTE** The switch does not support this parameter.
LDP Instance Information	Information about the LDP multi-instance.
Instance ID	ID of a VPN instance in the integer format.
VPN-Instance	Name of a VPN instance. The default name is **null**. **NOTE** The switch does not support this parameter.
Instance Status	Status of an instance: ● Active: The instance is in the Active state. ● NotInService: The instance is in the NotInService state temporarily due to certain operations. For example, after the **reset mpls ldp** or **graceful-restart** command is used, the instance is unavailable temporarily. ● Destroy: The instance is in the Destroy state. For example, after the **undo mpls ldp** command is used, the instance is in the Destroy state.
LSR ID	LSR ID of an LDP instance.
Loop Detection	Loop detection status: ● On: Loop detection is enabled. ● Off: Loop detection is disabled. To set the status of the loop detection, run the **loop-detect** command.
Path Vector Limit	Path vector limit for loop detection. To set the path vector limit for loop detection, run the **path-vectors** command.

Item	Description
Label Distribution Mode	Label distribution mode: ● Ordered ● Independent Currently, the switch supports only the ordered mode.
Label Retention Mode	● If label advertisement mode is DU, label retention mode will be Liberal. ● If label advertisement mode is DOD, label retention mode will be Conservative.
Instance Deleting State	Deletion status of an instance: ● Yes: The instance is being deleted. ● No: The instance is not being deleted.
Instance Resetting State	Resetting status of an instance: ● Yes: The instance is being reset. ● No: The instance is not being reset.
Graceful-Delete	Whether graceful deletion is enabled: ● On: enables graceful deletion. ● Off: disables graceful deletion. **NOTE** The switch does not support this parameter.
Graceful-Delete Timer	Value of the Graceful-delete Timer, in seconds.

9.1.22 display mpls ldp adjacency

Function

The **display mpls ldp adjacency** command displays information about LDP adjacencies.

Format

display mpls ldp adjacency [**interface** *interface-type interface-number* | **remote**] [**peer** *peer-id*] [**verbose**]

display mpls ldp adjacency all [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about the LDP adjacency of a specified interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
remote	Displays information about the LDP adjacency of a specified remote end.	-
peer *peer-id*	Displays information about the LDP adjacency of a specified peer.	The value is in dotted decimal notation.
verbose	Displays detailed information about LDP adjacencies.	-
all	Displays information about all the LDP adjacencies.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After an LDP session is established, run the **display mpls ldp adjacency** command to view real-time information about LDP adjacencies, for example, the number of received Hello messages.

Example

# Display information about LDP adjacencies.

```
<HUAWEI> display mpls ldp adjacency

 LDP Adjacency Information in Public Network
 Codes: R: Remote Adjacency, L: Local Adjacency
 A '*' before an adjacency means the adjacency is being deleted.
 -------------------------------------------------------------------------
 SN   SourceAddr      PeerID         VrfID AdjAge(DDDD:HH:MM) RcvdHello Type
 -------------------------------------------------------------------------
  1   10.1.2.2        2.2.2.2        0      0000:00:22        527       L
  2   10.2.3.3        3.3.3.3        0      0000:00:20        254       L
  3   3.3.3.3         3.3.3.3        0      0000:00:18        79        R
 -------------------------------------------------------------------------
 TOTAL: 3 Record(s) found.
```

Table 9-17 Description of the display mpls ldp adjacency command output

Item	Description
SN	Serial number.
SourceAddr	Source address of the Hello message received by an LDP adjacency.
PeerID	LSR ID of an LDP peer.
VrfID	ID of a VPN instance.
AdjAge(DDDD:HH:MM)	Time elapsed since the LDP adjacency was created, in DDDD:HH:MM format.
RcvdHello	Number of Hello messages received by an LDP adjacency.
Type	Type of an LDP adjacency: ● L: local LDP adjacency. ● R: remote LDP adjacency.

# Display detailed information about the LDP adjacency of the remote peer with the LSR ID of 3.3.3.3/32.

```
<HUAWEI> display mpls ldp adjacency remote peer 3.3.3.3 verbose

 LDP Adjacency Information in Public Network
 -----------------------------------------------------------------------------
                          LDP Peer ID : 3.3.3.3
                     VPNInstance name : -
                           CreateDate : 2005-07-27
                           CreateTime : 11:15:41+00:00
                        Adjacency Age : 0000:03:44
                        AdjacencyType : Remote Adjacency
                     Discovery-Source : -
                   UDP Source Address : 3.3.3.3
                        UDP Socket ID : 33
                         Sequence No. : 0
  Configuration Hello Hold Timer(sec) : 45
                   Hello Message Rcvd : 899
            Adjacency Deletion Status : No
 -----------------------------------------------------------------------------
 TOTAL: 1 Adjacency(s) found.
```

Table 9-18 Description of the display mpls ldp adjacency remote peer command output

Item	Description
LDP Peer ID	LSR ID of an LDP peer.
VPNInstance name	Name of a VPN instance. **NOTE** The switch does not support this parameter.
CreateDate	Creation date of an LDP adjacency.

Item	Description
CreateTime	Creation time of an LDP adjacency.
Adjacency Age	Time elapsed since the LDP adjacency was created, in DDDD:HH:MM format.
AdjacencyType	Type of an LDP adjacency: ● Local Adjacency. ● Remote Adjacency.
Discovery-Source	Discovery source of an LDP adjacency: ● Interface: a discovery source of the local LDP adjacency. ● Null: a discovery source of the remote LDP adjacency.
UDP Source Address	Source address of the UDP packet contained in the Hello message received by an LDP adjacency.
UDP Socket ID	Socket ID of the LDP adjacency to receive Hello message.
Sequence No	Serial number carried in the received Hello message. The default value is 0.
Configuration Hello Hold Timer(sec)	Hello hold timer configured on the peer, in seconds: ● Link Hello hold timer: maintains the local LDP adjacency. The default value is 15. ● Target Hello hold timer: maintains the remote LDP adjacency. The default value is 45.
Hello Message Rcvd	Number of Hello messages received by an LDP adjacency.
Adjacency Deletion Status	Deletion status of an LDP adjacency: ● Yes: The LDP adjacency is being deleted. ● No: The LDP adjacency is not being deleted.

9.1.23 display mpls ldp adjacency statistics

Function

The **display mpls ldp adjacency statistics** command displays statistics about LDP adjacencies.

Format

display mpls ldp adjacency statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mpls ldp adjacency statistics** command to view the number of LDP adjacencies that are classified into local and remote LDP adjacencies.

Example

# Display statistics about LDP adjacencies.

```
<HUAWEI> display mpls ldp adjacency statistics

 LDP Adjacency Statistics Information
 -------------------------------------------------
 AdjacencyType          Local   Remote   Total
 -------------------------------------------------
 AdjacencyNumber          1       2        3
 -------------------------------------------------
```

Table 9-19 Description of the display mpls ldp adjacency statistics command output

Item	Description
AdjacencyType	Type of LDP adjacencies.
AdjacencyNumber	Number of LDP adjacencies.
Local	Number of local LDP adjacencies.
Remote	Number of remote LDP adjacencies.
Total	Total number of LDP adjacencies.

9.1.24 display mpls ldp error packet

Function

The **display mpls ldp error packet** command displays information about LDP-related error messages.

Format

display mpls ldp error packet { **tcp** | **udp** | **l2vpn** } [*number*]

Parameters

Parameter	Description	Value
tcp	Displays information about TCP error messages related to LDP sessions.	-
udp	Displays information about UDP error messages related to LDP sessions.	-
l2vpn	Displays information about L2VPN error messages related to LDP sessions.	-
number	Specifies the number of LDP-related error messages to be displayed.	The value is an integer ranging from 1 to 100.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If an exception occurs on an MPLS network, run the **display mpls ldp error packet** command to view information about LDP-related error messages such as the number of received error messages.

Example

# Displays information about error UDP packets related to LDP.

```
<HUAWEI> display mpls ldp error packet udp

 LDP Error UDP Packet
 Total received error packet number: 58
 Record error packet number        : 10
 Max Record error packet number    : 10
------------------- Number 1 ----------------------
 Date&Time         : 2011-11-08 16:39:59+08:00
 Error Reason      : unknown
 Interface         : Vlanif100
 Instance ID       : 0
 Message Type      : Hello
 Length            : 34
 Packet content    :
 01 64 00 14 00 00 00 32 04 00 00 04 00 0f 00 00
 04 01 00 04 01 01 01 01 00 00 00 00 00 00 00 00
 00 00
```

Table 9-20 Description of the **display mpls ldp error packet** command output

Item	Description
Total received error packet number	Number of received error messages related to LDP sessions.
Record error packet number	Number of recorded error messages related to LDP sessions.
Max Record error packet number	Maximum number of error messages that can be recorded.
Date&Time	Date and time when an error message was received.
Error Reason	Cause for an error.
Interface	An interface that receives the message.
Instance ID	ID of an LDP instance to which the error message belongs.
Message Type	Message type, which includes but is not limited to the following: ● Address ● Address Withdraw ● Capability ● Hello ● Initialization ● KeepAlive ● Label Request ● Label Mapping ● Label Withdraw ● Label Release ● Label Abort Request ● Notification ● Unknown
Length	Length of the error message
Packet content	Contents of the error message in the binary format.

9.1.25 display mpls ldp error packet state

Function

The **display mpls ldp error packet state** command displays the record status of LDP-related error messages.

Format

display mpls ldp error packet state

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If an exception occurs on an MPLS network, run the **display mpls ldp error packet state** command to view the record status of UDP, TCP, and L2VPN error messages related to LDP sessions.

Example

# Display the record status of LDP-related error messages.

```
<HUAWEI> display mpls ldp error packet state
--------------------------------------------
 Error UDP packet state             : ON
 Max UDP error packet number        : 100
 Current UDP error packet number    : 0
 Error TCP packet state             : ON
 Max TCP error packet number        : 100
 Current TCP error packet number    : 0
 Error L2VPN packet state           : ON
 Max L2VPN error packet number      : 100
 Current L2VPN error packet number : 0
--------------------------------------------
```

Table 9-21 Description of the display mpls ldp error packet state command output

Item	Description
Error UDP packet state	Whether UDP error messages can be detected and recorded: ● ON: UDP error message detection is enabled. ● OFF: UDP error message detection is disabled.
Max UDP error packet number	Maximum number of UDP error messages that can be recorded.
Current UDP error packet number	Number of recorded UDP error messages.

Item	Description
Error TCP packet state	Whether TCP error messages can be detected and recorded: ● ON: TCP error message detection is enabled. ● OFF: TCP error message detection is disabled.
Max TCP error packet number	Maximum number of TCP error messages that can be recorded.
Current TCP error packet number	Number of recorded TCP error messages.
Error L2VPN packet state	Whether L2VPN error messages can be detected and recorded: ● ON: L2VPN error message detection is enabled. ● OFF: L2VPN error message detection is disabled.
Max L2VPN error packet number	Maximum number of L2VPN error messages that can be recorded.
Current L2VPN error packet number	Number of recorded L2VPN error messages.

9.1.26 display mpls ldp event adjacency-down

Function

The **display mpls ldp event adjacency-down** command displays events that LDP adjacencies go Down.

Format

display mpls ldp event adjacency-down [**interface** *interface-type interface-number* | **remote**] [**peer** *peer-id*] [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays events that LDP adjacencies on a specified interface go Down. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Parameter	Description	Value
remote	Indicates the remote LDP peer.	-
peer *peer-id*	Specifies the LSR ID of an LDP peer.	The value is in dotted decimal notation.
verbose	Displays details about events that LDP adjacencies go Down.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Run the **display mpls ldp event adjacency-down** command to view the event that an LDP adjacency went Down. The information includes the time, reason, and the duration of the LDP adjacency.

Precautions

A maximum of 1024 events can be displayed.

Example

# Display the events that LDP adjacencies go Down.

```
<HUAWEI> display mpls ldp event adjacency-down

 LDP Adjacency Down Information
 ------------------------------------------------------------------------
 PeerID            Down       Down                    Duration      Reason
                   Date       Time                    Time
 ------------------------------------------------------------------------
 2.2.2.2:0         2012-04-24 17:08:59+00:00          0h44m54s      C
 2.2.2.2:0         2012-04-26 15:43:54+00:00          46h34m54s     A
 -----------------------------------------------------------------------------
 TOTAL: 2 Record(s) Found.
 A : The Adjacency is down because Hello Timer Expired.
 C : The administrator configuration to trigger.
 D : The Adjacency is down because delay-deleting timer expired.
 P : The Adjacency is down because the peer is being deleted.
 O : Other reason.
```

Table 9-22 Description of the display mpls ldp event adjacency-down command output

Item	Description
PeerID	LSR ID of an LDP peer.

Item	Description
Down Date	Date when an LDP adjacency went Down.
Down Time	Time when an LDP adjacency went Down.
Duration Time	Time elapsed since an LDP adjacency established.
Reason	Causes for the LDP adjacency Down event: ● A: The Hello timer expires. ● C: The configuration is changed. ● D: The delay deleting timer expires. ● P: The peer is deleted. ● O: other causes.

# Display detailed information that LDP adjacencies go Down.

```
<HUAWEI> display mpls ldp event adjacency-down verbose

 LDP Adjacency-Down Information
 ------------------------------------------------------------------------
 SN                           : 1
 PeerID                        : 2.2.2.2
 VrfID                        : 0
 DownDate                         : 2012-04-24
 DownTime                         : 17:08:59+00:00
 DurationTime                     : 0h44m54s
 MaxInterval(sec)                 : 5
 Reason                         : configuration to trigger
 Type                         : Local Adjacency
 DiscoverySource                  : Vlanif60
 -------------------------------------------------------------------------------
 SN                           : 2
 PeerID                        : 2.2.2.2
 VrfID                        : 0
 DownDate                         : 2012-04-26
 DownTime                         : 15:43:54+00:00
 DurationTime                     : 46h34m54s
 MaxInterval(sec)                 : 6
 Reason                         : Hello Timer Expired
 Type                         : Local Adjacency
 DiscoverySource                  : Vlanif60
 -------------------------------------------------------------------------------
  TOTAL: 2 Record(s) Found.
```

Table 9-23 Description of the display mpls ldp event adjacency-down verbose command output

Item	Description
SN	Serial number.
PeerID	LSR ID of an LDP peer.

Item	Description
VrfID	ID of a VPN instance.
DownDate	Date when an LDP adjacency went Down.
DownTime	Time when an LDP adjacency went Down.
DurationTime	Time elapsed since an LDP adjacency established.
MaxInterval (sec)	Maximum interval for sending a Hello message.
Reason	Reason for the LDP adjacency Down event: ● A: The Hello timer expires. ● C: The configuration is changed. ● D: The delay deleting timer expires. ● P: The peer is deleted. ● O: other causes.
Type	Adjacency type: ● Local Adjacency: Directly connected adjacency. ● Remote Adjacency: Indirectly connected adjacency.
DiscoverySource	Interface where an LDP peer is discovered.

9.1.27 display mpls ldp event gr-helper

Function

The **display mpls ldp event gr-helper** command displays GR Helper information.

Format

display mpls ldp event gr-helper [**all** | *peer-id*]

Parameters

Parameter	Description	Value
all	Displays information about all GR Helpers.	-

Parameter	Description	Value
peer-id	Displays information about a GR Helper on a specified LDP peer.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If GR Helpers are configured, run the **display mpls ldp event gr-helper** command to view GR Helper information.

Example

# Display GR Helper information.

```
<HUAWEI> display mpls ldp event gr-helper
  LDP GR-Helper Peer Info
 ---------------------------------------------------------------------
 LDP InstanceId              : 0          Vpn Instance Name:
 Peer ID                     : 1.1.1.1
 Label Advertisement Mode    : Downstream Unsolicited
 Timer State                 :
 Recovery Timer Left         : 229(s)
 Peer Gr Timer Configuration:
 Reconnect Timer             : 300(s)     Recovery Timer   : 300(s)
 Stale Lsp State             :
 USCB Counter                : 3          DSCB Counter     : 3
 ---------------------------------------------------------------------
 Total GR Peer Counter: 1
```

Table 9-24 Description of the display mpls ldp event gr-helper command output

Item	Description
LDP InstanceId	LDP instance name.
Vpn Instance Name	VPN instance name. **NOTE** The device does not support this parameter.
Peer ID	LSR ID of an LDP peer.
Label Advertisement Mode	Mode used by LDP to advertise labels. To set the mode used by LDP to advertise labels, run the **mpls ldp advertisement** command.
Timer State	Status of the timer.

Item	Description
Recovery Timer Left	Remaining time before an LSP starts to be reestablished.
Peer Gr Timer Configuration	Configuration of the GR timers.
Reconnect Timer	Value of the LDP session reconnection timer. To set the value of the LDP session reconnection timer, run the **graceful-restart timer reconnect** command.
Recovery Timer	Value of the LSP recovery timer. To set the value of the LSP recovery timer, run the **graceful-restart timer recovery** command.
Stale Lsp state	Status of the primary LSP.
USCB Counter	Number of upstream control blocks (USCBs).
DSCB Counter	Number of downstream control blocks (DSCBs).
Total GR Peer Counter	Number of GR Helper.

9.1.28 display mpls ldp event session-down

Function

The **display mpls ldp event session-down** command displays events that LDP sessions go Down.

Format

display mpls ldp event session-down

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display mpls ldp event session-down** command to view events that LDP sessions go Down, including the cause and time.

Example

# Display events that LDP sessions go Down.

```
<HUAWEI> display mpls ldp event session-down

LDP Session Down Information
------------------------------------------------------------------------------
PeerID      Down       Down             Duration   Flag Reason
           Date       Time             Time
------------------------------------------------------------------------------
10.1.2.9:0  2011-12-15 10:14:11+00:00   0h6m15s    L    Recv Noti(0x000a)

10.1.2.9:0  2011-12-15 10:14:26+00:00   0h6m34s    L    Recv Noti(0x000a)

------------------------------------------------------------------------------
TOTAL: 2 Record(s) Found.
R: Remote peer.
L: Local peer.
B: Both of local and remote peer.
G: Graceful Restart Session.
Important notification message error code:
  0x0003: Bad PDU Length.
  0x0005: Bad Message Length.
  0x0007: Bad TLV Length.
  0x0009: Hello Hold Timer Expired.
  0x000a: Shutdown.
  0x0014: KeepAlive Timer Expired.
```

Table 9-25 Description of the display mpls ldp event session-down command output

Item	Description
PeerID	LSR ID of an LDP peer.
Down Date	Date when an LDP session went down.
Down Time	Time when an LDP session went down.
Duration Time	Time elapsed since an LDP adjacency established.
Flag	Peer type. ● R: Remote peer, indicating that a remote session has been established. ● L: Local peer, indicating that a local session has been established. ● B: Both of local and remote peer, indicating that both local and remote sessions have been established. ● G: Graceful Restart Session.
Reason	Description of the cause.

Item	Description
Important notification message error code	Important notification message error code.
Bad PDU Length	Incorrect PDU length.
Bad Message Length	Incorrect message length.
Bad TLV Length	Incorrect TLV length.
Hello Hold Timer Expired	Hello Hold timer expired.
Shutdown	The peer actively shuts down the session.
KeepAlive Timer Expired	Keepalive timer expired.

9.1.29 display mpls ldp interface

Function

The **display mpls ldp interface** command displays information about LDP-enabled interfaces.

Format

display mpls ldp interface [*interface-type interface-number* | [**all**] [**verbose**]]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. If the parameter is specified, the configurations of a specified LDP-enabled interface are displayed.	-
all	Displays information about all LDP-enabled interfaces.	-
verbose	Displays detailed information about LDP-enabled interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display mpls ldp interface** command to view configurations of LDP-enabled interfaces and some real-time information, such as the number of sent and received Hello messages.

Example

# Display information about LDP-enabled interfaces.

```
<HUAWEI> display mpls ldp interface

 LDP Interface Information in Public Network
 Codes:LAM(Label Advertisement Mode), IFName(Interface name)
 A '*' before an interface means the entity is being deleted.
 -------------------------------------------------------------------------------
 IFName         Status       LAM   TransportAddress   HelloSent/Rcv
 -------------------------------------------------------------------------------
Vlanif100       Active       DU    10.1.1.1           29574/29539
 -------------------------------------------------------------------------------
```

Table 9-26 Description of the display mpls ldp interface command output

Item	Description
IFName	Name of an LDP-enabled interface.
Status	Status of the local LSR: ● Active ● Inactive
LAM	Label advertisement mode: ● DU: downstream unsolicited mode. ● DoD: downstream on demand mode. To set the label advertisement mode, run the **mpls ldp advertisement** command.
TransportAddress	IP address of a node that initiates a TCP connection for an LDP session.
HelloSent/Rcv	Number of sent and received Hello messages.

# Display detailed information about LDP-enabled interfaces.

```
<HUAWEI> display mpls ldp interface verbose

 LDP Interface Information in Public Network
 -------------------------------------------------------------------------------
 Interface Name :Vlanif100
 LDP ID         : 10.1.1.1:0           Transport Address : 10.1.1.1
 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          : 10 Sec
 Label Advertisement Mode        : Downstream Unsolicited
 Hello Message Sent/Rcvd         : 29913/29878 (Message Count)
 Entity Deletion Status          : No
 mLDP P2MP Capability            : Disable
 mLDP MP2MP Capability           : Disable
 ------------------------------------------------------------------------------
```

Table 9-27 Description of the display mpls ldp interface verbose command output

Item	Description
Interface Name	Name of an LDP-enabled interface.
LDP ID	LDP identifier.
Transport Address	IP addresses used in the TCP connection of a session.
Entity Status	Status of this entity: ● Active ● Inactive
Effective MTU	MTU value used for creating an LSP.
Configured Hello Hold Timer	Timeout period of the configured Hello hold timer. To set the timeout period of the Hello hold timer, run the **mpls ldp timer hello-hold** command.
Negotiated Hello Hold Timer	Negotiated value of the Hello hold timer, which is the smaller value of the Hello hold timers configured on the local and remote LDP peers.
Configured Hello Send Timer	Timeout period of the configured Hello send timer. To set the timeout period of the Hello send timer, run the **mpls ldp timer hello-send** command.
Configured Keepalive Hold Timer	Timeout period of the configured Keepalive hold timer. To set the timeout period of the Keepalive hold timer, run the **mpls ldp timer keepalive-hold** command.
Configured Keepalive Send Timer	Timeout period of the configured Keepalive send timer. To set the timeout period of the Keepalive send timer, run the **mpls ldp timer keepalive-send** command.

Item	Description
Configured Delay Timer	Timeout period of the Delay timer, which, in LDP and IGP synchronization, is the time that an interface waits to establish an LSP after an LDP session is established.
Label Advertisement Mode	Label advertisement mode: ● Downstream Unsolicited ● Downstream on Demand To set the label advertisement mode, run the **mpls ldp advertisement** command.
Hello Message Sent/Rcvd	Number of sent and received Hello messages.
Entity Deletion Status	Deletion status of an instance: ● Yes: The instance is being deleted. ● No: The instance is not being deleted.
mLDP P2MP Capability	Whether mLDP P2MP is enabled: ● Enable ● Disable **NOTE** The switch does not support this function.
mLDP MP2MP Capability	Whether mLDP MP2MP is enabled: ● Enable ● Disable **NOTE** The switch does not support this function.

9.1.30 display mpls label all summary

Function

The **display mpls label all summary** displays allocation information about all MPLS labels.

Format

display mpls label all summary

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a session is established, the system collects statistics on label usage, including the allocation range and protocol type. You can use the **display mpls label all summary** command to view the allocation of label space and the corresponding protocol type.

Example

# Display allocation information about MPLS labels.

```
<HUAWEI> display mpls label all summary
TableType      MinValue    MaxValue    AvailableNum
Reserved              0          15              16
Static               16        1023            1008
Dynamic            1024      163840          162815
Block            163841      180244           16404
```

NOTE

The preceding information is an example. The allocation ranges of labels depend on the actual situation.

Table 9-28 Description of the **display mpls label all summary** command output

Item	Description
TableType	Label type. ● Reserved: indicates reserved labels. ● Static: indicates static labels, mainly for MPLS TE and BGP. ● Dynamic: indicates dynamic labels, mainly for LDP, MPLS TE, and BGP. ● Block: indicates block labels, mainly for BGP.
MinValue	Minimum label value.
MaxValue	Maximum label value.
AvailableNum	Number of labels that can be allocated.

9.1.31 display mpls ldp lsp

Function

The **display mpls ldp lsp** command displays information about an LDP LSP.

Format

display mpls ldp lsp [**all** | *destination-address mask-length*] [**peer** *peer-id*]

display mpls ldp lsp inbound-policy

Parameters

Parameter	Description	Value
all	Displays information about all LDP LSPs.	-
destination-address	Specifies the destination IPv4 address of an LDP LSP.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the specified IPv4 address.	The value is an integer ranging from 0 to 32.
peer *peer-id*	Specifies the peer ID.	The value is in dotted decimal notation.
inbound-policy	Displays information about the LSPs that have passed an inbound policy, in addition to information about the LSPs that are established without applying the inbound policy.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After LDP LSPs are set up, run the **display mpls ldp lsp** command to view detailed information about LSPs such as the outbound interfaces, next hop addresses, total number, and types.

Example

# Display information about LSPs.

```
<HUAWEI> display mpls ldp lsp

 LDP LSP Information
 -------------------------------------------------------------------------------
 Flag after Out IF: (I) - LSP Is Only Iterated by RLFA
 -------------------------------------------------------------------------------
 DestAddress/Mask   In/OutLabel    UpstreamPeer    NextHop        OutInterface
 -------------------------------------------------------------------------------
 10.3.3.3/32        3/NULL         10.4.4.9        127.0.0.1      InLoop0
 10.3.3.9/32        3/NULL         10.4.4.9        127.0.0.1      InLoop0
*10.3.3.9/32        Liberal/1024                  DS/10.4.4.9
 10.4.4.9/32        NULL/3         -              172.16.1.2     Vlanif100
 10.4.4.9/32        1029/3         10.4.4.9       172.16.1.2     Vlanif100
 -------------------------------------------------------------------------------
 TOTAL: 4 Normal LSP(s) Found.
 TOTAL: 1 Liberal LSP(s) Found.
 TOTAL: 0 Frr LSP(s) Found.
 A '*' before an LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stale
 A '*' before a UpstreamPeer means the session is stale
 A '*' before a DS means the session is stale
 A '*' before a NextHop means the LSP is FRR LSP
```

Table 9-29 Description of the display mpls ldp lsp command output

Item	Description
DestAddress/ Mask	Destination address and mask of an LSP.
In/OutLabel	Values of the incoming and outgoing labels. An asterisk (*) before In/OutLabel indicates that the LSP is in the Stale state and needs to be restored.
UpstreamPeer	Upstream peer of an LSP. An asterisk (*) before UpstreamPeer indicates that the session is in the GR state.
NextHop	Next hop IP address. An asterisk (*) before NextHop indicates that the LSP is an FRR LSP. DS is short for DownStream. The address next to DS/ is the LSR ID of a downstream peer.
OutInterface	Name of an outbound interface.
TOTAL: 4 Normal LSP(s) Found.	Total number of normal LSPs.
TOTAL: 1 Liberal LSP(s) Found.	Total number of liberal LSPs.
TOTAL: 0 Frr LSP(s) Found.	Total number of FRR LSPs.

9.1.32 display mpls ldp lsp statistics

Function

The **display mpls ldp lsp statistics** command displays statistics about LDP LSPs.

Format

display mpls ldp lsp statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls ldp lsp statistics** command displays the statistics about an LDP LSP, whereas the **display mpls lsp statistics** command displays the statistics about all types of LSPs.

Example

# Display statistics about LDP LSPs.

```
<HUAWEI> display mpls ldp lsp statistics

 LDP LSP Statistics Information
 A '*' before a number means the LSP is for longest-match
 ------------------------------------------------------------------------------
 VPNInstanceName   Total   Ingress   Transit   Egress   Liberal  FRR
 ------------------------------------------------------------------------------
 -                  14      4         4         3        3         0
                    *0     *0        *0        *0       *-        *0
 ------------------------------------------------------------------------------
```

Table 9-30 Description of the display mpls ldp lsp statistics command output

Item	Description
VPNInstanceName	Name of a VPN instance: ● A hyphen (-) indicates a public network instance. ● If LDP multi-instance is configured, the name of the created VPN instance is displayed. **NOTE** The switch does not support this parameter.

Item	Description
Total	Number of LDP LSPs in an instance.
Ingress	Number of ingress LSPs in an instance.
Transit	Number of transit LSPs in an instance.
Egress	Number of egress LSPs in an instance.
Liberal	Number of liberal LSPs in an instance.
FRR	Number of FRR LSPs in an instance. **NOTE** The switch does not support this parameter.

9.1.33 display mpls ldp peer

Function

The **display mpls ldp peer** command displays information about LDP peers.

Format

display mpls ldp peer [[**all**] [**verbose**] | *peer-id*]

Parameters

Parameter	Description	Value
verbose	Displays detailed information about LDP peers.	-
peer-id	Displays information about a specified LDP peer.	The value is in dotted decimal notation.
all	Displays information about all LDP peers.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If an LDP LSP fails to be established, run the **display mpls ldp peer** command to view the **DiscoverySource** field and check the interface through which the peer relationship is established.

The system supports the coexistent local and remote LDP peers. When you run the **display mpls ldp peer** command, information about both local and remote LDP peers is displayed.

You can set the *peer-id* parameter to specify a peer.

Precautions

You can view information about LDP peers only after the peers have been established using the **mpls ldp (interface view)** or **remote-ip** command.

Example

# Display information about LDP peers.

```
<HUAWEI> display mpls ldp peer

 LDP Peer Information in Public network
 A '*' before a peer means the peer is being deleted.
 ------------------------------------------------------------------------------
 PeerID                 TransportAddress   DiscoverySource
 ------------------------------------------------------------------------------
 2.2.2.2:0              2.2.2.2            Remote Peer : rtb
 3.3.3.3:0              3.3.3.3            Vlanif100
 ------------------------------------------------------------------------------
 TOTAL: 2 Peer(s) Found.
```

Table 9-31 Description of the display mpls ldp peer command output

Item	Description
PeerID	LDP identifier of the peer in the format of <LSR ID>:<label space>. The value of a label space can be either of the following: ● 0: per-platform label space. ● Non-0: per-interface label space.
TransportAddress	Transport address of an LDP peer. The transport address is used to set up TCP connections.
DiscoverySource	Discovery source of an LDP peer: ● Interface name: indicates the source that discovers the local LDP peer. ● Remote LDP peer name: indicates the source that discovers the remote LDP peer.

# Display detailed information about LDP peers.

```
<HUAWEI> display mpls ldp peer verbose

 LDP Peer Information in Public network
 ------------------------------------------------------------------------------
 Peer LDP ID          : 2.2.2.2:0
 Peer Max PDU Length : 4096          Peer Transport Address   : 2.2.2.2
 Peer Loop Detection : Off           Peer Path Vector Limit   : ----
 Peer FT Flag         : Off          Peer Keepalive Timer     : 45 Sec
```

```
Recovery Timer      : ----         Reconnect Timer          : ----
Peer Type           :Remote
Peer Label Advertisement Mode : Downstream Unsolicited
Peer Discovery Source         : remote peer: rtb
Peer Deletion Status          : No
Capability-Announcement       : Off
Peer mLDP P2MP Capability     : Off
Peer mLDP MBB Capability      : Off
------------------------------------------------------------------------------
Peer LDP ID         : 3.3.3.3:0
Peer Max PDU Length : 4096         Peer Transport Address   : 3.3.3.3
Peer Loop Detection : Off          Peer Path Vector Limit   : ----
Peer FT Flag        : Off          Peer Keepalive Timer     : 45 Sec
Recovery Timer      : ----         Reconnect Timer          : ----
Peer Type           : Local
Peer Label Advertisement Mode : Downstream Unsolicited
Peer Discovery Source         : Vlanif100
Peer Deletion Status          : No
Capability-Announcement       : Off
Peer mLDP P2MP Capability     : Off
Peer mLDP MBB Capability      : Off
------------------------------------------------------------------------------
```

Table 9-32 Description of the display mpls ldp peer verbose command output

Item	Description
Peer LDP ID	LDP identifier of the peer in the format of <LSR ID>:<label space>. The value of a label space can be either of the following: ● 0: per-platform label space. ● Non-0: per-interface label space.
Peer Max PDU Length	Maximum size of a PDU sent by an LDP peer.
Peer Transport Address	Transport address of an LDP peer. The transport address is used to set up TCP connections.
Peer Loop Detection	Whether loop detection of an LDP peer is enabled: ● On: Loop detection is enabled. ● Off: Loop detection is disabled. To configure the loop detection function, run the **loop-detect** command.
Peer Path Vector Limit	Indicates the upper limit of the Path Vector for an LDP peer. To set the upper limit of the Path Vector for an LDP peer, run the **path-vectors** command.
Peer FT Flag	GR FT flag of an LDP peer: ● On: LDP GR is enabled. ● Off: LDP GR is disabled. The flag can only be set after an Initialization message containing an FT TLV is received.

Item	Description
Peer Keepalive Timer	Configured value of the Keepalive timer on an LDP peer. To set the value of the Keepalive timer, run the **mpls ldp timer keepalive-hold** command.
Recovery Timer	Timeout period of the Recovery timer of an LDP peer. The value of the Recovery Timer field is not null only when the Peer FT Flag field is On. To set the timeout period of the Recovery timer, run the **graceful-restart timer recovery** command.
Reconnect Timer	Timeout period of the Reconnect timer of an LDP peer. The value of the Recovery Timer field is not null only when the Peer FT Flag field is On. To set the timeout period of the Reconnect timer, run the **graceful-restart timer reconnect** command.
Peer Type	Type of an LDP peer: ● Local ● Remote ● Local&Remote
Peer Label Advertisement Mode	Indicates the label advertisement mode of an LDP peer: ● Downstream Unsolicited ● Downstream on Demand The switch supports the Downstream Unsolicited (DU) mode.
Peer Discovery Source	Discovery source of an LDP peer: ● If the interface is displayed, the source of the local LDP peer is the local interface. ● If the configuration name of the remote peer is displayed, the source end of the remote LDP peer is the remote peer.
Peer Deletion Status	Deletion status of an LDP peer: ● Yes: LDP peer is being deleted. ● No: LDP peer is not being deleted.

Item	Description
Capability-Announcement	Status of the LDP dynamic capability announcement function: ● On: LDP dynamic capability announcement is enabled. ● Off: LDP dynamic capability announcement is disabled. **NOTE** The switch does not support this parameter.
Peer mLDP P2MP Capability	Whether the LDP peer supports mLDP P2MP: ● On: The LDP peer supports mLDP P2MP. ● Off: The LDP peer does not support mLDP P2MP.
Peer mLDP MBB Capability	Whether the LDP peer supports make-before-break: ● On: The LDP peer supports mLDP make-before-break. ● Off: The LDP peer does not support mLDP make-before-break.

9.1.34 display mpls ldp peer statistics

Function

The **display mpls ldp peer statistics** command displays statistics about LDP peers.

Format

display mpls ldp peer statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display mpls ldp peer statistics** command to view the number of local LDP peers, remote LDP peers, and coexistent local and remote LDP peers.

Example

# Display statistics about LDP peers.

```
<HUAWEI> display mpls ldp peer statistics

 LDP Peer Statistics Information
 ---------------------------------------------------------
 PeerType        Local   Remote   Local&Remote   Total
 ---------------------------------------------------------
 PeerNumber      0       1        1              2
 ---------------------------------------------------------
```

Table 9-33 Description of the display mpls ldp peer statistics command output

Item	Description
PeerType	Type of LDP peers.
PeerNumber	Number of LDP peers.
Local	Number of local LDP peers.
Remote	Number of remote LDP peers.
Local&Remote	Number of coexistent local and remote LDP peers.
Total	Total number of all types of LDP peers.

9.1.35 display mpls ldp remote-peer

Function

The **display mpls ldp remote-peer** command displays information about a remote LDP peer.

Format

display mpls ldp remote-peer [*remote-peer-name* | **peer-id** *lsr-id*]

Parameters

Parameter	Description	Value
remote-peer-name	Specifies the name of a remote LDP peer.	The value is an existing remote LDP peer.
peer-id *lsr-id*	Specifies the LSR ID of a remote LDP peer.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Remote LDP peers are used to set up remote LDP sessions to transmit VPN services.

To view information about the configured remote LDP peers, run the **display mpls ldp remote-peer** command.

Run the **display mpls ldp remote-peer** command to view information about the configured remote LDP peer. Different from the **display mpls ldp peer** command, the **display mpls ldp remote-peer** command is used to view the remote LDP peer that is configured on the local device if the configuration takes effect. The **display mpls ldp peer** command is used to view the LDP peer discovered by the local device only when the LDP peers are configured on local and peer devices and the LDP peer relationship is set up.

Example

# Display information about remote LDP peers.

```
<HUAWEI> 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          : 10 Sec
 Hello Packet sent/received      : 61/59
 Label Advertisement Mode        : Downstream Unsolicited
 Remote Peer Deletion Status     : No
 Auto-config                     : ---
------------------------------------------------------------------------------
 TOTAL: 1 Peer(s) Found.
```

Table 9-34 Description of the **display mpls ldp remote-peer** command output

Item	Description
Remote Peer Name	Name of a remote LDP peer.
Remote Peer IP	IP address of a remote LDP peer.
LDP ID	Local LDP ID.
Transport Address	Transport address, which is used to set up the LDP session between the local and remote peers.

Item	Description
Entity Status	Status of a remote LDP peer: - Active - Inactive
Configured Keepalive Hold Timer	Timeout period of the configured Keepalive hold timer.
Configured Keepalive Send Timer	Timeout period of the configured Keepalive send timer.
Configured Hello Hold Timer	Timeout period of the configured Hello hold timer.
Negotiated Hello Hold Timer	Timeout period of the negotiated Hello hold timer.
Configured Hello Send Timer	Timeout period of the configured Hello send timer.
Configured Delay Timer	Timeout period of the Delay timer, which, in LDP and IGP synchronization, is the time that an interface waits to establish an LSP after an LDP session is established.
Hello Packet sent/received	Number of sent and received Hello packets.
Label Advertisement Mode	Label advertisement mode in an LDP session. The default mode is DU. To set the label advertisement mode, run the **mpls ldp advertisement** command.
Remote Peer Deletion Status	Deletion status of an LDP peer: - Yes: The LDP peer is being deleted. - No: The LDP peer is not being deleted.
Auto-config	Source that triggers the creation of a remote peer: - ---: created using LDP configurations. - L2VPN: After an L2VPN is configured, the remote LDP peer is automatically configured. LDP configurations can also be involved. - RLFA: created using remote LFA. - Auto Accept: The remote LDP session is automatically established after a local device receives Targeted Hello messages.

9.1.36 display mpls ldp session

Function

The **display mpls ldp session** command displays information about LDP sessions.

Format

display mpls ldp session [*peer-id* | [**all**] [**verbose**]]

Parameters

Parameter	Description	Value
peer-id	Displays information about LDP sessions of a specified LSR ID.	The value is in dotted decimal notation.
all	Displays information about all LDP sessions.	-
verbose	Displays detailed information about LDP sessions.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After creating an LDP session, run the **display mpls ldp session** command to verify that the LDP session is created successfully and view information about the LDP session, such as the number of sent or received Keepalive messages.

Prerequisites

MPLS has been enabled globally using the **mpls** command, and MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

If you run the **display mpls ldp session** command without specifying any parameter, information about all LDP sessions is displayed.

Example

# Display information about all LDP sessions.

```
<HUAWEI> 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.
```

Table 9-35 Description of the display mpls ldp session command output

Item	Description
PeerID	LDP identifier of the peer in the format of <LSR ID>:<label space>. The value of a label space can be either of the following: ● 0: per-platform label space. ● 1: per-interface label space.
Status	Status of an LDP session: ● NonExistent: LDP peers at both ends of the LDP session exchange Hello messages to negotiate a TCP connection. After the TCP connection is established, the LDP session enters the Initialized state. The Non-Existent state is the initial state in the LDP session state machine. ● Initialized: The LDP session is in the initialization state. ● Open Sent: The LSR playing the active role in the LDP session sends an Initialization message to the LSR playing the passive role and waits for a reply during initialization. ● Open Recv: LDP peers at both ends of the LDP session wait for receiving a Keepalive message from each other during initialization. If they receive a Keepalive message from each other, the LDP session enters the Operational state. ● Operational: An LDP session is established successfully.
LAM	Label advertisement mode of an LDP peer. The default mode is DU. To set the label advertisement mode, run the **mpls ldp advertisement** command.

Item	Description
SsnRole	Role that an LSR plays in an LDP session: ● Active: an LSR with a larger LSR ID between two LSRs. ● Passive: an LSR with a smaller LSR ID between two LSRs.
SsnAge	Time elapsed since an LDP session was set up in DDDD:HH:MM format.
KASent/Rcv	Number of Keepalive messages sent and received by an LDP session.

# Display detailed information about all LDP sessions.

```
<HUAWEI> display mpls ldp session verbose

 LDP Session(s) in Public Network
 ------------------------------------------------------------------------------
 Peer LDP ID      : 2.2.2.2:0           Local LDP ID    : 1.1.1.1:0
 TCP Connection   : 1.1.1.1 <- 2.2.2.2
 Session State    : Operational          Session Role    : Passive
 Session FT Flag  : Off                  MD5 Flag        : Off
 Reconnect Timer  : ---                  Recovery Timer  : ---
 Keychain Name    : kc1
 Authentication applied:---

 Negotiated Keepalive Hold Timer   : 45 Sec
 Configured Keepalive Send Timer   : 3 Sec
 Keepalive Message Sent/Rcvd       : 438/438 (Message Count)
 Label Advertisement Mode          : Downstream Unsolicited
 Label Resource Status(Peer/Local) : Available/Available
 Session Age                       : 0000:01:49 (DDDD:HH:MM)
 Session Deletion Status           : No

 Capability:
  Capability-Announcement          : On
  mLDP P2MP Capability             : Off
  mLDP MP2MP Capability            : Off
  mLDP MBB Capability              : Off

 Outbound&Inbound Policies applied : NULL

 Addresses received from peer: (Count: 3)
 10.1.1.2           2.2.2.2            10.1.2.1
 ------------------------------------------------------------------------------
```

Table 9-36 Description of the display mpls ldp session verbose command output

Item	Description
Peer LDP ID	LDP identifier of the peer in the format of <LSR ID>:<label space>. The value of a label space can be either of the following: ● 0: per-platform label space. ● 1: per-interface label space.

Item	Description
Local LDP ID	Local LDP identifier in the format of <LSR ID>:<label space>. The value of a label space can be either of the following: ● 0: per-platform label space. ● 1: per-interface label space.
TCP Connection	TCP connection of an LDP session: ● The LSR with a larger LSR ID value plays an active role in establishing the TCP connection. ● The LSR with a smaller LSR ID value plays a passive role in establishing the TCP connection.
Session State	Status of an LDP session: ● NonExistent: LDP peers at both ends of the LDP session exchange Hello messages to negotiate a TCP connection. After the TCP connection is established, the LDP session enters the Initialized state. The Non-Existent state is the initial state in the LDP session state machine. ● Initialized: The LDP session is in the initialization state. ● Open Sent: The LSR playing the active role in the LDP session sends an Initialization message to the LSR playing the passive role and waits for a reply during initialization. ● Open Recv: LDP peers at both ends of the LDP session wait for receiving a Keepalive message from each other during initialization. If they receive a Keepalive message from each other, the LDP session enters the Operational state. ● Operational: An LDP session is established successfully.
Session Role	Role that an LSR plays in an LDP session: ● Active: an LSR with a larger LSR ID between two LSRs. ● Passive: an LSR with a smaller LSR ID between two LSRs.

Item	Description
Session FT Flag	Negotiated LDP GR capability: ● On: Negotiated LDP GR capability is enabled. ● Off: Negotiated LDP GR capability is disabled.
MD5 Flag	MD5 authentication flag: ● On: MD5 authentication is enabled during the TCP connection establishment. ● Off: MD5 authentication is disabled during the TCP connection establishment.
Reconnect Timer	Negotiated timeout period of the Reconnect timer. The value of the Recovery Timer field is not null only when the Session FT Flag field is On.
Recovery Timer	Negotiated timeout period of the Recovery timer. The value of the Recovery Timer field is not null only when the Session FT Flag field is On.
Keychain Name	Referenced keychain authentication name.
Authentication applied	Existing authentication mode: ● Peer: single peer authentication ● Peer-group PeerGroupName: peer-group authentication. PeerGroupName indicates a peer group name. ● ALl: All authentication
Negotiated Keepalive Hold Timer	Negotiated value of the Keepalive hold timer, which is the smallest value of the Keepalive hold timers configured on the local and remote LDP peers.
Configured Keepalive Send Timer	Timeout period of the configured Keepalive send timer.
Keepalive Message Sent/Rcvd	Number of Keepalive messages sent and received by an LDP session.

Item	Description
Label Advertisement Mode	Label advertisement mode: ● Downstream Unsolicited ● Downstream on Demand The default mode is Downstream Unsolicited (DU). To set the label advertisement mode, run the **mpls ldp advertisement** command.
Label Resource Status(Peer/Local)	Label resource status of the remote and local peers.
Session Age	Time elapsed since an LDP session was set up.
Session Deletion Status	Deletion status of an LDP session: ● Yes: The LDP session is being deleted. ● No: The LDP session is not being deleted.
Capability	LDP capability.
Capability-Announcement	LDP dynamic capability announcement function: ● On: LDP dynamic capability announcement is enabled. ● Off: LDP dynamic capability announcement is disabled. **NOTE** The switch does not support this parameter.
mLDP P2MP Capability	Whether mLDP P2MP is supported after a session is negotiated: ● On: mLDP P2MP is supported. ● Off: mLDP P2MP is not supported. **NOTE** The switch does not support this parameter.
mLDP MP2MP Capability	Whether mLDP MP2MP is supported after a session is negotiated: ● On: mLDP MP2MP is supported. ● Off: mLDP MP2MP is not supported. **NOTE** The switch does not support this parameter.

Item	Description
mLDP MBB Capability	Whether mLDP make-before-break is supported after a session is negotiated: ● On: mLDP make-before-break is supported. ● Off: mLDP make-before-break is not supported. **NOTE** The switch does not support this parameter.
Outbound&Inbound Policies applied	Outbound and inbound policies on the local node.
Addresses received from peer	Contents of an Address message sent by an LDP peer. The contents include the LSR ID of the peer and the IP address of the LDP-enabled interface.

9.1.37 display mpls ldp session statistics

Function

The **display mpls ldp session statistics** command displays statistics about sessions between LDP peers.

Format

display mpls ldp session statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display mpls ldp session statistics** command to view the number of sessions between LDP peers. Statistics are collected based on the session type and status. The session type can be local, remote, or coexistent local and remote. The session status can be Not Operational or Operational.

Example

# Display statistics about LDP sessions.

```
<HUAWEI> display mpls ldp session statistics

 LDP Session Statistics Information
 ------------------------------------------------------------
 SessionType        Local   Remote   Local&Remote   Total
 ------------------------------------------------------------
 Not Operational     0       0        0              0
 Operational        0       1        1              2
 ------------------------------------------------------------
 SessionStatistics   0       1        1              2
 ------------------------------------------------------------
```

Table 9-37 Description of the display mpls ldp session statistics command output

Item	Description
SessionType	Type of LDP sessions.
Local	Number of local LDP sessions.
Remote	Number of remote LDP sessions.
Local&Remote	Number of coexistent local and remote LDP sessions.
Total	Total number of sessions.
Not Operational	Number of sessions in the Not Operational state.
Operational	Number of sessions in the Operational state.
SessionStatistics	Total number of local sessions, remote sessions, and coexistent local and remote sessions.

9.1.38 display mpls lsp

Function

The **display mpls lsp** command displays information about LSPs.

The **display mpls lsp lsp-id** command displays information about CR-LSPs only.

Format

display mpls lsp lsp-id *ingress-lsr-id session-id lsp-id* [**verbose**]

display mpls lsp [[**vpn-instance** *vpn-instance-name* [**ipv4-family** | **ipv6-family**]] [**protocol** { **bgp** | **bgp-ipv6** | **rsvp-te** | **static** | **static-cr** }] | **asbr**] [{ **exclude** | **include** } *ip-address mask-length*] [**incoming-interface** *interface-type interface-number*] [**outgoing-interface** *interface-type interface-number*]

[**in-label** *in-label-value*] [**out-label** *out-label-value*] [**nexthop** *ip-address*] [**lsr-role** { **egress** | **ingress** | **transit** }] [**verbose**]

display mpls lsp [**vpn-instance** *vpn-instance-name* [**ipv4-family** | **ipv6-family**]] **protocol ldp** [{ **exclude** | **include** } *ip-address mask-length*] [**outgoing-interface** *interface-type interface-number*] [**in-label** *in-label-value*] [**out-label** *out-label-value*] [**nexthop** *ip-address*] [**lsr-role** { **egress** | **ingress** | **transit** }] [**verbose**]

display mpls lsp stale-incoming-interface *interface-index* [**outgoing-interface** *interface-type interface-number*] [**in-label** *in-label-value*] [**out-label** *out-label-value*] [**nexthop** *ip-address*] [**lsr-role** { **egress** | **ingress** | **transit** }] [**verbose**]

display mpls lsp stale-outgoing-interface *interface-index* [**in-label** *in-label-value*] [**out-label** *out-label-value*] [**nexthop** *ip-address*] [**lsr-role** { **egress** | **ingress** | **transit** }] [**verbose**]

Parameters

Parameter	Description	Value
lsp-id	Specifies the LSP ID.	The value is an integer ranging from 0 to 65535.
ingress-lsr-id	Specifies the ID of the ingress LSR.	The value is in dotted decimal notation.
session-id	Specifies the ID of a session.	The value is an integer ranging from 0 to 65535.
vpn-instance *vpn-instance-name*	Displays detailed configurations of LSPs of a specified VPN instance.	The value must be an existing VPN instance name.
ipv4-family	Indicates the IPv4 unicast address-family.	-
ipv6-family	Indicates the IPv6 unicast address-family.	-
protocol	Displays information about LSPs of a specified type.	-
ldp	Indicates LDP.	-
bgp	Indicates BGP.	-
bgp-ipv6	Indicates BGP IPv6.	-

Parameter	Description	Value
rsvp-te	Indicates RSVP-TE.	-
static	Indicates Static.	-
static-cr	Indicates Static-CR.	-
asbr	Displays information about LSPs of a specified ASBR.	-
exclude	Displays information about LSPs, excluding information about the specific FEC.	-
include	Displays information about LSPs, including information about the specific FEC.	-
ip-address	Displays information about LSPs of a specified IPv4 address or a specified IPv6 address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the specified IPv4 address or a specified IPv6 address.	The value is an integer ranging from 0 to 32. Alternatively, it specifies the mask length of the specified IPv6 address. The value is an integer ranging from 0 to 128.
incoming-interface *interface-type interface-number*	Specifies the type and number of an inbound interface. You can view the configuration of an LSP on a specified interface.	-
outgoing-interface *interface-type interface-number*	Indicates the type and number of an outbound interface. You can view the configuration of an LSP on a specified interface.	-
in-label *in-label-value*	Displays information about LSPs of a specified incoming label.	The value is an integer ranging from 0 to 1048575.
out-label *out-label-value*	Displays information about LSPs of a specified outgoing label.	The value is an integer ranging from 0 to 1048575.

Parameter	Description	Value
nexthop *ip-address*	Displays information about LSPs of a specified IPv4 or IPv6 next hop address.	The value is in dotted decimal notation.
lsr-role	Displays information about all LSPs on the current LSR that plays a specified role.	-
egress	Displays information about LSPs of an egress LSR.	-
ingress	Displays information about LSPs of an ingress LSR.	-
transit	Displays information about LSPs of a transit LSR.	-
verbose	Displays detailed information about LSPs.	-
stale-incoming-interface	Displays information about the stale inbound interface of an LSP.	-
stale-outgoing-interface	Displays information about the stale outbound interface of an LSP.	-
interface-index	Specifies the index of a specified stale interface.	The value is a hexadecimal integer ranging from 1 to FFFFFFFE.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you do not specify a parameter, information about all LSPs is displayed.

Run the **display mpls stale-interface** command without specifying a parameter to view the index of a stale interface.

Example

# Display information about all types of LSPs.

```
<HUAWEI> display mpls lsp
-------------------------------------------------------------------------------
                 LSP Information: RSVP LSP
-------------------------------------------------------------------------------
 FEC                In/Out Label  In/Out IF                      Vrf Name
 10.2.2.9/32        NULL/11264    -/Vlanif10

Flag after Out IF: (I) - LSP Is Only Iterated by RLFA
-------------------------------------------------------------------------------
                 LSP Information: LDP LSP
-------------------------------------------------------------------------------
 FEC                In/Out Label  In/Out IF                      Vrf Name

 10.2.2.9/32        NULL/3         -/Vlanif10
 10.2.2.9/32        1024/3        -/Vlanif10
 10.3.3.9/32        NULL/3         -/Vlanif20
 10.3.3.9/32        1025/3        -/Vlanif20
```

# Display information about all LSPs with the next hop of 192.168.1.1.

```
<HUAWEI> display mpls lsp nexthop 192.168.1.1

Flag after Out IF: (I) - LSP Is Only Iterated by RLFA
-------------------------------------------------------------------------------
            LSP Information: L3VPN Label-Per-Nexthop LSP
-------------------------------------------------------------------------------
IndirectID  NextHop          In/Out Label  In/Out IF      Vrf Name
0x1         192.168.1.1      13312/13312   -/-            ASBR LSP
```

# Display detailed information about all types of LSPs.

```
<HUAWEI> display mpls lsp verbose
-------------------------------------------------------------------------------
                 LSP Information: RSVP LSP
-------------------------------------------------------------------------------

 No                  :  1
 SessionID           :  300
 IngressLsrID        :  10.1.1.9
 LocalLspID          :  1
 Tunnel-Interface    :  Tunnel1
 Fec                 :  10.2.2.9/32
 TunnelTableIndex    :  0x1
 Nexthop             :  10.5.1.2
 In-Label            :  NULL
 Out-Label           :  11264
 In-Interface        :  ----------
 Out-Interface       :  Vlanif10
 LspIndex            :  3072
 Token               :  0x8002008
 LsrType             :  Ingress
 Mpls-Mtu            :  1500
 TimeStamp           :  1171sec
 Bfd-State           :  ---
 CBfd-Event          :  0x0
 Bed-State           :  ---
 Bed-LastNotifyValue :  ---
 Bed-LastNotifyLspId :  ---
 Flag after FEC: (I) - LSP Is Only Iterated by RLFA
-------------------------------------------------------------------------------
                 LSP Information: LDP LSP
-------------------------------------------------------------------------------
 No                  :  2
 VrfName             :
 Fec                 :  10.2.2.2/32
```

```
Nexthop            :  10.1.1.2
In-Label           :  NULL
Out-Label          :  3
In-Interface       :  ----------
Out-Interface      :  Vlanif10
LspIndex           :  9217
Token              :  0x802009
FrrToken           :  0x0
LsrType            :  Ingress
Outgoing token     :  0x0
Label Operation    :  PUSH
Mpls-Mtu           :  ------
TimeStamp          :  21086sec
Bfd-State          :  ---
BGPKey             :  -----

No                 :  3
VrfName            :
Fec                :  10.2.2.2/32
Nexthop            :  10.2.1.2
In-Label           :  NULL
Out-Label          :  3
In-Interface       :  ----------
Out-Interface      :  Vlanif20
LspIndex           :  9218
Token              :  0x80200a
FrrToken           :  0x0
LsrType            :  Ingress
Outgoing token     :  0x0
Label Operation    :  PUSH
Mpls-Mtu           :  ------
TimeStamp          :  19569sec
Bfd-State          :  ---
BGPKey             :  -----
```

Table 9-38 Description of the display mpls lsp command output

Item	Description
LSP Information	LSP information: ● STATIC LSP: manually created. ● LDP LSP: created using LDP. ● STATIC CR-LSP: a static MPLS TE tunnel created manually. ● RSVP LSP: an MPLS TE tunnel created using RSVP-TE. ● BGP LSP: an LSP created using BGP based on private or public IPv4 BGP routes. ● L3VPN LSP: an LSP based on IPv4 VPN routes received by means of BGP. ● BGP IPV6 LSP: an LSP based on private-network IPv6 routes received by means of BGP. ● L3VPN IPV6 LSP: an LSP based on IPv6 VPN routes received by means of BGP.
FEC/Fec	Forwarding equivalence class. Usually, the value is the destination address of an LSP.
In/Out Label	Values of the incoming and outgoing labels.

Item	Description
In/Out IF	Names of the incoming and outbound interfaces.
Vrf Name	Name of a VPN instance.
IndirectID	Index of the next hop of a BGP route.
No	Serial number of an LSP.
SessionID	Session ID of a CR-LSP.
IngressLsrID	Ingress LSR ID of a CR-LSP.
LocalLspID	Local LSP ID of a CR-LSP.
Tunnel-Interface	Tunnel interface.
VrfName	Name of a VPN instance. This value is available for only non-CR-LSPs.
Nexthop	IP address of the next hop of an LSP.
TunnelTableIndex	Index of a tunnel table.
In-Label	Value of an incoming label.
Out-Label	Value of an outgoing label.
In-Interface	Name of an inbound interface.
Out-Interface	Name of an outbound interface.
LspIndex	Index number of an LSP, which uniquely identifies an LSP that is established using a specific protocol.
Token	LSP token. It guides the packet forwarding.
FrrToken	Token of a standby LDP LSP. This value is available for only non-CR-LSPs.
LsrType	Role of an LSR on an LSP: ● Ingress ● Transit ● Egress
Outgoing token	Token that guides the packet forwarding, which is available for only non-CR-LSPs.
Label Operation	Type of a label operation, which is available for only non-CR-LSPs: ● PUSH ● SWAP ● POP ● SWAPPUSH

Item	Description
Mpls-Mtu	Maximum transmission unit (MTU) of an interface of an LSP.
TimeStamp	Time elapsed since an LSP was set up.
Bfd-State	BFD status.
CBfd-Event	Error code event that BFD reports to the RSVP LSP on the ingress node.
Bed-State	Error code status of an RSVP LSP on the ingress node.
Bed-LastNotifyValue	Error code association of which the RSVP LSP notifies BFD on the egress node.
Bed-LastNotifyLspId	ID of the reversed LSP that corresponds to the error code association event on the egress node. The association event is notified of BFD by the RSVP LSP.
BGPKey	Index of BGP.

9.1.39 display mpls lsp statistics

Function

The **display mpls lsp statistics** command displays statistics about the LSPs that are in the Up state and the number of the LSPs that are activated on the ingress, transit, and egress nodes.

Format

display mpls lsp statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display mpls lsp statistics** command to view statistics about the LSPs and CR-LSPs that are in the Up state.

To view detailed information about the LSPs and CR-LSPs, run the **display mpls lsp** command.

Example

# Display statistics about LSPs.

```
<HUAWEI> display mpls lsp statistics
Lsp Type        Total      Ingress    Transit    Egress
STATIC LSP      0          0          0          0
STATIC CRLSP    0          0          0          0
LDP LSP         4          3          0          1
RSVP CRLSP      0          0          0          0
BGP LSP         1          0          0          1
ASBR LSP        0          0          0          0
BGP IPV6 LSP    0          0          0          0
L3VPN IPV6 LSP 0           0          0          0
-------------------------------------------------------------------------
LSP             5          3          0          2
CRLSP           0          0          0          0
-------------------------------------------------------------------------
Lsp Type        IngressLspBypassState         TransitLspBypassState
                ExistNotUsed    InUse         ExistNotUsed    InUse
RSVP CRLSP      0               0             0               0
-------------------------------------------------------------------------
```

Table 9-39 Description of the display mpls lsp statistics command output

Item	Description
Lsp Type	Type of an LSP: ● STATIC LSP: a static LSP. ● STATIC CRLSP: a static CR-LSP. ● LDP LSP: created using LDP. ● RSVP CRLSP: an MPLS TE tunnel created using RSVP-TE. ● BGP LSP: an LSP created using BGP based on private or public IPv4 BGP routes. ● ASBR LSP: created using BGP based on received IPv4 VPN route. ● BGP IPV6 LSP: an LSP created using BGP based on private IPv6 routes. ● L3VPN IPV6 LSP: created using BGP based on received IPv6 VPN routes. ● LSP: Label Switched Path. ● CRLSP: Constraint-based Routed Label Switched Path.
Total	Number of LSPs of a specific type.
Ingress	Number of LSPs on the local ingress LSR.

Item	Description
Transit	Number of LSPs on the local transit LSR.
Egress	Number of LSPs on the local egress LSR.
IngressLspBypassState	State of the ingress LSP enabled with FRR: ● ExistNotUsed: Bypass LSP that is bound to the primary LSP but has no traffic. ● InUse: Traffic switched to the bypass LSP.
TransitLspBypassState	State of the Transit LSP enabled with FRR: ● ExistNotUsed: Bypass LSP that is bound to the primary LSP but has no traffic. ● InUse: Traffic switched to the bypass LSP.

9.1.40 display mpls route-state

Function

The **display mpls route-state** command displays routing information about a dynamic LSP.

Format

display mpls route-state [**vpn-instance** *vpn-instance-name*] [{ **exclude** | **include** } { **idle** | **ready** | **settingup** } * | *destination-address mask-length*] [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
exclude	Displays routing information excluding the specified route.	-

Parameter	Description	Value
include	Displays information about a specified route.	-
idle	Indicates that a route is not used to establish an LSP.	-
ready	Indicates that a route has been used to establish an LSP.	-
settingup	Indicates that a signaling protocol is creating an LSP.	-
destination-address	Specifies the destination address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of a specified destination address.	The value is an integer ranging from 0 to 32.
verbose	Displays detailed routing information about an LSP.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing LDP LSP configurations, run the **display mpls ldp lsp** command to view information about an LDP LSP. If the command output displays no information about the LDP LSP, run the **display mpls route-state** command to view LDP LSP routing information.

Precautions

Only routing states of the LSPs that are set up based on dynamic signaling protocols can be changed. Therefore, the **display mpls route-state** command displays only routing states of dynamic LSPs, but not routing information about static LSPs.

Example

# Display detailed information about routes of dynamic LSPs.

```
<HUAWEI> display mpls route-state verbose

Codes: B(BGP), I(IGP), L(Public Label BGP), O(Original BGP), U(Unknown)
-------------------------------------------------------------------------------
Dest/Mask         Next-Hop        Out-Interface        State    LSP   VRF Type
-------------------------------------------------------------------------------
10.21.21.21/32    10.22.22.21     Vlanif100            READY    2     0   I
    LspIndex: 30720     InLabel: NULL      OutLabel: 3
    LspIndex: 32728     InLabel: 1024      OutLabel: 3
10.0.0.6/32       10.21.22.21     Vlanif100            READY    1     0   I
    LspIndex: 33053     InLabel: NULL      OutLabel: 3338
```

Table 9-40 Description of the display mpls route-state verbose command output

Item	Description
Dest/Mask	Destination IP address and mask length.
Next-Hop	Next hop IP address.
Out-Interface	Outbound interface.
State	Routing state of the MPLS control plane: ● IDLE: The route is not used to establish an LSP. ● SETTINGUP: A signaling protocol is creating an LSP. ● READY: The route has been used to establish an LSP. Static LSPs are only in READY state.
LSP	Number of LSPs reachable to the destination address. If the displayed value is not 0, there are LSPs reachable to the destination address and LSP information about these LSPs is also displayed.
VRF	Index of a VPN instance. The value 0 indicates the public network.
Type	Route type: ● B: BGP routes ● I: IGP routes ● L: labeled BGP routes of a public network ● O: original BGP routes ● U: unidentified routes (such as multicast routes)
LspIndex	Index of an LSP established using the route.
InLabel	Incoming label of an LSP established using the route. If NULL is displayed, the current node is the ingress node of the LSP; if a number is displayed, the current node is the transit or egress node of the LSP.
OutLabel	Outgoing label of an LSP established using the route.

9.1.41 display mpls static-lsp

Function

The **display mpls static-lsp** command displays information about static LSPs.

Format

display mpls static-lsp [*lsp-name*] [{ **include** | **exclude** } *ip-address mask-length*] [**verbose**]

Parameters

Parameter	Description	Value
lsp-name	Specifies the name of an LSP.	The value is an existing static LSP name.
include	Displays information about LSPs, including information about the specific FEC.	-
exclude	Displays information about LSPs, excluding information about the specific FEC.	-
ip-address	Specifies the destination IPv4 address.	The value is in dotted decimal notation.
mask-length	Specifies the length of an IPv4 mask.	The value is an integer ranging from 0 to 32.
verbose	Displays detailed information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Static LSPs are configured locally, so you need to run the **ping lsp** command to check whether the static LSP can work normally. If the static LSP cannot work normally, run the **display mpls static-lsp** command to view information about static LSPs.

Example

# Display brief information about static LSPs.

```
<HUAWEI> 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                Status
lsp1       3.3.3.9/32        NULL/100   -/Vlanif100            Up
```

Table 9-41 Description of the display mpls static-lsp command output

Item	Description
TOTAL	Total number of static LSPs.
UP	Number of static LSPs that are in the Up state.
DOWN	Number of static LSPs that are in the Down state.
Name	Name of an LSP.
FEC	Destination IP address and mask length of an LSP.
I/O Label	Incoming and outgoing labels.
I/O If	Incoming and outbound interfaces.
Status	Current status of an LSP: ● Up ● Down

# Display detailed information about static LSPs.

```
<HUAWEI> display mpls static-lsp verbose
No             : 1
LSP-Name       : lsp1
LSR-Type       : Ingress
FEC            : 3.3.3.9/32
In-Label       : NULL
Out-Label      : 100
In-Interface   : -
Out-Interface  : Vlanif100
NextHop        : 10.1.1.2
Static-Lsp Type: Normal
Lsp Status     : Up
```

Table 9-42 Description of the display mpls static-lsp verbose command output

Item	Description
No	Serial number.
LSP-Name	Name of an LSP.
LSR-Type	Role of the current LSR on a static LSP: ● Ingress ● Transit ● Egress
FEC	Destination IP address and mask length of an LSP.

Item	Description
In-Label	Incoming label.
Out-Label	Outgoing label.
In-Interface	Inbound interface.
Out-Interface	Outbound interface.
NextHop	Next hop IP address.
Static-Lsp Type	Type of a static LSP.
Lsp Status	LSP status: ● Up ● Down

9.1.42 display ospf ldp-sync interface

Function

The **display ospf ldp-sync interface** command displays the status of LDP and OSPF synchronization on an interface.

Format

display ospf ldp-sync interface { **all** | *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays information about the synchronization status on all interfaces enabled with LDP and OSPF synchronization.	-
interface-type interface-number	Displays information about the synchronization status on a specified interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

For all interfaces that are enabled with LDP and OSPF synchronization, run the **display ospf ldp-sync interface** command to view information about the status of LDP and OSPF synchronization.

Example

# Display information about the status of LDP and OSPF synchronization on a specified interface.

```
<HUAWEI> display ospf ldp-sync interface vlanif 100
 Interface Vlanif100   HoldDown Timer: 9         HoldMaxCost Timer: 50
 LDP State: Up              OSPF Sync State: Sync-Achieved
```

Table 9-43 Description of the display ospf ldp-sync interface command output

Item	Description
Interface	Interface connected to neighbors.
HoldDown Timer	Interval at which the interface waits to create an LDP session without creating the OSPF neighbor relationship. The default interval is 10 seconds. To set the interval at which the interface waits to create an LDP session without creating the OSPF neighbor relationship, run the **ospf timer ldp-sync hold-down** command.
HoldMaxCost Timer	Interval at which OSPF advertises the maximum metric in LSAs sent by the local device. The default interval is 10 seconds. To set the interval at which OSPF advertises the maximum metric in LSAs sent by the local device, run the **ospf timer ldp-sync hold-max-cost** command. **NOTE** If the value of this field is **infinite**, OSPF keeps advertising the maximum metric value in LSAs sent by the local device before the LDP session is reestablished.
LDP State	Status of an LDP session: ● Up ● Down

Item	Description
OSPF Sync State	Status of LDP and OSPF synchronization: ● Sync-Achieved: The creation of an LDP session and establishment of the OSPF neighbor relationship are synchronized. ● HoldDown: The interface is waiting to create an LDP session without creating the OSPF neighbor relationship. ● HoldMaxCost: OSPF advertises the maximum metric in LSAs or LSPs sent by the local device. ● Init: the initial state.

9.1.43 display static-route ldp-sync

Function

The **display static-route ldp-sync** command displays information about the outbound interface of a static route configured with synchronization between LDP and static routes.

Format

display static-route ldp-sync [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display static-route ldp-sync** command to view synchronization between LDP and static routes to diagnose faults in static routes.

- If no outbound interface is specified, information about all outbound interfaces of the static routes configured with synchronization between LDP and static routes is displayed.

- If an outbound interface is specified, information about the specified outbound interface of the static routes configured with synchronization between LDP and static routes is displayed.

Example

# Display information about the outbound interface of the static route configured with synchronization between LDP and static routes.

```
<HUAWEI> display static-route ldp-sync
Total number of routes enable Ldp-Sync: 2
-----------------------------------------------------
Interface GigabitEthernet0/0/1
Enable ldp-sync static routes number: 1
Static-route ldp-sync holddown timer: 20s
Sync state: Normal
Dest = 4.4.4.4, Mask = 32, NextHop = 10.1.1.1.
-----------------------------------------------------
Interface GigabitEthernet0/0/2
Enable ldp-sync static routes number: 1
Static-route ldp-sync holddown timer: 10s
Sync state: Normal
Dest = 4.4.4.4, Mask = 32, NextHop = 20.1.1.1.
-----------------------------------------------------
```

Table 9-44 Description of the display static-route ldp-sync command output

Item	Description
Total number of routes enable Ldp-Sync	Number of static routes configured with synchronization between LDP and static routes.
Interface GigabitEthernet0/0/1	Outbound interface of the static route configured with synchronization between LDP and static routes.
Enable ldp-sync static routes number	Number of static routes enabled with synchronization between LDP and static routes, with an outbound interface of GE1/0/0.
Static-route ldp-sync holddown timer	Time during which the static route remains inactive and waits for an LDP session to be established.
Sync state	Status of synchronization between LDP and static routes: ● Normal ● HoldDown
Dest	Destination address of the static route.
Mask	Mask length of the destination address of the static route.
NextHop	Next hop address of the static route.

9.1.44 fec-list

Function

The **fec-list** command creates a FEC list used in dynamic BFD for LDP LSP.

The **undo fec-list** command deletes a FEC list.

By default, no FEC list is created.

Format

fec-list *list-name*

undo fec-list *list-name*

Parameters

Parameter	Description	Value
list-name	Specifies the name of a FEC list.	The value is a string of 1 to 31 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a BFD session is established based on the FEC list, run the **fec-list** command to create a FEC list. Run the **fec-node** command to specify a host route to trigger the establishment of BFD sessions.

Only a single FEC list can be configured globally.

Example

# Create FEC list 1.

```
<HUAWEI> system-view
[HUAWEI] fec-list 1
```

9.1.45 fec-node

Function

The **fec-node** command adds an FEC node.

The **undo fec-node** command deletes an FEC node.

By default, no FEC node is created.

Format

fec-node *ip-address* [**nexthop** *ip-address* | **outgoing-interface** *interface-type interface-number*]*

undo fec-node *ip-address* [**nexthop** *ip-address* | **outgoing-interface** *interface-type interface-number*]*

Parameters

Parameter	Description	Value
ip-address	Specifies the FEC address.	The value is in dotted decimal notation.
nexthop *ip-address*	Specifies the next-hop address.	The value is in dotted decimal notation.
outgoing-interface *interface-type interface-number*	Specifies the outbound interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Views

FEC-list view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the establishment of BFD sessions is triggered in FEC list mode, the system sets up BFD sessions for the added FEC nodes.

Prerequisites

An FEC list has been created by running the **fec-list** command.

Example

# Create FEC nodes in the FEC list.

```
<HUAWEI> system-view
[HUAWEI] fec-list 1
[HUAWEI-fec-list-1] fec-node 10.1.1.1 nexthop 10.2.1.1 outgoing-interface vlanif 100
```

9.1.46 graceful-restart (MPLS-LDP view)

Function

The **graceful-restart** command enables LDP GR.

The **undo graceful-restart** command disables LDP GR.

By default, LDP GR is disabled.

Format

graceful-restart

undo graceful-restart

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In LDP GR mode, when AMB/SMB switchover or protocol restart occurs on the neighboring device of the local device, the local device (GR helper) helps the device (restarter) to restart without interrupting packet forwarding.

If LDP GR is not enabled, during the AMB/SMB switchover or upgrade, the neighboring device deletes the LSP because the session is in the Down state. As a result, the traffic is interrupted in a short time. If LDP GR is enabled, the labels before and after unexpected AMB/SMB switchover or protocol restart can be consistent, and uninterrupted MPLS forwarding is ensured.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp(system view)** command in the system view.

Precautions

Enabling or disabling GR causes the reestablishment of all LDP sessions.

LDP GR must be enabled on both the GR Restarter and Helper.

Example

# Enable LDP GR.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] graceful-restart
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

9.1.47 graceful-restart timer neighbor-liveness

Function

The **graceful-restart timer neighbor-liveness** command sets the value of the Neighbor-liveness timer.

The **undo graceful-restart timer neighbor-liveness** command restores the default setting.

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

Format

graceful-restart timer neighbor-liveness *time*

undo graceful-restart timer neighbor-liveness

Parameters

Parameter	Description	Value
time	Specifies the value of the Neighbor-liveness timer.	The value is an integer ranging from 3 to 3600, in seconds.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The value of the neighbor-liveness timer defines the LDP GR period.

During LDP GR, the reestablishment time of the LDP session is negotiated as the smaller value between the value of the neighbor-liveness timer on the GR helper and the value of the Reconnect timer on the GR restarter.

In general, the default value of the timer is recommended. When the number of LSPs on a network is small, you can set a smaller value for the neighbor-liveness timer to shorten the GR period.

Prerequisites

MPLS and MPLS LDP have been enabled globally.

LDP GR has been enabled globally.

Precautions

Changing the value of the neighbor-liveness timer causes the reestablishment of all the LDP sessions.

Example

# Set the value of the Neighbor-liveness timer to 500 seconds.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] graceful-restart
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
[HUAWEI-mpls-ldp] graceful-restart timer neighbor-liveness 500
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

9.1.48 graceful-restart timer reconnect

Function

The **graceful-restart timer reconnect** command sets the value of the Reconnect timer of an LDP session.

The **undo graceful-restart timer reconnect** command restores the default setting.

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

Format

graceful-restart timer reconnect *time*

undo graceful-restart timer reconnect

Parameters

Parameter	Description	Value
time	Specifies the value of a Reconnect timer of an LDP session.	The value is an integer ranging from 3 to 3600, in seconds.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the GR restarter performs the active/standby switchover, the GR helper detects that the LDP session with the GR restarter fails, and then starts the Reconnect timer and waits for the reestablishment of the LDP session.

- If no LDP session between the GR helper and the GR restarter has been established after the Reconnect timer times out, the GR helper immediately deletes the MPLS forwarding entries associated with the GR restarter and exits from the GR help process.
- If the LDP session between the GR helper and the GR restarter is established before the Reconnect timer times out, the GR helper deletes the timer and starts the Recovery timer.

During LDP GR, when the reestablishment time of the LDP session is negotiated, the value of the Reconnect timer that actually takes effect on the local end is the smaller value between the value of the neighbor-liveness timer on the GR helper and the value of the Reconnect timer on the GR restarter.

Prerequisites

MPLS and MPLS LDP have been enabled globally.

LDP GR has been enabled globally.

Precautions

Changing the value of the Reconnect timer causes the reestablishment of all the LDP sessions.

Example

# Set the time of the Reconnect timer of an LDP session to 270 seconds.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] graceful-restart
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
[HUAWEI-mpls-ldp] graceful-restart timer reconnect 270
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

9.1.49 graceful-restart timer recovery

Function

The **graceful-restart timer recovery** command sets the value of the LSP Recovery timer.

The **undo graceful-restart timer recovery** command restores the default setting.

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

Format

graceful-restart timer recovery *time*

undo graceful-restart timer recovery

Parameters

Parameter	Description	Value
time	Specifies the value of an LSP Recovery timer.	The value is an integer ranging from 3 to 3600, in seconds.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the LDP session is reestablished, the GR helper starts the Recovery timer and waits for the recovery of the LSP.

- If the Recovery timer times out, the GR helper considers that the GR process is complete on the GR restarter and deletes the unrecovered LSPs.
- If all the LSPs recover before the Recovery timer times out, the GR helper considers that the GR process is complete on the GR restarter only after the Recovery timer times out.

When a network with a large number of routes is faulty, run the **graceful-restart timer recovery** command to increase the value of the Recovery timer to ensure that all the LSPs recover within the timeout period of the timer.

During the LDP GR process, the value of the LSP Recovery timer that actually takes effect on the local end is negotiated as the smaller one of the values of the LSP Recovery timers configured on both ends of an LDP session.

Prerequisites

MPLS and MPLS LDP have been enabled globally.

LDP GR has been enabled globally.

Precautions

Changing the value of the LSP Recovery timer causes the reestablishment of all the LDP sessions.

Example

# Set the value of the LSP Recovery timer to 330 seconds.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] graceful-restart
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
[HUAWEI-mpls-ldp] graceful-restart timer recovery 330
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

9.1.50 gtsm peer valid-ttl-hops

Function

The **gtsm peer valid-ttl-hops** command configures the generalized TTL security mechanism (GTSM) on a specified LDP peer.

The **undo gtsm** command deletes the GTSM on all LDP peers or a specified LDP peer.

By default, no LDP peer is configured with the GTSM.

Format

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

undo gtsm { **all** | **peer** *ip-address* }

Parameters

Parameter	Description	Value
peer *ip-address*	Specifies the transport address of an LDP peer.	The value is in dotted decimal notation.
valid-ttl-hops *hops*	Specifies the maximum number of valid hops permitted by the GTSM.	The value is an integer ranging from 1 to 255.
all	Indicates all LDP peers.	-

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The GTSM checks TTL values to verify packets and protect devices against attacks. LDP peers are configured with the GTSM and a valid TTL range to check TTLs in LDP packets exchanged between them. If the TTL in an LDP packet is out of the valid range, this LDP packet is considered invalid and discarded. The GTSM defends against CPU-based attacks initiated using a large number of forged packets and protects upper-layer protocols.

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 - Number of hops +1, 255], the packets are received; otherwise, the packets are discarded.

NOTE

Configuring the GTSM on both ends of an LDP session is recommended.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp (system view)** command.

Precautions

The valid TTL range is from 1 to 255 or from 1 to 64, depending on the specific vendor. If a Huawei device is connected to a non-Huawei device, set *hops* to a value in a valid range that both devices support; otherwise, the Huawei device will discard packets sent by the non-Huawei device, resulting in LDP session interruption.

Example

# On the LSR, set valid TTL values carried in LDP packets sent by the peer with transport address 10.1.1.1 to 254 and 255.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] gtsm peer 10.1.1.1 valid-ttl-hops 2
```

9.1.51 inbound peer fec

Function

The **inbound peer fec** command configures an inbound policy, which allows the LSR to receive Label Mapping messages for IGP routes only from a specified peer.

The **undo inbound peer fec** command restores the default setting.

By default, no inbound policy is configured.

Format

inbound peer { *peer-id* | **peer-group** *peer-group-name* | **all** } **fec** { **none** | **host** | **ip-prefix** *prefix-name* }

undo inbound peer { *peer-id* | **peer-group** *peer-group-name* | **all** } **fec**

undo inbound peer all

Parameters

Parameter	Description	Value
peer-id	Specifies the ID of an LDP peer.	The value is in dotted decimal notation.

Parameter	Description	Value
peer-group *peer-group-name*	Specifies the name of a peer group.	The value is an existing peer group name.
all	Indicates all LDP peers.	-
none	Forbids all Label Mapping messages. After the parameter **none** is configured, the specified LSR does not receive Label Mapping messages for IGP routes from its peers.	-
host	Allows only Label Mapping messages for host routes. After the parameter **host** is configured, the specified LSR receives only Label Mapping messages for host routes from its peers.	-
ip-prefix *prefix-name*	Allows only Label Mapping messages for IGP routes that are defined in the IP prefix list. After the parameter **ip-prefix** is configured, the specified LSR receives Label Mapping messages only for IGP routes that are defined in the IP prefix list by its peers.	The value is an existing IP prefix list name.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an LSR receives Label Mapping messages from all LDP peers to speed up LDP LSP convergence. This leads to establishment of a great number of unwanted LSPs, which wastes resources. To reduce the number of LSPs and save memory resources, configure an inbound policy to filter out LDP LSPs not matching the policy.

When running the **inbound peer fec** command to specify the peer ID and FEC of the IGP route, configure the peer to receive only Label Mapping messages for specified IGP routes.

To apply a policy associated with the same FEC range to an LDP peer group or all LDP peers receiving Label Mapping messages, configure either **peer-group** *peer-group-name* or **all** in the command.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

If multiple inbound policies are configured for a specified LDP peer, the earliest configuration takes effect. For example, the following two inbound policies are configured:

```
inbound peer 2.2.2.2 fec host
inbound peer peer-group group1 fec none
```

As group1 also contains an LDP peer with *peer-id* of 2.2.2.2, the following inbound policy takes effect:

```
inbound peer 2.2.2.2 fec host
```

If two inbound policies are configured in sequence and the **peer** parameters in the two commands are the same, the second command overrides the first one. For example, the following two outbound policies are configured:

```
inbound peer 2.2.2.2 fec host
inbound peer 2.2.2.2 fec none
```

The second configuration overrides the first one. This means that the following inbound policy takes effect on the LDP peer with *peer-id* of 2.2.2.2:

```
inbound peer 2.2.2.2 fec none
```

Creating a peer group before it is referenced is recommended. By default, nonexistent peer groups cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent peer group is referenced using the current command, the current command applies to all LDP peers.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, the device receives Label Mapping messages of all LDP FECs from the specified peer.

Example

# Configure all LSRs to receive Label Mapping messages only for host routes from peers.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] inbound peer all fec host
```

9.1.52 ip route-static ldp-sync

Function

The **ip route-static ldp-sync** command configures unicast static routes for synchronization with LDP.

The **undo ip route-static ldp-sync** command deletes unicast static routes for synchronization with LDP.

By default, unicast static routes for synchronization with LDP are not configured.

Format

ip route-static *ip-address* { *mask* | *mask-length* } *interface-type interface-number* [*nexthop-address*] [**preference** *preference* | **tag** *tag*] * **ldp-sync** [**description** *text*]

undo ip route-static *ip-address* { *mask* | *mask-length* } *interface-type interface-number* [*nexthop-address*] [**preference** *preference* | **tag** *tag*] * **ldp-sync**

ip route-static vpn-instance *vpn-source-name ip-address* { *mask* | *mask-length* } { *nexthop-address* [**public**] | *interface-type interface-number* [*nexthop-address*] | **vpn-instance** *vpn-destination-name nexthop-address* } [**preference** *preference* | **tag** *tag*] * **ldp-sync** [**description** *text*]

undo ip route-static vpn-instance *vpn-source-name ip-address* { *mask* | *mask-length* } [*nexthop-address* | *interface-type interface-number* [*nexthop-address*]] [**preference** *preference* | **tag** *tag*] * **ldp-sync**

Parameters

Parameter	Description	Value
vpn-instance *vpn-source-name*	Specifies the name of the source VPN instance. Each VPN instance has its own routing table. The configured static routes are added to the routing table of the specified VPN instance.	The value must be an existing VPN instance name.
vpn-instance *vpn-destination-name*	Specifies the name of the destination VPN instance.	The value must be an existing VPN instance name.
ip-address	Specifies a destination IP address.	The value is in dotted decimal notation.
mask	Specifies the subnet mask.	The value is in dotted decimal notation.
mask-length	Specifies the mask length. As 1s in a 32-bit mask must be consecutive, the mask in dotted decimal notation can be replaced by the mask length.	The value is an integer that ranges from 0 to 32.
interface-type interface-number	Specifies the type and number of the interface that forwards packets.	-
nexthop-address	Specifies the next-hop address.	The value is in dotted decimal notation.
public	Specifies the next-hop address as a public network address but not an address in the source VPN instance.	-
preference *preference*	Specifies the preference of a static route. A smaller value indicates a higher preference.	The value is an integer that ranges from 1 to 255. The default value is 60.

Parameter	Description	Value
tag *tag*	Specifies the tag value of a static route. By configuring different tag values, you can classify static routes to implement different routing policies. For example, other routing protocols can import static routes with specified tag values through routing policies.	The value is an integer that ranges from 1 to 4294967295. The default value is 0.
description *text*	Configures the description of a static route.	The value is a string of 1 to 80 characters that can contain spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

On an MPLS network with primary and backup links, LSRs establish LSPs based on static routes. When the LDP session of the primary link becomes faulty (the fault is not caused by a link failure) or the primary link recovers, configuring synchronization between LDP and static routes minimizes traffic loss during traffic switchover and switchback.

After synchronization between LDP and static routes is enabled, the recovered static route becomes temporarily inactive. It waits for the establishment of an LDP session before the Hold-down timer expires, which synchronizes LDP and the static route.

Example

# Configure static routes for synchronization with LDP.

```
<HUAWEI> system-view
[HUAWEI] ip route-static 10.1.1.0 255.255.255.0 vlanif 100 ldp-sync
```

9.1.53 isis ldp-sync

Function

The **isis ldp-sync** command enables synchronization between LDP and IS-IS on an interface.

The **undo isis ldp-sync** command disables synchronization between LDP and IS-IS on an interface.

By default, synchronization between LDP and IS-IS is disabled on an interface.

Format

isis ldp-sync

undo isis ldp-sync

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The LDP convergence speed depends on the convergence speed of IS-IS routes. To enable MPLS LDP on a network with the primary and backup links, the following problems may occur:

- Upon a fault on the primary link, IS-IS routes and ISP are both switched to the backup link using LDP FRR. When the primary link recovers, IS-IS routes are switched back to the primary link earlier than LDP traffic because IGP route convergence is faster than LDP convergence. As a result, LSP traffic is lost.
- If a fault occurs on the LDP session between nodes on the primary link where the IS-IS routes are working properly, the IS-IS routes still use the primary link and the LSP on the primary link is deleted. No IS-IS route exists on the backup link; therefore, no LSP can be established on the backup link. LSP traffic is lost.

Run the **isis ldp-sync** command to enable synchronization between LDP and IS-IS to prevent traffic loss in the preceding problems. Run this command on the interfaces on both ends of the link between the node where the primary LSP and the backup LSP diverge from each other and its LDP peer on the primary LSP.

Prerequisites

The IS-IS process has been started using the **isis enable** command in the interface view.

Example

# Enable synchronization between LDP and IS-IS on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis ldp-sync
```

# Enable synchronization between LDP and IS-IS on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
```

```
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis ldp-sync
```

9.1.54 isis ldp-sync block

Function

The **isis ldp-sync block** command blocks synchronization between LDP and IS-IS on an interface.

The **undo isis ldp-sync block** command restores the default setting.

By default, synchronization between LDP and IS-IS is not blocked on an interface.

Format

isis ldp-sync block

undo isis ldp-sync block

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ldp-sync enable** command run in the IS-IS view on a device enables synchronization between LDP and IS-IS on all local IS-IS interfaces. On an IS-IS interface transmits importance services, LDP and IS-IS synchronization may affect service transmission. If the link is working properly and an LDP session over the link fails, IS-IS sends link state PDUs (LSPs) to advertise the maximum cost of the link. As a result, IS-IS does not select the route for the link, which affects important service transmission.

To prevent the preceding problem, run the **isis ldp-sync block** command to block synchronization between LDP and IS-IS on the IS-IS interface that transmits important services.

Prerequisites

The IS-IS process has been started using the **isis enable** command in the interface view.

Example

# Block synchronization between LDP and IS-IS on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis ldp-sync block
```

# Block synchronization between LDP and IS-IS on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis ldp-sync block
```

9.1.55 isis timer ldp-sync hold-down

Function

The **isis timer ldp-sync hold-down** command sets the interval during which an interface waits for creating an LDP session before setting up the IS-IS neighbor relationship.

The **undo isis timer ldp-sync hold-down** command restores the default setting.

By default, the interval is 10 seconds.

Format

isis timer ldp-sync hold-down *value*

undo isis timer ldp-sync hold-down

Parameters

Parameter	Description	Value
value	Specifies the interval during which an interface waits for creating an LDP session before setting up the IS-IS neighbor relationship.	The value is an integer ranging from 0 to 65535, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network with both active and standby links, if the active link fails, traffic switches to a standby link. Therefore, the standby IS-IS route and backup LDP label switched path (LSP) along the standby link become reachable. After the active link recovers, its IS-IS route converges more rapidly than the LDP LSP. As a result, the IS-IS neighbor relationship is established earlier than the LDP session on the active link. Although traffic is directed over the IS-IS route to the active link, traffic fails to be forwarded because no LDP LSP is established.

To prevent the traffic forwarding failure, LDP and IS-IS synchronization can be configured. After the active link recovers from a physical fault, the IS-IS route for the active link is set to the Hold-down state, and the Hold-down timer starts. After an LDP session is established over the active link or the Hold-down timer expires, the IS-IS neighbor relationship starts to be established. This allows the LDP LSP and IS-IS route to go Up simultaneously. To set the Hold-down timer, run the **isis timer ldp-sync hold-down** command.

Prerequisites

The IS-IS process has been started using the **isis enable** command in the interface view.

Precautions

This command is circular in nature, and the latest configuration overrides the previous configurations.

Example

# Set the value of the Hold-down timer for VLANIF100 to 15 seconds, during which the interface waits for the establishment of an LDP session before setting up the IS-IS neighbor relationship.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis timer ldp-sync hold-down 15
```

# Set the value of the Hold-down timer for GE0/0/1 to 15 seconds, during which the interface waits for the establishment of an LDP session before setting up the IS-IS neighbor relationship.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis timer ldp-sync hold-down 15
```

9.1.56 isis timer ldp-sync hold-max-cost

Function

The **isis timer ldp-sync hold-max-cost** command sets the interval during which IS-IS sends LSPs to advertise the maximum metric on the local device.

The **undo isis timer ldp-sync hold-max-cost** command restores the default setting.

By default, the interval is 10 seconds.

Format

isis timer ldp-sync hold-max-cost { *value* | **infinite** }

undo isis timer ldp-sync hold-max-cost

Parameters

Parameter	Description	Value
value	Specifies the interval during which IS-IS sends LSPs to advertise the maximum metric on the local device.	The value is an integer ranging from 0 to 65535, in seconds.
infinite	Indicates that IS-IS keeps advertising the maximum metric in LSPs on the local device before an LDP session is reestablished.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network with active and standby links, when the IS-IS route of the active link is reachable and an LDP session between two nodes on the active link fails, traffic is transmitted over the IS-IS route of the active link, whereas the label switched path (LSP) on the active link fails. Although LSP traffic attempts to be switched to the backup LSP, the active IS-IS route is selected to direct traffic. As a result, traffic on the primary LSP is lost.

To prevent the traffic forwarding failure, LDP and IS-IS synchronization can be configured. If the LDP session over the active link fails, IS-IS advertises the maximum cost of the active link route. The IS-IS route for the standby link is selected, and the Hold-max-cost timer starts. After the LDP LSP over the standby link is established, and the IS-IS route for the standby link is reachable, traffic switches to the standby link. After the LDP session on the active link recovers or the Hold-max-cost timer expires, IS-IS advertises the actual cost of the active link route. To set the Hold-max-cost timer, run the **isis timer ldp-sync hold-max-cost** command.

Select one of the following parameters as required:

- When IS-IS carries LDP services only, configure **infinite** to keep the IS-IS route and LSP over the same link.
- If IS-IS carries multiple types of services including LDP services in the networking, configure *value* to ensure that interruption of an LDP session over the active link does not affect IS-IS routing and other services. The default is 10, in seconds, which is a recommended value.

Prerequisites

The IS-IS process has been started using the **isis enable** command in the interface view.

Precautions

This command is circular in nature, and the latest configuration overrides the previous configurations.

Example

# Set the interval to 8 seconds, during which IS-IS sends LSPs to advertise the maximum metric on the local device.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis timer ldp-sync hold-max-cost 8
```

# Set the interval to 8 seconds, during which IS-IS sends LSPs to advertise the maximum metric on the local device.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis timer ldp-sync hold-max-cost 8
```

9.1.57 label advertise

Function

The **label advertise** command enables the egress node to advertise labels of a specified type to the penultimate hop.

The **undo label advertise** command restores the default setting.

By default, the egress node assigns implicit null labels to the penultimate hop.

Format

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

undo label advertise

Parameters

Parameter	Description	Value
explicit-null	Disables Penultimate Hop Popping (PHP) and enables the egress node to assign explicit null labels to the penultimate hop.	The value of the explicit null label is 0.
implicit-null	Enables PHP and enables the egress node to assign implicit null labels to the penultimate hop.	The value of the implicit null label is 3.

Parameter	Description	Value
non-null	Disables PHP and enable the egress node to assign normal labels to the penultimate hop.	The value is equal to or greater than 16.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MPLS transmits packets along label switched paths (LSPs). The egress at the last hop on the LSP removes MPLS labels from packets before forwarding the packets over IP links or using next layer labels. MPLS labels are useless at the last hop on an LSP. Therefore, penultimate hop popping (PHP) can be configured to enable the penultimate hop to remove labels, which improves forwarding efficiency.

By default, PHP is enabled, and the egress assigns implicit-null labels to the penultimate hop. To specify the type of label that the egress assigns to the penultimate hop, run the following commands:

- In a bidirectional association LSP scenario, run the **label advertise non-null** command to enable the egress to assign a normal label to the penultimate hop.
- In an MPLS QoS scenario, run the **label advertise explicit-null** command to enable the egress to assign an explicit null label to the penultimate hop.

Prerequisites

MPLS has been enabled globally using the **mpls (system view)** command in the system view.

Precautions

After the **label advertise** command is run to specify a label, the egress on a newly established LDP LSP or constraint-based routed label switched path (CR-LSP) assigns the specified label to the penultimate hop. The **label advertise** command can take effect on existing LDP LSPs or CR-LSPs when one of the following conditions is met:

- A master/slave main control board switchover is performed.
- The **reset mpls ldp** command is run to reset an LDP public instance for an LDP LSP.
- If a CR-LSP is established, the **reset mpls rsvp-te** command is run to reset Resource Reservation Protocol-Traffic Engineering (RSVP-TE), or the **reset mpls te tunnel-interface tunnel** command is run to restart a specified TE tunnel.

If the **label advertise** command is run more than once, the latest configuration overrides the previous one.

Example

# Configure the egress node to assign explicit null labels to the penultimate hop.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] label advertise explicit-null
```

9.1.58 label distribution default-route

Function

The **label distribution default-route** command enables a device to assign a label to a default IGP route.

The **undo label distribution default-route** command restores the default configuration.

By default, the device is disabled from assigning a label to a default IGP route.

Format

label distribution default-route

undo label distribution default-route

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

To enable a device to use MPLS assign a label to a default IGP route in independent mode, run the **label distribution default-route** command. An LSP can be established using the default route.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Example

# Enable a device to assign a label to a default IGP route.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] label distribution default-route
```

9.1.59 label-withdraw-delay

Function

The **label-withdraw-delay** command enables a node to delay sending Label Withdraw messages.

The **undo label-withdraw-delay** command disables a node from delaying sending Label Withdraw messages.

By default, the label withdraw delay function is disabled.

Format

label-withdraw-delay

undo label-withdraw-delay

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The label withdraw delay function prevents downstream LSP flapping from spreading to upstream nodes. For example, an LSP on a local node flaps because an LDP session between the node and its downstream peer flaps, a route flaps, or an LDP policy is modified. The local node repeatedly sends Label Withdraw and Label Mapping messages in sequence to upstream nodes. This causes the upstream nodes to repeatedly tear down and reestablish LSPs. As a result, the entire LDP LSP flaps. The label withdraw delay function can be enabled on each node of the LDP LSP to suppress the spread of LSP flapping.

Follow-up Procedure

Use the default delay time of 5s or run the **label-withdraw-delay timer** command to set the delay time.

Example

# Enable the label withdraw delay function.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] label-withdraw-delay
```

9.1.60 label-withdraw-delay timer

Function

The **label-withdraw-delay timer** command sets the delay time before a node sends a Label Withdraw message.

The **undo label-withdraw-delay timer** command restores the default delay time.

The default delay time is 5 seconds.

Format

label-withdraw-delay timer *time*

undo label-withdraw-delay timer

Parameters

Parameter	Description	Value
time	Specifies the delay time before a Label Withdraw message can be sent.	The value is an integer ranging from 1 to 65535, in seconds.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The label withdraw delay function prevents downstream LSP flapping from spreading to upstream nodes. For example, an LSP on a local node flaps because an LDP session between the node and its downstream peer flaps, a route flaps, or an LDP policy is modified. The local node repeatedly sends Label Withdraw and Label Mapping messages in sequence to upstream nodes. This causes the upstream nodes to repeatedly tear down and reestablish LSPs. As a result, the entire LDP LSP flaps. To suppress the spread of LSP flapping, run the **label-withdraw-delay** command to enable the label withdraw delay function on each node and the **label-withdraw-delay timer** command to set the delay time before a node sends a Label Withdraw message to its upstream node.

Prerequisites

The label withdraw delay function has been enabled using the **label-withdraw-delay** command.

Example

# Enable the label withdraw delay function on the node and set the delay time to 10s.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] label-withdraw-delay
[HUAWEI-mpls-ldp] label-withdraw-delay timer 10
```

9.1.61 ldp-over-te enable

Function

The **ldp-over-te enable** command enables LDP over Traffic Engineering (TE).

The **undo ldp-over-te enable** command disables LDP over TE.

By default, LDP over TE is not enabled.

Format

ldp-over-te enable

undo ldp-over-te enable

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MPLS TE supports strong traffic engineering capabilities and provides various QoS guarantees. Due to live network limitations, such as application types and costs, deploying MPLS TE on the entire network is difficult. Therefore, LDP over TE can be used to deploy MPLS TE on a core area and LDP on non-core areas.

To enable LDP over TE on the ingress of a TE tunnel, run the **ldp-over-te enable** command.

Precautions

In LDP over TE networking, load balancing is supported when the ingress node of a TE tunnel is an S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, or S6730-H. When there are multiple TE tunnels or there are both TE tunnels and LDP tunnels in the MPLS TE domain, LDP LSP service traffic can be load balanced among multiple tunnels. To adjust the load balancing mode, run the **mpls ecmp load-balance** command in the system-view.

Example

# Enable LDP over TE.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] ldp-over-te enable
```

9.1.62 ldp-sync enable

Function

The **ldp-sync enable** command enables synchronization between LDP and IS-IS on all interfaces in an IS-IS process.

The **undo ldp-sync enable** command disables synchronization between LDP and IS-IS on all interfaces in an IS-IS process.

By default, synchronization between LDP and IS-IS is disabled on all interfaces in an IS-IS process.

Format

ldp-sync enable [**mpls-binding-only**]

undo ldp-sync enable

Parameters

Parameter	Description	Value
mpls-binding-only	Synchronization between LDP and IS-IS can only be enabled on MPLS LDP-enabled interfaces.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Synchronization between LDP and IGP reduces LSP traffic loss on a network with both primary and backup LSPs. Traffic loss occurs in either of the following situations:

- The primary LSP works properly and an LDP session between two nodes on the primary LSP fails. IGP guides traffic still through the primary LSP even though a primary/backup LSP switchover is performed.
- If a link on the primary LSP or the primary LSP recovers, IGP routes converge. IGP routes associated with the primary LSP become reachable earlier than the primary LSP because IGP routes converge faster than LDP routes. IGP routes guide traffic through the primary LSP before the primary LSP recovers.

Synchronization between LDP and IGP delays IGP route advertisement so that the LDP session and IGP route can converge simultaneously.

The **ldp-sync enable** command run in the IS-IS view can enable synchronization between LDP and IS-IS on all interfaces within a specified IS-IS process.

Follow-up Procedure

Run the **isis ldp-sync block** command to disable synchronization between LDP and IGP on desired IS-IS interfaces.

Precautions

Although the **undo ldp-sync enable** command has been run, synchronization between LDP and IS-IS configured using the **isis ldp-sync** command still takes effect on an IS-IS interface.

Example

# Enable synchronization between LDP and IS-IS on all interfaces in an IS-IS instance.

```
<HUAWEI> system-view
[HUAWEI] isis 100
[HUAWEI-isis-100] ldp-sync enable
```

9.1.63 longest-match

Function

The **longest-match** command configures inter-domain LDP extension capability and enables LDP to search for routes to establish LSPs based on the longest match rule.

The **undo longest-match** command restores the default setting.

By default, LDP searches for routes to establish LSPs based on the exact matching rule.

Format

longest-match

undo longest-match

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a large network, multiple IGP areas need to be configured for flexible network deployment and fast route convergence. In this situation, when advertising routes between IGP areas, to prevent a large number of routes from consuming too many resources, an Area Border Router (ABR) needs to aggregate the routes in an area and then advertise the aggregated route to neighbor IGP areas. By default, when establishing LSPs, LDP searches the routing table for the route that exactly matches the forwarding equivalence class (FEC) carried in the received Label Mapping message. For aggregated routes, only liberal LDP LSPs, not inter-area LDP LSPs, can be set up.

In this case, run the **longest-match** command to enable LDP to search for routes or establishing inter-area LDP LSPs based on the longest match rule.

Precautions

Configuring this command is not allowed during LDP GR.

Example

# Enable LDP to search for routes for establishing LDP LSPs based on the longest match rule.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] longest-match
```

9.1.64 loop-detect

Function

The **loop-detect** command enables a device to advertise the capability of loop detection during the initialization of an LDP session.

The **undo loop-detect** command disables a device from advertising the capability of loop detection during the initialization of an LDP session.

By default, a device cannot advertise the capability of loop detection during the initialization of an LDP session.

Format

loop-detect

undo loop-detect

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

The switch does not support the loop detection function. In the scenario where its neighbor supports the loop detection function and requires that the notification about whether the loop detection function is enabled be consistent on the two ends, run the **loop-detect** command to ensure that the switch sets up an LDP session with this neighbor.

Though the **loop-detect** command is run, the switch still does not support the LDP loop detection function but only has the loop detection negotiation capability.

Example

# Enable the device to advertise the capability of loop detection during the initialization of an LDP session.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] loop-detect
```

9.1.65 lsp-trigger bgp-label-route

Function

The **lsp-trigger bgp-label-route** command enables LDP to allocate labels to labeled BGP routes on the public network.

The **undo lsp-trigger bgp-label-route** command restores the default setting.

By default, LDP does not allocate labels to labeled BGP routes on the public network.

Format

lsp-trigger bgp-label-route [**ip-prefix** *ip-prefix-name*] [**not-only-host**]

undo lsp-trigger bgp-label-route

Parameters

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Specifies the name of the IP prefix list that triggers the labeled BGP routes on the public network to set up LDP LSPs.	The value is an existing IP prefix list name.
not-only-host	Uses labeled public network BGP routes with 0-bit to 32-bit masks based on the IP prefix list to establish LDP LSPs.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Both the **lsp-trigger bgp-label-route** command and the **lsp-trigger** command can be used to configure policies to trigger the establishment of LDP LSPs. The former command is used for labeled public network BGP routes with 0-bit to 32-bit masks, and the latter command is used for static routes and IGP routes.

If **not-only-host** is not configured, LDP distributes labels only for labeled public network BGP routes with 32-bit masks. If **not-only-host** is configured, LDP distributes labels for labeled public network BGP routes with 0-bit to 32-bit masks.

Precautions

Modifying the LSP-triggering policy during the LDP GR period is invalid.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all public-network labeled BGP routes trigger LDP LSP establishment.

Example

# Trigger the establishment of LDP LSPs according to labeled public network BGP routes with 32-bit masks.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] lsp-trigger bgp-label-route
```

9.1.66 lsp-trigger

Function

The **lsp-trigger** command sets a policy for establishing LDP LSPs.

The **undo lsp-trigger** command restores the default setting.

By default, LDP uses IP host routes with 32-bit addresses (excluding host routes with 32-bit interface addresses) to establish LSPs.

Format

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

undo lsp-trigger

Parameters

Parameter	Description	Value
all	Indicates that all static and IGP routes trigger the establishment of LSPs.	-
host	Indicates that IP host routes with 32-bit addresses (excluding host routes with 32-bit interface addresses) trigger the establishment of LSPs.	-
ip-prefix *ip-prefix-name*	Specifies the name of the IP prefix list that triggers the establishment of LSPs.	The value is an existing IP prefix list name.
none	Indicates that the establishment of an LSP is not triggered.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After MPLS LDP is enabled, LSPs are automatically established. If no policy is configured, an increasing number of LSPs are established, wasting resources.

The **lsp-trigger** command configures a policy to allow LDP to use specified routes to establish LSPs. This setting prevents unwanted LSPs from being established and helps reduce resource wastes.

NOTE

The **lsp-trigger all** command is not recommended. If this command is run, LDP uses all IGP routes to establish LSPs, causing a large number of unwanted LSPs to be established and wasting system resources. Before using this command, configure a policy for filtering out routes unnecessary for the LSP establishment. The policy helps reduce the number of LSPs to be established and save system resources.

Prerequisites

MPLS has been enabled globally using the **mpls (system view)** command.

Precautions

- Modifying the LSP-triggering policy during the LDP GR period is invalid.
- The **lsp-trigger** command can be used to configure policies only for ingress and egress LSPs on the public network and ingress and egress LSPs on the private network that are established using IGP routes. To configure a policy for triggering the transit LSP establishment, run the **propagate mapping** command.
- The **lsp-trigger host** command can be run on either of the following nodes to provide a specific function:
  - Ingress: This command enables the ingress to use all routes with a 32-bit mask to establish LDP LSPs.
  - Egress: This command enables the egress to use local routes with a 32-bit mask to establish LDP LSPs.

  The **lsp-trigger** { **all** | **ip-prefix** *ip-prefix-name* } command can be used to establish proxy egress LSPs. The **lsp-trigger host** command, however, cannot be used to establish proxy egress LSPs.
- Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all static and IGP routes trigger LDP LSP establishment.

Example

# Trigger the establishment of LSPs based on all static and IGP routes.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] lsp-trigger all
```

9.1.67 lspv mpls-lsp-ping echo enable

Function

The **lspv mpls-lsp-ping echo enable** command enables a device to respond to MPLS Echo Request packets.

The **undo lspv mpls-lsp-ping echo enable** command disables a device from responding to MPLS Echo Request packets.

By default, a device is enabled to respond to MPLS Echo Request packets.

Format

lspv mpls-lsp-ping echo enable

undo lspv mpls-lsp-ping echo enable

Parameters

None.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The ping and trace tests use ICMP packets to locate faulty nodes on a forwarding path. When an LSP fails, IP forwarding-based ICMP packets cannot be used to detect the faulty node.

In this case, the **ping lsp** and **tracert lsp** command can be used to locate the faulty node on the LSP. These commands use MPLS Echo Request and MPLS Echo Reply packets to detect the connectivity of an LSP. Both MPLS Echo Request and MPLS Echo Reply packets are encapsulated into UDP packets and transmitted through port 3503. The receiver distinguishes MPLS Echo Request and MPLS Echo Reply packets based on the port number. An MPLS Echo Request packet carries FEC information to be detected, and is sent along the same LSP as other packets with the same FEC information. In this manner, the connectivity of the LSP is checked. MPLS Echo Request packets are transmitted to the destination through MPLS, whereas MPLS Echo Reply packets are transmitted to the source through IP.

For network security or management, you can run the **lspv mpls-lsp-ping echo enable** command to enable a device to respond to MPLS Echo Request packets or run the **undo lspv mpls-lsp-ping echo enable** command to disable the device from responding to MPLS Echo Request packets. This function is implemented by enabling or disabling port 3503. By default, port 3503 is enabled.

After you run the **ping lsp** and **tracert lsp** command to detect the connectivity of an LSP, you are advised to run the **undo lspv mpls-lsp-ping echo enable** command to disable the device from responding to MPLS Echo Request packets to avoid occupation of system resources.

Precautions

If you run the **undo lspv mpls-lsp-ping echo enable** command to disable a device from responding to MPLS Echo Request packets, this device does not respond to the **ping lsp** and **tracert lsp** command. As a result, the ping or trace test with the address of the device as the destination address times out.

Example

# Disable a device to respond to MPLS Echo Request packets.

```
<HUAWEI> system-view
[HUAWEI] undo lspv mpls-lsp-ping echo enable
```

9.1.68 lspv packet-filter

Function

The **lspv packet-filter** command enables the filtering of MPLS Echo Request packets based on source addresses. Filtering rules are defined in ACL configurations.

The **undo lspv packet-filter** command disables the filtering of MPLS Echo Request packets based on source addresses.

By default, the filtering of MPLS Echo Request packets based on source addresses is disabled.

Format

lspv packet-filter *acl-number*

undo lspv packet-filter

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The ACL number is a decimal integer that ranges from 2000 to 3999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **lspv packet-filter** command often runs on the destination device of the LSPV check. In the case that the filtering of MPLS Echo Request packets based on source addresses is enabled, upon receiving MPLS Echo Request packets, the device matches the source addresses of the packets with a specified ACL. The packets permitted by the ACL are processed; those denied by the ACL are discarded.

Example

# Enable the filtering of the MPLS Echo Request packets based on source addresses based on ACL 2100.

```
<HUAWEI> system-view
[HUAWEI] lspv packet-filter 2100
```

9.1.69 lsr-id

Function

The **lsr-id** command sets the LSR ID of an LDP instance.

The **undo lsr-id** command restores the default setting.

By default, the LSR ID of an LDP instance is the LSR ID of the LSR where the LDP instance is configured

Format

lsr-id *lsr-id*

undo lsr-id

Parameters

Parameter	Description	Value
lsr-id	Specifies the LSR ID of an LDP instance.	The value is in dotted decimal notation.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the LSR ID of an LDP instance is the same as the MPLS LSR ID configured using the **mpls lsr-id** command. On some networks such as the BGP/MPLS VPNs to which VPN instances apply, if the VPN address space and the public network address space overlap, configure LSR IDs for LDP instances to ensure the correct establishment of TCP connections.

Prerequisites

- MPLS has been enabled globally using the **mpls (system view)** command.
- MPLS LDP has been enabled globally using the **mpls ldp (system view)** command.

Precautions

Modifying or deleting the LSR ID of an LDP instance causes the reestablishment of all sessions in the LDP instance.

Example

# Set the LSR ID of an LDP instance to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] lsr-id 10.1.1.1
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

9.1.70 maintain-session received-error-message

Function

The **maintain-session received-error-message** command enables LDP to maintain a session after receiving error TCP packets.

The **undo maintain-session received-error-message** command restores the default configuration.

By default, LDP tears down a session after receiving error TCP packets.

Format

maintain-session received-error-message

undo maintain-session received-error-message

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

According to RFC5036, LDP tears down a session after receiving error TCP packets. When a device from another vendor fails or a link fails, the LDP session alternates between Up and Down after processing in this way. If the LDP transmits L2VPN services, the L2VPN services will be interrupted. To prevent this problem, run the **maintain-session received-error-message** command to enable LDP to maintain a session after receiving error TCP packets. This prevents LDP session flapping and helps maintain upper-layer L2VPN services.

Example

# Enable LDP to maintain a session after receiving error TCP packets.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] maintain-session received-error-message
```

9.1.71 md5-password

Function

The **md5-password** command sets the password that is used by a TCP connection during the creation of an LDP session.

The **undo md5-password** command disables MD5 authentication.

By default, MD5 authentication is disabled during the creation of an LDP session.

Format

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

undo md5-password [**plain** | **cipher**] *peer-lsr-id*

Parameters

Parameter	Description	Value
plain	Displays the password in plain text. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. In this case, users at a lower level can easily obtain the password by viewing the configuration file. This brings security risks. Therefore, it is recommended that you select **cipher** to save the password in cipher text.	-
cipher	Displays the password in cipher text.	-
peer-lsr-id	Specifies the LSR ID of the peer, which identifies the peer LSR.	The value is in dotted decimal notation.

Parameter	Description	Value
password	Specifies the password.	The value is a string of characters, spaces not supported. For a plain password, the string is 1 to 255 characters. For an encrypted password, the string is 20 to 392 characters. When double quotation marks are used around the string, spaces are allowed in the string.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MD5 authentication can be configured for a TCP connection over which an LDP session is established, improving security. Note that the peers of an LDP session can be configured with different encryption modes (plain or cipher text mode), but must be configured with a single password.

LDP MD5 authentication generates a unique digest for an information segment to prevent LDP packets from being modified. LDP MD5 authentication is stricter than common checksum verification for TCP connections.

A password can be set either in cipher text or plain text. A plain text password is a character string that is pre-configured and directly recorded in a configuration file. A cipher text password is a character string that is recorded in a configuration file after being encrypted using a specified algorithm.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

- MD5 authentication and keychain authentication cannot be configured together on one peer. Note that MD5 encryption algorithm cannot ensure security. Keychain authentication is recommended.
- If the password on a peer changes, the LDP session is reestablished and the LSP associated with the original LDP session is deleted.

Example

# Configure the local node to perform MD5 authentication when it establishes an LDP session with its peer.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] md5-password cipher 2.2.2.2 YsHsjx_202206
```

9.1.72 md5-password all

Function

The **md5-password all** command enables LDP MD5 authentication in a batch for all LDP peers.

The **undo md5-password all** command disables LDP MD5 authentication in a batch for all LDP peers.

By default, MD5 authentication in a batch is disabled for all LDP peers.

Format

md5-password { **plain** | **cipher** } **all** *password*

undo md5-password all

Parameters

Parameter	Description	Value
plain	Indicates a simple text password. A simple text password is saved in simple text in a configuration file. This format poses risks. A ciphertext password is recommended. To improve device security, periodically modify the password.	-
cipher	Indicates a ciphertext password.	-
password	Specifies an authentication password.	A password must not contain spaces. A simple text password is a string of 1 to 255 characters. A ciphertext password is a string of 1 to 255 characters. An MD5 ciphertext password is 20 bits to 392 bits long. The string can contain spaces if it is enclosed with double quotation marks (").

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MD5 authentication can be configured for a TCP connection over which an LDP session is established, improving security. LDP MD5 authentication generates a unique digest for an information segment to prevent LDP packets from being modified. LDP MD5 authentication is stricter than common checksum verification for TCP connections.

If a great number of LDP peers are configured, run the **md5-password all** command to enable MD5 authentication in a batch for all LDP peers.

Precautions

- LDP authentication configurations are prioritized in descending order: for a single peer, for a specified peer group, for all peers. Keychain and MD5 configurations of the same priority are mutually exclusive. Keychain authentication and MD5 authentication can be configured simultaneously for a specified LDP peer, for this LDP peer in a specified peer group, and for all LDP peers. The configuration with a higher priority takes effect. For example, if MD5 authentication is configured for Peer1 and then keychain authentication is configured for all LDP peers, MD5 authentication takes effect on Peer1.
- The session is not re-established if the passwords on both ends are the same. If the interval between password settings on both ends exceeds the session Keepalive time and the passwords become different, the session is disconnected due to a timeout, causing an LSP to be deleted.
- Note that the peers of an LDP session can be configured with different authentication modes (simple text or ciphertext), but must be configured with a single password.
- After the **md5-password all** command is run, MD5 authentication takes effect on all LDP peers. If MD5 authentication fails, an LDP session fails to be established.
- MD5 encryption algorithm cannot ensure security. Keychain authentication is recommended.

Example

# Enable LDP MD5 authentication for all LDP peers.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] md5-password cipher all YsHsjx_202206
```

9.1.73 md5-password peer-group

Function

The **md5-password peer-group** command enables LDP MD5 authentication in a batch for a specified LDP peer group.

The **undo md5-password peer-group** command disables LDP MD5 authentication in a batch for a specified LDP peer group.

By default, MD5 authentication in a batch is disabled for all peer groups.

Format

md5-password { **plain** | **cipher** } **peer-group** *ip-prefix-name password*

undo md5-password peer-group

Parameters

Parameter	Description	Value
plain	Indicates a simple text password. A simple text password is saved in simple text in a configuration file. This format poses risks. A ciphertext password is recommended. To improve device security, periodically modify the password.	-
cipher	Indicates a ciphertext password.	-
ip-prefix-name	Specifies the name of an IP prefix list. The IP prefix list name is configured using the **ip ip-prefix** command.	The value is a string of 1 to 169 case-sensitive characters, spaces not supported. The string can contain spaces if it is enclosed with double quotation marks (").

Parameter	Description	Value
password	Specifies an authentication password.	A password must not contain spaces. A simple text password is a string of 1 to 255 characters. A ciphertext password is a string of 1 to 255 characters. An MD5 ciphertext password is 20 bits to 392 bits long. The string can contain spaces if it is enclosed with double quotation marks (").

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MD5 authentication can be configured for a TCP connection over which an LDP session is established, improving security. LDP MD5 authentication generates a unique digest for an information segment to prevent LDP packets from being modified. LDP MD5 authentication is stricter than common checksum verification for TCP connections.

If a great number of LDP peers are configured, run the **md5-password peer-group** command to enable MD5 authentication in a batch for LDP peers in a specified peer group. An IP prefix list can be specified to define the range of IP addresses in a group.

Prerequisites

An IP prefix list has been configured using the **ip ip-prefix** command.

Precautions

- LDP authentication configurations are prioritized in descending order: for a single peer, for a specified peer group, for all peers. Keychain and MD5 configurations of the same priority are mutually exclusive. Keychain authentication and MD5 authentication can be configured simultaneously for a specified LDP peer, for this LDP peer in a specified peer group, and for all LDP peers. The configuration with a higher priority takes effect. For example, if MD5 authentication is configured for Peer1 and then keychain authentication is configured for all LDP peers, MD5 authentication takes effect on Peer1.

- The session is not re-established if the passwords on both ends are the same. If the interval between password settings on both ends exceeds the session Keepalive time and the passwords become different, the session is disconnected due to a timeout, causing an LSP to be deleted.
- Note that the peers of an LDP session can be configured with different authentication modes (simple text or ciphertext), but must be configured with a single password.
- After the **md5-password peer-group** command is run, MD5 authentication takes effect on a specified LDP peer group. If MD5 authentication fails, an LDP session fails to be established.
- MD5 encryption algorithm cannot ensure security. Keychain authentication is recommended.
- Before a peer group is referenced, create it. By default, a nonexistent peer group cannot be specified in this command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent peer group is specified in this command, a local device performs MD5 authentication for each LDP session connected to each LDP peer.

Example

# Enable LDP MD5 authentication for LDP peers with IP addresses matching the IP prefix list named **list1**.

```
<HUAWEI>system-view
[HUAWEI] ip ip-prefix list1 permit 4.4.4.4 32
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] md5-password cipher peer-group list1 YsHsjx_202206
```

9.1.74 mpls (system view)

Function

The **mpls** command enables MPLS on the local node and displays the MPLS view.

The **undo mpls** command deletes all MPLS configurations.

By default, no node is enabled with MPLS.

Format

mpls

undo mpls

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run the **mpls** command on a network where MPLS services are to be deployed.

You can run MPLS-related commands only after running the **mpls** command.

Prerequisites

The LSR ID has been configured using the **mpls lsr-id** command.

Precautions

NOTICE

After the **undo mpls** command is run in the system view, MPLS services may be interrupted and all MPLS configurations in the system and interface views are deleted. To restore the MPLS services, reconfigure these commands.

Example

# Enable MPLS.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
Info: Mpls starting, please wait... OK!
```

9.1.75 mpls (interface view)

Function

The **mpls** command enables MPLS on an interface.

The **undo mpls** command disables MPLS on an interface.

By default, no interface is enabled with MPLS.

Format

mpls

undo mpls

Parameters

None

Views

Interface view

NOTE

The **mpls** command does not take effect in the sub-interface view or tunnel interface view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where MPLS services are deployed, after enabling MPLS on a node, enable MPLS on the interfaces of the node before performing other MPLS configurations.

Prerequisites

MPLS has been enabled globally using the **mpls (system view)** command.

Precautions

Running the **undo mpls** command in the interface view deletes all MPLS configurations on the interface.

Example

# Enable MPLS on the interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
```

# Enable MPLS on the interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
```

9.1.76 mpls bfd enable

Function

The **mpls bfd enable** command enables dynamic creation of BFD sessions on the ingress node of an LDP LSP.

The **undo mpls bfd enable** command disables the dynamic creation of BFD sessions on the ingress node of an LDP LSP.

By default, an ingress cannot dynamically create BFD sessions for monitoring LDP LSPs.

Format

mpls bfd enable

undo mpls bfd enable

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an MPLS network, use LDP to dynamically create LSP tunnels. Upon a fault on the link, the convergence is slow. Configure BFD to detect LDP LSP connectivity to speed up convergence.

To dynamically establish a BFD session, run the **mpls bfd enable** command on the source end of the LDP LSP.

NOTE

After the **mpls bfd enable** command is used, no BFD session is set up.

Prerequisites

BFD has been enabled globally using the **bfd** command.

Example

# Enable the dynamic creation of BFD sessions on the ingress node of an LDP LSP.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls bfd enable
```

9.1.77 mpls bfd

Function

The **mpls bfd** command sets the parameters of BFD sessions.

The **undo mpls bfd** command deletes the parameters of BFD sessions.

By default, no parameter of BFD sessions is set.

Format

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

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

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

Parameters

Parameter	Description	Value
min-tx-interval *tx-interval*	Specifies the interval at which BFD packets are sent.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
min-rx-interval *rx-interval*	Specifies the interval at which BFD packets are received.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
detect-multiplier *multiplier*	Specifies the local detection multiplier value of a BFD session.	An integer ranging from 3 to 50. The value is 3 by default.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

On an MPLS network, use BFD to detect LSP connectivity to increase the link fault detection speed. Users can change the values of BFD parameters based on actual networking. On an unstable link, if the BFD parameters are set small, the BFD session may flap. You can increase the values of BFD parameters.

Actual interval for the local device to send BFD packets = max { interval for sending BFD packets on the local end, interval for receiving BFD packets on the peer end }; actual interval for the local device to receive BFD packets = max { interval for sending BFD packets on the peer end, interval for receiving BFD packets on the local end }; and local BFD detection time = actual interval for receiving BFD packets on the local end x BFD detection multiplier on the peer end.

If no BFD packet is received from the peer device within the detection time, the link is considered as faulty and the BFD session enters the Down state. To reduce the usage of system resources, when the BFD session is detected in Down state, the system adjusts the sending interval to a random value greater than 1000 ms. When the BFD session becomes Up, the configured interval is restored.

Example

# Set the interval at which BFD packets are sent to 200 ms.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls bfd min-tx-interval 200
```

9.1.78 mpls bfd-trigger

Function

The **mpls bfd-trigger** command configures a trigger policy for an LDP BFD session.

The **undo mpls bfd-trigger** command deletes a trigger policy for an LDP BFD session.

By default, no trigger policy for an LDP BFD session is configured.

Format

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

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

Parameters

Parameter	Description	Value
host	Indicates that all host addresses are used to create LDP BFD sessions.	-
nexthop *next-hop-address*	Specifies the next hop address on an LSP.	The value is in dotted decimal notation.
outgoing-interface *interface-type interface-number*	Specifies the type and number of an outbound interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
fec-list *list-name*	Specifies the name of a FEC list, by which the creation of an LDP BFD session is triggered.	The value is an existing FEC list name.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The trigger policy for LDP BFD has two types: the host address and FEC list.

If you want all host addresses to trigger the establishment of BFD sessions, use the host trigger mode. Specify the LSPs that can set up BFD sessions by specifying the next hop address and the outbound interface.

If you only want part of hosts to trigger the establishment of BFD sessions, use the FEC list trigger mode to specify the corresponding host addresses. Before specifying the FEC list triggering mode, run the **fec-list** and **fec-node** commands to configure a FEC list.

Prerequisites

BFD has been enabled globally using the **bfd** command.

Example

# Configure the host trigger policy of BFD sessions in the MPLS view.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls bfd enable
[HUAWEI-mpls] mpls bfd-trigger host
```

9.1.79 mpls bfd-ldp-number threshold-alarm

Function

The **mpls bfd-ldp-number threshold-alarm** command configures the conditions that trigger the threshold-reaching alarm and its clear alarm for dynamic BFD sessions for LDP. The conditions include the upper and lower alarm thresholds (percent) for the proportion of established dynamic BFD sessions for LDP to all supported ones.

The **undo mpls bfd-ldp-number threshold-alarm** command restores the default settings.

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

Format

mpls bfd-ldp-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls bfd-ldp-number threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Sets the upper alarm threshold for the proportion of established dynamic BFD sessions for LDP to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Sets the lower alarm threshold for the proportion of established dynamic BFD sessions for LDP to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of dynamic BFD sessions for LDP reaches a specified upper limit, new dynamic BFD sessions for LDP cannot be configured due to insufficient resources. To alert the administrator in operation and maintenance, enable a device to generate an alarm when the proportion of established dynamic BFD sessions for LDP to all supported ones reaches a specified upper alarm threshold. The following parameters can be configured in the **mpls bfd-ldp-number threshold-alarm** command:

- *upper-limit-value*: upper alarm threshold. If the proportion of established dynamic BFD sessions for LDP to all supported ones reaches the upper alarm threshold, an alarm can be generated.
- *lower-limit-value*: lower alarm threshold. If the proportion of established dynamic BFD sessions for LDP to all supported ones falls below the lower alarm threshold, a clear alarm can be generated.

Precautions

- If the **mpls bfd-ldp-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- The **mpls bfd-ldp-number threshold-alarm** command only configures the trigger conditions for an alarm and its clear alarm. Although trigger conditions are met, the alarm and its clear alarm can be generated only after the **snmp-agent trap enable feature-name mpls_lspm trap-name** { **hwmplsresourcethresholdexceed** | **hwmplsresourcethresholdexceedclear** } command is run to enable the device to generate an MPLS resource insufficiency alarm and its clear alarm.

Example

# Configure conditions that trigger the threshold-reaching alarm and its clear alarm for dynamic BFD sessions for LDP.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls bfd-ldp-number threshold-alarm upper-limit 90 lower-limit 60
```

9.1.80 mpls bgp bfd

Function

The **mpls bgp bfd** command sets time parameters for BGP BFD sessions.

The **undo mpls bgp bfd** command restores default time parameters for BGP BFD sessions.

By default, the minimum interval for sending BFD packets is 1000 ms, the minimum interval for receiving BFD packets is 1000 ms, and the local detection multiplier is 3.

Format

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

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

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

Parameters

Parameter	Description	Value
min-tx-interval *interval*	Specifies the minimum interval at which BGP BFD packets are sent.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
min-rx-interval *interval*	Specifies the minimum interval at which BGP BFD packets are received.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
detect-multiplier *multiplier*	Specifies the local BGP BFD detection multiplier.	The value is an integer ranging from 3 to 50. The default value is 3.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

A BGP BFD session working in asynchronous mode monitor BGP label switched paths (LSPs) over BGP tunnels. The ingress and egress of E2E BGP LSPs exchange BFD packets periodically. If a node receives no BFD packet after the detection period elapses, the node considers the BGP LSP faulty.

Effective BFD time parameters are calculated using the following formulas:

- Effective local interval at which BFD packets are sent = MAX { Locally configured minimum interval at which BFD packets are sent, Remotely configured minimum interval at which BFD packets are received }
- Effective local interval at which BFD packets are received = MAX { Remotely configured minimum interval at which BFD packets are sent, Locally configured minimum interval at which BFD packets are received }
- Local BFD detection period = Effective local interval at which BFD packets are received x Remotely configured BFD detection multiplier

Example

# Set the minimum interval at which BGP BFD packets are sent to **200** ms.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] mpls bgp bfd min-tx-interval 200
```

9.1.81 mpls bgp bfd enable

Function

The **mpls bgp bfd enable** command enables the MPLS ability to dynamically create BGP BFD sessions.

The **undo mpls bgp bfd enable** command disables the MPLS ability to dynamically create BGP BFD sessions.

By default, the MPLS ability to dynamically create BGP BFD sessions is disabled.

Format

mpls bgp bfd enable

undo mpls bgp bfd enable

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD for BGP tunnel rapidly detects faults in E2E BGP tunnels. Before a BGP BFD session is established, run the **mpls bgp bfd enable** command on the ingress of a BGP tunnel to enable the MPLS ability to dynamically create a BGP BFD session.

Prerequisites

BFD has been globally enabled using the **bfd** command.

Follow-up Procedure

Run the **mpls bgp bfd-trigger-tunnel** command to establish a BGP BFD session.

Example

# Enable the MPLS ability to dynamically create a BGP BFD session on the ingress of a BGP tunnel.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] mpls bgp bfd enable
```

9.1.82 mpls bgp bfd-trigger-tunnel

Function

The **mpls bgp bfd-trigger-tunnel** command specifies a policy to establish BGP BFD sessions.

The **undo mpls bgp bfd-trigger-tunnel** command deletes a policy to establish BGP BFD sessions.

By default, no trigger policy is configured.

Format

mpls bgp bfd-trigger-tunnel { **host** | **ip-prefix** *ip-prefix-name* }

undo mpls bgp bfd-trigger-tunnel

Parameters

Parameter	Description	Value
host	Allows a device to use host addresses to establish BGP BFD sessions.	-

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Allows a device to use an IP address prefix list with a specified name to establish BGP BFD sessions.	The value is an existing IP address prefix list.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD for BGP tunnel rapidly detects faults in E2E BGP tunnels. Before a BGP BFD session is established, the **mpls bgp bfd enable** command must be run to enable the MPLS ability to dynamically establish BGP BFD sessions on the ingress of a BGP tunnel. Then to specify the policy for dynamically establish BGP BFD sessions, run the **mpls bgp bfd-trigger-tunnel** command.

Either of the following trigger policies can be used:

- Host address-based policy: used when all host addresses are available to trigger the creation of BGP BFD sessions.
- IP address prefix list-based policy: used when only some host addresses can be used to establish BFD sessions.

Prerequisites

BFD has been globally enabled using the **bfd** command.

Precautions

If the **mpls bgp bfd-trigger-tunnel** command is run more than once, the latest configuration overrides the previous one.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all host addresses trigger BGP BFD session establishment.

Example

# Allow a device to use host addresses to dynamically establish BGP BFD sessions.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] mpls bgp bfd enable
[HUAWEI-mpls] mpls bgp bfd-trigger-tunnel host
```

9.1.83 mpls bgp-lsp-number threshold-alarm

Function

The **mpls bgp-lsp-number threshold-alarm** command configures the alarm threshold for BGP LSP usage.

The **undo mpls bgp-lsp-number threshold-alarm** command restores the default settings.

The default upper limit of the alarm threshold for BGP LSP usage is 80%. The default lower limit of the clear alarm threshold for BGP LSP usage is 75%.

Format

mpls bgp-lsp-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

mpls bgp-lsp-number { **ingress** | **egress** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls bgp-lsp-number threshold-alarm

undo mpls bgp-lsp-number { **ingress** | **egress** } **threshold-alarm**

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper limit of the alarm threshold for BGP LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies the lower limit of the clear alarm threshold for BGP LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.
ingress	Specifies the alarm threshold for ingress BGP LSPs.	-
egress	Specifies the alarm threshold for egress BGP LSPs.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of BGP LSPs in the system reaches a specific limit, establishing additional BGP LSPs may fail because of insufficient resources. To facilitate user operation and maintenance, enable an alarm to be generated when the number of BGP LSPs reaches the specific limit. To configure the alarm threshold for BGP LSP usage, run the **mpls bgp-lsp-number threshold-alarm** command. The parameters in this command are described as follows:

- *upper-limit-value*: upper alarm threshold. If the proportion of BGP LSP usage to all supported ones reaches the upper alarm threshold, an alarm can be generated.
- *lower-limit-value*: lower alarm threshold. If the proportion of BGP LSP usage to all supported ones falls below the lower alarm threshold, a clear alarm can be generated.

If you want to set the alarm threshold for ingress BGP LSPs or egress BGP LSPs, run **mpls bgp-lsp-number** { **ingress** | **egress** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*.

Precautions

- If the **mpls bgp-lsp-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- This command configures the alarm threshold for BGP LSP usage. The alarm that the number of LSPs exceeded the upper threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceed** is configured, and the actual BGP LSP usage reaches the upper limit of the alarm threshold. The alarm that the number of LSPs fell below the upper threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceedclear** is configured, and the actual BGP LSP usage falls below the lower limit of the clear alarm threshold.

Example

# Configure the upper limit and the lower limit of the alarm threshold for BGP LSP usage.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls bgp-lsp-number threshold-alarm upper-limit 90 lower-limit 60
```

9.1.84 mpls bgpv6-lsp-number threshold-alarm

Function

The **mpls bgpv6-lsp-number threshold-alarm** command configures the alarm threshold for BGP IPv6 LSP usage.

The **undo mpls bgpv6-lsp-number threshold-alarm** command restores the default settings.

The default upper limit of the alarm threshold for BGP IPv6 LSP usage is 80%. The default lower limit of the clear alarm threshold for BGP IPv6 LSP usage is 75%.

Format

mpls bgpv6-lsp-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

mpls bgpv6-lsp-number egress threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls bgpv6-lsp-number threshold-alarm

undo mpls bgpv6-lsp-number egress threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper limit of the alarm threshold for BGP IPv6 LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies the lower limit of the clear alarm threshold for BGP IPv6 LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.
egress	Specifies the alarm threshold for egress BGP IPv6 LSPs.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of BGP IPv6 LSPs in the system reaches a specific limit, establishing additional BGP IPv6 LSPs may fail because of insufficient resources. To facilitate user operation and maintenance, enable an alarm to be generated when the number of BGP IPv6 LSPs reaches the specific limit. To configure the alarm threshold for BGP IPv6 LSP usage, run the **mpls bgpv6-lsp-number threshold-alarm** command. The parameters in this command are described as follows:

- *upper-limit-value*: upper alarm threshold. If the proportion of BGP IPv6 LSP usage to all supported ones reaches the upper alarm threshold, an alarm can be generated.
- *lower-limit-value*: lower alarm threshold. If the proportion of BGP IPv6 LSP usage to all supported ones falls below the lower alarm threshold, a clear alarm can be generated.

If you want to set the alarm threshold for egress BGP IPv6 LSPs, run **mpls bgpv6-lsp-number egress threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*.

Precautions

- If the **mpls bgpv6-lsp-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- This command configures the alarm threshold for BGP IPv6 LSP usage. The alarm that the number of LSPs exceeded the upper threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceed** is configured, and the actual BGP IPv6 LSP usage reaches the upper limit of the alarm threshold. The alarm that the number of LSPs fell below the upper threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceedclear** is configured, and the actual BGP IPv6 LSP usage falls below the lower limit of the clear alarm threshold.

Example

# Configure the upper limit and the lower limit of the alarm threshold for BGP IPv6 LSP usage.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls bgpv6-lsp-number threshold-alarm upper-limit 90 lower-limit 60
```

9.1.85 mpls dynamic-label-number threshold-alarm

Function

The **mpls dynamic-label-number threshold-alarm** command sets alarm thresholds of dynamic label usage.

The **undo mpls dynamic-label-number threshold-alarm** command restores the default settings.

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

Format

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

undo mpls dynamic-label-number threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper limit of dynamic label usage.	The value is a percent integer ranging from 1 to 100. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies the lower limit of dynamic label usage.	The value is a percent integer ranging from 1 to 100. The lower limit must be less than the upper limit. Using the default value 70 is recommended.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If dynamic labels run out but the system receives new dynamic label requests, the system fails to satisfy the requests because the dynamic labels are insufficient. As a result, the module that fails to be assigned labels works abnormally. The modules that apply for labels including MPLS TE, MPLS LDP, BGP, L3VPN and L2VPN. To facilitate operation and maintenance, run **mpls dynamic-label-number threshold-alarm** command to set alarm thresholds of dynamic label usage. The system can alert users to the issue that dynamic labels will exhaust.

This command enables the system to generate an alarm in either of the following situations:

- *upper-limit-value*: a percent indicating the upper limit of dynamic labels. If dynamic label usage reaches the upper limit, an alarm is generated.
- *lower-limit-value*: a percent indicating the lower limit of dynamic labels. If dynamic label usage falls below the lower limit, a clear alarm can be generated.

Precautions

If the **mpls dynamic-label-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.

The **mpls dynamic-label-number threshold-alarm** command only configures the trigger conditions for an alarm and its clear alarm. Although trigger conditions are met, the alarm and its clear alarm can be generated only after the **snmp-agent trap enable feature-name mpls_lspm trap-name** { **hwmplsdynamiclabelthresholdexceed** | **hwmplsdynamiclabelthresholdexceedclear** } command is run to enable the device to generate a dynamic label insufficiency alarm and its clear alarm.

Example

# Set the thresholds for triggering dynamic label alarms.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls dynamic-label-number threshold-alarm upper-limit 90 lower-limit 60
```

9.1.86 mpls ecmp load-balance

Function

The **mpls ecmp load-balance** command configures the load balancing mode when packets are forwarded through LSPs established by MPLS LDP.

The **undo mpls ecmp load-balance** command restores the default load balancing mode when packets are forwarded through LSPs established by MPLS LDP.

By default, the load balancing mode is **label** when packets are forwarded through LSPs established by MPLS LDP.

NOTE

Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H support this command.

Format

mpls ecmp load-balance { **sip** | **dip** | **label** | **l4-sport** | **l4-dport** } *

undo mpls ecmp load-balance

Parameters

Parameter	Description	Value
sip	Indicates that load balancing is performed based on source IP addresses in MPLS packets.	-
dip	Indicates that load balancing is performed based on destination IP addresses in MPLS packets.	-
label	Indicates that load balancing is performed based on labels in MPLS packets.	-
l4-sport	Indicates that load balancing is performed based on the transport-layer source port in MPLS packets.	-
l4-dport	Indicates that load balancing is performed based on the transport-layer destination port in MPLS packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In real-world scenarios, you need to configure a proper load balancing mode based on MPLS service traffic characteristics on a transit node. If a service traffic parameter changes frequently, it is easier to load balance the traffic if you use the load balancing mode based on this parameter. For example, if the IP addresses of MPLS packets change frequently, it is easier to load balance traffic among LSPs if you use the load balancing mode based on **dip** or **sip**.

Precautions

This command takes effect only on newly established LSPs. If you want this command to take effect on previously created LSPs, run the **reset mpls ldp** command to re-establish the LSPs.

Example

# Set the load balancing mode to **sip** when packets are forwarded through LSPs established by MPLS LDP.

```
<HUAWEI> system-view
[HUAWEI] mpls ecmp load-balance sip
```

9.1.87 mpls forward-resource threshold-alarm

Function

The **mpls forward-resource threshold-alarm** command configures the conditions that trigger the threshold-reaching alarm and its clear alarm for MPLS forwarding resources.

The **undo mpls forward-resource threshold-alarm** command restores the default settings.

By default, the upper alarm threshold is 85%, and the lower alarm threshold is 75%.

Format

mpls forward-resource threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls forward-resource threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Sets the upper alarm threshold.	The value is an integer ranging from 2 to 100, represented in percentage.
lower-limit *lower-limit-value*	Sets the lower alarm threshold.	The value is an integer ranging from 1 to (*upper-limit-value*-1), represented in percentage.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of MPLS forwarding resources reaches a specified upper limit, new MPLS forwarding entries cannot be configured due to insufficient resources. To alert the administrator in operation and maintenance, enable a device to generate an alarm when the proportion of MPLS forwarding resources reaches a specified upper alarm threshold. The following parameters can be configured in the **mpls forward-resource threshold-alarm** command:

- *upper-limit-value*: upper alarm threshold. If the proportion of MPLS forwarding resources reaches the upper alarm threshold, an alarm can be generated.
- *lower-limit-value*: lower alarm threshold. If the proportion of MPLS forwarding resources falls below the lower alarm threshold, a clear alarm can be generated.

Precautions

- If the **mpls forward-resource threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- The **mpls forward-resource threshold-alarm** command only configures the trigger conditions for an alarm and its clear alarm. Although trigger conditions are met, the alarm and its clear alarm can be generated only after the **snmp-agent trap enable feature-name mpls trap-name** { **hwboardmplsfwdreslack** | **hwboardmplsfwdreslackresume** } command is run to enable the device to generate MPLS forwarding resources insufficiency alarm and its clear alarm.

Example

# Configure conditions that trigger the threshold-reaching alarm and its clear alarm for MPLS forwarding resources.

```
<HUAWEI> system-view
[HUAWEI] mpls forward-resource threshold-alarm upper-limit 90 lower-limit 60
```

9.1.88 mpls remote-adjacency-number threshold-alarm

Function

The **mpls remote-adjacency-number threshold-alarm** command configures the conditions that trigger the threshold-reaching alarm and its clear alarm for remote LDP adjacencies.

The **undo mpls remote-adjacency-number threshold-alarm** command restores the default settings.

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

Format

mpls remote-adjacency-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls remote-adjacency-number threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Sets the upper alarm threshold for the proportion of established remote LDP adjacencies to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Sets the lower alarm threshold for the proportion of established remote LDP adjacencies to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of remote LDP adjacencies reaches a specified upper limit, new remote LDP adjacencies cannot be configured due to insufficient resources. To alert the administrator in operation and maintenance, enable a device to generate an alarm when the proportion of established remote LDP adjacencies to all supported ones reaches a specified upper alarm threshold. The following parameters can be configured in the **mpls remote-adjacency-number threshold-alarm** command:

- *upper-limit-value*: upper alarm threshold. If the proportion of established remote LDP adjacencies to all supported ones reaches the upper alarm threshold, an alarm can be generated.
- *lower-limit-value*: lower alarm threshold. If the proportion of established remote LDP adjacencies to all supported ones falls below the lower alarm threshold, a clear alarm can be generated.

Precautions

- If the **mpls remote-adjacency-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- The **mpls remote-adjacency-number threshold-alarm** command only configures the trigger conditions for an alarm and its clear alarm. Although trigger conditions are met, the alarm and its clear alarm can be generated only after the **snmp-agent trap enable feature-name mpls_lspm trap-name** { **hwmplsresourcethresholdexceed** | **hwmplsresourcethresholdexceedclear** } command is run to enable the device to generate an MPLS resource insufficiency alarm and its clear alarm.

Example

# Configure conditions that trigger the threshold-reaching alarm and its clear alarm for remote LDP adjacencies.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls remote-adjacency-number threshold-alarm upper-limit 90 lower-limit 60
```

9.1.89 mpls ldp advertisement

Function

The **mpls ldp advertisement** command configures the label advertisement mode.

The **undo mpls ldp advertisement** command restores the default setting.

By default, the label advertisement mode is downstream unsolicited (DU).

Format

mpls ldp advertisement { **dod** | **du** }

undo mpls ldp advertisement

Parameters

Parameter	Description	Value
dod	Indicates the downstream on demand (DoD) mode. After the upstream requests the downstream for a label, the downstream sends a Label Mapping message to the upstream.	-
du	Indicates the DU mode. Without a request, the downstream voluntarily sends a Label Mapping message to the upstream.	-

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, remote MPLS LDP peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, downstream LSRs unsolicitedly send Label Mapping messages to upstream LSRs. Establishing a large number of LSPs burdens an LSR such as a DSLAM (a low-performance access device) deployed on an MPLS network. On a large network, run the **mpls ldp advertisement dod** command. This setting allows a DSLAM to send Label Mapping messages to upstream LSRs only after receiving requests for labels. This setting helps minimize the number of unwanted MPLS forwarding entries forwarded by the DSLAM.

Prerequisites

MPLS LDP has been enabled on the interface using the **mpls ldp (interface view)** command.

Precautions

- When multiple links exist between neighbors, all interfaces must use the same label advertisement mode.
- Modifying the label advertisement mode causes reestablishment of LDP sessions.

Example

# Set the label advertisement mode to DoD.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls ldp
[HUAWEI-Vlanif100] mpls ldp advertisement dod
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

# Set the label advertisement mode to DoD.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls ldp
[HUAWEI-GigabitEthernet0/0/1] mpls ldp advertisement dod
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

9.1.90 mpls ldp (system view)

Function

The **mpls ldp** command enables LDP on the local node and displays the MPLS-LDP view.

The **undo mpls ldp** command deletes all LDP configurations.

By default, LDP is not enabled on a node.

Format

mpls ldp

undo mpls ldp

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where MPLS LDP needs to be deployed, run the **mpls ldp** command to enable MPLS LDP globally and create a public network instance running LDP.

Prerequisites

MPLS has been enabled globally using the **mpls (system view)** command.

Follow-up Procedure

You can perform other LDP configurations.

Precautions

NOTICE

After the **undo mpls ldp** command is run in the system view, MPLS LDP services may be interrupted and all MPLS LDP configurations in the system and interface views are deleted. To restore the MPLS LDP services, reconfigure these commands.

Example

# Enable LDP.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp]
```

9.1.91 mpls ldp (interface view)

Function

The **mpls ldp** command enables MPLS LDP function on an interface.

The **undo mpls ldp** command disables MPLS LDP function on an interface.

By default, no interface is enabled with MPLS LDP function.

Format

mpls ldp

undo mpls ldp

Parameters

None

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where MPLS LDP needs to be deployed, enable MPLS LDP function on an interface before configuring other LDP configurations.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

MPLS has been enabled on the interface using the **mpls** command in the interface view.

Follow-up Procedure

You can perform other MPLS LDP configurations.

Precautions

Running the **undo mpls ldp** command in the interface view deletes all MPLS LDP configurations on the interface.

Example

# Enable MPLS LDP function on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls ldp
```

# Enable MPLS LDP function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls ldp
```

9.1.92 mpls ldp frr nexthop

Function

The **mpls ldp frr nexthop** command enables LDP FRR on an interface.

The **undo mpls ldp frr** command disables LDP FRR on an interface.

By default, no interface is enabled with LDP FRR.

Format

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

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

Parameters

Parameter	Description	Value
nexthop-address	Specifies the next hop address on a backup LSP.	The value is in dotted decimal notation.

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Specifies the IP prefix name. Only the FEC that matches the specified IP prefix can trigger the generation of a backup LSP.	The value is an existing IP prefix name.
priority *priority*	Specifies the priority of a backup LSP. The greater the value is, the lower priority the backup LSP has.	The value is an integer ranging from 1 to 65535. By default, the value is 50.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The traditional IP FRR technology cannot effectively protect the traffic on an MPLS network. The device provides the LDP FRR function and the solution to port protection.

In the manual LDP FRR mode, you need to configure a backup LSP by specifying the outbound interfaces or the next hops. This mode applies to simple-structured networks.

When running the **mpls ldp frr nexthop** command to configure the next hop IP address, note that:

- You can configure multiple next hops on one interface. This allows you to configure multiple backup LSPs with different outbound interfaces for the primary LSP.
- You can configure different prefix lists for the same next hop on one interface.
  - If no prefix list is specified, LDP FRR tries to establish backup LSPs along the path specified by *nexthop-address* for all primary LSPs on the interface.
  - If only the DENY item is in a specified prefix list, no backup LSP is allowed to set up along the path specified by *nexthop-address* for the primary LSP mapping to the FEC denied by the interface.
  - If only PERMIT item is in the specified prefix list, backup LSPs are allowed to set up along the path specified by *nexthop-address* only for the primary LSPs mapping to the FEC permitted by the interface.
  - If both PERMIT and DENY items are in the prefix list, only the PERMIT item is effective. That is, backup LSPs are allowed to set up along the

path specified by *nexthop-address* only for the primary LSPs mapping to the FEC permitted by the interface.

- A single interface supports LDP FRR with a maximum of 10 priorities. Only a single backup LSP is generated.

Prerequisites

MPLS has been enabled in the interface view using the **mpls** command.

Precautions

- If the **undo mpls ldp** command is run in the system view or the **undo mpls ldp** command is run in the interface view to disable LDP functions, the LDP FRR configuration in the interface remains but does not take effect. During the LDP FRR configuration, the LSP that functions as the backup LSP must be in the liberal state. For a backup LSP, the routing status of the backup LSP from the ingress node to the egress node must be Inactive Adv.
- LDP FRR cannot be enabled or disabled during LDP GR.
- When both LDP FRR and IP FRR are enabled, IP FRR takes effect.
- Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, backup LSPs are established for all LDP LSPs on the local interface along the path to the specified next-hop IP address.

Example

# Enable LDP FRR on VLANIF100, and set the next hop IP address of the backup LSP to 10.1.1.2.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls ldp frr nexthop 10.1.1.2
```

# Enable LDP FRR on GE0/0/1, and set the next hop IP address of the backup LSP to 10.1.1.2.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls ldp frr nexthop 10.1.1.2
```

9.1.93 mpls ldp remote-peer

Function

The **mpls ldp remote-peer** command creates a remote peer and displays the remote peer view.

The **undo mpls ldp remote-peer** command deletes a remote peer.

By default, no remote peer is created.

Format

mpls ldp remote-peer *remote-peer-name*

undo mpls ldp remote-peer *remote-peer-name*

Parameters

Parameter	Description	Value
remote-peer-name	Specifies the name of a remote LDP peer.	A string of 1 to 32 case-insensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A remote LDP session applies to the following scenarios:

- Allocate inner L2VPN labels.

  If a Martini VLL or VPLS connection is to be established between two LSRs, the remote LDP session must be established between the LSRs to allocate inner labels.

- Configure LDP over TE.

  If the core devices on an MPLS network support TE while edge devices use LDP, you need to configure a remote LDP session between the two edge LSRs on the TE network. After LDP over TE is configured, the TE tunnel is regarded as a hop of the entire LDP LSP.

A remote LDP session can be established between two indirectly connected LSRs or two directly connected LSRs.

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

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp (system view)** command.

Follow-up Procedure

An IP address can be assigned to the LDP remote peer.

Precautions

When configuring a remote LDP peer, run the **mpls ldp remote-peer** command on the local LDP and remote LDP peers.

Example

# Create a remote peer.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] quit
[HUAWEI] mpls ldp remote-peer BJI
[HUAWEI-mpls-ldp-remote-bji]
```

9.1.94 mpls ldp timer hello-hold

Function

The **mpls ldp timer hello-hold** command sets the value of a Hello Hold timer.

The **undo mpls ldp timer hello-hold** command restores the default value.

By default, the link Hello Hold timer is 15 seconds and the target Hello Hold timer is 45 seconds.

Format

mpls ldp timer hello-hold *interval*

undo mpls ldp timer hello-hold

Parameters

Parameter	Description	Value
interval	Specifies the value of a Hello Hold timer.	The value is an integer ranging from 3 to 65535, in seconds. Value 65535 indicates that the timer never expires.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, remote MPLS LDP peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Two LDP peers periodically exchange Hello messages to maintain the Hello adjacency. If no Hello message is received after the target Hello hold timer expires, the Hello adjacency is deleted.

The default value of the timer is recommended. On a network where the link status is unstable or a large number of packets are sent, increase the value of the timer to prevent the session flapping.

Hello hold timers are classified into the following types:

- Link-Hello hold timer: maintains the local adjacency. The **mpls ldp timer hello-hold** command in the interface view sets a value of the timer.
- Target-Hello hold timer: maintains the remote adjacency. The **mpls ldp timer hello-hold** command in the remote MPLS LDP peer view sets a value of the timer.

Prerequisites

The remote LDP peer has been configured or MPLS LDP has been enabled on the interface.

Precautions

The value of the timer that actually takes effect is the smaller one between the two Hello holder timers configured on both ends of an LDP session. If the value is smaller than 9, the Hello hold timer is 9.

Example

# Set the value of the link Hello hold timer to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls ldp
[HUAWEI-Vlanif100] mpls ldp timer hello-hold 30
```

# Set the value of the link Hello hold timer to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls ldp
[HUAWEI-GigabitEthernet0/0/1] mpls ldp timer hello-hold 30
```

# Set the value of the target Hello hold timer to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp remote-peer bji
[HUAWEI-mpls-ldp-remote-bji] mpls ldp timer hello-hold 60
```

9.1.95 mpls ldp timer hello-send

Function

The **mpls ldp timer hello-send** command sets the value of a Hello send timer.

The **undo mpls ldp timer hello-send** command restores the default setting.

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

Format

mpls ldp timer hello-send *interval*

undo mpls ldp timer hello-send

Parameters

Parameter	Description	Value
interval	Specifies the value of a Hello send timer.	The value is an integer ranging from 1 to 65535, in seconds.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, remote MPLS LDP peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An LSR sends Hello messages to the neighboring LSR to advertise its presence on the network and sets up the Hello adjacency. The Hello messages are sent at an interval specified by the Hello send timer.

The default value of the Hello send timer is recommended. On a network with poor performance, you can reduce the value of the Hello send timer, enabling the network to recover from faults as soon as possible.

Hello send timers are classified into the following types:

- Link-Hello send timer: maintains the local adjacency. The **mpls ldp timer hello-send** command in the interface view sets a value of the timer.
- Target-Hello send timer: maintains the remote adjacency. The **mpls ldp timer hello-send** command in the remote MPLS LDP peer view sets a value of the timer.

Prerequisites

The remote LDP peer has been configured or MPLS LDP has been enabled on the interface.

Precautions

The value of the Hello send timer that takes effect is not necessarily the same as the set value. If the value of the Hello send timer is greater than one third of the value of the Hello hold timer, the value of the Hello send timer that takes effect is equal to one third of the value of the link-Hello hold timer. Run the **mpls ldp timer hello-hold** command to set the value for the Hello hold timer.

Example

# Set the value of the link Hello send timer to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls ldp
[HUAWEI-Vlanif100] mpls ldp timer hello-send 10
```

# Set the value of the link Hello send timer to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls ldp
[HUAWEI-GigabitEthernet0/0/1] mpls ldp timer hello-send 10
```

# Set the value of the target Hello send timer to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp remote-peer bji
[HUAWEI-mpls-ldp-remote-bji] mpls ldp timer hello-send 20
```

9.1.96 mpls ldp timer igp-sync-delay

Function

The **mpls ldp timer igp-sync-delay** command sets the interval during which an LSP is being set up after an LDP session is created.

The **undo mpls ldp timer igp-sync-delay** command restores the default setting.

By default, the interval is 10 seconds.

Format

mpls ldp timer igp-sync-delay *value*

undo mpls ldp timer igp-sync-delay

Parameters

Parameter	Description	Value
value	Specifies the interval, during which an LSP is being set up after an LDP session is created.	The value is an integer ranging from 0 to 65535, in seconds.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, remote MPLS LDP peer view

Default Level

2: Configuration level

Usage Guidelines

LDP-Interior Gateway Protocol (IGP) synchronization-enabled devices complete to establish an LDP session earlier than an LSP. The **mpls ldp timer igp-sync-delay** command can be used to switch traffic to the established LSP after a specified period of time. This setting prevents traffic loss that occurs if the LDP session in the Up state attempts to switch traffic to the LSP that has not been established. Using the default delay value is recommended.

Example

# After the LDP session is established on VLANIF100, the interval is set to 15 seconds, during which the LSP is being set up.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls ldp
[HUAWEI-Vlanif100] mpls ldp timer igp-sync-delay 15
```

# After the LDP session is established on GE0/0/1, the interval is set to 15 seconds, during which the LSP is being set up.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1]  mpls ldp
[HUAWEI-GigabitEthernet0/0/1]  mpls ldp timer igp-sync-delay 15
```

# After the LDP session is established in the remote MPLS LDP peer view, the interval is set to 15 seconds, during which the LSP is being set up.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp remote-peer rta
[HUAWEI-mpls-ldp-remote-rta] mpls ldp timer igp-sync-delay 15
```

9.1.97 mpls ldp timer keepalive-hold

Function

The **mpls ldp timer keepalive-hold** command sets the value of a Keepalive hold timer.

The **undo mpls ldp timer keepalive-hold** command restores the default setting.

By default, the value of the Keepalive-hold timers of both local and remote sessions is 45 seconds.

Format

mpls ldp timer keepalive-hold *interval*

undo mpls ldp timer keepalive-hold

Parameters

Parameter	Description	Value
interval	Specifies the timeout period of a Keepalive hold timer.	The value is an integer ranging from 30 to 65535, in seconds.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, remote MPLS LDP peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

LDP peers exchange LDP PDUs over session connections to maintain LDP sessions. If a node does not receive any LDP PDU after the Keepalive hold timer expires, the node closes the connection to terminate the session.

The default value of the Keepalive hold timer is recommended. On a network with unstable links, increase the value of a Keepalive hold timer, preventing the session flapping.

Keepalive hold timers are classified into the following types:

- Keepalive hold timer of the local session: maintains the local LDP session. The **mpls ldp timer keepalive-hold** command in the interface view sets a value of the timer.
- Keepalive hold timer of the remote session: maintains the remote LDP session. The **mpls ldp timer keepalive-hold** command in the remote MPLS LDP peer view sets a value of the timer.

Prerequisites

The remote LDP peer has been configured or MPLS LDP has been enabled on the interface.

Precautions

- The value of the Keepalive hold timer that takes effect is the smaller one between the two Keepalive hold timers configured on both ends of an LDP session.
- If more than one LDP link exists between two LSRs, the values of the Keepalive hold timers set for the links must be the same; otherwise, the LDP sessions may be unstable.
- Changing the value of a Keepalive hold timer causes the reestablishment of related LDP sessions.

Example

# Set the value of the Keepalive hold timer for a local session to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls ldp
[HUAWEI-Vlanif100] mpls ldp timer keepalive-hold 60
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

# Set the value of the Keepalive hold timer for a local session to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls ldp
[HUAWEI-GigabitEthernet0/0/1] mpls ldp timer keepalive-hold 60
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

# Set the value of the Keepalive hold timer for a remote session to 50 seconds.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp remote-peer bji
[HUAWEI-mpls-ldp-remote-bji] mpls ldp timer keepalive-hold 50
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

9.1.98 mpls ldp timer keepalive-send

Function

The **mpls ldp timer keepalive-send** command sets the value of a Keepalive send timer.

The **undo mpls ldp timer keepalive-send** command restores the default setting.

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

Format

mpls ldp timer keepalive-send *interval*

undo mpls ldp timer keepalive-send

Parameters

Parameter	Description	Value
interval	Specifies the timeout period of a Keepalive send timer.	The value is an integer ranging from 1 to 65535, in seconds.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, remote MPLS LDP peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an LDP session is set up, LSRs on the two ends of the session periodically exchange Keepalive messages to maintain the LDP session.

The default value of the Keepalive send timer is recommended. On a network with poor performance, reduce the value of the Keepalive send timer, enabling the network to recover as soon as possible.

Keepalive send timers are classified into the following types:

- Keepalive send timer of the local LDP session: controls the interval at which Keepalive messages are sent to the peer end of the local session. The **mpls ldp timer keepalive-send** command in the interface view sets a value of this timer.
- Keepalive send timer of the remote LDP session: controls the interval at which Keepalive messages are sent to the peer end of the remote session. The **mpls**

ldp timer keepalive-send command in the remote MPLS LDP peer view sets a value of the timer.

Prerequisites

The remote LDP peer has been configured or MPLS LDP has been enabled on the interface.

Precautions

The value of the Keepalive send timer that actually takes effect may be different from the configured one. If the value of the Keepalive send timer is greater than one third of the value of the Keepalive hold timer, the value of the Keepalive send timer that actually takes effect is equal to one third of the value of the Keepalive hold timer.

Example

# Set the value of the Keepalive send timer for setting up a local LDP session to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls ldp
[HUAWEI-Vlanif100] mpls ldp timer keepalive-send 10
```

# Set the value of the Keepalive send timer for setting up a local LDP session to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls ldp
[HUAWEI-GigabitEthernet0/0/1] mpls ldp timer keepalive-send 10
```

# Set the value of the Keepalive send timer for setting up a remote LDP session to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp remote-peer bji
[HUAWEI-mpls-ldp-remote-bji] mpls ldp timer keepalive-send 20
```

9.1.99 mpls ldp transport-address

Function

The **mpls ldp transport-address** command configures an LDP transport address.

The **undo mpls ldp transport-address** command restores the default setting.

By default, the transport address for a node on a public network is the LSR ID of the node, and the transport address for a node on a private network is the primary IP address of an interface on the node.

Format

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

undo mpls ldp transport-address

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. LDP uses the address of the interface as the TCP transport address.	-
interface	Indicates that LDP uses the IP address of the current interface as the TCP transport address.	-

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before two LSRs establish an LDP session, the two LSRs need to establish a TCP connection to exchange label messages. Run the **mpls ldp transport-address** command to set the address (the LDP transport address) for the TCP connection.

The transport address is used to establish a TCP connection between the local node and its peer. The peer must have a reachable route to this transport address. The default transport address is the loopback interface address (an LSR ID). When the address of the loopback interface is a public network address, configure different transport addresses for LSRs so that LSRs can set up connections with private network addresses.

You can run the **mpls ldp transport-address** command in the interface view to set the transport address for a TCP connection. When more than one link exists between two LSRs, and the links are bound to VPN instances, the default transport address is the IP address of an interface rather than the LSR ID of an LSR.

NOTE

- If LDP sessions are to be established over multiple links connecting two LSRs, LDP-enabled interfaces of either LSR must use the default transport address or the same transport address. If interfaces on either of the LSRs are assigned different transport addresses, a single transport address can be used and a single LDP session can be established.
- When the LDP transport address changes, the session is not interrupted immediately. The session is interrupted after the Hello hold timer times out.

Prerequisites

MPLS LDP has been enabled on the interface using the **mpls ldp (interface view)** command.

An IP address must be assigned to the specified interface. If no IP address is assigned, 0.0.0.0 is used as a transport address, causing a failure to establish an LDP session.

Precautions

Changing an LDP transport address interrupts an LDP session. Exercise caution when running the **mpls ldp transport-address** command.

Example

# Set the transport address for link Hello messages to the current interface address.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls ldp
[HUAWEI-Vlanif100] mpls ldp transport-address interface
```

# Set the transport address for link Hello messages to the current interface address.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls ldp
[HUAWEI-GigabitEthernet0/0/1] mpls ldp transport-address interface
```

9.1.100 mpls ldp-lsp-number threshold-alarm

Function

The **mpls ldp-lsp-number threshold-alarm** command configures the alarm threshold for LDP LSP usage.

The **undo mpls ldp-lsp-number threshold-alarm** command restores the default settings.

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

Format

mpls ldp-lsp-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

mpls ldp-lsp-number { **ingress** | **transit** | **egress** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls ldp-lsp-number threshold-alarm

undo mpls ldp-lsp-number { **ingress** | **transit** | **egress** } **threshold-alarm**

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper limit of the alarm threshold for LDP LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies the lower limit of the clear alarm threshold for LDP LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.
ingress	Specifies the alarm threshold for ingress LDP LSPs.	-
transit	Specifies the alarm threshold for transit LDP LSPs.	-
egress	Specifies the alarm threshold for egress LDP LSPs.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of LDP LSPs in the system reaches a specific limit, establishing additional LDP LSPs may fail because of insufficient resources. To facilitate user operation and maintenance, enable an alarm to be generated when the number of LDP LSPs reaches the specific limit. To configure the alarm threshold for LDP LSP usage, run the **mpls ldp-lsp-number threshold-alarm** command. The parameters in this command are described as follows:

- *upper-limit-value*: upper alarm threshold. If the proportion of LDP LSP usage to all supported ones reaches the upper alarm threshold, an alarm can be generated.

- *lower-limit-value*: lower alarm threshold. If the proportion of LDP LSP usage to all supported ones falls below the lower alarm threshold, a clear alarm can be generated.

If you want to set the alarm threshold for ingress LDP LSPs, transit LDP LSPs or egress LDP LSPs, run **mpls ldp-lsp-number** { **ingress** | **transit** | **egress** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*.

Precautions

- If the **mpls ldp-lsp-number threshold-alarm** command is run several times, the latest configuration overrides the previous one.
- This command configures the alarm threshold for LDP LSP usage. The alarm that the number of LSPs exceeded the upper threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceed** is configured, and the actual LDP LSP usage reaches the upper limit of the alarm threshold. The alarm that the number of LSPs fell below the upper threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceedclear** is configured, and the actual LDP LSP usage fells to the lower limit of the clear alarm threshold.

Example

# Configure the upper limit and the lower limit of the alarm threshold for LDP LSP usage.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls ldp-lsp-number threshold-alarm upper-limit 90 lower-limit 60
```

9.1.101 mpls local-adjacency-number threshold-alarm

Function

The **mpls local-adjacency-number threshold-alarm** command configures the conditions that trigger the threshold-reaching alarm and its clear alarm for local LDP adjacencies. The conditions include the upper and lower alarm thresholds (percent) for the proportion of established local LDP adjacencies to all supported ones.

The **undo mpls local-adjacency-number threshold-alarm** command restores the default settings.

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

Format

mpls local-adjacency-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls local-adjacency-number threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Sets the upper alarm threshold for the proportion of established local LDP adjacencies to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Sets the lower alarm threshold for the proportion of established local LDP adjacencies to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of local LDP adjacencies reaches a specified upper limit, new local LDP adjacencies cannot be configured due to insufficient resources. To alert the administrator in operation and maintenance, enable a device to generate an alarm when the proportion of established local LDP adjacencies to all supported ones reaches a specified upper alarm threshold. The following parameters can be configured in the **mpls local-adjacency-number threshold-alarm** command:

- *upper-limit-value*: upper alarm threshold. If the proportion of established local LDP adjacencies to all supported ones reaches the upper alarm threshold, an alarm can be generated.
- *lower-limit-value*: lower alarm threshold. If the proportion of established local LDP adjacencies to all supported ones falls below the lower alarm threshold, a clear alarm can be generated.

Precautions

- If the **mpls local-adjacency-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- The **mpls local-adjacency-number threshold-alarm** command only configures the trigger conditions for an alarm and its clear alarm. Although trigger conditions are met, the alarm and its clear alarm can be generated only after the **snmp-agent trap enable feature-name mpls_lspm trap-name** { **hwmplsresourcethresholdexceed** | **hwmplsresourcethresholdexceedclear** } command is run to enable the device to generate an MPLS resource insufficiency alarm and its clear alarm.

Example

# Configure conditions that trigger the threshold-reaching alarm and its clear alarm for local LDP adjacencies.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls local-adjacency-number threshold-alarm upper-limit 90 lower-limit 60
```

9.1.102 mpls lsr-id

Function

The **mpls lsr-id** command sets an LSR ID.

The **undo mpls lsr-id** command deletes an LSR ID.

By default, no LSR ID is set.

Format

mpls lsr-id *lsr-id*

undo mpls lsr-id

Parameters

Parameter	Description	Value
lsr-id	Specifies the LSR ID of a device, which identifies the LSR.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An LSR ID identifies an LSR on a network. On a network where MPLS services are deployed, you must configure the LSR IDs for devices.

An LSR does not have the default LSR ID, and you must configure an LSR ID for it. To enhance network reliability, you are advised to use the IP address of a loopback interface on the LSR as the LSR ID.

Follow-up Procedure

You can configure MPLS and associated services.

Precautions

Before changing or deleting a configured LSR ID, you must run the **undo mpls** command in the system view to delete all MPLS configurations. Exercise caution when you run the **undo mpls** command.

NOTICE

Running the **undo mpls** command deletes all MPLS configurations (including established LDP sessions and LSPs).

Example

# Set the LSR ID to 1.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 1.1.1.1
```

9.1.103 mpls mtu

Function

The **mpls mtu** command configures the MTU of MPLS packets on an interface.

The **undo mpls mtu** command restores the default setting.

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

Format

mpls mtu *mtu*

undo mpls mtu

Parameters

Parameter	Description	Value
mtu	Specifies the MPLS MTU of an interface.	The value range varies according to the interface type.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, Tunnel interface view

NOTE

The **mpls mtu** command does not take effect in the tunnel interface view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An MTU value determines the maximum number of bytes that can be sent each time. If the size of packets exceeds the MTU supported by a transit node or a receiver, the transit node or receiver fragments the packets or even discards them, increasing the network transmission load. MTU values must be correctly negotiated between LSRs to enable packets to successfully reach the receiver.

To calculate the MPLS MTU, an LSR on the path to a specified FEC compares all MTUs advertised by downstream devices with the interface MTU of its own, and adds the smaller MTU (the MPLS MTU) to the MTU TLV field in the Label Mapping message, and send the Label Mapping message upstream.

If an MTU value changes (for example when the local outbound interface or its configuration changes), an LSR recalculates the MTU value and sends a Label Mapping message carrying the new MTU value to all upstream devices.

The relationships between the MPLS MTU and the interface MTU are as follows:

- If no MPLS MTU is configured on an interface, the interface MTU is used to control forwarding of MPLS packets.
- If both an MPLS MTU and an interface MTU are configured on an interface, the smaller value between the two MTUs is used to control forwarding of MPLS packets.

Prerequisites

MPLS has been enabled on the interface using the **mpls (interface view)** command.

Precautions

After changing the MTU using the **mpls mtu** or **mtu** command on an interface, you need to restart the interface to make the new MTU take effect. To restart the interface, run the **shutdown** command and then the **undo shutdown** command, or run the **restart** command in the interface view.

After the **mpls mtu** command is run, LDP compares the MPLS MTU and the interface MTU, and uses the smaller value between the two MTUs.

After the **mpls mtu** command is run:

- The device checks the MTU of packets on the control plane.
- On the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H, the MTU of packets on the forwarding plane is checked only when the following conditions are met:
  - IP packet fragmentation has been enabled using the **ipv4 fragment enable** command.
  - In an MPLS LDP, MPLS TE, static LSP, or L3VPN scenario, IP packets on a PE enter an MPLS network for MPLS encapsulation and forwarding.

Example

# Set the MPLS MTU to 1500 bytes on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls mtu 1500
```

# Set the MPLS MTU to 1500 bytes on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls mtu 1500
```

9.1.104 mpls total-lsp-number threshold-alarm

Function

The **mpls total-lsp-number threshold-alarm** command configures the alarm threshold for total LSP usage.

The **undo mpls total-lsp-number threshold-alarm** command restores the default settings.

The default upper limit of the alarm threshold for total LSP usage is 80%. The default lower limit of the clear alarm threshold for total LSP usage is 75%.

Format

mpls total-lsp-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

mpls total-lsp-number { **ingress** | **transit** | **egress** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls total-lsp-number threshold-alarm

undo mpls total-lsp-number { **ingress** | **transit** | **egress** } **threshold-alarm**

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper limit of the alarm threshold for total LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies the lower limit of the clear alarm threshold for total LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.

Parameter	Description	Value
ingress	Specifies the alarm threshold for total ingress LSPs.	-
transit	Specifies the alarm threshold for total transit LSPs.	-
egress	Specifies the alarm threshold for total egress LSPs.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of total LSPs (including static LSPs, LDP LSPs, BGP LSPs, BGP IPv6 LSPs) in the system reaches a specific limit, establishing subsequent LSPs may fail because of insufficient resources. To facilitate user operation and maintenance, enable an alarm to be generated when the number of total LSPs reaches the specific limit. To configure the alarm threshold for total LSP usage, run the **mpls total-lsp-number threshold-alarm** command. The parameters in this command are described as follows:

- *upper-limit-value*: upper alarm threshold. If the proportion of total LSP usage to all supported ones reaches the upper alarm threshold, an alarm can be generated.
- *lower-limit-value*: lower alarm threshold. If the proportion of total LSP usage to all supported ones falls below the lower alarm threshold, a clear alarm can be generated.

If you want to set the alarm threshold for total ingress LSPs, total transit LSPs or total egress LSPs, run **mpls total-lsp-number** { **ingress** | **transit** | **egress** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*.

Precautions

- If the **mpls total-lsp-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- This command configures the alarm threshold for total LSP usage. The alarm that the number of LSPs exceeded the upper threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm**

trap-name hwmplslspthresholdexceed is configured, and the actual total LSP usage reaches the upper limit of the alarm threshold. The alarm that the number of LSPs fell below the lower threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceedclear** is configured, and the actual total LSP usage falls below the lower limit of the clear alarm threshold.

Example

# Configure the upper limit and the lower limit of the alarm threshold for total LSP usage.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls total-lsp-number threshold-alarm upper-limit 90 lower-limit 60
```

9.1.105 mpls-passive

Function

The **mpls-passive** command enables the egress node of an LSP to passively create a BFD session.

The **undo mpls-passive** command disables the egress node of an LSP from passively creating a BFD session.

By default, the egress node of an LSP cannot passively create a BFD session.

Format

mpls-passive

undo mpls-passive

Parameters

None

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a unidirectional LSP, the ingress node creates a BFD session, which triggers the sending of an LSP ping packet. After the egress node receives the ping packet, a BFD session can be automatically created on the egress node. Run the **mpls-passive** command to enable the BFD session to be created passively on the egress node of an LSP. If the feature is disabled, the egress node cannot automatically create a BFD session.

Prerequisites

BFD has been enabled globally using the **bfd** command.

Precautions

You need to run the **mpls-passive** command on the egress node. Then, the egress node can create a BFD session in an opposite direction after receiving an LSP ping request packet carrying a BFD TLV.

Example

# Enable the egress node of an LSP to automatically and passively create a BFD session.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] mpls-passive
```

9.1.106 mpls ping interval

Function

The **mpls ping interval** command sets the interval at which LSP ping packets are sent in a dynamic BFD session.

The **undo mpls ping interval** command restores the default setting.

By default, the interval at which LSP ping packets are sent in a dynamic BFD session is 60 seconds.

Format

mpls ping interval *interval*

undo mpls ping interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending LSP ping packets.	The value is an integer ranging from 30 to 600, in seconds. The default value is 60.

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an LSP, when the active role (the ingress node) creates a dynamic BFD session, an LSP ping request packet carrying a BFD TLV is sent. After receiving the LSP ping request packet, the passive role (the egress node) replies with an LSP ping response packet carrying the BFD TLV. Then, a BFD session is established. To set the interval for sending the LSP ping packet by dynamic BFD, run the **mpls ping interval** command.

Prerequisites

BFD has been enabled globally using the **bfd** command in the system view.

Precautions

A small interval for sending LSP ping packets imposes a heady burden on links.

Set the interval for sending the LSP ping packet according to the actual networking because the egress node can establish a BFD session only after receiving an LSP ping packet.

Example

# Set the interval to 80 seconds for sending LSP ping packets in a dynamic BFD session.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] mpls ping interval 80
```

9.1.107 mtu-signalling

Function

The **mtu-signalling** command enables the switch to send Label Mapping messages carrying the MTU TLV and determines the MTU TLV type.

The **undo mtu-signalling** command disables the switch to send Label Mapping messages carrying the MTU TLV

By default, the switch with MPLS LDP globally enabled sends Label Mapping messages carrying the MTU TLV, in compliance with draft-ietf-mpls-ldp-mtu-extensions.

Format

mtu-signalling [**apply-tlv**]

undo mtu-signalling [**apply-tlv**]

Parameters

Parameter	Description	Value
apply-tlv	Indicates the type of MTU TLV carried in Label Mapping messages to be sent. After this parameter is configured, the implementation is in compliance with RFC 3988. If this parameter is not configured, the implementation is in compliance with draft-ietf-mpls-ldp-mtu-extensions.	-

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If different types of links on an MPLS network support different MTU values, this function enables devices to negotiate MTU values, prevents packets from being discarded if the packet size exceeds an MTU.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

By default, after MPLS LDP is globally enabled, a device sends Label Mapping messages carrying an MTU TLV in compliance with draft-ietf-mpls-ldp-mtu-extensions. If an LDP peer does not identify the MTU TLV carried in a received message, the peer must process the TLV as an unknown TLV defined in RFC 5036.

Changing the configuration disconnects an existing LDP session and causes the LDP session to be reestablished.

Example

# Enable LDP to send Label Mapping messages carrying the MTU TLV, as defined in RFC3988.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] mtu-signalling apply-tlv
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

9.1.108 no-renegotiate session-parameter-change graceful-restart

Function

The **no-renegotiate session-parameter-change graceful-restart** command disables a device from re-establishing existing LDP sessions when LDP GR status or a GR parameter is changed.

The **undo no-renegotiate session-parameter-change graceful-restart** command restores the default configuration.

By default, a device re-establishes LDP sessions when LDP GR status or a GR parameter is changed.

Format

no-renegotiate session-parameter-change graceful-restart

undo no-renegotiate session-parameter-change graceful-restart

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

After the **no-renegotiate session-parameter-change graceful-restart** command is run, running the following commands does not affect the existing LDP sessions.

- **graceful-restart (MPLS-LDP view)**
- **graceful-restart timer neighbor-liveness**
- **graceful-restart timer reconnect**
- **graceful-restart timer recovery**

Example

# Disable a device from re-establishing existing LDP sessions when LDP GR status or a GR parameter is changed.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] no-renegotiate session-parameter-change graceful-restart
```

9.1.109 ospf ldp-sync

Function

The **ospf ldp-sync** command enables synchronization between LDP and OSPF on an interface.

The **undo ospf ldp-sync** command disables synchronization between LDP and OSPF on an interface.

By default, synchronization between LDP and OSPF is disabled on an interface.

Format

ospf ldp-sync

undo ospf ldp-sync

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The LDP convergence speed depends on the convergence speed of OSPF routes. To enable MPLS LDP on a network with the primary and backup links, the following problems may occur:

- Upon a fault on the active link, OSPF routes and ISP are switched to the backup link using LDP FRR. When the primary link recovers, OSPF routes are switched back to the primary link earlier than LDP traffic because IGP route convergence is faster than LDP convergence. As a result, LSP traffic is lost.
- If a fault occurs on the LDP session between nodes on the primary link where the OSPF routes are working properly, the OSPF routes still use the primary link and the LSP on the primary link is deleted. No OSPF route exists on the backup link; therefore, no LSP can be established on the backup link. LSP traffic is lost.

Run the **ospf ldp-sync** command to enable synchronization between LDP and OSPF to prevent traffic loss in the preceding problems. Run this command on the interfaces on both ends of the link between the node where the primary LSP and the backup LSP diverge from each other and its LDP peer on the primary LSP.

Example

# Enable synchronization between LDP and OSPF on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf ldp-sync
```

# Enable synchronization between LDP and OSPF on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf ldp-sync
```

9.1.110 ospf timer ldp-sync hold-down

Function

The **ospf timer ldp-sync hold-down** command sets the interval during which an interface waits for creating an LDP session before setting up the OSPF neighbor relationship.

The **undo ospf timer ldp-sync hold-down** command restores the default setting.

By default, the interval during which an interface waits for creating an LDP session before setting up the OSPF neighbor relationship is 10 seconds.

Format

ospf timer ldp-sync hold-down *value*

undo ospf timer ldp-sync hold-down

Parameters

Parameter	Description	Value
value	Specifies the interval during which an interface waits for creating an LDP session before setting up the OSPF neighbor relationship.	The value is an integer ranging from 0 to 65535, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After this command is configured, OSPF routes are not immediately switched to the primary link after the primary link is restored and before the LDP session is established. LSP traffic is transmitted through the backup link in a period of time specified by this command.

Prerequisites

LDP and OSPF synchronization has been enabled using the **ospf ldp-sync** command in the interface view.

Precautions

This command is circular in nature, and the latest configuration overrides the previous configurations.

Example

# Set the value of the Hold-down timer for VLANIF100 to 15 seconds, during which the interface waits for the establishment of an LDP session before setting up the OSPF neighbor relationship.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf timer ldp-sync hold-down 15
```

# Set the value of the Hold-down timer for GE0/0/1 to 15 seconds, during which the interface waits for the establishment of an LDP session before setting up the OSPF neighbor relationship.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf timer ldp-sync hold-down 15
```

9.1.111 ospf timer ldp-sync hold-max-cost

Function

The **ospf timer ldp-sync hold-max-cost** command sets the interval at which OSPF LSAs are sent to advertise the maximum metric on the local device.

The **undo ospf timer ldp-sync hold-max-cost** command restores the default setting.

By default, the interval is 10 seconds.

Format

ospf timer ldp-sync hold-max-cost { *value* | **infinite** }

undo ospf timer ldp-sync hold-max-cost

Parameters

Parameter	Description	Value
value	Specifies the interval for sending OSPF LSAs to advertise the maximum metric on the local device.	The value is an integer ranging from 0 to 65535, in seconds.
infinite	Indicates that OSPF always advertises the maximum metric in LSAs on the local device before an LDP session is reestablished.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the primary LSP recovers from a fault, run the **ospf timer ldp-sync hold-max-cost** command to set the interval during which traffic is still transmitted along the backup LSP before the LDP session of the primary LSP is reestablished.

You can choose different parameters as required.

- When OSPF carries only LDP services, to ensure that OSPF routing is always consistent with the LDP LSP, specify **infinite**.
- When OSPF carries multiple services including LDP services, to ensure that OSPF route selection and other services still run properly in case the LDP session of the primary LSP fails, specify *value*.

Prerequisites

LDP and OSPF synchronization has been enabled using the **ospf ldp-sync** command in the interface view.

Precautions

This command is circular in nature, and the latest configuration overrides the previous configurations.

Example

# Set the interval at which OSPF LSAs are sent to advertise the maximum metric on the local device to 8 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf ldp-sync
[HUAWEI-Vlanif100] ospf timer ldp-sync hold-max-cost 8
```

# Set the interval at which OSPF LSAs are sent to advertise the maximum metric on the local device to 8 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf ldp-sync
[HUAWEI-GigabitEthernet0/0/1] ospf timer ldp-sync hold-max-cost 8
```

9.1.112 outbound peer split-horizon

Function

The **outbound peer split-horizon** command enables split horizon on an LSR to allow the LSR to distribute labels only to its upstream LDP peers.

The **undo outbound peer split-horizon** command restores the default setting.

By default, split horizon is not enabled, which means that an LSR distributes labels to both upstream and downstream LDP peers.

Format

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

undo outbound peer { *peer-id* | **all** } **split-horizon**

Parameters

Parameter	Description	Value
peer-id	Specifies the LSR ID of an LDP peer.	The value is in dotted decimal notation.
all	Indicates all LDP peers.	-

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An LSR sends Label Mapping messages to both upstream and downstream LDP peers by default, speeding up LDP LSP convergence. This leads to the establishment of a great number of unwanted LSPs, wasting resources. To reduce the number of LSPs and saving memory resources, run the **outbound peer** { *peer-id* | **all** } **split-horizon** command to configure an LDP split horizon policy, enabling the LSR to send Label Mapping messages only to upstream LDP peers.

In the **outbound peer split-horizon** command, configure either of the following parameters to prevent an LSR from distributing labels to specified downstream peers:

- *peer-id*: prevents the LSR from distributing labels to a specified downstream peer.
- **all**: prevents the LSR from distributing labels to all downstream peers.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

The **all** parameter takes preference over the *peer-id* parameter. For example, the **outbound peer all split-horizon** and then **outbound peer 2.2.2.2 split-horizon** commands are run, the **outbound peer all split-horizon** command can be saved in the configuration file and take effect, not the **outbound peer 2.2.2.2 split-horizon** command.

Example

# Enable split horizon for all LDP peers.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] outbound peer all split-horizon
```

9.1.113 path-vectors

Function

The **path-vectors** command sets the maximum number of hops of the path vector that is used for LDP loop detection.

The **undo path-vectors** command restores the default setting.

By default, a maximum of 32 hops of the path vector are used for LDP loop detection.

Format

path-vectors *integer*

undo path-vectors

Parameters

Parameter	Description	Value
integer	Specifies the path vector.	The value is an integer ranging from 1 to 32.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A scenario assumes that LDP loop detection is configured using the path vector, and the maximum number of hops of the path vector is n. The egress LSP triggered by local routes detects loop after n + 1 hops, whereas the egress LSP triggered by non-local routes (proxy egress) detects loops after n hops.

Prerequisites

The **path-vectors** command has been configured before LDP is enabled on all interfaces. The **path-vectors** command takes effect only after **MPLS LDP** is enabled in the related view.

Example

# Set the maximum value of the path vector to 3.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] path-vectors 3
```

9.1.114 ping lsp

Function

The **ping lsp** command checks the LSP connectivity and LSP forwarding status.

Format

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**]

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** *interface-number* [**hot-standby** | **primary**] [**draft6**]

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**] * **vpn-instance** *vpn-name* **remote** *remote-address mask-length* [**vpn-frr-path**]

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**] * **bgp** *destination-address mask-length* [*ip-address*]

Parameters

Parameter	Description	Value
-a *source-ip*	Specifies the source IP address of MPLS Echo Request packets to be sent. If the source IP address is not specified, the IP address of the outbound interface from which MPLS Echo Request packets are sent is used as the source IP address. **NOTE** If an E2E BGP LSP has been established between two devices and the LSR ID is not used on the ingress, to run the **ping lsp** command with **bgp** specified on the ingress, you must specify **-a** *source-ip* as the IP address used for establishing the E2E BGP LSP.	-
-c *count*	Specifies the number of MPLS Echo Request packets to be sent. In the case of poor network quality, you can set this parameter to a comparatively large value to check the network quality based on the packet loss rate.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-exp *exp-value*	Specifies the EXP value of MPLS Echo Request packets to be sent. **NOTE** If DSCP priority has been configured by running the **set priority** command, the *exp-value* parameter does not take effect.	The value is an integer that ranges from 0 to 7. The default value is 0.

Parameter	Description	Value
-h *ttl-value*	Specifies the value of the TTL. Each time the **ping lsp** command is run, an MPLS Echo Request packet carrying a sequence number is sent. The sequence number of the MPLS Echo Request packet starts from 1 and is increased by 1. By default, a maximum of five MPLS Echo Request packets are sent. You can set the number of MPLS Echo Request packets to be sent through the parameter *ttl-value*. If the destination is reachable, the source can receive five MPLS Echo Reply packets from the destination, with sequence numbers corresponding to those of MPLS Echo Request packets. If the TTL field is decreased to 0 during packet forwarding, the switch that the packet reaches sends an MPLS timeout packet to the source, indicating that the destination is unreachable.	The value is an integer that ranges from 1 to 255. The default value is 64.
-m *interval*	Specifies the time to wait before sending the next MPLS Echo Request packet. Each time the source sends an MPLS Echo Request packet using the **ping lsp** command, the source waits a period of time (2000 ms by default) before sending the next MPLS Echo Request packet. You can set the time to wait before sending the next ICMP Echo Request message using the parameter *interval*. In the case of poor network condition, the value should be equal to or larger than 2000, in milliseconds.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 2000.

Parameter	Description	Value
-r *reply-mode*	Specifies the mode in which the peer returns MPLS Echo Reply packets.	The value is an integer that ranges from 1 to 4. The default value is 2. ● 1: The peer does not return MPLS Echo Reply packets. ● 2: The peer end responds to MPLS Echo Reply packets with IPv4 or IPv6 User Datagram Protocol (UDP) packets. ● 3: The peer end responds to MPLS Echo Reply packets with IPv4 or IPv6 UDP packets containing the Router alert option. ● 4: The peer end responds to MPLS Echo Reply packets through the control channel on the application plane.
-s *packet-size*	Indicates the length of the payload in a packet, excluding the IP header and UDP header.	The value is an integer that ranges from 65 to 8100, in bytes. The default value is 100. The configured value must be smaller than the MTU of the interface.
-t *time-out*	Indicates the timeout period to wait for an MPLS Echo Reply packet after an MPLS Echo Request packet is sent.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000.

Parameter	Description	Value
-v	Displays MPLS Echo Reply packets not for the local user. By default, only MPLS Echo Reply packets for the local user are displayed. ● If **-v** is not specified, the system displays only the MPLS Echo Reply packets received by the local user. ● If **-v** is specified, the system displays all received MPLS Echo Reply packets.	By default, the system displays only the MPLS Echo Reply packets received by the local user.
ip *destination-address mask-length*	Specifies the IPv4 address and mask length of the destination.	The destination IPv4 address is in dotted decimal notation. The mask length is an integer that ranges from 0 to 32.
ip-address	Specifies the destination IP address carried in the IP header of an MPLS Echo Request packet.	The value is in dotted decimal notation. By default, the destination IP address carried in the IP header of an MPLS Echo Request packet is 127.0.0.1.
nexthop *nexthop-address*	Specifies the IP address of the next hop.	The value is in dotted decimal notation.
draft6	Specifies the version of the **ping lsp** command. If this parameter is specified, the ping operation is performed according to "draft-ietf-mpls-lsp-ping-06". By default, the ping operation is performed according to RFC 4379.	-
te tunnel *interface-number*	Specifies the number of a tunnel interface.	-
hot-standby	Indicates that the hot-standby CR-LSP is to be detected.	-

Parameter	Description	Value
primary	Indicates that the primary CR-LSP is to be monitored.	-
vpn-instance *vpn-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
remote *remote-address mask-length*	Specifies the destination IP address and mask of the VPN LSP to be monitored.	The IP address is in dotted decimal notation. The mask length is an integer that ranges from 0 to 32.
bgp *destination-address mask-length*	Specifies the IP address and mask length of the BGP destination.	-
vpn-frr-path	Specifies that the connectivity of the backup VPN FRR LSP will be checked. **NOTE** Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H support this parameter.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

On an MPLS network, you can run the **ping lsp** command to check LSP connectivity after an LSP is established.

The LSP ping uses Echo Request messages and MPLS Echo Reply messages to monitor the connectivity of LSPs. Both Echo Request and Echo Reply messages are encapsulated into UDP packets and transmitted through port 3503. The receiver distinguishes Echo Request and MPLS Echo Reply messages based on the port number. An Echo Request message carries FEC information to be monitored and travels along the same LSP as other packets with the same Forwarding Equivalence Class (FEC) to monitor the connectivity of the LSP. Echo Request messages are transmitted to the destination using MPLS, whereas MPLS Echo Reply messages are transmitted to the source using IP.

The LSP ping can be used to monitor the following types of links:

- LDP LSP Ping: Run the **ping lsp ip** *destination-address mask-length* command on the ingress node to ping the egress node to monitor the connectivity of the LSP.
- TE Tunnel Ping: If a tunnel exists, run the **ping lsp te tunnel** *interface-number* command on the ingress node to ping the egress node to monitor the connectivity of the tunnel.
- L3VPN LSP Ping: After a VPN is correctly configured, run the **ping lsp vpn-instance** *vpn-name* **remote** *remote-address mask-length* command on the ingress node to ping the egress node to monitor the connectivity of the VPN LSP established using BGP.

If the **ping lsp** command detects a fault on an LSP that packets transmitted along this LSP cannot reach the egress node, you can run the **tracert lsp** command to locate the fault.

Prerequisites

Before running the **ping lsp** command, ensure that the MPLS module is working properly.

Precautions

To prevent the egress node from forwarding the received MPLS Echo Request packet to other nodes, the destination address in the IP header of the Echo Request packet is set to 127.0.0.1/8 (the local loopback address), and the TTL value contained in the IP header is set to 1.

Example

# Ping 10.1.1.1/32 by sending ten 200-byte MPLS Echo Request packets.

```
<HUAWEI> ping lsp -c 10 -s 200 ip 10.1.1.1 32
  LSP PING FEC: IPV4 PREFIX 10.1.1.1/32/ : 200 data bytes, press CTRL_C to break
    Reply from 10.1.1.1: bytes=200 Sequence=1 time = 11 ms
    Reply from 10.1.1.1: bytes=200 Sequence=2 time = 6 ms
    Reply from 10.1.1.1: bytes=200 Sequence=3 time = 6 ms
    Reply from 10.1.1.1: bytes=200 Sequence=4 time = 6 ms
    Reply from 10.1.1.1: bytes=200 Sequence=5 time = 12 ms
    Reply from 10.1.1.1: bytes=200 Sequence=6 time = 9 ms
    Reply from 10.1.1.1: bytes=200 Sequence=7 time = 12 ms
    Reply from 10.1.1.1: bytes=200 Sequence=8 time = 9 ms
    Reply from 10.1.1.1: bytes=200 Sequence=9 time = 12 ms
    Reply from 10.1.1.1: bytes=200 Sequence=10 time = 12 ms

  --- FEC: IPV4 PREFIX 10.1.1.1/32 ping statistics ---
    10 packet(s) transmitted
    10 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 6/10/12 ms
```

# Ping an MPLS TE tunnel.

```
<HUAWEI> ping lsp te tunnel 1
  LSP PING FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel1 : 100 data bytes, press CTRL_C to break
    Reply from 10.1.1.2: bytes=100 Sequence=1 time = 50 ms
    Reply from 10.1.1.2: bytes=100 Sequence=2 time = 28 ms
    Reply from 10.1.1.2: bytes=100 Sequence=3 time = 33 ms
    Reply from 10.1.1.2: bytes=100 Sequence=4 time = 52 ms
    Reply from 10.1.1.2: bytes=100 Sequence=5 time = 8 ms
  --- FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 8/34/52 ms
```

# Ping 10.2.1.1/32 and output detailed information.

```
<HUAWEI> ping lsp -v ip 10.2.1.1 32
 LSP PING FEC: IPV4 PREFIX 10.2.1.1/32 : 100 data bytes, press CTRL_C to break
  Reply from 10.2.1.1: bytes=100 Sequence=1 time = 4 ms Return Code 3, Subcode 1
  Reply from 10.2.1.1: bytes=100 Sequence=2 time = 4 ms Return Code 3, Subcode 1
  Reply from 10.2.1.1: bytes=100 Sequence=3 time = 4 ms Return Code 3, Subcode 1
  Reply from 10.2.1.1: bytes=100 Sequence=4 time = 4 ms Return Code 3, Subcode 1
  Reply from 10.2.1.1: bytes=100 Sequence=5 time = 5 ms Return Code 3, Subcode 1
 --- FEC: IPV4 PREFIX 10.2.1.1/32 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 4/4/5 ms
```

Table 9-45 Description of the **ping lsp** command output

Item	Description
Reply from	IP address in an Echo Reply packet.
bytes	Length of an Echo Reply packet.
Sequence	Serial number of an Echo Reply packet.
time	RTT of an Echo Reply packet.

Item	Description
Return Code	Return code. The meaning of each value is as follows: ● 0: No return code is received. ● 1: Incorrect request is received. ● 2: An unknown TLV is received. ● 3: There is the outbound interface of one LSP. ● 4: No mapping between the request device and the replying device exists. ● 5: The mapping does not match that on the downstream device. ● 6: An unknown upstream interface exists. ● 7: The return code is reserved. ● 8: indicates label switching. ● 9: indicates label switching without MPLS forwarding. ● 10: indicates mapping without labels. ● 11: indicates the entity without labels. ● 12: No protocol is loaded on the interface. ● 13: The ping operation is ended ahead of schedule because of shortened labels.
Subcode	Number of labels. Usually, the value is 1.

Item	Description
xxx ping statistics	Statistics collected after the ping test. The statistics include the following information: ● packet(s) transmitted: indicates the number of sent ICMP Echo Request messages. ● packet(s) received: indicates the number of received ICMP Echo Reply messages. ● % packet loss: indicates the percentage of unresponded messages to total sent messages. ● round-trip min/avg/max: indicates the minimum, average, and maximum RTTs. The unit is ms.

9.1.115 propagate mapping

Function

The **propagate mapping for ip-prefix** command allows the system to filter out the received routes using an IP prefix list. LDP uses routes that match the addresses in the prefix list to establish an LSP.

The **undo propagate mapping** command restores the default setting.

By default, when LDP establishes an LSP, LDP does not filter out received routes.

Format

propagate mapping for ip-prefix *ip-prefix-name*

undo propagate mapping

Parameters

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list used to filter out routes.	The value is an existing IP prefix list name.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After MPLS LDP is enabled, LDP LSPs are automatically established, leading to a large number of LSPs and wasting resources. Run the **propagate mapping** command to configure a policy for establishing an LSP, allowing LDP to use routes that match the specified conditions to establish LSPs.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp (system view)** command.

Precautions

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, the device does not filter received routes.

Example

# Allow routes that match the IP prefix list named **policy1** to set up an LSP.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] propagate mapping for ip-prefix policy1
```

9.1.116 proxy-egress disable

Function

The **proxy-egress disable** command disables a device from establishing proxy egress LSPs.

The **undo proxy-egress disable** command enables a device to establish proxy egress LSPs.

By default, a device is enabled to establish proxy egress LSPs.

Format

proxy-egress disable

undo proxy-egress disable

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a policy allows a device to use all static and IGP routes to establish LSPs or use an IP address prefix list to establish LSPs, the policy also triggers proxy egress LSP establishment. However, the proxy egress LSPs may be unavailable, which wastes system resources. To prevent this problem, run the **proxy-egress disable** command to disable a device from establishing such proxy egress LSPs.

Prerequisites

MPLS has been enabled using the **mpls** command.

Precautions

During the LDP GR, the **proxy-egress disable** command cannot be run.

Example

# Disable a device from establishing proxy egress LSPs in the MPLS view.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] proxy-egress disable
```

9.1.117 remote-ip

Function

The **remote-ip** command allows you to assign an IP address to a remote LDP peer.

The **undo remote-ip** command deletes the configuration.

By default, the IP address of the remote LDP peer is not configured.

Format

remote-ip *ip-address* [**pwe3**]

undo remote-ip [**pwe3**]

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of a remote peer.	The value is in decimal notation. The IPv4 address of a local interface is not supported.
pwe3	Prohibits labels from being distributed to a specified remote peer.	-

Views

Remote MPLS LDP peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a remote LDP peer is configured, to assign an IP address to the remote LDP peer, run the **remote-ip** command in the remote MPLS LDP peer view.

The IP address must be the LSR ID of the remote LDP peer. When the LDP LSR ID and the MPLS LSR ID are different, the LDP LSR ID takes effect.

The remote peer uses the LSR ID as the transport address to create a TCP connection.

PEs on both ends of an MPLS L2VPN that runs LDP signaling can establish a remote LDP session. The MPLS L2VPN can be a Martini VLL, PWE3, or Martini VPLS network. The remote LDP session is expected to transmit Label Mapping messages carrying VC labels, not LDP labels. By default, the PE distributes LDP labels to its peer. To disable the PE from distributing LDP labels to its peer, run either of the following commands, which helps prevent LDP label wastes and minimize memory usage.

- **remote-ip** *ip-address* **pwe3** command: prevents the LSR from distributing labels to a specified remote peer.
- **remote-peer pwe3** command: prevents the LSR from distributing labels to all remote peers.

NOTE

When a backbone network is transmitting TE services in the LDP over TE scenario, do not disable a device from distributing labels to remote peers.

Prerequisites

Remote LDP peers have been configured.

Precautions

- Modifying or deleting the configured IP address of a remote peer leads to the deletion of a remote LDP session.
- After a remote peer IP address is specified using the **remote-ip** *ip-address* command, *ip-address* cannot be used as a local interface IP address. If it is used as a local interface IP address, the remote LDP session is interrupted.

Example

# Configure the address for a remote peer.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp remote-peer bji
[HUAWEI-mpls-ldp-remote-bji] remote-ip 10.3.3.3
```

# Prohibit labels from being distributed to the remote peer at 10.1.1.1/32.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp remote-peer rtc
[HUAWEI-mpls-ldp-remote-rtc] remote-ip 10.1.1.1 pwe3
```

9.1.118 remote-ip auto-dod-request

Function

The **remote-ip auto-dod-request** command configures automatic triggering of a request to a specified downstream remote LDP peer for a Label Mapping message in DoD mode.

The **undo remote-ip auto-dod-request** command restores the default setting.

By default, the configuration of the **remote-peer auto-dod-request** command is inherited.

Format

remote-ip auto-dod-request [**block**]

undo remote-ip auto-dod-request [**block**]

Parameters

Parameter	Description	Value
block	Disables the automatic triggering of a request to a downstream node for a Label Mapping message associated with a remote LDP peer of a specified LSR ID in DoD mode.	-

Views

Remote MPLS LDP peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a large-scale network, to reduce the burden on edge devices, use the DoD mode. Because edge devices cannot learn the accurate route to the remote peer, an LDP LSP cannot be set up even if LDP extensions for inter-area LSPs are configured. You can configure the DoD mode in which the local LSR requests a Label Mapping message from a specified downstream LSR or all LSRs to set up an LDP LSP.

To block this function, run the **remote-ip auto-dod-request block** command.

Precautions

Before running the **remote-ip auto-dod-request** command, ensure that the following operations has been performed:

- Configure a remote LDP session.
- Run the **longest-match** command to configure LDP extensions for inter-area LSPs.
- Run the **mpls ldp advertisement dod** command to set the DoD mode.

Example

# Enable automatic triggering of a request to a downstream specified remote LDP peer for a Label Mapping message in DoD mode.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp remote-peer lsrc
[HUAWEI-mpls-ldp-remote-lsrc] remote-ip 4.4.4.4
[HUAWEI-mpls-ldp-remote-lsrc] remote-ip auto-dod-request
```

9.1.119 remote-peer auto-dod-request

Function

The **remote-peer auto-dod-request** command configures automatically trigger requests for Label Mapping messages in DoD mode from all downstream remote LDP peers.

The **undo remote-peer auto-dod-request** command restores the default setting.

By default, the device does not automatically trigger requests for Label Mapping messages in DoD mode from all downstream remote LDP peers.

Format

remote-peer auto-dod-request

undo remote-peer auto-dod-request

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a large-scale network, to reduce the burden on edge devices, use the DoD mode. Because edge devices cannot learn the accurate route to the remote peer, an LDP LSP cannot be set up even if LDP extensions for inter-area LSPs are configured. You can configure the DoD mode in which the local LSR requests a Label Mapping message from a specified downstream LSR or all LSRs to set up an LDP LSP.

Precautions

Before running the **remote-peer auto-dod-request** command, ensure that the following operations have been performed:

- Configure a remote LDP session.
- Run the **longest-match** command to configure LDP extensions for inter-area LSPs.
- Run the **mpls ldp advertisement dod** command to set the DoD mode.

Example

# Enable automatically trigger requests for Label Mapping messages in DoD mode from all downstream remote LDP peers.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] remote-peer auto-dod-request
Warning: The operation will affect all the remote peers on which the attribute is not manually configured.
Continue?[Y/N]:y
```

9.1.120 remote-peer pwe3

Function

The **remote-peer pwe3** command prevents LSP transport labels from being distributed to all remote peers.

The **undo remote-peer pwe3** command restores the default setting.

By default, an LSR is permitted to distribute LSP transport labels to all remote peers.

Format

remote-peer pwe3

undo remote-peer pwe3

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PEs on both ends of an MPLS L2VPN that runs LDP signaling can establish a remote LDP session. The MPLS L2VPN can be a Martini VLL, PWE3, or Martini VPLS network. The remote LDP session is expected to transmit Label Mapping messages carrying VC labels, not LDP labels.

By default, the PE distributes LDP labels to its peer. To disable the PE from distributing LDP labels to its peer, run either of the following commands, which helps prevent LDP label wastes and minimize memory usage.

- The **remote-peer pwe3** command prohibits an LSR from distributing labels to all remote peers.
- The **remote-ip** *ip-address* **pwe3** command in the remote MPLS LDP peer view prohibits an LSR from distributing labels to a specified remote peer.

When you create a remote LDP session, run the **remote-peer pwe3** or **remote-ip** *ip-address* **pwe3** command to prevent LSP transport labels from being distributed to remote peers. If you do not run either of the preceding commands, the command configuration may affect system performance.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

The configuration will take effect on all remote LDP peers, including existing remote peers.

Example

# Prevent LSP transport labels from being distributed to all remote peers.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
```

```
[HUAWEI-mpls-ldp] remote-peer pwe3
Warning: The modification has impact on all remote peers including the existing ones. Continue? [Y/N]: y
```

9.1.121 reset lspv statistics

Function

The **reset lspv statistics** command clears LSPV statistics.

Format

reset lspv statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **display lspv statistics** command can be used to display LSPV statistics of an LSP ping or trace test instance. LSPV statistics of multiple test instances are accumulated, which obsesses the analysis. The **reset lspv statistics** command can be used to clear LSPV statistics.

If the **reset lspv statistics** command is run before an LSP ping or trace test instance starts, the **display lspv statistics** command displays LSPV statistics of the current test instance.

Precautions

Statistics cannot be restored after being cleared. Therefore, exercise caution before running the **reset lspv statistics** command.

Example

# Clear LSPV statistics collected on the device.

```
<HUAWEI> reset lspv statistics
```

9.1.122 reset mpls ldp

Function

The **reset mpls ldp** command resets LDP instances of the public network.

The **reset mpls ldp all** command resets all LDP instances.

Format

reset mpls ldp [**peer** *peer-id*]

reset mpls ldp all

Parameters

Parameter	Description	Value
peer *peer-id*	Specifies the LSR ID of a peer.	Expressed in dotted decimal notation.
all	Specifies all LDP instances.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When there is a new LDP configuration, to validate the configuration, you can run the **reset mpls ldp** command.

Run the **reset mpls ldp peer** command to reset sessions, and LSPs, and CR-LSPs of a specified peer.

Precautions

The **reset mpls ldp** command cannot be run during GR.

If this command is run in an attempt to restart LDP and the interval at which LDP is restarted is small, the attempt fails. The interval varies according to the number of LSPs. The more the LSPs are established, the longer the interval is. The interval can be set to 30, 60, 90, or 120, in seconds.

Example

# Reset the global LDP function.

```
<HUAWEI> reset mpls ldp
Warning: The MPLS LDP services will be reset. Continue? [Y/N]:y
```

# Reset all LDP instances.

```
<HUAWEI> reset mpls ldp all
Warning: The MPLS LDP services will be reset. Continue? [Y/N]:y
```

# Reset the peer.

```
<HUAWEI> reset mpls ldp peer 10.2.2.9
```

9.1.123 reset mpls ldp error packet

Function

The **reset mpls ldp error packet** command deletes information about LDP-related error messages.

Format

reset mpls ldp error packet { **tcp** | **udp** | **l2vpn** | **all** }

Parameters

Parameter	Description	Value
tcp	Deletes information about TCP error messages.	-
udp	Deletes information about UDP error messages.	-
l2vpn	Deletes information about L2VPN error messages.	-
all	Deletes information about all LDP-related error messages.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

By default, the system records information about LDP-related error messages. To delete the information, run the **reset mpls ldp error packet** command.

Example

# Delete information about LDP-related TCP error messages.

```
<HUAWEI> reset mpls ldp error packet tcp
```

9.1.124 reset mpls ldp event adjacency-down

Function

The **reset mpls ldp event adjacency-down** command deletes the recorded events that LDP adjacencies go Down.

Format

reset mpls ldp event adjacency-down

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

By default, the system records the events that LDP adjacencies go Down. To delete the recorded events, run the **reset mpls ldp event adjacency-down** command.

Example

# Delete the recorded events that LDP adjacencies go Down.

```
<HUAWEI> reset mpls ldp event adjacency-down
```

9.1.125 reset mpls ldp event session-down

Function

The **reset mpls ldp event session-down** command deletes the recorded events that LDP sessions go Down.

Format

reset mpls ldp event session-down

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

By default, the system records events that LDP sessions go Down. To delete the recorded events, run the **reset mpls ldp event session-down** command.

Example

# Delete the recorded events that LDP sessions go Down.

```
<HUAWEI> reset mpls ldp event session-down
```

9.1.126 route recursive-lookup tunnel

Function

The **route recursive-lookup tunnel** command enables tunnel recursion.

The **undo route recursive-lookup tunnel** command disables tunnel recursion.

By default, tunnel recursion is disabled.

Format

route recursive-lookup tunnel [**only**] [**ip-prefix** *ip-prefix-name*]

undo route recursive-lookup tunnel

Parameters

Parameter	Description	Value
only	Recurses unlabeled public routes only to LSPs.	-
ip-prefix *ip-prefix-name*	Specifies the name of an IP-prefix list.	The value is an existing IP-prefix list name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an unlabeled BGP public network route or a static route can only recurse to the outbound interface and next hop, but not a tunnel. After tunnel recursion is enabled, this route preferentially recurses to an LSP. If no LSP exists, the route can also recurse to the outbound interface and next hop.

After **ip-prefix** *ip-prefix-name* is set, only the unlabeled BGP routes or static routes that match the specified IP prefix list recurse to LSPs.

If the **ip-prefix** *ip-prefix-name* parameter is not set, all static routes and non-labeled public BGP routes will preferentially recurse to LSP tunnels.

Precautions

If the **route recursive-lookup tunnel** command is run for several times, the latest configuration overrides the previous one.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all routes match the IP prefix list.

Example

# Recurse the unlabeled public routes to the LSP tunnel.

```
<HUAWEI> system-view
[HUAWEI] route recursive-lookup tunnel
```

# Recurse unlabeled public routes only to LSPs.

```
<HUAWEI> system-view
[HUAWEI] route recursive-lookup only
```

9.1.127 snmp-agent trap suppress feature-name lsp

Function

The **snmp-agent trap suppress feature-name lsp** command configures the interval for suppressing the display of excessive LSP traps.

The **undo snmp-agent trap suppress feature-name lsp** command restores the default configuration.

By default, the interval for suppressing the display of excessive LSP traps is 300 seconds, and a maximum of three LSP traps can be sent in the suppression interval.

Format

snmp-agent trap suppress feature-name lsp trap-name { **mplsxcup** | **mplsxcdown** } **trap-interval** *trap-interval* [**max-trap-number** *max-trap-number*]

undo snmp-agent trap suppress feature-name lsp trap-name { **mplsxcup** | **mplsxcdown** } **trap-interval**

Parameters

Parameter	Description	Value
mplsxcup	Indicates the excessive traps generated when an LSP goes Up.	-
mplsxcdown	Indicates the excessive traps generated when an LSP goes Down.	-

Parameter	Description	Value
trap-interval *trap-interval*	Specifies the interval for suppressing the display of excessive LSP traps.	The value is an integer ranging from 0 to 65535, in seconds. By default, the value is 300.
max-trap-number *max-trap-number*	Sets the maximum number of traps to be sent during the suppression interval.	The value is an integer ranging from 1 to 65535. By default, the value is 3. If only *trap-interval* is specified, but *max-trap-number* is not, at most one trap can be sent during the suppression interval.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To prevent excessive traps from being displayed because of frequent LSP status changes, run the **snmp-agent trap suppress feature-name lsp** command to set the interval for suppressing the display of excessive LSP traps. During a specified suppression interval, a trap of a specified type is displayed only once. This setting reduces traps to be displayed.

For example, when the interval for suppressing the display of excessive traps when the LSP goes Down is set to 60s, only one trap indicating that the LSP goes Down is displayed every 60s. Within this interval, no other trap of the same type is displayed, but the number of the same traps generated is logged. During the next 60s, another trap indicating that an LSP goes Down can be displayed.

Example

# Set the interval for suppressing the display of excessive traps when an LSP goes Up to 80s.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap suppress feature-name lsp trap-name mplsxcup trap-interval 80
```

9.1.128 static-lsp egress

Function

The **static-lsp egress** command configures the egress node for a static LSP.

The **undo static-lsp egress** command deletes the configuration.

By default, no static LSP is configured for the egress node.

Format

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

undo static-lsp egress *lsp-name*

Parameters

Parameter	Description	Value
lsp-name	Specifies the name of an LSP.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
incoming-interface *interface-type interface-number*	Specifies the inbound interface of an LSP. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
in-label	Specifies the value of an incoming label.	The value is an integer ranging from 16 to 1023.
lsrid *ingress-lsr-id*	Specifies the ingress LSR ID.	The value is in dotted decimal notation.
tunnel-id *tunnel-id*	Specifies the ID of a tunnel.	The value is an integer ranging from 1 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run the **static-lsp egress** command on the egress node to configure a static LSP.

After configuring a static LSP, run the **display mpls static-lsp** command to verify that the static LSP is established successfully.

Precautions

To modify **incoming-interface** *interface-type interface-number* or **in-label** *in-label*, run the **static-lsp egress** command to set a new value. You do not need to run the **undo static-lsp egress** command before changing a configured value.

Example

# Configure the local LSR as the egress node of the static LSP **bj-sh**, with the inbound interface of VLANIF100 and incoming label of 233.

```
<HUAWEI> system-view
[HUAWEI] static-lsp egress bj-sh incoming-interface vlanif 100 in-label 233
```

9.1.129 static-lsp ingress

Function

The **static-lsp ingress** command configures the ingress node for a static LSP.

The **undo static-lsp ingress** command deletes the configuration.

By default, no static LSP is configured for the ingress node.

Format

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*

static-lsp ingress tunnel-interface tunnel *interface-number* **destination** *ip-address* { **nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number* } * **out-label** *out-label*

undo static-lsp ingress { *lsp-name* | **tunnel-interface tunnel** *interface-number* }

Parameters

Parameter	Description	Value
lsp-name	Specifies the name of an LSP.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
tunnel-interface tunnel *interface-number*	Specifies the index of a tunnel interface.	Numeral type. Range: varies with the configuration.
destination *ip-address*	Specifies the destination IP address.	It is in dotted decimal notation.
mask-length	Specifies the mask length of the destination IP address.	An integer ranging from 0 to 32.

Parameter	Description	Value
mask	Specifies the mask of the IP address.	It is in dotted decimal notation.
nexthop *next-hop-address*	Specifies the next-hop address.	It is in dotted decimal notation.
outgoing-interface *interface-type interface-number*	Specifies the type and number of an interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
out-label *out-label*	Specifies the value of an outgoing label.	An integer ranging from 16 to 1048575.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run the **static-lsp ingress** command on the ingress node to configure a static LSP.

NOTE

The local IP address cannot be designated as the next hop address.

After configuring a static LSP, run the **display mpls static-lsp** command to verify that the static LSP is established successfully.

Precautions

To modify the parameter **destination** *destination-address*, **nexthop** *next-hop-address*, **outgoing-interface** *interface-type interface-number*, or **out-label** *out-label*, run the **static-lsp ingress** command to set a new value. You do not need to run the **undo static-lsp ingress** command before changing a configured value.

When configuring a static LSP, ensure that the route of the static LSP exactly matches the routing information. For example:

- If you specify a next hop when configuring a static LSP, specify a next hop when configuring a static IP route. If you do not specify a next hop, the static LSP cannot be set up. For example:

```
[HUAWEI] ip route-static 10.1.0.0 16 10.1.1.2
[HUAWEI] static-lsp ingress staticlsp1 destination 10.1.0.0 16 nexthop 10.1.1.2 out-label 100
```

- If a dynamic routing protocol applies to the link between LSRs, the next-hop IP address along the LSP must be the same as the IP address of the next hop in the routing table.

If **outgoing-interface** is configured and *next-hop-address* is not configured, Ethernet forwarding failures occur.

Example

# Configure the local LSR as the ingress node of the static LSP whose destination address is 10.25.38.1, next hop IP address is 10.55.25.33, and outgoing label is 237.

```
<HUAWEI> system-view
[HUAWEI] static-lsp ingress bj-sh destination 10.25.38.1 24 nexthop 10.55.25.33 out-label 237
```

9.1.130 static-lsp transit

Function

The **static-lsp transit** command configures the transit node for the static LSP.

The **undo static-lsp transit** command deletes the configuration.

By default, the transit node for the static LSP is not configured.

Format

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*

undo static-lsp transit *lsp-name*

Parameters

Parameter	Description	Value
lsp-name	Specifies the name of an LSP.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
incoming-interface	Specifies the inbound interface.	-
interface-type interface-number	Specifies the type and number of an interface.	-
next-hop-address	Specifies the next-hop address.	The value is in dotted decimal notation.
outgoing-interface	Specifies the outbound interface.	-

Parameter	Description	Value
in-label	Specifies the value of an incoming label.	The value is an integer ranging from 16 to 1023.
out-label	Specifies the value of an outgoing label.	The value is an integer ranging from 16 to 1048575.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run the **static-lsp transit** command on the transit node to configure a static LSP.

After configuring a static LSP, run the **display mpls static-lsp** command to verify that the static LSP is established successfully.

Precautions

To modify the parameter **incoming-interface** *interface-type interface-number*, **in-label** *in-label*, **nexthop** *next-hop-address*, **outgoing-interface** *interface-type interface-number*, or **out-label** *out-label*, run the **static-lsp transit** command to set a new value. You do not need to run the **undo static-lsp transit** command before changing a configured value.

If **outgoing-interface** is configured and *next-hop-address* is not configured, Ethernet forwarding failures occur.

Example

# Configure the LSR, with the inbound interface of VLANIF100, the incoming label of 123, and the outgoing label of 253, as the transit node of a static LSP named **bj-sh**.

```
<HUAWEI> system-view
[HUAWEI] static-lsp transit bj-sh incoming-interface vlanif 100 in-label 123 nexthop 10.1.1.1 out-label
253
```

9.1.131 static-route timer ldp-sync hold-down

Function

The **static-route timer ldp-sync hold-down** command sets the time during which a static route remains inactive and waits for the establishment of an LDP session.

The **undo static-route timer ldp-sync hold-down** command restores the default setting.

By default, the time during which a static route remains inactive and waits for the establishment of an LDP session is 10 seconds.

Format

static-route timer ldp-sync hold-down { *timer* | **infinite** }

undo static-route timer ldp-sync hold-down

Parameters

Parameter	Description	Value
timer	Specifies the time during which a static route remains inactive and waits for an LDP session to be established.	The value is an integer ranging from 0 to 65535, in seconds.
infinite	Indicates that the Hold-down timer never expires. A static route becomes active only after an LDP session is established.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an MPLS network with primary and backup links, LSRs establish LSPs based on static routes. When the LDP session of the primary link becomes faulty (the fault is not caused by a link failure) or the primary link recovers, configuring synchronization between LDP and static routes minimizes traffic loss during traffic switchover and switchback. After synchronization between LDP and static routes is enabled, and the **static-route timer ldp-sync hold-down** command is run, the recovered static route becomes temporarily inactive. It waits for the establishment of an LDP session before the Hold-down timer expires, which synchronizes LDP and the static route.

If the Hold-down timer expires, the static route becomes active regardless of whether an LDP session has been established.

- If the Hold-down timer is set to 0 seconds, synchronization between LDP and static routes is disabled on an interface.
- If the Hold-down timer is set to **infinite**, the timer never expires. In this case, the static route becomes active and MPLS traffic is switched only after an LDP session is established.

Precautions

The Hold-down timer cannot be set on loopback interfaces, Layer 2 Ethernet interfaces, or null interfaces.

Example

# Set the time during which a static route remains inactive and waits for the establishment of an LDP session to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] static-route timer ldp-sync hold-down 20
```

9.1.132 timer ldp-sync hold-down

Function

The **timer ldp-sync hold-down** command sets the Hold-down time for all IS-IS interfaces within an IS-IS process so that these interfaces remain in the Hold-down state before LDP sessions are established.

The **undo timer ldp-sync hold-down** command restores the default Hold-down time.

The default Hold-down time is 10 seconds.

Format

timer ldp-sync hold-down *value*

undo timer ldp-sync hold-down

Parameters

Parameter	Description	Value
value	Specifies the period of time during which all IS-IS interfaces within an IS-IS process remain in the Hold-down state before LDP sessions are established.	The value is an integer ranging from 0 to 65535, in seconds.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an active link between two devices enabled with synchronization between LDP and IS-IS recovers from a fault, the IS-IS module enters the Hold-down state and starts a Hold-down timer. This timer allows the devices to create an LDP session and set up an IS-IS neighbor relationship at the same time. Traffic can be switched back to the active link over a reachable IS-IS route for an established LDP LSP.

To set the Hold-down time for all interfaces within an IS-IS process, run the **timer ldp-sync hold-down** command.

Precautions

If both the **timer ldp-sync hold-down** command and the **isis timer ldp-sync hold-down** command in the interface view are executed, the **isis timer ldp-sync hold-down** command takes effect.

Example

# Set the Hold-down time for all interfaces within an IS-IS process 100 to **15** seconds.

```
<HUAWEI> system-view
[HUAWEI] isis 100
[HUAWEI-isis-100] timer ldp-sync hold-down 15
```

9.1.133 timer ldp-sync hold-max-cost

Function

The **timer ldp-sync hold-max-cost** command sets the Hold-max-cost time during which all interfaces enabled with synchronization between LDP and IS-IS advertise link state PDUs (LSPs) carrying the maximum route cost.

The **undo timer ldp-sync hold-max-cost** command restores the default setting.

The default Hold-max-cost time is 10 seconds.

Format

timer ldp-sync hold-max-cost { **infinite** | *interval* }

undo timer ldp-sync hold-max-cost

Parameters

Parameter	Description	Value
infinite	Enables IS-IS to advertise LSPs carrying the maximum route cost before LDP sessions are reestablished.	-
interval	Specifies the Hold-max-cost time during which IS-IS advertises LSPs carrying the maximum route cost on a local device.	The value is an integer ranging from 0 to 65535, in seconds.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After synchronization between LDP and IS-IS is enabled, if the LDP session over the active link fails but the IS-IS route for the active link is reachable, IS-IS advertises the LSPs carrying the maximum route cost so that the IS-IS route and LDP session over a standby link can become reachable at the same time.

To set the Hold-max-cost time, run the **timer ldp-sync hold-max-cost** command.

Select parameters based on networking requirements:

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

Precautions

- If the **timer ldp-sync hold-max-cost infinite** command is executed and the LDP session is Down, interfaces enabled with LDP and IS-IS synchronization keep advertising LSPs carrying the maximum route cost, which affects IS-IS routing.
- If both the **timer ldp-sync hold-max-cost** command and the **isis timer ldp-sync hold-max-cost** command in the interface view are executed, the **isis timer ldp-sync hold-max-cost** command takes effect.

Example

# Configure IS-IS to keep advertising the maximum cost by sending Link State PDUs until the LSP is established.

```
<HUAWEI> system-view
[HUAWEI] isis 100
[HUAWEI-isis-100] timer ldp-sync hold-max-cost infinite
```

9.1.134 tracert lsp

Function

The **tracert lsp** command detects the gateways along the LSP from the source to the destination.

Format

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

tracert lsp [**-a** *source-ip* | **-exp** *exp-value* | **-h** *ttl-value* | **-r** *reply-mode* | **-t** *time-out*] * **te tunnel** *interface-number* [**hot-standby** | **primary**] [**draft6**]

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

Parameters

Parameter	Description	Value
-a *source-ip*	Specifies the source IP address of Echo Request packets to be sent. If no source IP address is specified, the IP address of the outbound interface through which Echo Request packets are sent is used as a source IP address. **NOTE** If an E2E BGP LSP has been established between two devices and the LSR ID is not used on the ingress, to run the **tracert lsp** command with **bgp** specified on the ingress, you must specify **-a** *source-ip* as the IP address used for establishing the E2E BGP LSP.	-
-exp *exp-value*	Specifies the EXP value of Echo Request packets to be sent. The EXP value represents the priority of Echo Request packets. **NOTE** If DSCP priority has been configured by running the **set priority** command, the *exp-value* parameter does not take effect.	An integer that ranges from 0 to 7. The default value is 0.
-h *ttl-value*	Specifies the TTL value of MPLS Echo Request packets to be sent. The TTL field indicates the lifetime of the MPLS Echo Request packet and specifies the maximum number of hops that the packet can pass through. The TTL value is set on the source and reduced by 1 each time the packet passes through a hop. When the TTL value is reduced to 0, the packet is discarded. At the same time, an ICMP Timeout message is sent to notify the source host.	An integer that ranges from 1 to 255. The default value is 30.

Parameter	Description	Value
-r *reply-mode*	Specifies the mode in which the peer returns MPLS Echo Reply packets.	An integer that ranges from 1 to 4. The default value is 2. The meaning of each value is as follows: ● 1: No MPLS Echo Reply packet is returned. ● 2: The MPLS Echo Reply packet is encapsulated into IPv4/IPv6 UDP packets. ● 3: MPLS Echo Reply packets are encapsulated into IPv4/IPv6 UDP packets carrying the Router Alert option. ● 4: MPLS Echo Reply packets are responded using the control channels on the application plane. If the value of *reply-mode* is 1, the initiator starts a unidirectional test. If the test succeeds, the initiator prompts that the test times out; if the test fails, the initiator prompts that the LSP does not exist.
-t *time-out*	Specifies the period of time for waiting for an MPLS Echo Reply packet.	An integer that ranges from 0 to 65535, in milliseconds. The default value is 2000.
-v	Displays the MPLS label carried in the ICMP Time Exceeded packet. This parameter is used when LSP transport labels need to be displayed after tracert is initiated on the PE.	-
ip *destination-address mask-length*	Specifies the destination IPv4 address and the mask length.	The destination IPv4 address is in dotted decimal notation. The mask length is an integer that ranges from 0 to 32.

Parameter	Description	Value
ip-address	Specifies the destination IP address carried in the IP header of an MPLS Echo Request packet.	The value is in dotted decimal notation. By default, the destination IP address carried in the IP header of an MPLS Echo Request packet is 127.0.0.1.
nexthop *nexthop-address*	Specifies the next-hop address.	The value is in dotted decimal notation.
draft6	Specifies the version of the **tracert lsp** command. If this parameter is specified, the tracert operation is performed according to "draft-ietf-mpls-lsp-ping-06". By default, the tracert operation is performed according to RFC 4379.	-
te tunnel *interface-number*	Specifies the number of the TE tunnel interface.	-
hot-standby	Indicates that the hot-standby CR-LSP is to be monitored.	-
primary	Indicates that the primary CR-LSP is to be monitored.	-
bgp *destination-address mask-length*	Specifies the destination IP address and mask length of BGP.	*destination-address* is in dotted decimal notation. *mask-length* is an integer that ranges from 0 to 32.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

When a fault occurs on the LSPs of an MPLS network, you can run the **ping lsp** command to check the LSP connectivity based on the reply packet, and then run the **tracert lsp** command to locate the fault.

The **tracert lsp** command uses MPLS Echo Request messages and MPLS Echo Reply messages to monitor the connectivity of the LSP. Both MPLS Echo Request and MPLS Echo Reply messages are encapsulated into UDP packets and transmitted through port 3503. The receiver distinguishes MPLS Echo Request and MPLS Echo Reply messages based on the port number. An MPLS Echo Request message carries FEC information to be monitored, and is sent along the same LSP as other packets with the same FEC. In this manner, the connectivity of the LSP is checked. Echo Request messages are transmitted to the destination using MPLS, whereas MPLS Echo Reply messages are transmitted to the source using IP.

The LSP tracert can be used to monitor the following types of links:

- LDP LSP Tracert: Run the **tracert lsp ip** *destination-address mask-length* command on the ingress node to trace the egress node to detect the fault on the LSP.
- TE Tunnel Tracert: You can run the **tracert lsp te tunnel** *interface-number* command on the ingress node to trace the egress node to check the connectivity of a tunnel.
  - To check the connectivity of a hot-standby tunnel, run the **tracert lsp te tunnel** *interface-number* **hot-standby** command.
  - To check the connectivity of a primary tunnel, run the **tracert lsp te tunnel** *interface-number* **primary** command.

Prerequisites

- The UDP module of each node is working properly; otherwise, the tracert operation fails.
- The MPLS module of each node is enabled and is working properly.
- The ICMP module of each node is working properly; otherwise, three asterisks (* * *) are displayed.

Procedure

The execution process of the **tracert lsp** command is as follows:

- The source sends an MPLS Echo Request packet with the TTL being 1. After the TTL times out, the first hop sends an MPLS Echo Reply packet to the source.
- The source sends an MPLS Echo Request packet with the TTL being 2. After the TTL times out, the second hop sends an MPLS Echo Reply packet to the source.
- The source sends an MPLS Echo Request packet with the TTL being 3. After the TTL times out, the third hop sends an MPLS Echo Reply packet to the source.
- The preceding process proceeds until the MPLS Echo Request packet reaches the destination.

When the device on the destination hop receives the MPLS Echo Request packet, it returns an MPLS Echo Reply packet, indicating the end of the tracert. The purpose behind this is to record the source of each ICMP Timeout packet to provide a trace of the path the packet took to reach the destination.

Precautions

When you run the **tracert lsp te tunnel** *interface-number* command to detect a tunnel, if a transit node is not enabled with LDP, a packet is returned, indicating that the destination is unreachable.

To prevent the egress node from forwarding the received MPLS Echo Request packet to other nodes, you can set the destination address in the IP header of the Echo Request packet to a loopback address with the prefix being 127.0.0.1/8.

Example

# Tracert the LSP to 10.4.4.9/32.

```
<HUAWEI> tracert lsp ip 10.4.4.9 32
  LSP Trace Route FEC: IPV4 PREFIX 10.4.4.9/32 , press CTRL_C to break.
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   10.1.2.2/[1028 ]
  1     10.1.2.2           94 ms   Transit   10.4.4.9/[3 ]
  2     10.4.4.9           94 ms   Egress
```

# Tracert the LSP to 10.3.3.9/32 with the MTU value.

```
<HUAWEI> tracert lsp -v ip 10.3.3.9 32
  LSP Trace Route FEC: IPV4 PREFIX 10.3.3.9/32 , press CTRL_C to break.
  TTL   Replier            Time    Type      Downstream/Label/MTU
  0                                Ingress   172.16.1.1/[3 ]/1500
  1     10.3.3.9           20 ms   Egress
```

# Tracert a TE tunnel.

```
<HUAWEI> tracert lsp te tunnel 1
  LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel1 , press CTRL_C to break.
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   10.1.2.2/[13312 ]
  1     10.1.2.2           63 ms   Transit   10.4.4.9/[3 ]
  2     10.6.6.6           93 ms   Egress
```

Table 9-46 Description of the tracert lsp command output

Item	Description
TTL	Indicates the TTL value in an Echo Request packet. It represents the number of hops of the tunnel an Echo Request packet passes.
Replier	IP address of a switching node that returns an MPLS Echo Reply packet.
Time	RTT, in milliseconds.
Type	Type of a node. Available node types: ● Ingress node ● Transit node ● Egress node
Downstream	Address of a downstream device.
Label	Label of a downstream device.
MTU	Link Maximum Transmission Unit.

9.1.135 ttl expiration pop

Function

The **ttl expiration pop** command enables a device to use the local IP route to forward ICMP response packets after the MPLS TTL expires.

The **undo ttl expiration pop** command disables this function. Therefore, ICMP response packets are sent along LSPs.

By default, the LSR returns an ICMP packet using the local IP route if the received MPLS TTL-expired packet contains one label.

Format

ttl expiration pop

undo ttl expiration pop

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an MPLS network, when an LSR receives MPLS packets with the TTL value of 1, the LSR generates an ICMP TTL-expired message.

The LSR returns the TTL-expired message to the sender in the following ways:

- If the LSR has a reachable route to the sender, it directly sends the TTL-expired message to the sender through the IP route.
- If the LSR has no reachable route to the sender, it forwards the TTL-expired message along the LSP. The egress node forwards the TTL-expired message to the sender.

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

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

Precautions

The **undo mpls (system view)** command deletes all configurations of the **ttl expiration pop** command.

Example

# Forward ICMP packets through an LSP after the MPLS TTL expires.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] undo ttl expiration pop
```

9.1.136 ttl propagate

Function

The **ttl propagate** command sets the TTL propagate mode of MPLS packets to uniform.

The **undo ttl propagate** command sets the TTL propagate mode of MPLS packets to pipe.

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

Format

ttl propagate

undo ttl propagate

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MPLS TTL processing modes include uniform and pipe:

- Uniform

  When IP packets reach the ingress node of an MPLS network, the IP TTL decreases by one and is mapped to the MPLS TTL field. In this manner, packets are processed in the standard mode used on the MPLS network. On the egress node, the MPLS TTL decreases by one and is mapped to the IP TTL field. The traceroute output shows the path that the packets pass by.

- Pipe

  On an MPLS network, the IP TTL does not decrease by one at each hop. The traceroute output hides all the hops on the MPLS backbone network, as if the ingress node is directly connected to the egress node.

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

Precautions

The **ttl propagate** command only take effect on LSPs that are to be set up. Before using the function on LSPs that have been set up, run the **reset mpls ldp** command to reestablish the LSPs.

Example

# Set the TTL propagate mode of MPLS packets to uniform.

```
<HUAWEI> system-view
[HUAWEI] ttl propagate
```

9.1.137 ttl propagate public

Function

The **ttl propagate public** command enables IP TTL propagation for MPLS packets of the public network.

The **undo ttl propagate public** command disables IP TTL propagation for MPLS packets of the public network.

By default, IP TTL propagation for MPLS packets of the public network is enabled.

Format

ttl propagate public

undo ttl propagate public

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

The **ttl propagate public** and **undo ttl propagate public** commands only take effect on LSPs that are to be set up. Before using the function on LSPs that have been set up, run the **reset mpls ldp** command to reestablish the LSPs.

Example

# Enable the IP TTL propagation for MPLS packets of the public network.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] ttl propagate public
```

9.1.138 ttl propagate vpn

Function

The **ttl propagate vpn** command enables IP TTL propagation for MPLS packets of the VPN.

The **undo ttl propagate vpn** command disables IP TTL propagation for MPLS packets of the VPN.

By default, IP TTL propagation is disabled for VPN packets.

Format

ttl propagate vpn

undo ttl propagate vpn

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

The **ttl propagate vpn** and **undo ttl propagate vpn** commands only take effect on LSPs that are to be set up. Before using the function on LSPs that have been set up, run the **reset mpls ldp** command to reestablish the LSPs.

Configure the IP TTL propagation consistently on all PEs. If you enable the IP TTL propagation only on some PEs, the traceroute output cannot reflect the real network situation.

Example

# Enable the IP TTL propagation for MPLS packets of the VPN.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] ttl propagate vpn
```

9.1.139 undo outbound peer all

Function

The **undo outbound peer all** command deletes all outbound policies.

Format

undo outbound peer all

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before MPLS LDP is used, the **outbound peer split-horizon** command needs to be executed to configure an outbound policy to control LDP LSP establishments. If multiple outbound policies have been configured, run the **undo outbound peer all** command to simultaneously delete all the outbound policies.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

Running the **undo outbound peer all** command deletes all outbound policies. Therefore, exercise caution when running this command.

Example

# Delete all outbound policies.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] undo outbound peer all
```

9.1.140 undo inbound peer all

Function

The **undo inbound peer all** command deletes all inbound policies.

Format

undo inbound peer all

Parameters

None.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To delete all inbound policies in batches, run the **undo inbound peer all** command.

Before MPLS LDP is used, the **inbound peer fec** command needs to be executed to configure an inbound policy to control LDP LSP establishments. If multiple inbound policies have been configured, run the **undo inbound peer all** command to simultaneously delete all the inbound policies.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

Running the **undo inbound peer all** command deletes all inbound policies. Therefore, exercise caution when running this command.

Example

# Delete all inbound policies.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] undo inbound peer all
```

9.2 MPLS QoS Configuration Commands

9.2.1 Command Support

Only the following switch models support MPLS QoS:

S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H

9.2.2 diffserv-mode

Function

The **diffserv-mode** command configures a DiffServ mode for MPLS L2VPN or MPLS L3VPN labels to implement end-to-end QoS.

The **undo diffserv-mode** command restores the default DiffServ mode of an MPLS network.

By default, the uniform mode is used for MPLS L2VPN or MPLS L3VPN labels.

Format

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

undo diffserv-mode

Parameters

Parameter	Description	Value
pipe	Indicates that the DiffServ mode of an MPLS network is pipe.	-
short-pipe	Indicates that the DiffServ mode of an MPLS network is short pipe.	-
uniform	Indicates that the DiffServ mode of an MPLS network is uniform.	-
mpls-exp *mpls-exp*	Specifies the EXP priority in the private label. This parameter is valid only when the DiffServ mode on the ingress PE is set to pipe or short pipe. It is invalid on the egress PE. If a DiffServ domain is configured, the inner label specified by *mpls-exp* is preferred for the mapping. When the *mpls-exp* parameter is set to a large value, the packets have high priority and packet forwarding quality is high.	The value is an integer that ranges from 0 to 7. The default value is 0.

Parameter	Description	Value
domain *ds-name*	Indicates the name of the DiffServ domain. The default DiffServ domain name is **default**. This parameter is specified in the **diffserv domain** command.	The value is an existing DiffServ domain name.

Views

Interface view, VSI view, VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide QoS guarantee for VPN traffic on an MPLS VPN network, set the DiffServ mode based on actual needs.

- If you want to differentiate priorities of different services in a VPN, set the DiffServ mode to uniform. You can also set the DiffServ mode to pipe or short pipe, but you need to specify the DiffServ domain in which the mode applies.
- If you want to differentiate priorities of services in different VPNs but not priorities of services in a VPN, set the DiffServ mode to pipe or short pipe and specify EXP values in private labels.

If you do not want to change priorities carried in original packets, you are advised to set the DiffServ mode to pipe or short pipe. In uniform and pipe modes, the egress node determines the per-hop behavior (PHB) based on EXP priorities of packets. In short pipe mode, the egress node determines the PHB based on DSCP or 802.1p priorities of packets.

Precautions

Before configuring the MPLS Diff-Serv mode for IPv4 services, ensure that an IPv4 address family is configured in the VPN instance view using the **ipv4-family** command.

Before configuring the MPLS Diff-Serv mode for IPv6 services, ensure that an IPv6 address family is configured in the VPN instance view using the **ipv6-family** command.

On the ingress, all the three modes can be set. On the egress, only the short pipe mode can be set.

- If you specify the DiffServ domain in the **diffserv-mode** command, ensure that the specified DiffServ domain is already created using the **diffserv domain** command in the system view.
- Before running this command, use the **undo portswitch** command to set the working mode of the Ethernet interfaces to Layer 3 mode.

- The **diffserv-mode** command takes effect only for the new LSPs. To make the command take effect for the existing LSPs, run the **reset mpls ldp** command to reestablish LSPs.

Example

# On VLANIF100, set the MPLS DiffServ mode to pipe and the value of *mpls-exp* to 3.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] diffserv-mode pipe mpls-exp 3
```

# On GE0/0/1, set the MPLS DiffServ mode to pipe and the value of *mpls-exp* to 3.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] diffserv-mode pipe mpls-exp 3
```

9.2.3 mpls-exp-inbound

Function

The **mpls-exp-inbound** command maps EXP priorities of MPLS packets to PHBs and colors in a DiffServ domain on an inbound interface.

The **undo mpls-exp-inbound** command restores the default mapping.

The following table shows the default mappings from EXP priorities to PHBs and colors of MPLS packets in a DiffServ domain on an inbound interface.

Table 9-47 Default mappings from EXP priorities to PHBs and colors of MPLS packets in a DiffServ domain on an inbound interface

EXP Priority	PHB	Color
0	BE	green
1	AF1	green
2	AF2	green
3	AF3	green
4	AF4	green
5	EF	green
6	CS6	green
7	CS7	green

Format

mpls-exp-inbound *exp-value* **phb** *service-class* [*color*]

undo mpls-exp-inbound [*exp-value*]

Parameters

Parameter	Description	Value
exp-value	Specifies the EXP priority of an MPLS packet.	The value is an integer ranging from 0 to 7. A larger value indicates a higher EXP priority of MPLS packets.
service-class	Specifies a PHB.	The value can be BE, AF1 to AF4, EF, CS6, or CS7.
color	Specifies the color of a packet.	The value can be green, yellow, or red.

Views

DiffServ domain view

Default Level

2: Configuration level

Usage Guidelines

To implement QoS scheduling on the MPLS packets that come from the upstream device, run the **mpls-exp-inbound** command to map EXP priorities of MPLS packets to PHBs and colors. After a DiffServ domain is bound to the inbound interface of packets, the QoS mechanism performs congestion management and congestion avoidance according to PHBs and colors of the packets.

Example

# In the DiffServ domain **ds1**, map EXP priority 2 of MPLS packets to PHB AF1 and color incoming MPLS packets as yellow.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain ds1
[HUAWEI-dsdomain-ds1] mpls-exp-inbound 2 phb af1 yellow
```

9.2.4 mpls-exp-outbound

Function

The **mpls-exp-outbound** command maps PHBs and colors of MPLS packets to EXP priorities in a DiffServ domain on an outbound interface.

The **undo mpls-exp-outbound** command restores the default mapping.

The following table shows the default mappings from PHBs and colors to EXP priorities of MPLS packets in a DiffServ domain on an outbound interface.

Table 9-48 Default mappings from PHBs and colors to EXP priorities of MPLS packets in a DiffServ domain on an outbound interface

PHB	Color	EXP Priority
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	1
AF1	yellow	1
AF1	red	1
AF2	green	2
AF2	yellow	2
AF2	red	2
AF3	green	3
AF3	yellow	3
AF3	red	3
AF4	green	4
AF4	yellow	4
AF4	red	4
EF	green	5
EF	yellow	5
EF	red	5
CS6	green	6
CS6	yellow	6
CS6	red	6
CS7	green	7
CS7	yellow	7
CS7	red	7

Format

mpls-exp-outbound *service-class color* **map** *exp-value*

undo mpls-exp-outbound [*service-class color*]

Parameters

Parameter	Description	Value
service-class	Specifies a PHB.	The value can be BE, AF1 to AF4, EF, CS6, or CS7.
color	Specifies the color of a packet.	The value can be green, yellow, or red.
exp-value	Specifies the EXP priority of an MPLS packet.	The value is an integer ranging from 0 to 7. A larger value indicates a higher EXP priority of the MPLS packet.

Views

DiffServ domain view

Default Level

2: Configuration level

Usage Guidelines

After QoS scheduling is performed on the MPLS packets, run the **mpls-exp-outbound** command to map the PHB and color of the MPLS packets in a DiffServ domain to the EXP priority. After the DiffServ domain is bound to the outbound interface of MPLS packets, the downstream device implements QoS scheduling according to EXP priority.

The switch can map PHBs and colors in MPLS packets to EXP priorities and 802.1p priorities on an outbound interface.

Example

# In the DiffServ domain **ds1**, map the PHB AF1 of outgoing MPLS packets marked yellow to EXP priority 2.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain ds1
[HUAWEI-dsdomain-ds1] mpls-exp-outbound af1 yellow map 2
```

9.2.5 mpls-qos egress

Function

The **mpls-qos egress** command maps the mapping from the EXP priority of the public tunnel to the PHB/color on the egress node.

The **undo mpls-qos egress** command restores the default settings.

By default, mapping of the EXP priority of the public tunnel is performed according to the settings in the default domain.

Format

mpls-qos egress trust upstream { *ds-name* | **default** }

undo mpls-qos egress trust upstream

mpls-qos egress trust upstream none

undo mpls-qos egress trust upstream none

Parameters

Parameter	Description	Value
trust upstream	Trusts the specified DiffServ domain.	-
ds-name	Specifies the name of a DiffServ domain.	The value is an existing DiffServ domain name.
default	Specifies the DiffServ domain as a default domain.	-
none	Indicates that the system does not perform EXP priority mapping in the public network tunnel, and sets the EXP field to 0 in the public network tunnel.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement certain QoS functions on an MPLS network, the device 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.

Prerequisites

The specified DiffServ domain has been created using the **diffserv domain** command in the system view.

Precautions

Run the **mpls-qos egress** command before setting up the public tunnel; otherwise, you must reestablish the MPLS LDP session to make the command take effect.

If you modify the settings of the global DiffServ domain or change the DiffServ mode of the interface, VSI, or VPN instance, you must reestablish the MPLS LDP session; otherwise, the modification cannot take effect.

Example

# Map the mapping from the EXP priority of the public tunnel to the PHB/color on the egress node.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain ds1
[HUAWEI-dsdomain-ds1] quit
[HUAWEI] mpls-qos egress trust upstream ds1
```

9.2.6 mpls-qos ingress

Function

The **mpls-qos ingress** command maps the PHB/color of packets to the EXP priority of the public tunnel on the ingress node.

The **undo mpls-qos ingress** command restores the default settings.

By default, mapping of the EXP priority of the public tunnel is performed according to the settings in the default domain.

Format

mpls-qos ingress { **use vpn-label-exp** | **trust upstream** { *ds-name* | **default** } }

undo mpls-qos ingress { **use vpn-label-exp** | **trust upstream** }

mpls-qos ingress trust upstream none

undo mpls-qos ingress trust upstream none

Parameters

Parameter	Description	Value
use vpn-label-exp	Indicates the EXP value in the inner label of a packet.	-
trust upstream	Trusts the specified DiffServ domain.	-
ds-name	Specifies the name of a DiffServ domain.	The value is an existing DiffServ domain name.

Parameter	Description	Value
default	Specifies the DiffServ domain as a default domain.	-
none	Indicates that the system does not perform EXP priority mapping in the public network tunnel, and sets the EXP field to 0 in the public network tunnel.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement certain QoS functions on an MPLS network, the device 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. You can specify **use vpn-label-exp**.

Prerequisites

The specified DiffServ domain has been created using the **diffserv domain** command in the system view.

Precautions

Run the **mpls-qos ingress** command before setting up the public tunnel; otherwise, you must reestablish the MPLS LDP session to make the command take effect.

Example

# Map the PHB/color of packets to the EXP priority of the public tunnel on the ingress node.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain ds1
[HUAWEI-dsdomain-ds1] quit
[HUAWEI] mpls-qos ingress trust upstream ds1
```

System Response

None

9.2.7 mpls-qos transit

Function

The **mpls-qos transit** command performs the priority mapping based on the EXP priority of the public tunnel on the transit node.

The **undo mpls-qos transit** command restores the default settings.

By default, mapping of the EXP priority of the public tunnel is performed according to the settings in the default domain.

Format

mpls-qos transit trust upstream { *ds-name* | **default** }

undo mpls-qos transit trust upstream

mpls-qos transit trust upstream none

undo mpls-qos transit trust upstream none

Parameters

Parameter	Description	Value
trust upstream	Trusts the specified DiffServ domain.	-
ds-name	Specifies the name of a DiffServ domain.	The value is an existing DiffServ domain name.
default	Specifies the DiffServ domain as a default domain.	-
none	Indicates that the system does not perform EXP priority mapping in the public network tunnel, and sets the EXP field to 0 in the public network tunnel.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement certain QoS functions on an MPLS network, the device 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.

Prerequisites

The specified DiffServ domain has been created using the **diffserv domain** command in the system view.

Precautions

Run before setting up the public tunnel; otherwise, you must reestablish the MPLS LDP session to make the command take effect.

If you modify the settings of the global DiffServ domain or change the DiffServ mode of the interface, VSI, or VPN instance, you must reestablish the MPLS LDP session; otherwise, the modification cannot take effect.

Example

# Perform the priority mapping based on the EXP priority of the public tunnel on the transit node.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain ds1
[HUAWEI-dsdomain-ds1] quit
[HUAWEI] mpls-qos transit trust upstream ds1
```

9.3 MPLS TE Configuration Commands

9.3.1 Command Support

Only the following switch models support MPLS TE:

S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H

9.3.2 add hop

Function

The **add hop** command adds a specified node on an MPLS TE explicit path.

Format

add hop *ip-address1* [**include** [[**loose** | **strict**] | [**incoming** | **outgoing**]] * | **exclude**] { **after** | **before** } *ip-address2*

Parameters

Parameter	Description	Value
ip-address1	Specifies the IP address of the added node.	The value is in dotted decimal notation.

Parameter	Description	Value
include [[**loose** | **strict**] | [**incoming** | **outgoing**]] *	Specifies the node with an IP address *ip-address1* on the explicit path. ● **strict**: indicates that the node is added in **strict** mode. The node of *ip-address1* is directly connected to the node of *ip-address2*. ● **loose**: indicates that the node is added in **loose** mode. The node of *ip-address1* may not be directly connected to the node of *ip-address2*. ● **incoming**: indicates that the *ip-address1* is the IP address of an inbound interface of a new-added node. ● **outgoing**: indicates that the *ip-address1* is the IP address of an outbound interface of a new-added node.	By default, an explicit path is added in **include strict** mode.
exclude	Excludes the node of *ip-address1* from the explicit path.	-
after	Indicates that the node of *ip-address1* is added after the node of *ip-address2*.	-
before	Indicates that the node of *ip-address1* is added before the node of *ip-address2*.	-
ip-address2	Specifies the IP address of an interface or the Router ID of a node on the explicit path.	The value is in dotted decimal notation.

Views

Explicit path view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following commands are used to adjust nodes on a created explicit path:

- The **add hop** command is used to add a node to the explicit path.
- The **modify hop** command is used to delete a node from the explicit path and replace the node with a specified node.
- The **delete hop** command is used to delete a node from the explicit path.

Prerequisites

The **next hop** command must have been run to specify a next-hop IP address before the **add hop** command is run.

Follow-up Procedure

Run the **display explicit-path** command to view information about the explicit path.

Precautions

A node can be added to an explicit path using the **add hop** command only when the following conditions are met:

- *ip-address2* is the IP address of a node that exists on the explicit path.
- If an explicit path over which a TE tunnel has been established is modified, the make-before-break mechanism is triggered, and a CR-LSP is reestablished without traffic loss.

Example

# Exclude the next hop of 10.2.2.2 after 10.1.1.1 from the explicit path named **p1**.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] quit
[HUAWEI] explicit-path p1
[HUAWEI-explicit-path-p1] next hop 10.1.1.1
[HUAWEI-explicit-path-p1] add hop 10.2.2.2 exclude after 10.1.1.1
```

9.3.3 affinity property

Function

The **affinity property** command configures the affinity property for a CR-LSP attribute template.

The **undo affinity property** command deletes the affinity property from a CR-LSP attribute template.

By default, no affinity property for a CR-LSP attribute template is configured.

Format

affinity property *affinity-value* [**mask** *mask-value*]

undo affinity property

Parameters

Parameter	Description	Value
affinity-value	Specifies the value of the affinity property.	The value ranges from 0x0 to 0xFFFFFFFF, in hexadecimal format. By default, the affinity value is 0.

Parameter	Description	Value
mask *mask-value*	Specifies the mask value of an affinity property. Then an operation is performed between the mask value and the affinity property value, and the result indicates the bits of the affinity property to be checked.	The value ranges from 0x0 to 0xFFFFFFFF, in hexadecimal format. By default, the value is 0.

Views

LSP attribute view

Default Level

2: Configuration level

Usage Guidelines

Affinity property and masks determine the link properties that should be checked by a device.

Example

# Set the affinity property to 123 and the mask to fff in the CR-LSP attribute template.

```
<HUAWEI> system-view
[HUAWEI] lsp-attribute lsp-attribute-name
[HUAWEI-lsp-attribute-lsp-attribute-name] affinity property 123 mask fff
```

9.3.4 bandwidth (LSP attribute view)

Function

The **bandwidth** command configures the bandwidth in the CR-LSP attribute template.

The **undo bandwidth** command deletes the bandwidth in the CR-LSP attribute template.

By default, no bandwidth in the CR-LSP attribute template is configured.

Format

bandwidth { **ct0** *ct0-bandwidth* | **ct1** *ct1-bandwidth* }

undo bandwidth { **all** | **ct0** | **ct1** }

Parameters

Parameter	Description	Value
ct0 *ct0-bandwidth*	Specifies the bandwidth of an LSP of CT0.	The value is an integer that ranges from 1 to 4000000000, in kbit/s. By default, the bandwidth is 0 kbit/s.
ct1 *ct1-bandwidth*	Specifies the bandwidth of an LSP of CT1.	The value is an integer that ranges from 1 to 4000000000, in kbit/s. By default, the bandwidth is 0 kbit/s.
all	Deletes the bandwidth configured for the LSP of each CT.	-

Views

LSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The **undo bandwidth** command can be used to delete the bandwidth of all CTs or a specified CT:

- **undo bandwidth all**: deletes all configured bandwidth.
- **undo bandwidth** { **ct0** | **ct1** }: deletes the bandwidth of the specified CT configured on the current TE tunnel.

Example

# Configure the bandwidth of an LSP of CT0 as 20 kbit/s in the CR-LSP attribute template.

```
<HUAWEI> system-view
[HUAWEI] lsp-attribute lsp-attribute-name
[HUAWEI-lsp-attribute-lsp-attribute-name] bandwidth ct0 20
```

9.3.5 bfd bind mpls-te

Function

The **bfd bind mpls-te** command configures BFD to monitor TE tunnels, or the primary or backup LSP bound to a TE tunnel.

The **undo bfd** command deletes a specified BFD session.

By default, no TE tunnel applies BFD.

Format

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

undo bfd *cfg-name*

Parameters

Parameter	Description	Value
cfg-name	Specifies the BFD configuration name.	The value is a string of 1 to 15 case-insensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface tunnel *interface-number*	Specifies the interface number of the TE tunnel bound to a BFD session.	-
te-lsp [**backup**]	Indicates that BFD monitors the LSP bound to the TE tunnel. ● If **backup** is not selected, BFD monitors the primary LSP bound to the TE tunnel. ● If **backup** is selected, BFD monitors the backup LSP bound to the TE tunnel.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **bfd bind mpls-te** command to configure BFD to monitor TE tunnels, or the primary or backup LSP bound to a TE tunnel.

Prerequisites

Before configuring BFD to monitor TE tunnels, the following tasks must have been completed:

- BFD has been enabled globally using the **bfd** command.
- An MPLS TE tunnel interface has been configured.

Precautions

BFD can monitor a TE tunnel and the primary or backup LSP bound to the TE tunnel.

- If BFD is configured to monitor the primary or backup LSP bound to a TE tunnel, a BFD session cannot be created if the LSP status is Down.
- If the tunnel status is Down when BFD is configured to monitor a TE tunnel, the BFD session can still be created, but its status is Down.

  Multiple LSPs can be bound to a TE tunnel. When BFD detects the tunnel, the BFD session will go Down only if all LSPs bound to the TE tunnel fail.

Example

# Configure BFD to detect the primary LSP bound to the TE tunnel.

```
<HUAWEI> system-view
[HUAWEI] bfd 1to4rsvp bind mpls-te interface Tunnel 1 te-lsp
[HUAWEI-bfd-lsp-session-1to4rsvp]
```

# Configure BFD to detect the backup LSP bound to the TE tunnel.

```
<HUAWEI> system-view
[HUAWEI] bfd 1to4backup bind mpls-te interface Tunnel 1 te-lsp backup
[HUAWEI-bfd-lsp-session-1to4backup]
```

9.3.6 bypass-attributes

Function

The **bypass-attributes** command configures bypass CR-LSP attributes in a CR-LSP attribute template.

The **undo bypass-attributes** command deletes bypass CR-LSP attributes from a CR-LSP attribute template.

By default, no bypass CR-LSP attributes are configured.

Format

bypass-attributes { **bandwidth** *bandwidth* | **priority** *setup_priority_value* [*hold_priority_value*] }*

undo bypass-attributes

Parameters

Parameter	Description	Value
bandwidth *bandwidth*	Specifies the bandwidth value assigned to a bypass CR-LSP. **NOTE** The function of bandwidth value assigned to a bypass CR-LSP does not take effect on the devices.	An integer ranging from 1 to 4000000000, in kbit/s. By default, the bandwidth is 0 kbit/s.
priority *setup_priority_value*	Specifies the setup priority of a bypass CR-LSP.	An integer ranging from 0 to 7. The smaller the value, the higher the priority. By default, the setup priority is 7.
hold_priority_value	Specifies the holding priority of the bypass CR-LSP.	An integer ranging from 0 to 7. The smaller the value, the higher the priority. By default, the holding priority is 7.

Views

LSP attribute view

Default Level

2: Configuration level

Usage Guidelines

To configure the **bypass-attributes** command in the CR-LSP attribute template, note the following preconditions:

- The **fast-reroute bandwidth** command must be configured in the CR-LSP attribute template, and the bandwidth of the bypass CR-LSP must be less than or equal to that of the primary CR-LSP.
- The bandwidth of the bypass CR-LSP must be less than or equal to that of the CR-LSP attribute template.
- The values of the setup and holding priority of the CR-LSP attribute template must be less than or equal to those of the bypass CR-LSP.

Example

# Configure the bypass CR-LSP attributes in the CR-LSP attribute template.

```
<HUAWEI> system-view
[HUAWEI] lsp-attribute lsp-attribute-name
[HUAWEI-lsp-attribute-lsp-attribute-name] fast-reroute bandwidth
[HUAWEI-lsp-attribute-lsp-attribute-name] bypass-attributes bandwidth 30 priority 5 5
```

9.3.7 commit (LSP attribute view)

Function

The **commit** command commits the configurations of the CR-LSP attribute template.

Format

commit

Parameters

None

Views

LSP attribute view

Default Level

2: Configuration level

Usage Guidelines

When the CR-LSP attribute template is modified, if the commands that conflict with the CR-LSP attribute template are configured on a tunnel interface, the configurations of the CR-LSP attribute template cannot be committed.

When the CR-LSP attribute template is applied by a tunnel, you can modify the tunnel attributes by modifying the configurations of the CR-LSP attribute template. Different modifications in the CR-LSP attribute template have different impacts on the setup of the tunnel. If the priorities of the CR-LSP attribute template are modified, Break-Before-Make (BBM) is performed on the tunnel. If the Make-Before-Break (MBB) attribute of the CR-LSP attribute template is modified, MBB may be performed on the tunnel.

Example

# Configure the CR-LSP attribute template and commit relevant configurations.

```
<HUAWEI> system-view
[HUAWEI] lsp-attribute lsp-attribute-name
[HUAWEI-lsp-attribute-lsp-attribute-name] hop-limit 15
[HUAWEI-lsp-attribute-lsp-attribute-name] commit
```

9.3.8 delete hop

Function

The **delete hop** command deletes a specified node from an MPLS TE explicit path.

Format

delete hop *ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of an interface on a node.	In dotted decimal notation.

Views

Explicit path view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following commands are used to adjust nodes on a created explicit path:

- The **add hop** command is used to add a node to the explicit path.
- The **modify hop** command is used to delete a node from the explicit path and replace the node with a specified node.
- The **delete hop** command is used to delete a node from the explicit path.

Follow-up Procedure

Run the **display explicit-path** command to view information about the explicit path.

Precautions

A node can be deleted from an explicit path using the **delete hop** command only when the following conditions are met:

- The node must exist on the explicit path
- If an explicit path over which a TE tunnel has been established is modified, the make-before-break mechanism is triggered, and a CR-LSP is reestablished without traffic loss.

Example

# Delete the node of 10.10.10.10 from the MPLS TE explicit path.

```
<HUAWEI> system-view
[HUAWEI] explicit-path p1
[HUAWEI-explicit-path-p1] list hop
 Path Name : p1         Path Status : Enabled
 1      2.2.2.2           Strict      Include
 2      10.10.10.10       Strict      Include
 3      10.20.20.20       Strict      Include
[HUAWEI-explicit-path-p1] delete hop 10.10.10.10
```

```
[HUAWEI-explicit-path-p1] list hop
 Path Name : p1         Path Status : Enabled
 1       2.2.2.2            Strict       Include
 2       10.20.20.20        Strict       Include
```

9.3.9 display default-parameter mpls rsvp-te

Function

The **display default-parameter mpls rsvp-te** command displays the default parameters of MPLS RSVP-TE.

Format

display default-parameter mpls rsvp-te

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the default configurations of MPLS RSVP-TE, run the **display default-parameter mpls rsvp-te** command.

Example

# Display default MPLS RSVP-TE parameters.

```
<HUAWEI> display default-parameter mpls rsvp-te
  RSVP-TE View Default Configurations:
  -------------------------------------------
  Resv Confirmation Request  : Disabled
  RSVP Hello Extension       : Disabled
  GR Capability              : Disabled
  GR Basic-Restart-Time      : 90000 ms
  Hello Interval             : 3000 ms
  Max Times Of Hello Misses  : 3
  Path/Resv Message Refresh Interval    : 30000 ms
  Path/Resv Message Refresh Retry Times : 3
  Challenge Retransmission Interval     : 1000 ms
  Max Times Of Challenge Lost           : 3
  Soft Preemption Timeout               : 30 s

  Interface View Default Configurations:
  -------------------------------------------
  SRefresh Feature           : Disabled
  Authentication Feature     : Disabled
  BFD Feature                : Disabled
  Hello Feature              : Disabled
  BFD Min-Tx                 : 1000
  BFD Min-Rx                 : 1000
  BFD Detect-Multi           : 3
  MPLS MTU                   : 1500
  SRefresh Interval          : 30000 ms
  SRefresh Retransmission Interval        : 5000 ms
  SRefresh Retransmission Increment Value : 1
  Authentication Life Time                : 1800000 ms
```

Table 9-49 Description of the display default-parameter mpls rsvp-te command output

Item	Description
Resv Confirmation Request	Whether the request for reservation confirmation is enabled.
RSVP Hello Extension	Whether the Hello extension is enabled.
GR Capability	RSVP GR capability.
GR Basic-Restart-Time	Basic RSVP GR time.
Hello Interval	Interval of Hello message.
Max Times Of Hello Misses	Maximum number of Hello messages that consecutively fail to be received.
Path/Resv Message Refresh Interval	Interval for refreshing Path or Resv messages.
Path/Resv Message Refresh Retry Times	Interval for retrying refreshing Path or Resv messages.
Challenge Retransmission Interval	Interval for resending Challenge messages.
Max Times Of Challenge Lost	Maximum number of Challenge messages that consecutively fail to be received.
Soft Preemption Timeout	The timeout of soft preemption
SRefresh Feature	Whether Srefresh is enabled.
Authentication Feature	Whether authentication is enabled.
BFD Feature	Whether BFD is enabled.
Hello Feature	Whether the Hello feature is enabled.
BFD Min-Tx	Actual interval for sending BFD packets.
BFD Min-Rx	Actual interval for receiving BFD packets.
BFD Detect-Multi	Actual local BFD detection multiplier.
MPLS MTU	Actual MTU value used for MPLS forwarding.
SRefresh Interval	Srefresh interval.
SRefresh Retransmission Interval	Srefresh retransmission interval.

Item	Description
SRefresh Retransmission Increment Value	Increment value of Srefresh retransmission.
Authentication Life Time	Authentication lifetime.

9.3.10 display default-parameter mpls te cspf

Function

The **display default-parameter mpls te cspf** command displays the default CSPF configurations.

Format

display default-parameter mpls te cspf

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the default configurations of CSPF, run the **display default-parameter mpls te cspf** command.

Example

# Display the default CSPF configurations.

```
<HUAWEI> display default-parameter mpls te cspf
-----------------------------------------------
        CSPF Default Configuration
-----------------------------------------------
        Preferred-IGP : OSPF
        Failed-link Interval(Sec): 10
```

Table 9-50 Description of the display default-parameter mpls te cspf command output

Item	Description
Preferred-IGP	The IGP type whose database is in CSPF TEDB and that will be preferred for path calculation.
Failed-link Interval(Sec)	The default value of the failed link timer.

9.3.11 display default-parameter mpls te management

Function

The **display default-parameter mpls te management** command displays the default configurations of the MPLS TE management module.

Format

display default-parameter mpls te management

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the default configurations of the MPLS TE management module, run the **display default-parameter mpls te management** command.

Example

# Display the default configurations of the MPLS TE management module.

```
<HUAWEI> display default-parameter mpls te management

  Global Information
  ----------------------------------------------------------
  DS-TE MODE                        : NON-IETF
  Bandwidth constraint model             : RDM
  Switch-delay time(ms)               : 5000
  Delete-delay time(ms)               : 7000
  Auto-bandwidth timer(sec)              : 300
  FRR timer(sec)                    : 300
  Path metric-type                   : TE
  Tie-breaking                     : Random
```

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

Interface Information
------------------------------------------------------------
Administrative group value               : 0
TE metric value                          : 0
Bandwidth change thresholds up           : 10
Bandwidth change thresholds down         : 10
------------------------------------------------------------

Tunnel Interface Information
------------------------------------------------------------
Retry timer(sec)                         : 30
Set priority                             : 7
Hold priority                            : 7
Default signal protocol                  : Rsvp
Default resv-style                       : SE
Default classtype                        : CT0
Reoptimization frequency(sec)            : 3600
Auto-bandwidth adjustment frequency(sec) : 86400
Auto-bandwidth max-bw                    : 4294901760
Auto-bandwidth min-bw                    : 0
Auto-bandwidth threshold                 : 0
Hop-limit                                : 32
Diffserv-mode                            : Uniform
------------------------------------------------------------

Explicit-path Information
------------------------------------------------------------
Default type                             : include strict
------------------------------------------------------------

Default TEClass Mapping
------------------------------------------------------------
TE-Class     ID      Class Type      Priority
TE-Class     0       0               0
TE-Class     1       1               0
TE-Class     2       2               0
TE-Class     3       3               0
TE-Class     4       0               7
TE-Class     5       1               7
TE-Class     6       2               7
TE-Class     7       3               7
------------------------------------------------------------
```

Table 9-51 Description of the display default-parameter mpls te management command output

Item	Description
DS-TE MODE	DS-TE mode: ● IETF: indicates DS-TE in IETF mode. ● NON-IETF: indicates DS-TE in non-IETF mode.
Bandwidth constraint model	Bandwidth Constraints model: ● RDM: indicates the Russian Dolls Model. ● MAM: indicates the Maximum Allocation Model. ● Extended MAM: indicates the extended Maximum Allocation Model.

Item	Description
Switch-delay time(ms)	Delay time before switching TE traffic from the primary CR-LSP to the modified CR-LSP in milliseconds.
Delete-delay time(ms)	Delay before deleting the primary CR-LSP after TE traffic is switched to the modified CR-LSP, in milliseconds.
Auto-bandwidth timer(sec)	Time interval at which the output rate of each tunnel configured with automatic bandwidth adjustment is sampled, in seconds.
FRR timer(sec)	FRR switching time, in seconds.
Path metric-type	Link metric type for path selection for tunnels.
Tie-breaking	Rule for selecting a route to the destination if multiple routes of equal cost are available.
Administrative group value	Administrative-group attribute.
TE metric value	TE metric of a link.
Bandwidth change thresholds up	Upper threshold of the bandwidth of an MPLS TE tunnel to be flooded.
Bandwidth change thresholds down	Lower threshold of the bandwidth of an MPLS TE tunnel to be flooded.
Retry timer(sec)	Time interval between attempts to establish a tunnel, in seconds.
Set priority	Setup priority.
Hold priority	Holding priority.
Default signal protocol	Signaling protocol used to set up an LSP.
Default resv-style	Resource reservation style.
Default classtype	Class type.
Reoptimization frequency(sec)	Time interval between attempts of re-optimization, in seconds.
Auto-bandwidth adjustment frequency(sec)	Time interval between attempts of automatic bandwidth adjustment, in seconds.
Auto-bandwidth max-bw	Maximum bandwidth allowed by automatic bandwidth adjustment.
Auto-bandwidth min-bw	Minimum bandwidth allowed by automatic bandwidth adjustment.
Auto-bandwidth threshold	Indicates the threshold of the difference between the new and existing bandwidth. The value is expressed in percentage.

Item	Description
Hop-limit	Maximum number of hops.
Diffserv-mode	DiffServ mode.
Default type	Default type.
TE-Class ID	TE-class ID. The value is an integer that ranges from 0 to 7.
Class Type	Service type. When the TE-class is not configured, "--" is displayed.
Priority	Preemption priority of a tunnel. The value is an integer that ranges from 0 to 7. The smaller the value, the higher tunnel preemption priority.

9.3.12 display explicit-path

Function

The **display explicit-path** command displays information about an explicit path and the tunnels using it.

Format

display explicit-path [[**name**] *path-name*] [**tunnel-interface** | **lsp-attribute** | **verbose**]

Parameters

Parameter	Description	Value
name	Displays information about the specified explicit path.	-
path-name	Specifies the explicit path name.	The value is an existing explicit path name.
tunnel-interface	Displays information about the interface of the tunnel that uses the explicit path.	-
lsp-attribute	Displays information about the LSP attribute template that uses the explicit path.	-
verbose	Displays detailed information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no path name is specified, information about all explicit paths is displayed.

Example

# Display detailed information about the explicit path named p1.

```
<HUAWEI> display explicit-path p1 verbose
Path Name : p1          Path Status : Enabled
 1      1.1.1.1           Strict      Include
 2      2.2.2.2           Strict      Exclude
 3      3.3.3.3           Loose        Include            Outgoing
 4      4.4.4.4           Strict      Include            Incoming
 List of p2p tunnels using this path:
     Tunnel1
 Number of p2p tunnels using this path: 1
 List of lsp-attributes referring this path:
     a1
 Number of lsp-attributes referring this path: 1
```

Table 9-52 Description of the display explicit-path verbose command output

Item	Description
Path Name	Name of an explicit path.
Path Status	Status of an explicit path. ● Enabled ● Disabled
Strict	The address is a strict next hop. The address is the ingress address or the address of the node that is connected directly to the previous node.
Loose	The address is a loose next hop.
Include	The explicit path contains the node of this IP address.
Exclude	The explicit path does not contain the node of this IP address.

Item	Description
Incoming or Outgoing	Type of an interface to which the IP address belongs: ● Incoming ● Outgoing If this field is not displayed, the IP address belongs to either an outbound interface or an inbound interface.
List of p2p tunnels using this path	List of tunnels using the path.
Number of p2p tunnels using this path	Number of tunnels using the path.
List of lsp-attributes referring this path	List of CR-LSP attribute templates using the path.
Number of lsp-attributes referring this path	Number of CR-LSP attribute templates using the path.

9.3.13 display lsp-attribute

Function

The **display lsp-attribute** command displays the configurations of the CR-LSP attribute template and the tunnels using it.

Format

display lsp-attribute [**name** *lsp-attribute-name*] [**tunnel-interface** | **verbose**]

Parameters

Parameter	Description	Value
name *lsp-attribute-name*	Specifies the name of the CR-LSP attribute template.	The value is an existing CR-LSP attribute template name.
tunnel-interface	Displays information about the interface of the tunnel that uses the explicit path.	-
verbose	Displays detailed information about the CR-LSP attribute template, including information about the tunnels using it.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the name of the CR-LSP attribute template is not specified, information about all CR-LSP attribute templates is displayed in the command output.

Example

# Display information about the tunnel-interface using the attribute templates of lspattr1.

```
<HUAWEI> display lsp-attribute name lspattr1 tunnel-interface
lsp-attribute Name : lspattr1
explicit-path 2
commit
List of tunnels using this lsp-attribute:
    Tunnel1                         Tunnel2
Number of tunnels using this lsp-attribute: 2
```

# Display detailed information about all CR-LSP attribute templates.

```
<HUAWEI> display lsp-attribute verbose

lsp-attribute Name : lsp-attribute-name11
bandwidth ct0 100
explicit-path path-name
affinity property 2 mask 2
priority 4
hop-limit 20
record-route label
fast-reroute bandwidth
bypass-attributes bandwidth 10 priority 4
commit
List of tunnels using this lsp-attribute:
    Tunnel1                       Tunnel2
Number of tunnels using this lsp-attribute: 2
```

Table 9-53 Description of the display lsp-attribute verbose command output

Item	Description
lsp-attribute Name	Name of a CR-LSP attribute template. To set the name of a CR-LSP attribute template, run the **lsp-attribute** command.
bandwidth ct0 100	Bandwidth of the LSP of each CT configured in the CR-LSP attribute template. To set the bandwidth of the LSP of each CT configured in the CR-LSP attribute template, run the **bandwidth** command.

Item	Description
explicit-path path-name	Explicit path in the CR-LSP attribute template. To set the explicit path in the CR-LSP attribute template, run the **explicit-path** command.
affinity property 2 mask 2	Affinity property and affinity mask in a CR-LSP attribute template. To set the affinity property and affinity mask in a CR-LSP attribute template, run the **affinity property** command.
priority 4	Setup and holding priorities in a CR-LSP attribute template. To set the setup and holding priorities in a CR-LSP attribute template, run the **priority** command.
hop-limit 20	Hop limit in a CR-LSP attribute template. To set the hop limit in a CR-LSP attribute template, run the **hop-limit** command.
record-route label	Route and label storing function that is enabled in the CR-LSP attribute template. To set the route and label storing function, run the **record-route** command.
fast-reroute bandwidth	FRR enabled and bandwidth protection configured in a CR-LSP attribute template. To set the FRR and bandwidth protection in a CR-LSP attribute template, run the **fast-reroute** command.
bypass-attributes bandwidth 10 priority 4	Bypass tunnel attributes in a CR-LSP attribute template. To set the bypass tunnel attributes in a CR-LSP attribute template, run the **bypass-attributes** command.
commit	Committing configurations of a CR-LSP attribute template. To set the committing configurations of a CR-LSP attribute template, run the **commit** command.

Item	Description
List of tunnels using this lsp-attribute	List of tunnels that use a CR-LSP attribute template.
Number of tunnels using this lsp-attribute	Number of tunnels that use a CR-LSP attribute template.

9.3.14 display mpls aps statistics global

Function

The **display mpls aps statistics global** command displays statistics about MPLS TE tunnel protection group.

Format

display mpls aps statistics global

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After MPLS TE tunnel protection groups are configured, this command can be used to view statistics about these MPLS TE tunnel protection groups.

Example

# Display statistics about MPLS TE tunnel protection groups.

```
<HUAWEI> display mpls aps statistics global
  Max APS Instance Num                  :  10240
  Created APS Instance Num               :  2
```

Table 9-54 Description of the **display mpls aps statistics global** command output

Item	Description
Max APS Instance Num	Maximum number of supported APS instances

Item	Description
Created APS Instance Num	Number of created MPLS TE tunnel protection groups

9.3.15 display mpls lsp attribute

Function

The **display mpls lsp attribute** command displays information about the local bypass LSP attributes.

Format

display mpls lsp attribute { **bypass-inuse** { **exists-not-used** | **inuse** | **not-exists** } | **bypass-tunnel** *tunnel-name* }

Parameters

Parameter	Description	Value
bypass-inuse	Displays the attribute of the bypass LSPs in use.	-
exists-not-used	Displays the attributes of the existing bypass LSPs that are not in use.	-
inuse	Displays the attribute of the bypass LSPs in use.	-
not-exists	Displays the attributes of the bypass LSPs that are not in use.	-
bypass-tunnel	Displays the attribute of the specified bypass tunnel.	-
tunnel-name	Specifies the name of the bypass tunnel.	The value is an existing tunnel name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mpls lsp attribute** command to view information about attributes of local bypass LSPs in the TE FRR scenarios.

Example

# Display information about attributes of the existing bypass LSPs that are not in use.

```
<HUAWEI> display mpls lsp attribute bypass-inuse exists-not-used
-------------------------------------------------------------------------------
              LSP Information: RSVP LSP
-------------------------------------------------------------------------------

 No                  :  1
 SessionID           :  300
 IngressLsrID        :  3.3.3.9
 LocalLspID          :  5
 Tunnel-Interface    :  Tunnel1
 Fec                 :  1.1.1.9/32
 TunnelTableIndex    :  0x1
 Nexthop             :  -------
 In-Label            :  3
 Out-Label           :  NULL
 In-Interface        :  Vlanif100
 Out-Interface       :  ----------
 LspIndex            :  2049
 Token               :  0x0
 LsrType             :  Egress
 Mpls-Mtu            :  ------
 TimeStamp           :  333sec
 Bfd-State           :  ---
 CBfd-Event          :  ---
 Bed-State           :  ---
 Bed-LastNotifyValue :  ---
 Bed-LastNotifyLspId :  ---
```

Table 9-55 Description of the display mpls lsp attribute command output

Item	Description
No	Sequence number of an LSP.
SessionID	Session ID of a CR-LSP.
IngressLsrID	Ingress LSR ID of a CR-LSP.
LocalLspID	Local LSP ID of a CR-LSP.
Tunnel-Interface	Tunnel interface.
Fec	Forwarding Equivalence Class, which is destination address of an LSP.
TunnelTableIndex	Index of a tunnel table.
Nexthop	IP address of the next hop of an LSP.
In-Label	Value of an incoming label.
Out-Label	Value of an outgoing label.
In-Interface	Name of an incoming interface.
Out-Interface	Name of an outgoing interface.

Item	Description
LspIndex	Index number of an LSP, which uniquely identifies an LSP that is established using a specified protocol.
Token	LSP token, which guides the packet forwarding.
LsrType	Role of an LSR on an LSP: ● Ingress ● Transit ● Egress
Mpls-Mtu	Maximum transmission unit (MTU) of an interface of an LSP.
TimeStamp	Time elapsed since an LSP was set up.
Bfd-State	BFD status.
CBfd-Event	BFD-reported error code event received on the ingress of an RSVP LSP.
Bed-State	Error code status received on the ingress of an RSVP LSP.
Bed-LastNotifyValue	Event of association relationship related to error codes informed on the egress of an RSVP LSP.
Bed-LastNotifyLspId	ID of a reverse LSP when an event of association relationship related to error codes is informed on the egress of an RSVP LSP.

9.3.16 display mpls rsvp-te

Function

The **display mpls rsvp-te** command displays the RSVP-TE configurations.

Format

display mpls rsvp-te

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When configuring a dynamic MPLS TE tunnel, you can run the **display mpls rsvp-te** command to view RSVP-TE configurations.

Example

# Display information about RSVP-TE.

```
<HUAWEI> display mpls rsvp-te
 LSR ID: 1.1.1.9
 RSVP-TE Function Capability: Enable
 Resv Confirmation Request: DISABLE
 RSVP Hello Extension: ENABLE
 Hello interval: 3 sec         Max Hello misses: 3
 Path and Resv message refresh interval: 30 sec
 Path and Resv message refresh retries count: 3
 Blockade Multiplier: 4
 Graceful-Restart Capability: GR-Support GR-Self
 Restart Time:  90000 Millisecond
 Recovery Time: 0 Millisecond
 Bfd Enabled: DISABLE                 Bfd Min-Tx: 1000
 Bfd Min-Rx: 1000                     Bfd Detect-Multi: 3
 Soft Preemption Timeout: 30 sec
```

Table 9-56 Description of the display mpls rsvp-te command output

Item	Description
LSR ID	LSR ID in the format X.X.X.X.
RSVP-TE Function Capability	Whether RSVP-TE is enabled. To enable the RSVP-TE function, run the **mpls rsvp-te** command.
Resv Confirmation Request	Whether reservation confirmation is requested. To enable the reservation confirmation mechanism, run the **mpls rsvp-te resvconfirm** command.
RSVP Hello Extension	Whether the RSVP Hello extension is enabled. To enable the RSVP Hello extension, run the **mpls rsvp-te hello** command.
Hello interval	The interval at which Hello messages are sent, in seconds. To specify the interval, run the **mpls rsvp-te timer hello** command.
Max Hello misses	Maximum number of times for the consecutively lost Hello messages. To specify the maximum number, run the **mpls rsvp-te hello-lost** command.
Path and Resv message refresh interval	Time interval at which the Path and Resv messages are refreshed, in seconds. To specify the interval, run the **mpls rsvp-te timer refresh** command.

Item	Description
Path and Resv message refresh retries count	Number of retry times allowed for refreshing the Path and Resv messages. To specify the number, run the **mpls rsvp-te keep-multiplier** command.
Blockade Multiplier	Multiplier for keeping the blocked state.
Graceful-Restart Capability	RSVP GR capability of a device: ● GR-Support GR-Self: indicates that the RSVP GR on the local node is enabled and the RSVP GR of the neighbor is supported. ● GR-Self: indicates that the RSVP GR is enabled only on the local node. ● GR-Support: indicates that the RSVP GR of the neighbor is supported. ● DISABLE: indicates that the RSVP GR is disabled. To enable the RSVP GR capability, run the **mpls rsvp-te hello support-peer-gr** command or**mpls rsvp-te hello full-gr** command.
Restart Time	Start time of the GR process, in milliseconds. It is displayed only after the command **mpls rsvp-te hello basic-restart-time** is run.
Recovery Time	Time spent on recovering all LSPs, in milliseconds. It is displayed only after the command **mpls rsvp-te hello basic-restart-time** is run.
Bfd Enabled	Whether the BFD for RSVP is enabled globally in the MPLS view: ● ENABLE: indicates that BFD for RSVP is globally enabled in the MPLS view. ● DISABLE: indicates that BFD for RSVP is globally disabled in the MPLS view. To enable the BFD for RSVP function, run the **mpls rsvp-te bfd all-interfaces enable** command.
Bfd Min-Tx	Local interval at which BFD packets are sent, in milliseconds. To specify the interval, run the **mpls rsvp-te bfd all-interfaces** command.

Item	Description
Bfd Min-Rx	Local interval at which BFD packets are received, in milliseconds. To specify the interval, run the **mpls rsvp-te bfd all-interfaces** command.
Bfd Detect-Multi	Local BFD detection multiplier. To specify the multiplier, run the **mpls rsvp-te bfd all-interfaces** command.
Soft Preemption Timeout	Timeout period of soft preemption.

9.3.17 display mpls rsvp-te bfd session

Function

The **display mpls rsvp-te bfd session** command displays information about the BFD session for RSVP.

Format

display mpls rsvp-te bfd session { **all** | **interface** *interface-type interface-number* | **peer** *ip-address* } [**verbose**]

Parameters

Parameter	Description	Value
all	Displays information about all the BFD sessions for RSVP.	-
interface *interface-type interface-number*	Displays information about the BFD session for RSVP on the specified interface.	-
peer *ip-address*	Displays information about the BFD session for RSVP of the specified peer.	The value is in dotted decimal notation.
verbose	Displays detailed information about a BFD session for RSVP.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the information about the BFD session for RSVP, run the **display mpls rsvp-te bfd session** command.

Example

# Display information about a BFD session for RSVP.

```
<HUAWEI> display mpls rsvp-te bfd session all
Total Nbrs/Rsvp triggered sessions : 1/1
--------------------------------------------------------------------
Local     Remote    Local        Peer         Interface     Session
Discr     Discr     Addr         Addr         Name          State
--------------------------------------------------------------------
8192      8192      10.1.1.1     10.1.1.2     VLANIF100     UP
```

# Display detailed information about a BFD session for RSVP.

```
<HUAWEI> display mpls rsvp-te bfd session all verbose
Total Nbrs/Rsvp triggered sessions : 1/1
--------------------------------------------------------------------
  Local Discriminator      :  8192
  Remote Discriminator     :  8192
  Local Address            :  10.1.1.1
  Peer Address             :  10.1.1.2
  Interface Name           :  VLANIF100
  ActTx                    :  1000
  ActRx                    :  1000
  ActMulti                 :  3
  Session State            :  UP
```

Table 9-57 Description of the display mpls rsvp-te bfd session command output

Item	Description
Total Nbrs/Rsvp triggered sessions	Number of BFD neighbors or RSVP-triggered sessions in the system or interface view.
Local Discr/Local Discriminator	Local discriminator of a BFD session. The value 0 indicates an invalid discriminator. To specify a local discriminator of a BFD session, run the **discriminator** command.
Remote Discr/ Remote Discriminator	Remote discriminator of a BFD session. The value 0 indicates an invalid discriminator. To specify a remote discriminator of a BFD session, run the **discriminator** command.
Local Addr/Local Address	IP address of the local node in a BFD session.
Peer Addr/Peer Address	IP address of the peer in a BFD session.
Interface Name	Outgoing interface of a BFD session.

Item	Description
ActTx/ActRx/ActMulti	Parameters of a BFD session: To specify parameters of a BFD session, run the **mpls rsvp-te bfd all-interfaces** command. ● ActTx: indicates the actual interval at which BFD packets are sent, in milliseconds. ● ActRx: indicates the actual interval at which BFD packets are received, in milliseconds. ● ActMulti: indicates the actual local detection multiplier. The default value is 3.
Session State	Status of a BFD session: ● UP: indicates that the BFD session is Up. ● DOWN: indicates that the BFD session is Down. ● NONE: indicates that no BFD session is created. ● ADMIN DOWN: indicates that the administrator manually closes the BFD session. ● INITIAL: indicates the BFD session is in the Initial state.

9.3.18 display mpls rsvp-te established

Function

The **display mpls rsvp-te established** command displays information about RSVP resource reservation based on an interface, and about the RSVP-TE LSPs that pass through the interface.

Format

display mpls rsvp-te established [**interface** *interface-type interface-number peer-ip-address*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Parameter	Description	Value
peer-ip-address	Specifies the IP address of an interface on the RSVP peer connected to the local device.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If an interface is specified, information about the establishment of the RSVP-TE LSP on this interface is displayed.

Example

# Display information about the establishment of the RSVP-TE LSPs of all interfaces.

```
<HUAWEI> display mpls rsvp-te established
Interface: Outgoing-Interface at the Egress
 Token Bucket Rate: 0.00          Peak Data Rate: 0.00
 Tunnel Addr: 10.1.1.9            Ingress LSR ID: 10.3.3.9
 Local LSP ID: 4                  Session Tunnel ID: 301
 Next Hop Addr:  -----
 Upstream Label: 3

 Token Bucket Rate: 0.00          Peak Data Rate: 0.00
 Tunnel Addr: 10.1.1.9            Ingress LSR ID: 10.3.3.9
 Local LSP ID: 4                  Session Tunnel ID: 300
 Next Hop Addr:  -----
 Upstream Label: 3

 Token Bucket Rate: 0.00          Peak Data Rate: 0.00
 Tunnel Addr: 10.3.3.9            Ingress LSR ID: 10.1.1.9
 Local LSP ID: 3                  Session Tunnel ID: 300
 Next Hop Addr: 172.16.1.2
 Upstream Label: NULL             Downstream Label: 1040

 Token Bucket Rate: 0.00          Peak Data Rate: 0.00
 Tunnel Addr: 10.3.3.9            Ingress LSR ID: 10.1.1.9
 Local LSP ID: 2                  Session Tunnel ID: 301
 Next Hop Addr: 172.16.1.2
 Upstream Label: NULL             Downstream Label: 1038
```

Table 9-58 Description of the display mpls rsvp-te established command output

Item	Description
Interface: Outgoing-Interface at the Egress	Information about RSVP resource reservation based on the outgoing interface on the egress node and about the RSVP LSPs that pass through the interface.
Token Bucket Rate	Token bucket rate, in byte/s.
Peak Data Rate	Peak data rate, in byte/s.
Tunnel Addr	Tunnel address in the format X.X.X.X.
Ingress LSR ID	LSR ID on the ingress in the format X.X.X.X.
Local LSP ID	Local LSP ID.
Session Tunnel ID	Tunnel ID.
Next Hop Addr	Next-hop address in the format X.X.X.X.
Upstream Label	Value of an incoming label.
Downstream Label	Value of an outgoing label.

9.3.19 display mpls rsvp-te graceful-restart

Function

The **display mpls rsvp-te graceful-restart** command displays the status of RSVP GR.

Format

display mpls rsvp-te graceful-restart

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After completing the RSVP GR configuration, you can run the **display mpls rsvp-te graceful-restart** command to view the RSVP-TE GR status.

Example

# Display the status of RSVP-TE GR.

```
<HUAWEI> display mpls rsvp-te graceful-restart
Display Mpls Rsvp te graceful restart information
 LSR ID: 1.1.1.9
 Graceful-Restart Capability:   GR-Self GR-Support
 Restart Time:  90000 Milli Second
 Recovery Time: 0 Milli Second
 GR Status:  Gracefully Restart Not going on
 Number of Restarting neighbors: 0
 Number of LSPs recovered: 0
 Received Gr Path message count: 0
 Send Gr Path message count: 0
 Received RecoveryPath message count: 0
 Send RecoveryPath message count: 0
```

Table 9-59 Description of the display mpls rsvp-te graceful-restart command output

Item	Description
LSR ID	LSR ID.
Graceful-Restart Capability	RSVP GR capability of a device.
Restart Time	Restart time for a device, in milliseconds. To set the restart time, run the **mpls rsvp-te hello basic-restart-time** command.
Recovery Time	Time spent on recovering all LSPs, in milliseconds. To set the recovery time, run the **mpls rsvp-te hello basic-restart-time** command.
GR Status	RSVP GR status of the local device: ● Gracefully Restart Not going on: indicates that the protocol is not entering the GR process. ● Gracefully Restart on going restarting: indicates that the protocol has entered the GR process. ● Gracefully Restart on going recovery: indicates that the configurations are being restored.
Number of Restarting neighbors	Number of supporting nodes.
Number of LSPs recovered	Number of recovered LSPs.
Received Gr Path message count	Number of Path messages received by restarting nodes.

Item	Description
Send Gr Path message count	Number of Path messages sent by supporting nodes.
Received RecoveryPath message count	Number of Recovery Path messages received by restarting nodes.
Send RecoveryPath message count	Number of Recovery Path messages sent by supporting nodes.

9.3.20 display mpls rsvp-te graceful-restart peer

Function

The **display mpls rsvp-te graceful-restart peer** command displays the status of RSVP GR on a neighbor.

Format

display mpls rsvp-te graceful-restart peer [{ **interface** *interface-type interface-number* | **node-id** } [*ip-address*]]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the RSVP GR status of a neighbor on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
node-id	Displays the RSVP GR status of a manually-configured neighbor.	-
ip-address	Specifies the IP addresses of a neighbor.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the RSVP-TE GR status of a specified RSVP neighbor, run the **display mpls rsvp-te graceful-restart peer** command.

Example

# Display the RSVP-TE GR status of the neighbor.

```
<HUAWEI> display mpls rsvp-te graceful-restart peer
 Neighbor on Interface Vlanif100
 Neighbor Addr: 172.16.1.2            Last Attribute: Added Usually
 SrcInstance: 0x7C832B3D              NbrSrcInstance: 0x6A48E0F5
 Neighbor Capability:
                  Can Do Self GR
                  Can Support GR
 GR Status:          Normal
 Restart Time:  90000 Millisecond
 Recovery Time: 0 Millisecond
 Stored GR message number: 0
 PSB Count: 0                         RSB Count: 1
 Total to be Recover PSB Count: 0     Recovered PSB Count: 0
 Total to be Recover RSB Count: 0     Recovered RSB Count: 0
 P2MP PSB Count: 0                    P2MP RSB Count: 0
 Total to be Recover P2MP PSB Count: 0     Recovered P2MP PSB Count: 0
 Total to be Recover P2MP RSB Count: 0     Recovered P2MP RSB Count: 0
```

Table 9-60 Description of the display mpls rsvp-te graceful-restart peer command output

Item	Description
Neighbor Addr	IP address of a neighbor.
Last Attribute	Neighbor attribute: ● Added Usually: indicates the neighbor is discovered based on an interface. ● Added by Node-Id: indicates the neighbor is discovered based on the configured node ID. ● To be deleted: indicates the neighbor that is to be deleted because of the Hello timeout. ● Add by Frr: indicates an FRR neighbor.
SrcInstance	Source instance.
NbrSrcInstance	Source instance of a neighbor.

Item	Description
Neighbor Capability	GR capability of a neighbor: ● Can Do Self GR: indicates that the neighbor can perform GR. ● Can Support GR: indicates that the neighbor has the capability of supporting GR. ● Can Transmit Recovery Path Messages: indicates that the neighbor can send Recovery Path messages. ● No Gr capabilities: indicates that the neighbor does not have the capability of supporting GR.
GR Status	GR status of a neighbor: ● Normal: indicates that the neighbor does not perform GR. ● Supporting: indicates that the neighbor is supporting the local node of performing GR. ● Restarting: indicates that the neighbor is supporting the local node of the restart.
Restart Time	Restart time of a neighbor, in milliseconds.
Recovery Time	Recovery time of a neighbor, in milliseconds.
Stored GR message number	Number of GR messages stored on the supporting node.
PSB Count	Number of PSBs.
RSB Count	Number of RSBs.
Total to be Recover PSB Count	Total number of the PSBs to be recovered.
Recovered PSB Count	Number of the recovered PSBs.
Total to be Recover RSB Count	Total number of the RSBs to be recovered.
Recovered RSB Count	Number of recovered RSBs.
P2MP PSB Count	Number of P2MP PSBs
P2MP RSB Count	Number of P2MP RSBs
Total to be Recover P2MP PSB Count	Number of P2MP PSBs to be restored after the GR process is complete
Recovered P2MP PSB Count	Number of P2MP PSBs that have been restored after the GR process is complete
Total to be Recover P2MP RSB Count	Number of P2MP RSBs to be restored after the GR process is complete

Item	Description
Recovered P2MP RSB Count	Number of P2MP RSBs that have been restored after the GR process is complete

9.3.21 display mpls rsvp-te interface

Function

The **display mpls rsvp-te interface** command displays the RSVP-TE configurations on an interface.

Format

display mpls rsvp-te interface [*interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the type and number of an interface is not specified, the **display mpls rsvp-te interface** command displays the RSVP-TE information of all RSVP TE-enabled interfaces.

Example

# Display information about RSVP-TE of a specified interface.

```
<HUAWEI> display mpls rsvp-te interface vlanif 100
Interface: Vlanif100
 Interface Address: 11.11.11.11
 Interface state: UP             Interface Index: 0x4
 Total-BW: 0                    Used-BW: 0
 Hello configured: NO              Num of Neighbors: 0
 SRefresh feature: DISABLE           SRefresh Interval: 30 sec
 Mpls Mtu: 1500                  Retransmit Interval: 5000 msec
```

```
Increment Value: 1
Authentication: DISABLE
Bfd Enabled: DISABLE              Bfd Min-Tx: 400
Bfd Min-Rx: 300                 Bfd Detect-Multi: 4
```

Table 9-61 Description of the display mpls rsvp-te interface command output

Item	Description
Interface	Name of a tunnel interface.
Interface Address	IP address of an interface.
Interface state	Interface status: ● UP ● DOWN
Interface Index	Index of an interface.
Total-BW	Total available bandwidth of an interface, in kbit/s.
Used-BW	Total bandwidth of an interface in use, in kbit/s.
Hello configured	Whether the Hello feature is configured on an interface: ● YES: indicates that the Hello feature is configured. ● NO: indicates that the Hello feature is not configured.
Num of Neighbors	Number of neighbor devices of the local node.
SRefresh feature	Whether the Srefresh feature is enabled. To enable the Srefresh feature, run the **mpls rsvp-te srefresh** command in the interface view.
SRefresh Interval	Value of the Srefresh timer, in seconds. To specify the value of the Srefresh timer, run the **mpls rsvp-te timer refresh** command.
Mpls Mtu	MTU value used in MPLS forwarding.
Retransmit Interval	Value of the Retransmit timer, in milliseconds. To specify the value of the Retransmit timer, run the **mpls rsvp-te timer retransmission** command.
Increment Value	Retransmission increment. To specify the retransmission increment, run the **mpls rsvp-te timer retransmission** command.

Item	Description
Authentication	Whether the authentication function is enabled: ● ENABLE: indicates that the authentication function is enabled. ● DISABLE: indicates that the authentication function is disabled. To enable the authentication function, run the **mpls rsvp-te authentication** command.
Bfd Enabled	Whether BFD for RSVP is enabled on the interface: ● ENABLE: indicates that BFD for RSVP is enabled on the interface. ● DISABLE: indicates that BFD for RSVP is not enabled on the interface. To enable BFD for RSVP, run the **mpls rsvp-te bfd enable** command.
Bfd Min-Tx	Local interval at which BFD packets are sent, in milliseconds. To specify the local minimum interval at which BFD packets are sent, run the **mpls rsvp-te bfd** command.
Bfd Min-Rx	Local interval at which BFD packets are received, in milliseconds. To specify the local minimum interval at which BFD packets are received, run the **mpls rsvp-te bfd** command.
Bfd Detect-Multi	Local BFD detection multiplier. To specify the local BFD detection multiplier, run the **mpls rsvp-te bfd** command.

9.3.22 display mpls rsvp-te peer

Function

The **display mpls rsvp-te peer** command displays information about RSVP-TE neighbor devices on an RSVP-TE-enabled interface.

Format

display mpls rsvp-te peer [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about RSVP-TE of a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no interface is specified, information about RSVP-TE neighbors of all interfaces is displayed.

Example

# Display information about RSVP-TE neighbors of all interfaces.

```
<HUAWEI> display mpls rsvp-te peer
 Remote Node id Neighbor
 Neighbor Addr:  -----
 SrcInstance: 0x3A76A0FA              NbrSrcInstance: 0x0
 PSB Count: 2                     RSB Count: 2
 Hello Type Sent: REQ
 SRefresh Enable: NO
 Last valid seq # rcvd: NULL

Interface: Vlanif10
 Neighbor Addr: 172.16.1.2
 SrcInstance: 0x3A76A0FA              NbrSrcInstance: 0x22A6B5C2
 PSB Count: 2                     RSB Count: 2
 Hello Type Sent: REQ                Neighbor Hello Extension: ENABLE
 SRefresh Enable: NO
 Last valid seq # rcvd: NULL
```

Table 9-62 Description of the display mpls rsvp-te peer command output

Item	Description
Neighbor Addr	Neighboring device address.
SrcInstance	Source instance.
NbrSrcInstance	Source instance of a neighbor device.
PSB Count	Number of Path State Blocks (PSBs).
RSB Count	Number of Reservation State Blocks (RSBs).

Item	Description
Hello Type Sent	Type of Hello message sent to the neighbor device: ● REQ ● ACK ● NONE
Neighbor Hello Extension	Whether the Hello extension feature of the neighboring device is enabled.
SRefresh Enable	Whether the Srefresh mechanism is enabled: ● YES ● NO
Last valid seq # rcvd	Serial number of the valid RSVP message last received.

9.3.23 display mpls rsvp-te psb-content

Function

The **display mpls rsvp-te psb-content** command displays information about an RSVP TE Path State Block (PSB).

Format

display mpls rsvp-te psb-content [*ingress-lsr-id tunnel-id lsp-id*]

Parameters

Parameter	Description	Value
ingress-lsr-id	Specifies the LSR ID of the ingress.	The value is in dotted decimal notation.
tunnel-id	Specifies the tunnel ID.	The value is an integer that ranges from 0 to 65535.
lsp-id	Specifies the LSP ID.	The value is an integer that ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no parameter is specified, information about all RSVP-TE PSBs is displayed.

Example

# Display information about the PSB.

```
<HUAWEI> display mpls rsvp-te psb-content 10.1.1.9 100 7
==============================================================
                 The PSB Content
==============================================================
 Tunnel Addr: 10.4.4.9                   Exist time: 17h 12m 57s
 Tunnel ExtID: 10.1.1.9                  Session ID: 100
 Ingress LSR ID: 10.1.1.9                Local LSP ID: 7
 Previous Hop : 172.16.1.1/0x2d    Next Hop : 172.20.1.2
 Incoming / Outgoing Interface: Vlanif100  / Vlanif20
 InLabel : 1028                          OutLabel : 1028
 Send Message ID : 30                    Recv Message ID : 0
 Refresh Timer : 510224684               Cleanup Timer : 408260940
 Session Attribute-
  SetupPrio: 7         HoldPrio: 7
  SessionAttrib: Local Protect desired. Node Protect desired. Label Recording de
sired. SE Style desired.
 LSP Type: -
 FRR Flag : Will be MP                   Local RRO Flag : 0x1
 ERO Information-
    L-Type         ERO-IPAddr       ERO-PrefixLen
   ERHOP_STRICT    172.20.1.2           32
   ERHOP_STRICT    172.30.1.1           32
   ERHOP_STRICT    172.30.1.2           32
 Bypass ERO Information-
    L-Type         ERO-IPAddr       ERO-PrefixLen
   ERHOP_STRICT    10.3.3.9             32
   ERHOP_STRICT    172.30.1.1           32
   ERHOP_STRICT    172.30.1.2           32
 RRO Information-
   RRO-CType: IPV4   IPAddress: 172.16.1.1        PrefixLen: 32  Flag: 0x9
   RRO-CType: IPV4   IPAddress: 10.1.1.9          PrefixLen: 32  Flag: 0x20
 SenderTspec Information-
  Token bucket rate: 0.00
  Token bucket size: 1000.00
  Peak data rate: 0.00
  Minimum policed unit: 0
  Maximum packet size: 1500
 Path Message arrive on Vlanif100 from PHOP 172.16.1.1
 Path Message sent to NHOP 172.20.1.2  on Vlanif20
 Resource Reservation OK

 LSP Statistics Information:
   SendPacketCounter: 3623        RecvPacketCounter: 3648
   SendPathCounter: 1794          RecvPathCounter: 1791
   SendResvCounter: 1829          RecvResvCounter: 1857
```

Table 9-63 Description of the display mpls rsvp-te psb-content command output

Item	Description
Tunnel Addr	Tunnel address in the format X.X.X.X.
Exist time	Duration that an LSP has been established.
Tunnel ExtID	Tunnel extended ID.
Session ID	RSVP session ID

Item	Description
Ingress LSR ID	Ingress address in the format X.X.X.X.
Local LSP ID	Local LSP ID.
Previous Hop	Previous-hop address in the format X.X.X.X.
Next Hop	Next-hop address in the format X.X.X.X.
Incoming / Outgoing Interface	Incoming or outgoing interface through which a tunnel passes on the local device.
InLabel	Value of an incoming label.
OutLabel	Value of an outgoing label.
Send Message ID	ID of the sent refresh reduction message.
Recv Message ID	ID of the received refresh reduction message.
Refresh Timer	Refresh timer.
Cleanup Timer	Timeout timer.
Session Attribute	Attribute of an RSVP session.
SetupPrio	Setup priority of an RSVP session.
HoldPrio	Holding priority of an RSVP session.
SessionAttrib	RSVP session attributes, such as resource reservation style.
LSP Type	Type of LSP.
FRR Flag	State of MPLS TE FRR
Local RRO Flag	Flag bit of the local RRO.
ERO Information	Information about the Explicit Route Object (ERO).
L-Type	Types of the explicit route.
ERO-IPAddr	Explicit route address.
ERO-PrefixLen	Explicit route prefix length.
RRO Information	Information about the Record Route Object (RRO).
RRO-CType	RRO of the C type, IPv4 or label.
IPAddress	IP address of a record route.
PrefixLen	Prefix length of a recorded route.
Flag	Flag bit of a recorded route.

Item	Description
SenderTspec Information	Information about the traffic specification of the sender.
Token bucket rate	Token bucket rate, in byte/s.
Token bucket size	Token bucket size.
Peak data rate	Peak data rate, in byte/s.
Minimum policed unit	Minimum policed unit.
Maximum packet size	Maximum packet size.
Path Message arrive on	Incoming interfaces and previous-hop addresses of messages.
Path Message sent to NHOP	Next-hop addresses and outgoing interfaces of messages.
Resource Reservation OK	Ready state of resource reservation that is displayed only when the resource reserved flag is set.
LSP Statistics Information	Statistics of LSPs.
SendPacketCounter	Number of sent packets.
RecvPacketCounter	Number of received packets.
SendPathCounter	Number of sent Path messages.
RecvPathCounter	Number of received Path messages.
SendResvCounter	Number of sent Resv messages.
RecvResvCounter	Number of received Resv messages.

9.3.24 display mpls rsvp-te request

Function

The **display mpls rsvp-te request** command displays information about the RSVP-TE request messages on interfaces.

Format

display mpls rsvp-te request [**interface** *interface-type interface-number peer-ip-address*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about RSVP TE request messages on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
peer-ip-address	Specifies the IP address of a neighbor device.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no interface name is specified, the command displays information about the RSVP-TE request information of all RSVP-TE-enabled interfaces.

Example

# Display information about RSVP-TE of a specified interface.

```
<HUAWEI> display mpls rsvp-te request interface vlanif 10 172.16.1.1
Interface: Vlanif10
 Tunnel Addr: 10.2.2.9              Ingress LSR ID: 10.1.1.9
 Local LSP ID: 0                    Session Tunnel ID: 100
 NextHopAddr:  -----
 SessionAttrib: Label Recording desired. SE Style desired.
 Token bucket rate: 0.00            Token bucket size: 1000.00
 Out Interface:  -----
```

Table 9-64 Description of the display mpls rsvp-te request command output

Item	Description
Interface	Name of the interface that is enabled with RSVP-TE.
Tunnel Addr	Tunnel destination address in the format X.X.X.X.
Ingress LSR ID	LSR ID of the ingress node in the format X.X.X.X.

Item	Description
Local LSP ID	Local identifier of an LSP.
Session Tunnel ID	Tunnel ID
NextHopAddr	Next-hop address in the format X.X.X.X.
SessionAttrib	Session attribute: ● Local protection desired ● Label record desired ● Resource reservation style
Token bucket rate	Token bucket rate.
Token bucket size	Token bucket size.
Out Interface	Outgoing interface of an LSP.

9.3.25 display mpls rsvp-te reservation

Function

The **display mpls rsvp-te reservation** command displays RSVP-TE resource reservation information of an interface enabled with RSVP-TE.

Format

display mpls rsvp-te reservation [**interface** *interface-type interface-number peer-ip-address*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the RSVP-TE reservation information of the interface that is not in stale state. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
peer-ip-address	Specifies the IP address of an RSVP-TE neighbor device.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no interface name is specified, the command displays the resource reservation information of all RSVP-TE-enabled interfaces.

Example

# Display information about the RSVP-TE resource reservation information of all interfaces.

```
<HUAWEI> display mpls rsvp-te reservation
Interface: Outgoing-Interface at the Egress
 Tunnel Addr: 1.1.1.9              Ingress LSR ID: 3.3.3.9
 Local LSP ID: 4                 Session Tunnel ID: 301
 Upstream Label: 3
 Token bucket rate: 0.00           Token bucket size: 1000.00

 Tunnel Addr: 1.1.1.9              Ingress LSR ID: 3.3.3.9
 Local LSP ID: 4                 Session Tunnel ID: 300
 Upstream Label: 3
 Token bucket rate: 0.00           Token bucket size: 1000.00

 Tunnel Addr: 3.3.3.9              Ingress LSR ID: 1.1.1.9
 Local LSP ID: 3                 Session Tunnel ID: 300
 Upstream Label: NULL
 Token bucket rate: 0.00           Token bucket size: 1000.00

 Tunnel Addr: 3.3.3.9              Ingress LSR ID: 1.1.1.9
 Local LSP ID: 2                 Session Tunnel ID: 301
 Upstream Label: NULL
 Token bucket rate: 0.00           Token bucket size: 1000.00
```

Table 9-65 Description of the display mpls rsvp-te reservation command output

Item	Description
Interface	Name of the interface that is enabled with RSVP-TE
Tunnel Addr	Tunnel destination address in the format X.X.X.X.
Ingress LSR ID	LSR ID of the ingress node in the format X.X.X.X.
Local LSP ID	Local identifier of an LSP.
Session Tunnel ID	Tunnel ID.
Upstream Label	Incoming label.
Token bucket rate	Token bucket rate.
Token bucket size	Token bucket size.

9.3.26 display mpls rsvp-te rsb-content

Function

The **display mpls rsvp-te rsb-content** command displays information about the RSVP TE Reserve State Block (RSB).

Format

display mpls rsvp-te rsb-content [*ingress-lsr-id tunnel-id lsp-id*]

Parameters

Parameter	Description	Value
ingress-lsr-id	Specifies the ingress LSR ID.	The value is in dotted decimal notation.
tunnel-id	Specifies the tunnel ID.	The value is an integer that ranges from 0 to 65535.
lsp-id	Specifies the LSP ID.	The value is an integer that ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no parameter is specified, information about all RSVP TE RSBs is displayed.

Example

# Display information about the RSVP TE Reserve State Block.

```
<HUAWEI> display mpls rsvp-te rsb-content 10.1.1.9 300 3
==============================================================
                   The RSB Content
==============================================================
 Tunnel Addr: 10.3.3.9               Session Tunnel ID: 300
 Tunnel ExtID: 10.1.1.9
 Next Hop: 172.16.1.2                Reservation Style: SE Style
 Reservation Incoming Interface: Vlanif100
 Reservation Interface: Vlanif100
 Filter Spec Information-
   The filter number: 1
   Ingress LSR ID: 10.1.1.9        Local LSP ID: 3       OutLabel: 1040
   Cleanup Timer : 504613260
   RRO Information-
```

```
    RRO-CType: IPV4   RRO-IPAddress: 172.16.1.2       RRO-IPPrefixLen: 32
    RRO-CType: Label    RRO-Label: 1040
    RRO-CType: IPV4   RRO-IPAddress: 10.2.2.9         RRO-IPPrefixLen: 32
    RRO-CType: Label    RRO-Label: 1040
    RRO-CType: IPV4   RRO-IPAddress: 172.20.1.1       RRO-IPPrefixLen: 32
    RRO-CType: IPV4   RRO-IPAddress: 172.20.1.2       RRO-IPPrefixLen: 32
    RRO-CType: Label    RRO-Label: 3
    RRO-CType: IPV4   RRO-IPAddress: 10.3.3.9         RRO-IPPrefixLen: 32
    RRO-CType: Label    RRO-Label: 3
  Message ID : 0
FlowSpec Information-
  Token bucket rate: 0.00
  Token bucket size: 1000.00
  Peak data rate: 0.00
  Minimum policed unit: 0
  Maximum packet size: 1500
  Bandwidth guarantees: 0.00
  Delay guarantees: 0
  Qos Service is Controlled
Resv Message arrive on Vlanif100 from NHOP 172.16.1.2
```

Table 9-66 Description of the display mpls rsvp-te rsb-content command output

Item	Description
Tunnel Addr	Tunnel destination address in the format X.X.X.X.
Session Tunnel ID	Tunnel ID.
Tunnel ExtID	Tunnel extension ID (ingress LSR ID) in the format X.X.X.X.
Next Hop	Next-hop address in the format X.X.X.X.
Reservation Style	Reservation style: ● SE ● FF
Reservation Incoming Interface	Incoming interface for the reservation message.
Reservation Interface	Name of the interface on which bandwidth is reserved.
Message ID	ID of the Refresh Reduction message.
Filter Spec Information	Filtering conditions.
The filter number	Total number of filters.
Ingress LSR ID	LSR ID of the ingress node in the format X.X.X.X.
Local LSP ID	Local identifier of an LSP.
OutLabel	Outgoing label.
Cleanup Timer	Timeout timer.
RRO Information	Information about the RRO.

Item	Description
RRO-CType	Class type in the RRO: ● IPv4 ● Label
RRO-IPAddress	IP address in the RRO, in the format X.X.X.X.
RRO-IPPrefixLen	Length of the route prefix in the RRO.
RRO-Label	Label information in the RRO
FlowSpec Information	Traffic information including flow specifications.
Token bucket rate	Token bucket rate, in byte/s.
Token bucket size	Token bucket size.
Peak data rate	Peak data rate, in byte/s.
Minimum policed unit	Minimum policed unit.
Maximum packet size	Maximum packet size.
Bandwidth guarantees	Bandwidth guarantee.
Delay guarantees	Delay guarantee.
Qos Service	QoS guarantee/control.
Resv Message	Reservation message received on an interface.

9.3.27 display mpls rsvp-te sender

Function

The **display mpls rsvp-te sender** command displays information about an RSVP-TE enabled interface as an RSVP-TE sender.

Format

display mpls rsvp-te sender [**interface** *interface-type interface-number peer-ip-address*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the interface receiving Path messages. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
peer-ip-address	Specifies the IP address of the outgoing interface on the previous hop sending Path messages.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no interface name is specified, the command displays the information about all RSVP-TE enabled interfaces as RSVP-TE senders.

Example

# Display information about all RSVP-TE enabled interfaces as RSVP-TE senders.

```
<HUAWEI> display mpls rsvp-te sender
Interface: Incoming-Interface at the Ingress
 Tunnel Addr: 10.3.3.9              Ingress LSR ID: 10.1.1.9
 Local LSP ID: 3                  Session Tunnel ID: 300
 Session Name: Tunnel1
 Previous Hop Address:  -----
 Token bucket rate: 0.00           Token bucket size: 1000.00

 Tunnel Addr: 10.1.1.9              Ingress LSR ID: 10.3.3.9
 Local LSP ID: 4                  Session Tunnel ID: 300
 Session Name: Tunnel1
 Previous Hop Address: 172.16.1.2
 Token bucket rate: 0.00           Token bucket size: 1000.00
```

Table 9-67 Description of the display mpls rsvp-te sender command output

Item	Description
Tunnel Addr	Tunnel destination address in the format X.X.X.X.
Ingress LSR ID	LSR ID of the ingress node in the format X.X.X.X.
Local LSP ID	Local LSP ID.

Item	Description
Session Tunnel ID	Tunnel ID.
Session Name	Name of a session.
Previous Hop Address	Previous-hop address in the format X.X.X.X.
Token bucket rate	Token bucket rate.
Token bucket size	Token bucket size.
Interface: Incoming-Interface at the Ingress	Information about the RSB functioning as the ingress on the local node.

9.3.28 display mpls rsvp-te session

Function

The **display mpls rsvp-te session** command displays all information about any specified RSVP session.

Format

display mpls rsvp-te session *ingress-lsr-id tunnel-id egress-lsr-id*

Parameters

Parameter	Description	Value
ingress-lsr-id	Specifies the ingress LSR ID.	The value is in dotted decimal notation.
tunnel-id	Specifies the tunnel ID.	The value is an integer that ranges from 0 to 65535.
egress-lsr-id	Specifies the egress LSR ID.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Information about the RSVP session includes information about the Path State Block (PSB), Reservation State Block (RSB), and ReFresh State Block (RFSB).

Example

# Display all information about the RSVP session between nodes 10.1.1.9 and 10.3.3.9 (Tunnel ID is 300).

```
<HUAWEI> display mpls rsvp-te session 10.1.1.9 300 10.3.3.9
===============================================================
  Display PSB, RSB and RFSB information in session table
===============================================================
===============================================================
                   The PSB Content
===============================================================
 Tunnel Addr: 10.3.3.9                  Exist time: 1h 1m 4s
 Tunnel ExtID: 10.1.1.9                 Session ID: 300
 Ingress LSR ID: 10.1.1.9               Local LSP ID: 4
 Previous Hop :  ----- /0x0      Next Hop : 172.16.1.2
 Incoming / Outgoing Interface: -----  / Vlanif100
 InLabel : NULL                         OutLabel : 1042
 Send Message ID : 29                   Recv Message ID : 0
 Refresh Timer : 504613692               Cleanup Timer : ---
 Session Attribute-
  SetupPrio: 0         HoldPrio: 0
  SessionAttrib: Local Protect desired. Node Protect desired. Label Recording de
sired. SE Style desired.
 LSP Type: -
 FRR Flag : No protection                Local RRO Flag : 0x0
 ERO Information-
     L-Type         ERO-IPAddr       ERO-PrefixLen
   ERHOP_STRICT    172.16.1.2           32
   ERHOP_STRICT    172.20.1.1           32
   ERHOP_STRICT    172.20.1.2           32
 RRO Information-
    -----
 SenderTspec Information-
  Token bucket rate: 0.00
  Token bucket size: 1000.00
  Peak data rate: 0.00
  Minimum policed unit: 0
  Maximum packet size: 4294967295
 Path Message arrive on ----- from PHOP  -----
 Path Message sent to NHOP 172.16.1.2  on Vlanif100
 Resource Reservation OK

 LSP Statistics Information:
   SendPacketCounter: 106         RecvPacketCounter: 115
   SendPathCounter: 106           RecvPathCounter: 0
   SendResvCounter: 0             RecvResvCounter: 115

===============================================================
                   The RSB Content
===============================================================
 Tunnel Addr: 10.3.3.9               Session Tunnel ID: 300
 Tunnel ExtID: 10.1.1.9
 Next Hop: 172.16.1.2                Reservation Style: SE Style
 Reservation Incoming Interface: Vlanif100
 Reservation Interface: Vlanif100
 Message ID : 0
 Filter Spec Information-
   The filter number: 1
   Ingress LSR ID: 10.1.1.9        Local LSP ID: 4       OutLabel: 1042
   Cleanup Timer : 504613800
   RRO Information-
     RRO-CType: IPV4   RRO-IPAddress: 172.16.1.2       RRO-IPPrefixLen: 32
     RRO-CType: Label    RRO-Label: 1042
     RRO-CType: IPV4   RRO-IPAddress: 10.2.2.9         RRO-IPPrefixLen: 32
     RRO-CType: Label    RRO-Label: 1042
     RRO-CType: IPV4   RRO-IPAddress: 172.20.1.1       RRO-IPPrefixLen: 32
     RRO-CType: IPV4   RRO-IPAddress: 172.20.1.2       RRO-IPPrefixLen: 32
     RRO-CType: Label    RRO-Label: 3
     RRO-CType: IPV4   RRO-IPAddress: 10.3.3.9        RRO-IPPrefixLen: 32
     RRO-CType: Label    RRO-Label: 3
 FlowSpec Information-
   Token bucket rate: 0.00
   Token bucket size: 1000.00
   Peak data rate: 0.00
   Minimum policed unit: 0
   Maximum packet size: 1500
   Bandwidth guarantees: 0.00
   Delay guarantees: 0
   Qos Service is Controlled
 Resv Message arrive on Vlanif100 from NHOP 172.16.1.2
```

Table 9-68 Description of the display mpls rsvp-te session command output

Item	Description
The PSB Content	Contents of the PSB.
Tunnel Addr	Tunnel destination address in the format X.X.X.X.
Exist time	Time elapsed since the PSB is created.
Tunnel ExtID	Tunnel extension ID (ingress LSR ID) in the format X.X.X.X.
Session ID/ Session Tunnel ID	Tunnel ID.
Ingress LSR ID	LSR ID of the ingress node in the format X.X.X.X.
Local LSP ID	Local LSP ID.
Previous Hop	Previous-hop address in the format X.X.X.X.
Next Hop	Next-hop address in the format X.X.X.X.
Incoming / Outgoing Interface	Name of the incoming or outgoing interface.
InLabel	Value of an incoming label.
OutLabel	Value of an outgoing label.
Send Message ID	ID of the sent refresh reduction message.
Recv Message ID	ID of the received refresh reduction message.
Refresh Timer	ID of the Refresh timer.
Cleanup Timer	ID of the Cleanup timer.
Session Attribute	Attribute of a session.
SetupPrio	Setup priority of a session.

Item	Description
HoldPrio	Holding priority of a session.
SessionAttrib	Session attributes, including required local protection, bandwidth protection, node protection, label record, and reservation style.
LSP Type	Type of an LSP.
FRR Flag	Flag bit of FRR: ● No protection: indicates no FRR protection. ● PLR in use: provides protection on the Point of Local Repair. ● MP in use: provides protection on the Merge Point. ● Under protecting: provides FRR protection.
Local RRO Flag	Flag bit of the local RRO.
ERO Information	Information about the Explicit Route Object (ERO).
L-Type	Types of the explicit route: ● ERHOP_STRICT ● ERHOP_LOOSE
ERO-IPAddr	Explicit route address.
ERO-PrefixLen	Explicit route prefix length.
RRO Information	Information about the Record Route Object (RRO).
RRO-CType	Class C routes, including IPv4 or IPv6 addresses and labels recorded.
RRO-IPAddress	IPv4 or IPv6 address of the recorded route.
RRO-IPPrefixLen	Prefix length of a recorded route.
RRO-Label	Label information in the RRO.
SenderTspec Information	Information about the traffic specification of the sender.
Token bucket rate	Token bucket rate, in byte/s.
Token bucket size	Token bucket size.
Peak data rate	Peak data rate, in byte/s.

Item	Description
Minimum policed unit	Minimum policed unit.
Maximum packet size	Maximum packet size, in bytes.
Path Message arrive on	Pre-hop addresses and incoming interfaces of messages.
Path Message sent to	Next-hop addresses and outgoing interfaces of messages.
Resource Reservation OK	Displayed only when the resource reservation flag is set.
LSP Statistics Information	Statistics of LSPs.
SendPacketCounter	Number of sent packets.
RecvPacketCounter	Number of received packets.
SendPathCounter	Number of sent Path messages.
RecvPathCounter	Number of received Path messages.
SendResvCounter	Number of sent Resv messages.
RecvResvCounter	Number of received Resv messages.
The RSB Content	Number of Reservation State Blocks (RSBs).
Reservation Style	Reservation style: ● SE: Shared Explicit Style ● FF: Fixed-Filter Style
Reservation Incoming Interface	Incoming interface for the reservation message.
Reservation Interface	Name of the interface on which bandwidth is reserved.
Message ID	Message ID locally allocated, used in the Srefresh feature and reliability.
Filter Spec Information	Filtering conditions.
The filter number	Total number of filters.
FlowSpec Information	Information about flow specifications.
Bandwidth guarantees	Bandwidth guarantee.
Delay guarantees	Delay guarantee.
Qos Service is Controlled	QoS guarantee.
Resv Message arrive on	Incoming interfaces and previous-hop addresses of messages.

9.3.29 display mpls rsvp-te statistics

Function

The **display mpls rsvp-te statistics** command displays statistics on RSVP-TE.

Format

display mpls rsvp-te statistics { **global** | **interface** [*interface-type interface-number*] }

Parameters

Parameter	Description	Value
global	Displays the global statistics on RSVP-TE.	-
interface	Displays statistics on RSVP-TE on all interface that enabled RSVP-TE function.	-
interface-type interface-number	Displays statistics on RSVP-TE on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the statistics on RSVP-TE, run the **display mpls rsvp-te statistics** command.

Example

# Display the global RSVP-TE statistics.

```
<HUAWEI> display mpls rsvp-te statistics global
 LSR ID: 10.1.1.1                    LSP Count: 0
 PSB Count: 0                        RSB Count: 0
 RFSB Count: 0

Total Statistics Information:
 PSB CleanupTimeOutCounter: 0         RSB CleanupTimeOutCounter: 0
 SendPacketCounter: 0                RecPacketCounter: 0
 SendCreatePathCounter: 0             RecCreatePathCounter: 0
 SendRefreshPathCounter: 0            RecRefreshPathCounter: 0
```

```
SendCreateResvCounter: 0              RecCreateResvCounter: 0
SendRefreshResvCounter: 0             RecRefreshResvCounter: 0
SendResvConfCounter: 0                RecResvConfCounter: 0
SendHelloCounter: 0                   RecHelloCounter: 0
SendAckCounter: 0                     RecAckCounter: 0
SendPathErrCounter: 0                 RecPathErrCounter: 0
SendResvErrCounter: 0                 RecResvErrCounter: 0
SendPathTearCounter: 0                RecPathTearCounter: 0
SendResvTearCounter: 0                RecResvTearCounter: 0
SendSrefreshCounter: 0                RecSrefreshCounter: 0
SendAckMsgCounter: 0                  RecAckMsgCounter: 0
SendChallengeMsgCounter: 0            RecChallengeMsgCounter: 0
SendResponseMsgCounter: 0             RecResponseMsgCounter: 0
SendErrMsgCounter: 0                  RecErrMsgCounter: 0
SendRecoveryPathMsgCounter: 0         RecRecoveryPathMsgCounter: 0
SendGRPathMsgCounter: 0               RecGRPathMsgCounter: 0
ResourceReqFaultCounter: 0            RecGRPathMsgFromLSPMCounter: 0
Bfd neighbor count: 0                 Bfd session count: 0
```

Table 9-69 Description of the display mpls rsvp-te statistics command output

Item	Description
LSR ID	Local LSR ID.
PSB Count	Number of PSBs.
RSB Count	Number of RSBs.
RFSB Count	Number of RFSBs.
LSP Count	Number of LSPs established through RSVP TE.
Total Statistics Information	Total statistics information.
PSB CleanupTimeOutCounter	Number of times that the PSB is reset after the timer expires.
RSB CleanupTimeOutCounter	Number of times that the RSB is reset after the timer expires.
SendPacketCounter	Number of sent packets.
RecPacketCounter	Number of received packets.
SendCreatePathCounter	Number of sent CreatePath messages.
RecCreatePathCounter	Number of received CreatePath messages.
SendRefreshPathCounter	Number of sent RefreshPath messages.
RecRefreshPathCounter	Number of received RefreshPath messages.
SendCreateResvCounter	Number of sent CreateResv messages.
RecCreateResvCounter	Number of received CreateResv messages.
SendRefreshResvCounter	Number of sent RefreshResv messages.
RecRefreshResvCounter	Number of received RefreshResv messages.
SendResvConfCounter	Number of sent ResvConf messages.

Item	Description
RecResvConfCounter	Number of received ResvConf messages.
SendHelloCounter	Number of sent Hello messages.
RecHelloCounter	Number of received Hello messages.
SendAckCounter	Number of sent Ack messages.
RecAckCounter	Number of received Ack messages.
SendPathErrCounter	Number of sent PathErr messages.
RecPathErrCounter	Number of received PathErr messages.
SendResvErrCounter	Number of sent ResvErr messages.
RecResvErrCounter	Number of received ResvErr messages.
SendPathTearCounter	Number of sent PathTear messages.
RecPathTearCounter	Number of received PathTear messages.
SendResvTearCounter	Number of sent ResvTear messages.
RecResvTearCounter	Number of received ResvTear messages.
SendSrefreshCounter	Number of sent Srefresh messages.
RecSrefreshCounter	Number of received Srefresh messages.
SendAckMsgCounter	Number of sent Msg_ID_ACK messages.
RecAckMsgCounter	Number of received Msg_ID_ACK messages.
SendChallengeMsgCounter	Number of sent Challenge messages.
RecChallengeMsgCounter	Number of received Challenge messages.
SendResponseMsgCounter	Number of sent Response messages.
RecResponseMsgCounter	Number of received Response messages.
SendErrMsgCounter	Number of sent Msg_ID_NACK messages.
RecErrMsgCounter	Number of received Msg_ID_NACK messages.
SendRecoveryPathMsgCounter	Number of sent Recovery Path messages.
RecRecoveryPathMsgCounter	Number of received Recovery Path messages.
SendGRPathMsgCounter	Number of sent GR Path messages.
RecGRPathMsgCounter	Number of received GR Path messages.
ResourceReqFaultCounter	Number of failed attempts to request resources.

Item	Description
RecGRPathMsgFromLSPM-Counter	Number of GR Path messages received from the LSPM module.
Bfd neighbor count	Number of upstream or downstream BFD peers through which at least one LSP in the Up state passes.
Bfd session count	Number of BFD sessions.

9.3.30 display mpls rsvp-te statistics fast-reroute

Function

The **display mpls rsvp-te statistics fast-reroute** command displays the CR-LSP statistics on the local node serving as a Point of Local Repair (PLR) or Merge Point (MP).

Format

display mpls rsvp-te statistics fast-reroute

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command can be used to check the following information:

- Number of CR-LSPs in the PLR Available state
- Number of CR-LSPs in the PLR Inuse state
- Number of CR-LSPs in the MP Available state
- Number of CR-LSPs in the MP Inuse state

Example

# Display CR-LSP statistics information on the local node serving as PLR or MP.

```
<HUAWEI> display mpls rsvp-te statistics fast-reroute
FRR statistics information:
 PLR AvailLsps: 0                    PLR InuseLsps: 0
 MP AvailLsps: 0                     MP InuseLsps: 0
```

Table 9-70 Description of the display mpls rsvp-te statistics fast-reroute command output

Item	Description
PLR AvailLsps	Number of CR-LSPs whose local node is the PLR in the PLR Available state (the CR-LSPs are bound to the bypass tunnel but FRR does not occur on the PLR).
PLR InuseLsps	Number of CR-LSPs whose local node is the PLR in the PLR Inuse state.
MP AvailLsps	Number of CR-LSPs whose local node is the MP in the MP Available state (the CR-LSPs are bound to the bypass tunnel but FRR does not occur on the MP).
MP InuseLsps	Number of CR-LSPs whose local node is the MP in the MP Inuse state.

9.3.31 display mpls static-cr-lsp

Function

The **display mpls static-cr-lsp** command displays information about a static CR-LSP.

Format

display mpls static-cr-lsp [*lsp-name*] [{ **include** | **exclude** } *ip-address mask-length*] [**verbose**]

Parameters

Parameter	Description	Value
lsp-name	Specifies the name of an LSP.	The value is an existing LSP name.
exclude	Displays information about the CR-LSPs without specified destination IP addresses.	-
include	Displays information about the CR-LSPs of specified destination IP addresses.	-
ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of a destination address.	The value is an integer that ranges from 0 to 32.

Parameter	Description	Value
verbose	Displays detailed information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the information about static CR-LSPs, run the **display mpls static-cr-lsp** command.

Example

# Display brief information about static CR-LSPs.

```
<HUAWEI> 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          Status
Tunnel1       3.3.3.3/32        NULL/20      -/Vlanif10        Up
Tunnel2       -/-              130/NULL     Vlanif10/-        Up
```

Table 9-71 Description of the display mpls static-cr-lsp command output

Item	Description
TOTAL	Total number of static CR-LSPs.
UP	Number of the static CR-LSPs in the Up state.
DOWN	Number of the static CR-LSPs in the DOWN state.
Name	Name of a static CR-LSP.
FEC	Destination IP address and mask length.
I/O Label	Incoming and outgoing labels.
I/O If	Incoming and outgoing interfaces.
Status	Current status of a CR-LSP.

# Display detailed information about static CR-LSPs.

```
<HUAWEI> display mpls static-cr-lsp verbose
No             : 1
LSP-Name       : tunnel1
```

```
LSR-Type       : Transit
FEC            : -/-
In-Label       : 20
Out-Label      : 30
In-Interface   : Vlanif10
Out-Interface  : Vlanif20
NextHop        : 10.1.3.2
Lsp Status     : Up
```

Table 9-72 Description of the display mpls static-cr-lsp verbose command output

Item	Description
No	Sequence number of a static CR-LSP.
LSP-Name	Name of a static CR-LSP.
LSR-Type	Type of a static CR-LSP: ● Ingress ● Transit ● Egress
FEC	Destination address and mask length. "-/-" is displayed for the transit node and egress node.
In-Label	Value of an incoming label.
Out-Label	Value of an outgoing label.
In-Interface	Incoming interface.
Out-Interface	Outgoing interface.
NextHop	Next-hop address in the format X.X.X.X.
Lsp Status	Status of a static CR-LSP: ● Up: indicates that the static CR-LSP is successfully established. ● Down: indicates that the static CR-LSP fails to be established.

9.3.32 display mpls stale-interface

Function

The **display mpls stale-interface** command displays information about MPLS interfaces in the Stale state.

Format

display mpls stale-interface [*interface-index*] [**verbose**]

Parameters

Parameter	Description	Value
interface-index	Specifies the index of a specified stale interface.	The value is a hexadecimal integer ranging from 1 to FFFFFFFE.
verbose	Displays detailed information about an interface, for example, whether FRR is configured. If FRR is configured, information about the bound tunnels is also displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The outbound interface of the primary tunnel protected by TE FRR becomes a stale interface in one of the following situations:

MPLS is disabled on the interface when the primary tunnel is in the FRR In-used state.

The **display mpls stale-interface** command displays information about the stale interfaces.

Run the **display mpls stale-interface** command without specifying a parameter to view the index of a stale interface.

Example

# Display information about all MPLS interfaces in the Stale state.

```
<HUAWEI> display mpls stale-interface
Stale-Interface       Status    TE Attr   LSP Count  CRLSP Count Effective MTU
0x81a                 Up        Dis       0          1           1500
```

Table 9-73 Description of the display mpls stale-interface command output

Item	Description
Stale-Interface	Index of an MPLS interface in the Stale state.
Status	Status of the stale interface. ● Up ● Down

Item	Description
TE Attr	Whether MPLS TE is enabled on an interface: ● Dis: MPLS TE is not enabled on the interface. ● En: MPLS TE is enabled on the interface.
LSP Count	Number of LSPs on an interface.
CRLSP Count	Number of CR-LSPs on an interface.
Effective MTU	MTU value used in the MPLS forwarding. ● If the MPLS MTU is not set, the interface MTU takes effect. ● If the MPLS MTU is set, the smaller one between the MPLS MTU and the interface MTU takes effect.

# Display detailed information about all MPLS interfaces in the Stale state.

```
<HUAWEI> display mpls stale-interface verbose
No                    :  1
Interface             :  0x81a
Status                :  Up
TE Attribute          :  Disable
Static LSPCount       :  0
Static CR-LSPCount    :  0
LDP LSPCount          :  0
RSVP LSPCount         :  1
MPLS MTU              :  -
Interface MTU         :  -
Effective MTU         :  1500
TE FRR                :  Enable
Manual Bypass         :  Tun1
Interface State       :  Stale
```

Table 9-74 Description of the display mpls stale-interface verbose command output

Item	Description
No	Serial number.
Interface	Index of an MPLS interface in the Stale state.
Status	Status of the stale interface, which is the Up state in this example.
TE Attribute	Whether MPLS TE is enabled on the interface: ● Disable: MPLS TE is disabled. ● Enable: MPLS TE is enabled.
Static LSPCount	Number of static LSPs created on the interface.
Static CR-LSPCount	Number of static CR-LSPs created on the interface.
LDP LSPCount	Number of LDP LSPs created on the interface.

Item	Description
RSVP LSPCount	Number of RSVP-TE LSPs created on the interface.
MPLS MTU	MPLS MTU set using the **mpls mtu** command. When the interface is in the Stale state, a hyphen (-) is displayed.
Interface MTU	MTU configured on the interface. To set the MTU, run the **mtu** command.
Effective MTU	MTU value used in the MPLS forwarding. ● If the MPLS MTU is not set, the interface MTU takes effect. ● If the MPLS MTU is set, the smaller one between the MPLS MTU and the interface MTU takes effect.
TE FRR	Whether MPLS TE is enabled on the interface: ● Disable: No bypass tunnel is set up in manual FRR mode to protect the interface. ● Enable: A bypass tunnel is set up in manual FRR mode to protect the interface.
Manual Bypass	Name of a bypass tunnel set up in manual FRR mode.
Interface State	Interface status. Stale indicates that the interface is to be deleted.

9.3.33 display mpls te cspf destination

Function

The **display mpls te cspf destination** command helps you check whether the specified path is available or not. You can specify relevant parameters in the command to set constraint conditions.

Format

display mpls te cspf destination *ip-address* [**affinity** *properties* [**mask** *mask-value*] | **bandwidth** { **ct0** *ct0-bandwidth* | **ct1** *ct1-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** }] * [**hot-standby** [**explicit-path** *path-name* | **overlap-path** | **affinity** *properties* [**mask** *mask-value*] | **hop-limit** *hop-limit-number* | **srlg** { **preferred** | **strict** }] *]

Parameters

Parameter	Description	Value
destination *ip-address*	Specifies the destination IP address of an MPLS TE tunnel.	The value is in dotted decimal notation.
affinity *properties*	Specifies the affinity property of an MPLS TE tunnel.	The value is a hexadecimal number that ranges from 0 to FFFFFFFF.
mask *mask-value*	Specifies the value of the affinity property mask.	The value is a hexadecimal number that ranges from 0 to FFFFFFFF.
bandwidth	Specifies the required bandwidth of an MPLS TE tunnel.	-
ct0 *ct0-bandwidth* | **ct1** *ct1-bandwidth*	Specifies the bandwidth values of CR-LSPs of CT0 to CT1.	The value is an integer that ranges from 1 to 4000000000.
explicit-path *path-name*	Specifies the explicit path of an MPLS TE tunnel.	The value is an existing explicit path name.
hop-limit *hop-limit-number*	Specifies the maximum number of hops on an MPLS TE tunnel.	The value is an integer that ranges from 1 to 32. By default, the maximum number of hops is 32.
metric-type	Specifies the metric type for the CSPF calculation.	-
igp	Specifies the metric type as IGP.	-
te	Specifies the metric type as TE.	-
priority *setup-priority*	Specifies the setup priority of an MPLS TE tunnel.	The value is an integer that ranges from 0 to 7.
srlg-strict *exclude-path-name*	Specifies the path of a specified SRLG.	The value is an existing explicit path name.

Parameter	Description	Value
tie-breaking	Configures a tie-breaking mode for CSPF.	-
random	Configures the random mode.	-
most-fill	Configures the most-fill mode, meaning the path with the highest ratio of used bandwidth to maximum reservable bandwidth is selected.	-
least-fill	Configures the least-fill mode, meaning the path with the lowest ratio of used bandwidth to the maximum capacity of reservable bandwidth is selected.	-
hot-standby	Configures hot-standby path excluding primary path.	-
overlap-path	Specifies that if a completely disjoint path is not available, a maximally disjoint path should be computed for the Hot-standby.	-
srlg preferred	Specifies that the SRLG attribute is an optional constraint used by CSPF to calculate the path for the hot-standby CR-LSP. If CSPF fails to calculate the path for the hot-standby CR-LSP based on the SRLG attribute, CSPF recalculates the path, regardless of the SRLG attribute.	-
srlg strict	Specifies that the SRLG attribute is a required constraint used by CSPF to calculate the path for the hot-standby CR-LSP. The links of the hot-standby CR-LSP and the primary CR-LSP cannot be in the same SRLG.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Prerequisites

Before running this command, the CSPF function must have been enabled by using the **mpls te cspf** command.

Precautions

When this command is run, the device uses CSPF to check whether there is a path satisfying the specified constraints. If such a path exists, its information is displayed; otherwise, the display is empty.

Example

# Display the path with the destination address being 10.3.3.9 by performing the CSPF calculation.

```
<HUAWEI> display mpls te cspf destination 10.3.3.9
Path for the given constraints is:
10.1.1.9                Include       LSR-ID
172.16.1.1               Include
172.16.1.2               Include
10.2.2.9                Include       LSR-ID
172.17.1.1               Include
172.17.1.2               Include
10.3.3.9                Include       LSR-ID
The total metrics of the calculated path is :   2
```

# Display the explicit path named path1 with the destination address being 10.3.3.9 by performing the CSPF calculation.

```
<HUAWEI> display mpls te cspf destination 10.3.3.9 explicit-path path1
Path for the given constraints is:
10.1.1.9                Include       LSR-ID
172.16.1.1               Include
172.16.1.2               Include
10.2.2.9                Include       LSR-ID
172.17.1.1               Include
172.17.1.2               Include
10.3.3.9                Include       LSR-ID
The total metrics of the calculated path is :   2
```

# Display the hot standby path with the destination address being 10.3.3.9 by performing the CSPF calculation.

```
<HUAWEI> display mpls te cspf destination 10.3.3.9 hot-standby
Path for the given constraints is:
10.1.1.9                Include       LSR-ID
172.16.1.1               Include
172.16.1.2               Include
10.2.2.9                Include       LSR-ID
172.17.1.1               Include
172.17.1.2               Include
10.3.3.9                Include       LSR-ID
The total metrics of the calculated path is :   2

Hot-standby path for the given constraints is:
10.1.1.9                Include       LSR-ID
172.19.1.1               Include
```

```
172.19.1.2                Include
10.6.6.9                Include        LSR-ID
172.20.1.1                Include
172.20.1.2                Include
10.3.3.9                Include        LSR-ID
Complete disjoint path computed and the total metrics of the calculated path is :    2
```

# Display the hot standby path with the destination address being 10.4.4.9 and partial overlapping by performing the CSPF calculation.

```
<HUAWEI> display mpls te cspf destination 10.4.4.9 hot-standby overlap-path
Main path for the given constraints is:
10.1.1.9                Include        LSR-ID
172.16.1.1                Include
172.16.1.2                Include
10.2.2.9                Include        LSR-ID
172.17.1.1                Include
172.17.1.2                Include
10.3.3.9                Include        LSR-ID
172.18.1.1                Include
172.18.1.2                Include
10.4.4.9                Include        LSR-ID
The total metrics of the calculated path is :   3

Hot-standby path for the given constraints is:
10.1.1.9                Include        LSR-ID
172.21.1.1                Include
172.21.1.2                Include
10.6.6.9                Include        LSR-ID
172.22.1.1                Include
172.22.1.2                Include
10.3.3.9                Include        LSR-ID
172.18.1.1                Include
172.18.1.2                Include
10.4.4.9                Include        LSR-ID
Partial Overlap path computed and the total metrics of the calculated path is :
   3
```

Table 9-75 Description of the display mpls te cspf destination command output

Item	Description
Path for the given constraints is	Path calculated by CSPF. If * is displayed, it indicates the node does not exist on the explicit path calculated by CSPF. If * is not displayed, it indicates that the node exists on the path calculated by CSPF.
10.1.1.9 Include LSR-ID	Path information. 10.1.1.9 is the next hop address, Include is the node name, and LSR-ID indicates that the LSR ID is used as the address.
The total metrics of the calculated path is	Calculated metric value of a path.
Main path for the given constraints is	Path for the main request, when both main and hot-standby are requested.
Hot-standby path for the given constraints is	Path calculated by CSPF for the hot-standby.

Item	Description
Complete disjoint path computed and the total metrics of the calculated path is	CSPF has calculated complete disjoint path from main path for hot-standby.
Partial Overlap path computed and the total metrics of the calculated path is	CSPF has calculated partial overlap path from main path for hot-standby.

9.3.34 display mpls te cspf tedb

Function

The **display mpls te cspf tedb** command displays the CSPF TEBD information based on specified conditions.

Format

display mpls te cspf tedb { **all** | **area** { *area-id* | *area-id-ip* } | **interface** *ip-address* | **network-lsa** | **node** [*router-id*] | **srlg** *srlg-number* | **overload-node** }

Parameters

Parameter	Description	Value
all	Displays information about all TEDB nodes.	-
area *area-id*	Specifies the ID of an area.	For an OSPF area, the value is an integer that ranges from 0 to 4294967295. For an IS-IS area, the value is 1 or 2.
area *area-id-ip*	Specifies the ID of an area in IP address format.	For an OSPF area, the value is in dotted decimal notation.
interface *ip-address*	Specifies the IP address of an interface	The value is in dotted decimal notation.
network-lsa	Displays information about all network LSAs.	-
node	Displays information about a node.	-
router-id	Specifies the router ID.	The value is in dotted decimal notation.
srlg *srlg-number*	Specifies the SRLG number.	The value is an integer that ranges from 0 to 4294967295.
overload-node	Displays information of all the overload-nodes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the CSPF TEBD information, run the **display mpls te cspf tedb** command.

Example

# Display information about network LSAs in a TEDB.

```
<HUAWEI> display mpls te cspf tedb network-lsa
Maximum Network LSA Supported    : 512
Current Total Network LSA Number : 6

ID : 1
   IGP-Type: OSPF
   Process-ID: 1
   DR-Router-ID : 10.2.2.9
   DR-Address : 172.16.1.2
   Area : 0
   DR-OSPF-Router-ID : 10.2.2.9
     NBR-Router-ID      NBR-OSPF-Router-ID
     10.2.2.9           10.2.2.9
     10.1.1.9           10.1.1.9

ID : 2
   IGP-Type: OSPF
   Process-ID: 1
   DR-Router-ID : 10.2.2.9
   DR-Address : 172.20.1.1
   Area : 0
   DR-OSPF-Router-ID : 10.2.2.9
     NBR-Router-ID      NBR-OSPF-Router-ID
     10.2.2.9           10.2.2.9
     10.3.3.9           10.3.3.9

ID : 3
   IGP-Type: ISIS
   Process-ID: 1
   DR-Router-ID : 10.1.1.9
   DR-Address : 172.16.1.1
   Area : Level-2
   DR-ISIS-System-ID : 0000.0000.0001.01
     NBR-Router-ID      NBR-ISIS-System-ID
     10.1.1.9           0000.0000.0001.00
     10.2.2.9           0000.0000.0002.00

ID : 4
   IGP-Type: ISIS
   Process-ID: 1
   DR-Router-ID : 10.1.1.9
   DR-Address : 172.16.1.1
   Area : Level-1
   DR-ISIS-System-ID : 0000.0000.0001.01
     NBR-Router-ID      NBR-ISIS-System-ID
     10.1.1.9           0000.0000.0001.00
     10.2.2.9           0000.0000.0002.00

ID : 5
```

```
  IGP-Type: ISIS
  Process-ID: 1
  DR-Router-ID : 10.3.3.9
  DR-Address : 172.20.1.2
  Area : Level-1
  DR-ISIS-System-ID : 0000.0000.0003.01
    NBR-Router-ID       NBR-ISIS-System-ID
    10.3.3.9            0000.0000.0003.00
    10.2.2.9            0000.0000.0002.00

ID : 6
  IGP-Type: ISIS
  Process-ID: 1
  DR-Router-ID : 10.3.3.9
  DR-Address : 172.20.1.2
  Area : Level-2
  DR-ISIS-System-ID : 0000.0000.0003.01
    NBR-Router-ID       NBR-ISIS-System-ID
    10.3.3.9            0000.0000.0003.00
    10.2.2.9            0000.0000.0002.00
```

Table 9-76 Description of the display mpls te cspf tedb network-lsa command output

Item	Description
Maximum Network LSA Supported	Maximum network LSAs supported.
Current Total Network LSA Number	Current total number of network LSAs.
IGP-Type	IGP type: ● OSPF ● IS-IS
Process-ID	IGP process ID.
ID	Sequence number.
DR-Router-ID	DR Router ID.
DR-Address	Interface address of the DR.
Area	Area to which the device belongs.
DR-OSPF-Router-ID	OSPF router ID of a DR.
DR-ISIS-System-ID	IS-IS system ID of a DR.
NBR-Router-ID	Neighbor Router ID.
NBR-OSPF-Router-ID	Neighbor OSPF router ID.
NBR-ISIS-System-ID	Neighbor IS-IS system ID.

# Display information about all TEDBs.

```
<HUAWEI> display mpls te cspf tedb all
Maximum Nodes Supported: 512   Current Total Node Number: 6
Maximum Links Supported: 2048   Current Total Link Number: 12
Maximum SRLGs supported: 5120   Current Total SRLG Number: 0
ID     Router-ID         IGP      Process-ID     Area            Link-Count
1      10.1.1.9          OSPF     1              0               1
2      10.2.2.9          OSPF     1              0               2
3      10.3.3.9          OSPF     1              0               1
4      10.1.1.9          ISIS     1              Level-1,2       2
5      10.2.2.9          ISIS     1              Level-1,2       4
6      10.3.3.9          ISIS     1              Level-1,2       2
```

Table 9-77 Description of the **display mpls te cspf tedb all** command output

Item	Description
Maximum Nodes Supported	Maximum number of nodes supported.
Maximum Links Supported	Maximum number of links supported.
Maximum SRLGs supported	Maximum SRLGs supported.
Current Total Node Number	Current total number of nodes.
Current Total Link Number	Current total number of links.
Current Total SRLG Number	Current total number of SRLGs.
ID	Sequence number.
Router-ID	Router ID in dotted decimal notation.
IGP	IGP type: ● OSPF ● IS-IS
Process-ID	IGP process ID.
Area	Area to which the device belongs.
Link-Count	Total number of connected links with a specified IGP and process ID.

# Display TEDB information of a specified area.

```
<HUAWEI> display mpls te cspf tedb area 0
 Router Node Information for Area 0:
ID     Router-ID         IGP      Process-ID     Area            Link-Count
1      10.1.1.9          OSPF     1              0               1
2      10.2.2.9          OSPF     1              0               2
3      10.3.3.9          OSPF     1              0               1

Network LSA Information for Area 0:

ID : 1
   IGP-Type: OSPF
   Process-ID: 1
   DR-Router-ID : 10.2.2.9
   DR-Address : 172.16.1.2
   Area : 0
   DR-OSPF-Router-ID : 10.2.2.9
     NBR-Router-ID       NBR-OSPF-Router-ID
     10.2.2.9            10.2.2.9
     10.1.1.9            10.1.1.9

ID : 2
   IGP-Type: OSPF
   Process-ID: 1
   DR-Router-ID : 10.2.2.9
   DR-Address : 172.20.1.1
   Area : 0
   DR-OSPF-Router-ID : 10.2.2.9
     NBR-Router-ID       NBR-OSPF-Router-ID
     10.2.2.9            10.2.2.9
     10.3.3.9            10.3.3.9
```

Table 9-78 Description of the display mpls te cspf tedb area command output

Item	Description
Router Node Information for Area 0	Router node information for area 0.
Network LSA Information for Area 0	Network LSA information for area 0.
Link-Count	Total number of connected links with a specified IGP and process ID.
ID	Sequence number.
Router-ID	Router ID in dotted decimal notation.
IGP	IGP type: ● OSPF ● IS-IS
IGP-Type	IGP type: ● OSPF ● IS-IS
Process-ID	IGP process ID.
DR-Router-ID	Router ID of the DR.
DR-Address	Interface address of the DR.
Area	Area to which the device belongs.
DR-OSPF-Router-ID	OSPF router ID of the designated router.
NBR-Router-ID	Router ID of a neighbor router.
NBR-OSPF-Router-ID	OSPF router ID of a neighbor device.

# Display TEDB information of a specified node.

```
<HUAWEI> display mpls te cspf tedb node 10.1.1.9
 Router ID: 10.1.1.9
 IGP Type: OSPF       Process ID: 1
  MPLS-TE Link Count: 1
  Link[1]:
   OSPF Router ID: 10.1.1.9              Opaque LSA ID: 10.0.0.1
   Interface IP Address: 172.16.1.1
   DR Address: 172.16.1.2
   IGP Area: 0
   Link  Type: Multi-access  Link Status: Active
   IGP Metric: 1               TE Metric: 1           Color: 0x0
   Bandwidth Allocation Model : Russian Dolls Model
   Maximum Link Bandwidth: 40000 (kbps)
   Maximum Reservable Bandwidth: 40000 (kbps)
   Bandwidth Constraints:        Local Overbooking Multiplier:
       BC[0]:      40000 (kbps)          LOM[0]:         1
       BC[1]:      30000 (kbps)          LOM[1]:         1
       BC[2]:      20000 (kbps)          LOM[2]:         1
       BC[3]:          0 (kbps)          LOM[3]:         1
       BC[4]:          0 (kbps)          LOM[4]:         1
       BC[5]:          0 (kbps)          LOM[5]:         1
       BC[6]:          0 (kbps)          LOM[6]:         1
       BC[7]:          0 (kbps)          LOM[7]:         1
   BW Unreserved:
       Class  ID:
       [0]:          0 (kbps),           [1]:          0 (kbps)
       [2]:          0 (kbps),           [3]:          0 (kbps)
       [4]:          0 (kbps),           [5]:          0 (kbps)
       [6]:          0 (kbps),           [7]:          0 (kbps)
Router ID: 10.1.1.9
IGP Type: ISIS      Process ID: 1
 MPLS-TE Link Count: 2
 Link[1]:
   ISIS System ID: 0000.0000.0001.00      Opaque LSA ID: 0.0.0.0
   Interface IP Address: 172.16.1.1
   DR Address: 172.16.1.1
   DR ISIS System ID: 0000.0000.0001.01
   IGP Area: Level-2
   Link  Type: Multi-access  Link Status: Active
   IGP Metric: 10              TE Metric: 10          Color: 0x0
   Bandwidth Allocation Model : Russian Dolls Model
   Maximum Link Bandwidth: 40000 (kbps)
   Maximum Reservable Bandwidth: 40000 (kbps)
   Bandwidth Constraints:        Local Overbooking Multiplier:
       BC[0]:      40000 (kbps)          LOM[0]:         1
       BC[1]:      30000 (kbps)          LOM[1]:         1
       BC[2]:      20000 (kbps)          LOM[2]:         1
       BC[3]:          0 (kbps)          LOM[3]:         1
       BC[4]:          0 (kbps)          LOM[4]:         1
       BC[5]:          0 (kbps)          LOM[5]:         1
       BC[6]:          0 (kbps)          LOM[6]:         1
       BC[7]:          0 (kbps)          LOM[7]:         1
   BW Unreserved:
       Class  ID:
       [0]:          0 (kbps),           [1]:          0 (kbps)
       [2]:          0 (kbps),           [3]:          0 (kbps)
       [4]:          0 (kbps),           [5]:          0 (kbps)
       [6]:          0 (kbps),           [7]:          0 (kbps)
```

Table 9-79 Description of the display mpls te cspf tedb node command output

Item	Description
Router ID	Router ID in the format X.X.X.X.
IGP Type	IGP type: ● OSPF ● IS-IS
Process ID	IGP Process ID.

Item	Description
MPLS-TE Link Count	Number of MPLS TE link.
OSPF Router ID	OSPF Route ID.
ISIS System ID	IS-IS system ID.
Interface IP Address	Interface IP address.
DR Address	DR address.
DR ISIS System ID	IS-IS system ID of the DR.
IGP Area	IGP area.
Link Type	Link type.
Link Status	Link status.
Link [x]	Link information, with "x" being the link number.
IGP Metric	IGP metric of a link.
TE Metric	TE metric of a link.
Color	Color of a link.
Maximum Link Bandwidth	Maximum bandwidth of a link.
Maximum Reservable Bandwidth	Maximum capacity of reserved bandwidth for a link.
Bandwidth Allocation Model	Bandwidth allocation model.
Bandwidth Constraints	Bandwidth constraints.
Local Overbooking Multiplier	Local overbooking multiplier.
BC	Bandwidth constraints.
LOM	Local overbooking multiplier.
BW Unreserved	Unreserved bandwidth for LSPs.
Class ID: [x]:	Class 0 to Class 7.

# Display information about overloaded nodes in a TEDB.

```
<HUAWEI> display mpls te cspf tedb overload-node
Current Total Overload Node Number : 4
ID    Router-ID    IGP    Process-ID   Area      IGP_ID
1     10.3.3.3     ISIS   1            Level-1   3333.3333.3333.00
2     10.1.1.1     ISIS   1            Level-1   1111.1111.1111.00
3     10.1.1.1     ISIS   2            Level-1   1111.1111.1112.00
4     10.2.2.2     ISIS   1            Level-1   2222.2222.2222.00
```

Table 9-80 Description of the display mpls te cspf tedb overload-node command output

Item	Description
ID	Sequence number.
Router-ID	Router ID in dotted decimal notation.
IGP	IGP type: ● OSPF ● IS-IS
Process-ID	IGP Process ID.
Area	Area to which a device belongs.
IGP_ID	● OSPF router ID of a neighbor device. ● IS-IS system ID of a neighbor device.

9.3.35 display mpls te hot-standby state

Function

The **display mpls te hot-standby state** command displays the hot-standby status of all tunnels or a specified tunnel.

Format

display mpls te hot-standby state { **all** [**verbose**] | **interface tunnel** *interface-number* }

Parameters

Parameter	Description	Value
all	Displays the status of all hot-standby tunnels.	-
verbose	Displays detailed information about hot-standby tunnels.	-
interface tunnel *interface-number*	Displays the status of a specified hot-standby tunnel.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When running the **display mpls te hot-standby state** command, note the following issues:

- The command displays the status of only hot-standby TE tunnels.
- If a tunnel interface is deleted or traffic switches from the tunnel to an ordinary backup tunnel, no command output is displayed.

Example

# Display the hot-standby status of Tunnel 1.

```
<HUAWEI> display mpls te hot-standby state interface tunnel 1
(s): same path
----------------------------------------------------------------------
Verbose information about the Tunnel1 hot-standby state
----------------------------------------------------------------------
session id                         : 300
main LSP token                       : 0x9
hot-standby LSP token                  : 0x0
HSB switch result                    : Primary LSP
HSB switch reason                     : -
WTR config time                       : 10s
WTR remain time                        : -
using overlapped path                   : -
```

Table 9-81 Description of the display mpls te hot-standby state command output

Item	Description
session id	Session ID, which is the configured tunnel ID.
main LSP token	Index of the primary CR-LSP.
hot-standby LSP token	Index of the hot-standby CR-LSP.
HSB switch result	Result of a switchover: ● Primary LSP: indicates that data is switched to the primary CR-LSP. ● Hot-standby LSP: indicates that data is switched to the hot-standby CR-LSP. ● Ordinary LSP: indicates that data is switched to the ordinary CR-LSP. ● Best-Effort LSP: indicates that data is switched to the best-effort path.
HSB switch reason	Reason why traffic is switched to the hot-standby LSP.

Item	Description
WTR config time	WTR time. If a primary CR-LSP recovers from a fault, the system waits for a period of time, or the WTR time, to switch data from the hot-standby CR-LSP or best-effort path to the primary LSP.
WTR remain time	WTR remain time.
using overlapped path	Whether the path of the primary tunnel and the path of the backup tunnel overlap: ● yes: indicates that they overlap. ● no: indicates that they do not overlap. ● -: indicates that the system does not check whether they overlap.

# Display the hot-standby status of all hot-standby tunnels.

```
<HUAWEI> display mpls te hot-standby state all
(s): same path
------------------------------------------------------------------------------
No.       tunnel name        session id      switch result       overlap
------------------------------------------------------------------------------
1         Tunnel1            3               Best-Effort LSP     -
2         Tunnel2            9               Primary LSP         -
```

Table 9-82 Description of the display mpls te hot-standby state all command output

Item	Description
No.	Sequence number.
tunnel name	Name of a tunnel.
session id	Session ID, which is the configured tunnel ID.
switch result	Result of a switchover: ● Primary LSP: indicates that data is switched to the primary CR-LSP. ● Hot-standby LSP: indicates that data is switched to the hot-standby CR-LSP. ● Ordinary LSP: indicates that data is switched to the ordinary CR-LSP. ● Best-Effort LSP: indicates that data is switched to the best-effort path.

Item	Description
overlap	Whether the primary path overlaps the hot-standby path: - yes: They share one or multiple links. - no: They do not share links. - -: Their paths cannot be compared. - yse(s): They overlap each other.

9.3.36 display mpls te link-administration admission-control

Function

The **display mpls te link-administration admission-control** command displays CR-LSP information received by all links, including bandwidth and priority.

Format

display mpls te link-administration admission-control [**interface** *interface-type interface-number* | **stale-interface** *interface-index*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about admission control of a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
stale-interface *interface-index*	Displays information about admission control of a stale interface. *interface-index* specifies the index of the stale interface.	The value is a hexadecimal integer that ranges from 1 to FFFFFFFE.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mpls stale-interface** command without specifying any parameter to view the index of a stale interface.

Example

# Display information about the admission control of all MPLS TE links.

```
<HUAWEI> display mpls te link-administration admission-control
LspID                    In/Out IF                    S/H Prio CT BW(kbps)
10.3.3.9:300:4             Vlanif10 / ---                 7 /7     -  -
```

# Display information about admission control of a stale interface.

```
<HUAWEI> display mpls te link-administration admission-control stale-interface 18000106
LspID                    In/Out IF              S/H Prio  CT        BW (kbps)
10.1.1.1:600:1          --- / 0x18000106           0 /0      0         0
```

Table 9-83 Description of the display mpls te link-administration admission-control command output

Item	Description
LspID	LSP ID, uniquely identified in the form of <Ingress-LSR-ID:Tunnel-ID:Local-LSP-ID>.
In/Out IF	Incoming and outgoing interfaces.
S/H Prio	Setup and holding priorities. Setup priority: An integer ranging from 0 to 7. The smaller the value, the higher the priority. Holding priority: An integer ranging from 0 to 7. The smaller the value, the higher the priority.
CT	Class type.
BW	Bandwidth.

9.3.37 display mpls te link-administration bandwidth-allocation

Function

The **display mpls te link-administration bandwidth-allocation** command displays information about bandwidth allocation of a specified MPLS TE interface or all MPLS TE interfaces.

Format

display mpls te link-administration bandwidth-allocation [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about bandwidth allocation of a specified interface. ● *interface-type*: indicates the interface type. ● *interface-number*: indicates the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the information about bandwidth allocation of the MPLS TE interfaces, run the **display mpls te link-administration bandwidth-allocation** command.

Example

# Display information about the bandwidth allocation of all MPLS TE interfaces.

```
<HUAWEI> display mpls te link-administration bandwidth-allocation
  Link ID:  Vlanif10
  Bandwidth Constraint Model   :  Russian Dolls Model (RDM)
  Physical Link Bandwidth(Kbits/sec)          :  1000000
  Maximum Link Reservable Bandwidth(Kbits/sec):  1000000
  Reservable Bandwidth BC0(Kbits/sec)         :  500000
  Reservable Bandwidth BC1(Kbits/sec)         :  4000
  Downstream Bandwidth (Kbits/sec)            :  0
  IPUpdown Link Status                        :  UP
  PhysicalUpdown Link Status                  :  UP
  GracefulUpdown Link Status                  :  DOWN
  ----------------------------------------------------------------------
  TE-CLASS  CT    PRIORITY   BW RESERVED   BW AVAILABLE   DOWNSTREAM
                             (Kbit/sec)     (Kbit/sec) RSVPLSPNODE COUNT
  ----------------------------------------------------------------------
     0      0       0          0           500000         0
     1      0       1          0           500000         0
     2      0       2          0           500000         0
     3      0       3          0           500000         0
     4      0       4          0           500000         0
     5      0       5          0           500000         0
     6      0       6          0           500000         0
     7      0       7          0           500000         0
     8      1       0          0           4000           0
     9      1       1          0           4000           0
    10      1       2          0           4000           0
    11      1       3          0           4000           0
    12     1        4           0            4000            0
    13     1        5           0            4000            0
    14     1        6           0            4000            0
    15     1        7           0            4000            0

----------------------------------------------------------------------


  Link ID:  GigabitEthernet0/0/1
  Bandwidth Constraint Model   :  Russian Dolls Model (RDM)
  Physical Link Bandwidth(Kbits/sec)          :  1000000
  Maximum Link Reservable Bandwidth(Kbits/sec):  1000000
  Reservable Bandwidth BC0(Kbits/sec)         :  500000
  Reservable Bandwidth BC1(Kbits/sec)         :  4000
  Downstream Bandwidth (Kbits/sec)            :  0
  IPUpdown Link Status                        :  UP
  PhysicalUpdown Link Status                  :  UP
  GracefulUpdown Link Status                  :  DOWN
  ----------------------------------------------------------------------
  TE-CLASS  CT    PRIORITY   BW RESERVED    BW AVAILABLE   DOWNSTREAM
                              (Kbit/sec)      (Kbit/sec)  RSVPLSPNODE COUNT
  ----------------------------------------------------------------------
     0      0       0          0           500000          0
     1      0       1          0           500000          0
     2      0       2          0           500000          0
     3      0       3          0           500000          0
     4      0       4          0           500000          0
     5      0       5          0           500000          0
     6      0       6          0           500000          0
     7      0       7          0           500000          0
     8      1       0          0           4000            0
     9      1       1          0           4000            0
    10      1       2          0            4000           0
    11      1       3          0            4000           0
    12      1       4          0            4000           0
    13      1       5          0            4000           0
    14      1       6          0            4000           0
    15      1       7          0            4000           0
  ----------------------------------------------------------------------
```

Table 9-84 Description of the display mpls te link-administration bandwidth-allocation command output

Item	Description
Link ID	MPLS TE interface number.
Bandwidth Constraint Model	Bandwidth Constraints Model used by a TE tunnel: ● RDM: Russian Dolls Model ● MAM: Maximum Allocation Model ● Extended MAM: Extended Maximum Allocation Model
Physical Link Bandwidth(Kbits/sec)	Indicates the capacity of bandwidth for a physical link.

Item	Description
Maximum Link Reservable Bandwidth(Kbits/sec)	Maximum capacity of reserved bandwidth for a link. To set the maximum capacity of reserved bandwidth for a link, run the **mpls te bandwidth max-reservable-bandwidth** command.
Reservable Bandwidth BCi(0≤i≤7) (Kbits/sec)	Bandwidth that is reserved for BCi. To set the bandwidth that is reserved for BCi, run the **mpls te bandwidth** command.
Downstream Bandwidth (Kbits/ sec)	Bandwidth of an outgoing interface.
IPUpdown Link Status	IP link status of an interface: ● UP: IP link is available. ● DOWN: IP link is unavailable.
PhysicalUpdown Link Status	Physical link status of an interface: ● UP: The physical link is available. ● DOWN: The physical link is unavailable.
GracefulUpdown Link Status	Graceful link status of an interface: ● UP: The graceful link is available. ● DOWN: The graceful link is unavailable.
TE-CLASS	TE class.
CT	Class type.
PRIORITY	Preemption priority of an MPLS TE tunnel. To set the preemption priority of an MPLS TE tunnel, run the **mpls te priority** command.
BW RESERVED (Kbit/sec)	Reserved bandwidth for LSPs of the CT.
BW AVAILABLE (Kbit/sec)	Available bandwidth for LSPs of the CT.
DOWNSTREAM RSVPLSPNODE COUNT	Number of downstream RSVP LSP nodes.

9.3.38 display mpls te link-administration srlg-information

Function

The **display mpls te link-administration srlg-information** command displays SRLG(s) to which the interface belongs.

Format

display mpls te link-administration srlg-information [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring the SRLG in the interface view, you can run the **display mpls te link-administration srlg-information** command to check the configuration.

Example

# Display the SLRG(s) to which VLANIF100 belongs to.

```
<HUAWEI> display mpls te link-administration srlg-information interface vlanif100

 SRLGs on Vlanif100 :
         2          3          9
```

Table 9-85 Description of the display mpls te link-administration srlg-information command output

Item	Description
SRLGs on Vlanif100	SRLG number to which an interface belongs.

9.3.39 display mpls te protection binding protect-tunnel

Function

The **display mpls te protection binding protect-tunnel** command displays the tunnel protection relationship.

Format

display mpls te protection binding protect-tunnel { *tunnel-id* | **interface tunnel** *interface-number* }

Parameters

Parameter	Description	Value
tunnel-id	Displays information about the protection relationship related to a protection tunnel (that is, a backup tunnel) with a specified ID.	The value is an integer that ranges from 1 to 10000.
tunnel *interface-number*	Displays information about the protection relationship related to the specified tunnel interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the tunnel protection relationship, run the **display mpls te protection binding protect-tunnel** command.

Example

# Display the protection relationship related to the protection tunnel with the ID of 10.

```
<HUAWEI> display mpls te protection binding protect-tunnel 10
------------------------------------------------------------------------
Binding information of( tunnel id:  10 )
------------------------------------------------------------------------
    Protect-tunnel id                    :10
    Protect-tunnel name                  :Tunnel1
    Maximum number of bound work-tunnels :16
    Currently bound work-tunnels         :Total( 1 )
                                          :Tunnel2
```

Table 9-86 Description of the display mpls te protection binding protect-tunnel command output

Item	Description
Protect-tunnel id	ID of a protection tunnel (the backup tunnel).
Protect-tunnel name	Name of a protection tunnel (the interface name).

Item	Description
Maximum number of bound work-tunnels	Maximum number of tunnels that a protection tunnel can protect.
Currently bound work-tunnels	Information about the working tunnel to which a protection tunnel is currently bound, including the quantity and list.

9.3.40 display mpls te protection tunnel

Function

The **display mpls te protection tunnel** command displays information about a specified tunnel and its tunnel protection group.

Format

display mpls te protection tunnel { **all** | *tunnel-id* | **interface tunnel** *interface-number* } [**verbose**]

Parameters

Parameter	Description	Value
all	Displays information about all tunnel protection groups.	-
tunnel-id	Specifies the ID of a working tunnel or its protection tunnel.	The value is an integer that ranges from 1 to 10000.
interface	Displays information about tunnel protection groups on an interface.	-
tunnel *interface-number*	Specifies the name of a working tunnel or its protection tunnel.	-
verbose	Displays detailed information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls te protection tunnel** command can be used to display information about a specified tunnel protection group. The following parameters can be specified to display various types of information:

- If the ID or tunnel interface of the working tunnel is specified, information about the working tunnel and its protection tunnel is displayed.
- If the ID or tunnel interface of a protection tunnel is specified, information about the protection tunnel and all its protected working tunnels is displayed.

Example

# Display information about a working tunnel with the tunnel ID of 100 and its protection tunnel.

```
<HUAWEI> display mpls te protection tunnel 100
------------------------------------------------------------------------
No. Work-tunnel status  /id  Protect-tunnel status /id    Switch-Result
------------------------------------------------------------------------
1          in defect   /100        non-defect     /300  protect-tunnel
```

Table 9-87 Description of the display mpls te protection tunnel command output

Item	Description
No.	Sequence number of a tunnel protection group.
Work-tunnel status /id	Status and ID of a working tunnel. The tunnel status can be: ● non-defect: The tunnel functions properly. ● in defect: The tunnel fails.
Protect-tunnel status /id	Status and ID of a protection tunnel. The tunnel status can be: ● non-defect: The tunnel functions properly. ● in defect: The tunnel fails.
Switch-Result	Switching result: ● work-tunnel: Traffic switches to the working tunnel. ● protect-tunnel: Traffic switches to the protection tunnel.

# Display detailed information about working tunnels and their protection tunnels.

```
<HUAWEI> display mpls te protection tunnel all verbose
----------------------------------------------------------------
Verbose information about the No.1 protection-group
-----------------------------------------------------------------
Work-tunnel id                        : 1
Protect-tunnel id                     : 2
```

```
Work-tunnel name                         : Tunnel1
Protect-tunnel name                      : Tunnel2
Work-tunnel reverse-lsp                  : -
Protect-tunnel reverse-lsp               : -
Bridge type                              : 1:1
Switch type                              : unidirectional
Switch result                            : work-tunnel
Tunnel using Best-Effort                 : none
Tunnel using Ordinary                    : none
Work-tunnel frr in use                   : none
Work-tunnel defect state                 : non-defect
Protect-tunnel defect state              : non-defect
Work-tunnel forward-lsp defect state     : non-defect
Protect-tunnel forward-lsp defect state  : non-defect
Work-tunnel reverse-lsp defect state     : non-defect
Protect-tunnel reverse-lsp defect state  : non-defect
HoldOff config time                      : 0ms
HoldOff remain time                      : -
WTR config time                          : 30s
WTR remain time                          : -
Mode                                     : revertive
Using same path                          : -
Local state                              : no request
Far end request                          : no request
```

Table 9-88 Description of the display mpls te protection tunnel all verbose command output

Item	Description
Work-tunnel id	ID of the working tunnel.
Protect-tunnel id	ID of the protection tunnel.
Work-tunnel name	Tunnel interface name of the working tunnel.
Protect-tunnel name	Tunnel interface name of the protection tunnel.
Work-tunnel reverse-lsp	Name of the reverse CR-LSP in the working tunnel.
Protect-tunnel reverse-lsp	Name of the reverse CR-LSP in the protection tunnel.
Bridge type	Bridge mode.
Switch type	Switch mode.
Switch result	Switching result: ● work-tunnel: Traffic switches to the working tunnel. ● protect-tunnel: Traffic switches to the protection tunnel.
Tunnel using Best-Effort	Whether a best-effort path is used as a protection tunnel.
Tunnel using Ordinary	Whether an ordinary backup tunnel is used as a protection tunnel.

Item	Description
Work-tunnel frr in use	Whether the working tunnel is in the FRR in-use state.
Work-tunnel defect state	Working tunnel status: ● non-defect: The working tunnel functions properly. ● in defect: The working tunnel fails.
Protect-tunnel defect state	Protection tunnel status: ● non-defect: The protection tunnel functions properly. ● in defect: The protection tunnel fails.
Work-tunnel forward-lsp defect state	Status of the forward CR-LSP in the working tunnel: ● non-defect: The forward CR-LSP functions properly. ● in defect: The forward CR-LSP fails.
Protect-tunnel forward-lsp defect state	Status of the forward CR-LSP in the protection tunnel: ● non-defect: The forward CR-LSP functions properly. ● in defect: The forward CR-LSP fails.
Work-tunnel reverse-lsp defect state	Status of the reverse CR-LSP in the working tunnel: ● non-defect: The reverse CR-LSP functions properly. ● in defect: The reverse CR-LSP fails.
Protect-tunnel reverse-lsp defect state	Status of the reverse CR-LSP in the protection tunnel: ● non-defect: The reverse CR-LSP functions properly. ● in defect: The reverse CR-LSP fails.
HoldOff config time	Switching delay time. To set the switching delay time, run the **mpls te protection tunnel** command.
HoldOff remain time	Remain time of switching delay time.
WTR config time	Wait-to-restore time. To set the wait-to-restore time, run the **mpls te protection tunnel** command.
WTR remain time	Remain time of wait-to-restore time.

Item	Description
Mode	Switchback mode: ● revertive: supports a switchback. ● non-revertive: does not support a switchback. To set the switchback mode, run the **mpls te protection tunnel** command.
Using same path	Whether a path of the working tunnel and a path of the protection tunnel overlap: ● yes: The two tunnels have an overlapped path. ● no: The two tunnels do not have an overlapped path. ● -: Undetected.
Local state	Switching mode on the local end: ● signal fail for protection ● no request
Far end request	Switching mode on the remote end.

9.3.41 display mpls te session-entry

Function

The **display mpls te session-entry** command displays detailed information about LSP sessions of tunnels.

Format

display mpls te session-entry [*ingress-lsr-id tunnel-id egress-lsr-id*]

Parameters

Parameter	Description	Value
ingress-lsr-id	Specifies the LSR ID of the ingress.	In dotted decimal notation.
tunnel-id	Specifies the ID of a tunnel.	The value is an integer that ranges from 0 to 65535.
egress-lsr-id	Specifies the LSR ID of the egress.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view detailed information about LSP sessions of tunnels, run the **display mpls te session-entry** command.

Example

# Display detailed information about LSP sessions of a tunnel.

```
<HUAWEI> display mpls te session-entry

 Ingress-ID                :  1.1.1.9
 Tunnel-ID                 :  300
 Egress-ID                 :  3.3.3.9
 Crlsp num                 :  1
 First TunnelTable index   :  4
 LSP No.     :  1
 LSP ID      :  1.1.1.9:300:6
 In/Out IF   :  -/Vlanif10
 Bandwidth(Kbit/sec):
   CT0 : 500         CT1 : 0
```

Table 9-89 Description of the display mpls te session-entry command output

Item	Description
Ingress-ID	LSR ID of the ingress.
Tunnel-ID	Tunnel ID, which is the session ID.
Egress-ID	LSR ID of the egress.
Crlsp num	Number of CR-LSPs of the session entry.
First TunnelTable index	Index of the first CR-LSP of the session entry.
LSP No.	Sequence number of a CR-LSP.
LSP ID	LSP ID, uniquely identified in the form of <Ingress-LSR-ID:Tunnel-ID:Local-LSP-ID>.
In/Out IF	Incoming and outgoing interface through which the CR-LSP passes on the local node.
Bandwidth(Kbit/sec)	Bandwidth, in kbit/s.
CT0	Bandwidth value of CR-LSPs of CT0.
CT1	Bandwidth value of CR-LSPs of CT1.

9.3.42 display mpls te srlg

Function

The **display mpls te srlg** command displays the Shared Risk Link Group (SRLG) configurations and the interfaces that belong to it.

Format

display mpls te srlg { *srlg-number* | **all** }

Parameters

Parameter	Description	Value
srlg-number	Specifies the number of the SRLG to which an interface belongs.	The value is an integer that ranges from 0 to 4294967295.
all	Displays information about all SRLGs on the node and the interfaces that belong to the SRLG groups.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the configuring the SRLG on an interface, you can run the **display mpls te srlg** command to check the configuration.

The **display mpls te srlg** command displays the following information:

- Maximum of SRLGs that a node can support
- Number of SRLGs that are configured on the node
- Member interfaces of each SRLG

Example

# Display information about all SRLGs on the node.

```
<HUAWEI> display mpls te srlg all
Total SRLG supported : 1024
Total SRLG configured : 1
SRLG  239:           Vlanif30
```

Table 9-90 Description of the display mpls te srlg all command output

Item	Description
Total SRLG supported	Total SRLGs supported.
Total SRLG configured	Total SRLGs configured.
SRLG	Shared risk link group. To set the shared risk link group, run the **mpls te srlg** command.

9.3.43 display mpls te tunnel-interface

Function

The **display mpls te tunnel-interface** command displays information about tunnel interfaces on the local LSR.

Format

display mpls te tunnel-interface [**tunnel** *interface-number* | **auto-bypass-tunnel** [*tunnel-name*]]

Parameters

Parameter	Description	Value
tunnel *interface-number*	Specifies the number of a tunnel interface on the local LSR.	-
auto-bypass-tunnel *tunnel-name*	Specifies the name of an MPLS TE tunnel. If the *tunnel-name* parameter is configured, information about the specified Auto bypass tunnel is displayed. If this parameter is not configured, information about all Auto bypass tunnels is displayed.	The value is an existing tunnel name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you do not specify any parameters, information about all tunnel interfaces is displayed.

Example

# Display information about Tunnel 1.

```
<HUAWEI> display mpls te tunnel-interface tunnel 1
    ----------------------------------------------------------------
                          Tunnel1
    ----------------------------------------------------------------
    Tunnel State Desc   :  GRACEFUL SWITCH
    Active LSP          :  Best-Effort LSP
    Traffic Switch      :  Best-Effort LSP -> Ordinary LSP
    Session ID          :  50
    Ingress LSR ID      :  1.1.1.1          Egress LSR ID:  2.2.2.2
    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  : 32799
      Modify LSP State     : SETTING UP
    Ordinary LSP State     : UP
      Main LSP State       : READY              LSP ID  : 32782
    Best-Effort LSP State  : UP
      Main LSP State       : READY              LSP ID  : 32780
```

Table 9-91 Description of the display mpls te tunnel-interface command output

Item	Description
Tunnel State Desc	Tunnel status: ● UP: indicates that the tunnel is successfully set up. ● DOWN: indicates that the tunnel fails to be set up. ● GRACEFUL SWITCH: indicates that the tunnels are switched through GR. ● GRACEFUL DELETE: indicates that during the GR process a type of LSP is deleted.
Active LSP	Type of CR-LSP in use: ● Primary LSP: indicates the primary CR-LSP. ● Hot-Standby LSP: indicates the hot-standby CR-LSP. ● Ordinary LSP: indicates the ordinary backup CR-LSP. ● Best-Effort LSP: indicates the best-effort path.
Traffic Switch	Traffic switching status.
Session ID	Session ID of a CR-LSP.
Ingress LSR ID	LSR ID of the ingress.
Egress LSR ID	LSR ID of the egress.
Admin State	Administrative status.
Oper State	Operating status.

Item	Description
Primary LSP State	Status of a primary CR-LSP: ● UP: indicates that the primary CR-LSP is successfully set up. ● DOWN: indicates that no primary CR-LSP is set up. ● GRACEFUL SWITCH: indicates that the primary CR-LSP is being switched to the Modified CR-LSP. ● GRACEFUL DELETE: indicates that during the GR process, the primary CR-LSP is deleted.
Main LSP State	Status of the primary CR-LSP: ● READY: indicates that the primary CR-LSP is successfully set up. ● SETTING UP: indicates that the primary CR-LSP is being set up.
Hot-Standby LSP State	Status of a hot-standby CR-LSP: ● UP: indicates that a hot-standby CR-LSP is successfully set up. ● DOWN: indicates that no hot-standby CR-LSP is set up. ● GRACEFUL SWITCH: indicates that the primary CR-LSP is being switched to the Modified CR-LSP. ● GRACEFUL DELETE: indicates that during the GR process, the primary CR-LSP is deleted.
Modify LSP State	Status of a modified CR-LSP: ● READY: indicates that the Modified CR-LSP is successfully set up. ● SETTING UP: indicates that the Modified CR-LSP is being set up.
Ordinary LSP State	Status of an ordinary backup CR-LSP: ● UP: indicates that the ordinary backup CR-LSP is successfully set up. ● DOWN: indicates that no ordinary backup CR-LSP is set up. ● GRACEFUL SWITCH: indicates that the main CR-LSP is being switched to the modified CR-LSP. ● GRACEFUL DELETE: indicates that during the GR process, the main CR-LSP is deleted.

Item	Description
Best-Effort LSP State	Status of a best-effort path: ● UP: indicates that the best-effort path is successfully set up. ● DOWN: indicates that no best-effort path is set up. ● GRACEFUL SWITCH: indicates that the main CR-LSP is being switched to the Modified CR-LSP. ● GRACEFUL DELETE: indicates that during the GR process, the main CR-LSP is deleted.
LSP ID	LSP ID.

9.3.44 display mpls te tunnel-interface failed

Function

The **display mpls te tunnel-interface failed** command displays the MPLS TE tunnels that fail to be set up or that are being set up.

Format

display mpls te tunnel-interface failed

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring multiple MPLS TE tunnels, you can use the **display mpls te tunnel-interface failed** command to check whether there are any tunnels that fail to be set up or are still being set up.

Example

# Display the MPLS TE tunnels that fail to be set up or that are being set up.

```
<HUAWEI> display mpls te tunnel-interface failed
  Tunnel name       SessionId       State Desc
  ----------------------------------------------------------
  Tunnel1           39              DOWN
```

Table 9-92 Description of the display mpls te tunnel-interface failed command output

Item	Description
Tunnel name	Name of a tunnel interface.
SessionId	Session ID, which is the tunnel ID.
State Desc	Description of the tunnel status: ● UP: The tunnel is in Up state. ● DOWN: The tunnel is in Down state.

9.3.45 display mpls te tunnel-interface last-error

Function

The **display mpls te tunnel-interface last-error** command displays the last errors of a tunnel interface on the local node.

Format

display mpls te tunnel-interface last-error [*tunnel-name*]

Parameters

Parameter	Description	Value
tunnel-name	Displays the last errors of a specified tunnel interface.	The value is an existing tunnel name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display mpls te tunnel-interface last-error** command on the ingress to view the error of a local node or the error carried in an RSVP PathErr message sent by a downstream node. The errors can be as follows:

- CSPF computation fails.
- RSVP times out.

- One or more LSPs are deleted during RSVP GR smooth.
- One or more LSPs are deleted during RSVP aging.
- RSVP GR fails to be triggered.

Precautions

The **display mpls te tunnel-interface last-error** command shows the last 20 recorded errors of each TE tunnel and LSP on which the errors occur, including errors about the primary CR-LSP, modified LSP, and backup CR-LSP.

If an RSVP PathErr message sent by a downstream node carries the error information, the ErroInfo field in the command output shows the IP address of the faulty downstream node and the cause of the error. If an error occurs on the ingress, the command output only shows the cause of the error.

Example

# Display information about the last errors of Tunnel1.

```
<HUAWEI> display mpls te tunnel-interface last-error Tunnel1
  Tunnel name: Tunnel1


    Error No.  : 1
    LSP Type   : Hot-Standby LSP              LSP ID     : 10.1.1.9:300:32776
    Error Code : 0x3e8                     Occur Time : 2013/01/07 14:42:23+00:00
    Error Info : Link 172.20.1.2 is excluded, IGP: ISIS Process-ID: 1 Area: Level
-1.

    Error No.  : 2
    LSP Type   : Primary LSP                  LSP ID     : 10.1.1.9:300:1
    Error Code : 0x5080007                   Occur Time : 2013/01/07 11:13:45+00:00
    Error Info : error node = 172.16.1.1    error lsrid = 10.1.1.9
                 BKGD error SHUTDOWN IF

    Error No.  : 3
    LSP Type   : Primary LSP                  LSP ID     : 10.1.1.9:300:1
    Error Code : 0x3e8                     Occur Time : 2013/01/07 09:55:06+00:00
    Error Info : Cannot find the same IGP type and process ID for 10.1.1.9 and 17
10.1.1.2 (inter area scenario).

    Error No.  : 4
    LSP Type   : Primary LSP                  LSP ID     : 10.1.1.9:300:1
    Error Code : 0x3e8                     Occur Time : 2013/01/07 09:43:06+00:00
    Error Info : Cspf failed to calculate a path for Tunnel.

    Error No.  : 5
    LSP Type   : Primary LSP                  LSP ID     : 10.1.1.9:300:1
    Error Code : 0x3e8                     Occur Time : 2013/01/07 08:43:06+00:00
    Error Info:  error node = 172.16.1.1    error lsrid = 10.1.1.9
    Routing Problem: No route available toward destination.

    Error No.  : 6
    LSP Type   : Primary LSP                  LSP ID     : 10.1.1.9:300:1
    Error Code : 0x180001                     Occur Time : 2013/01/07 07:47:19+00:00
    Error Info : error node = 172.16.1.2    error lsrid = 0.0.0.0
                 Routing Problem Bad EXPLICIT_ROUTE object

    Error No.  : 7
    LSP Type   : Primary LSP                  LSP ID     : 10.1.1.9:300:1
    Error Code : 0x5080002                   Occur Time : 2013/01/6 20:03:05+00:00
    Error Info : error node = 0.0.0.0    error lsrid = 10.1.1.9
                 BKGD error TEAR ALL LSP
```

Table 9-93 Description of the display mpls te tunnel-interface last-error command output

Item	Description
Tunnel name	Name of an MPLS TE tunnel.
Error No	Number of errors.
LSP Type	Type of LSP: ● Modified LSP: indicates the LSP which is in modified state. ● Primary LSP: indicates the primary LSP. ● Backup LSP: indicates the backup LSP. ● Hot-Standby LSP: indicates the hot-standby LSP.
LSP ID	LSP ID, uniquely identified in the form of Ingress-LSR-ID:Tunnel-ID:Local-LSP-ID.
Error Code	Returned code, which specifies a unique type of error. The value is an integer in hexadecimal notation. For specific error information, see the **Error Info** field.
Occur Time	Time when an error occurred.
Error Info	Error description.
error node	Node on which an error occurs.
error lsrid	LSR ID of the node on which an error occurred.
Routing Problem	Error information carried in a received RSVP PathErr message: No route available toward destination: indicates that no route to the destination address of the tunnel is available. Bad EXPLICIT_ROUTE object: indicates that an unknown EXPLICIT_ROUTE object is received. bad strict node: indicates that a certain node cannot be found on the strict explicit path.
Cspf failed to calculate a path for Tunnel	CSPF computation failure.

9.3.46 display mpls te tunnel-interface lsp-constraint

Function

The **display mpls te tunnel-interface lsp-constraint** command displays information about the CR-LSP attribute template on an MPLS TE tunnel interface.

Format

display mpls te tunnel-interface lsp-constraint [**tunnel** *interface-number*]

Parameters

Parameter	Description	Value
tunnel *interface-number*	Specifies information about the CR-LSP attribute template on a specified MPLS TE tunnel interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the information about the CR-LSP attribute template on an MPLS TE tunnel interface, run the **display mpls te tunnel-interface lsp-constraint** command.

Example

# Display information about the CR-LSP attribute template on all MPLS TE tunnel interfaces.

```
<HUAWEI> display mpls te tunnel-interface lsp-constraint
   Tunnel Name                       :  Tunnel1
   Primary-lsp-constraint Name      :  p1
   Hotstandby-lsp-constraint Number:  2
   Hotstandby-lsp-constraint Name  :  p1
   Ordinary-lsp-constraint Number  :  2
   Ordinary-lsp-constraint Name     :  p1
```

Table 9-94 Description of the display mpls te tunnel-interface lsp-constraint command output

Item	Description
Tunnel Name	Name of a tunnel.

Item	Description
Primary-lsp-constraint Name	Name of a CR-LSP attribute template.
Hotstandby-lsp-constraint Number	Number of the hot-standby CR-LSP attribute template, which indicates the sequence in which the template is used. To set the number of the hot-standby CR-LSP attribute template, run the **mpls te hotstandby-lsp-constraint** command.
Hotstandby-lsp-constraint Name	Name of a hot-standby CR-LSP attribute template. To set the name of a hot-standby CR-LSP attribute template, run the **mpls te hotstandby-lsp-constraint** command.
Ordinary-lsp-constraint Number	Number of the ordinary CR-LSP attribute template, which indicates the sequence in which the template is used. To set the number of the ordinary CR-LSP attribute template, run the **mpls te ordinary-lsp-constraint** command.
Ordinary-lsp-constraint Name	Name of an ordinary CR-LSP attribute template. To set the name of an ordinary CR-LSP attribute template, run the **mpls te ordinary-lsp-constraint** command.

9.3.47 display mpls te tunnel-interface traffic-state

Function

The **display mpls te tunnel-interface traffic-state** command displays information about the traffic on the tunnel interface of the local LSR.

Format

display mpls te tunnel-interface traffic-state [*tunnel-name*]

Parameters

Parameter	Description	Value
tunnel-name	Specifies a tunnel name.	The value is an existing tunnel name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the traffic protection mode, traffic state, and traffic switchover reasons of a tunnel interface on a local LSR, run the **display mpls te tunnel-interface traffic-state** command.

Example

# Display information about the traffic on the tunnel interface of the local LSR.

```
<HUAWEI> display mpls te tunnel-interface traffic-state
 Protect Config: HSB - Hot-Standby,       OBK - Ordinary Backup
                 FRR - Fast Reroute,      BBK - Best-Effort Backup
                 PS  - Protection Switch

 -------------------------------------------------------------------------------
 Tunnel Interface    Protect Config   Traffic State          Switch Reason
 -------------------------------------------------------------------------------
 Tunnel1           OBK             Primary LSP            --
 Tunnel2           HSB             Primary LSP            Signal Fail
```

Table 9-95 Description of the display mpls te tunnel-interface traffic-state command output

Item	Description
Tunnel Interface	Tunnel interface name.
Protect Config	Protection modes. The protection modes are displayed using short names. If two protection modes are performed, both the two protection modes are displayed. ● HSB: indicates the hot standby. ● OBK: indicates ordinary backup. ● BBK: indicates the best-effort path. ● FRR: indicates FRR. ● PS: indicates the tunnel protection group.

Item	Description
Traffic State	Traffic protection state, including the following types: ● Hot-Standby LSP: Traffic is switched to the hot-standby LSP. ● Primary LSP FRR In Use: Traffic is on the primary LSP that is in the FRR in use state. ● Best-Effort LSP: Traffic is on the best-effort LSP. ● Ordinary LSP: Traffic is on the ordinary backup LSP. ● Protection Tunnel: Traffic is on the protection tunnel. ● Primary LSP: Traffic is on the primary LSP, and no switchover is performed.
Switch Reason	Reason why traffic is not on the primary LSP. If the traffic is on the primary LSP, or the traffic is on the primary LSP which is in the FRR in use state, this field is not displayed. If multiple reasons exist, only one reason with the highest priority is displayed. Following are the reasons listed in descending order of priorities: ● Manual Command: The user uses a command to enable a switchover. ● Signal Fail: The signaling protocol or detection protocol is Down. ● Signal Degrade: The detection protocol signal degrades. This field is also displayed when bit errors occur. ● Wait To Restore (WTR): The system waits for the WTR period to elapse and then switches traffic back to the primary LSP. ● Do Not Revertive: Traffic is not switched back to the primary LSP even if the primary LSP recovers.

9.3.48 display mpls te tunnel

Function

The **display mpls te tunnel** command displays information about an MPLS TE tunnel.

Format

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**]

display mpls te tunnel { **stale-incoming-interface** | **stale-interface** | **stale-outgoing-interface** } *interface-index* [**verbose**]

Parameters

Parameter	Description	Value
destination *ip-address*	Displays information about an MPLS TE tunnel with a specified destination address.	-
lsp-id	Displays information about an MPLS TE tunnel with a specified LSP ID.	-
ingress-lsr-id	Specifies the LSR ID of the ingress.	The value is in dotted decimal notation.
session-id	Specifies the ID of a session.	The value is an integer that ranges from 0 to 65535.
local-lsp-id	Specifies the local LSP ID.	The value is an integer that ranges from 0 to 65535.
lsr-role	Displays information about an MPLS TE tunnel according to the specified role of the local LSR.	-
all	Displays information of all MPLS TE tunnels.	-
egress	Displays information about an MPLS TE tunnel with the local LSR as the egress.	-
ingress	Displays information about an MPLS TE tunnel with the local LSR as the ingress.	-
remote	Displays information about an MPLS TE tunnel with the local LSR as the egress or the transit node.	-

Parameter	Description	Value
transit	Displays information about an MPLS TE tunnel with the local LSR as a transit node.	-
name *tunnel-name*	Displays the MPLS TE tunnel whose name is specified.	*tunnel-name* must be the name of an existing tunnel and its format, including the upper and lower casing, and blank spaces, must be consistent with that of the configuration file. For example, when the tunnel interface in a configuration file is named "interface Tunnel1", the tunnel name to be specified must also be Tunnel1. "tunnel1" or "Tunnel 1" is incorrect.
incoming-interface *interface-type interface-number*	Displays information about all MPLS TE tunnels with a specified incoming interface.	-
interface *interface-type interface-number*	Displays information about all MPLS TE tunnels with an outgoing or incoming interface of the specified type and number.	-
outgoing-interface *interface-type interface-number*	Displays information about all MPLS TE tunnels with a specified outgoing interface.	-
verbose	Displays detailed information.	-
stale-incoming-interface	Displays information about MPLS TE tunnels with a specified incoming interface in the stale state.	-
stale-interface	Displays information about MPLS TE tunnels on an interface in the stale state.	-

Parameter	Description	Value
stale-outgoing-interface	Displays information about MPLS TE tunnels with a specified outgoing interface in the stale state.	-
interface-index	Specifies the index of a specified stale interface.	The value is a hexadecimal integer that ranges from 1 to FFFFFFFE.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When **verbose** is configured, the command output varies with the signaling protocol used by the MPLS TE tunnel.

Example

# Display information about an MPLS TE tunnel.

```
<HUAWEI> display mpls te tunnel
------------------------------------------------------------------------------
Ingress LsrId    Destination      LSPID   In/Out Label     R  Tunnel-name
------------------------------------------------------------------------------
10.1.1.9         10.3.3.9         6       --/1027          I  Tunnel1
```

Table 9-96 Description of the display mpls te tunnel command output

Item	Description
Ingress LsrId	Ingress LSR ID.
Destination	Destination IP address.
LSPID	LSP ID of the ingress.
In/Out Label	Incoming and outgoing labels.
R	LSR role: ● I: Ingress ● T: Transit ● E: Egress
Tunnel-name	Tunnel name.

# Display information about the MPLS TE tunnel with the ingress IP address being 10.1.1.9 and the LSP ID being 1.

```
<HUAWEI> display mpls te tunnel lsp-id 10.1.1.9 1 1
-------------------------------------------------------------------------------
Ingress LsrId    Destination      LSPID   In/Out Label     R  Tunnel-name
-------------------------------------------------------------------------------
10.1.1.9         10.2.2.9         1       --/3             I  Tunnel1
```

# Display detailed information about an MPLS TE tunnel.

```
<HUAWEI> display mpls te tunnel verbose
    No                       :  1
    Tunnel-Name              :  LSRAtoLSRC
    Tunnel Interface Name    :  Tunnel1
    TunnelIndex              :  0            LSP Index          :  1024
    Session ID               :  100          LSP ID             :  1
    LSR Role                 :  Ingress      LSP Type           :  Primary
    Ingress LSR ID           :  10.1.1.1
    Egress LSR ID            :  10.2.2.2
    In-Interface             :  -
    Out-Interface            :  Vlanif10
    Sign-Protocol            :  Static CR    Resv Style         :
    IncludeAnyAff            :  0x0          ExcludeAnyAff      :  0x0
    IncludeAllAff            :  0x0
    LspConstraint            :  1
    ER-Hop Table Index       :  -            AR-Hop Table Index:  -
    C-Hop Table Index        :  -
    PrevTunnelIndexInSession:  -             NextTunnelIndexInSession:  -
    PSB Handle               :  0
    Created Time             :  2013/01/29 18:21:36+00:00
    RSVP LSP Type            :  -
    --------------------------------
             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           :  7            Hold-Priority      :  7
    --------------------------------
               FRR Information
    --------------------------------
    Primary LSP Info
    TE Attribute Flag        :  0x63         Protected Flag     : 0x0
    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)
    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          :  -
```

Table 9-97 Description of the display mpls te tunnel verbose command output

Item	Description
No	Number of an MPLS TE tunnel.
Tunnel-Name	Name of an MPLS TE tunnel.
Tunnel Interface Name	Interface name of an MPLS TE tunnel.
TunnelIndex	Index of an MPLS TE tunnel.
LSP Index	Index of an LSP.
Session ID	Session ID, which is the tunnel ID.
LSP ID	LSP ID.
LSR Role	Role of the LSR: ● Ingress: indicates the node is the ingress of the tunnel. ● Egress: indicates the node is the egress of the tunnel. ● Transit: indicates the node is the transit of the tunnel.
LSP Type	Type of an LSP: ● Primary: indicates the primary CR-LSP. ● Hot-Standby: indicates the hot-standby CR-LSP. ● Ordinary: indicates the ordinary backup CR-LSP. ● Best-Effort: indicates the best-effort path.
Ingress LSR ID	LSR ID of the ingress.
Egress LSR ID	LSR ID of the egress.
In-Interface	Incoming interface of the LSP on the local node.
Out-Interface	Outgoing interface of the LSP on the local node.
Sign-Protocol	Tunnel protocol: ● Static: indicates Static LSP. ● Static CR: indicates Static CR-LSP. ● RSVP TE: uses RSVP TE signaling.

Item	Description
Resv Style	Style of resource reservation. For a static CR-LSP, no resource reservation style is displayed. For an RSVP-TE tunnel, shared explicit (SE) or fixed filter (FF) is displayed.
IncludeAnyAff	Valid affinity property. The default value is 0x0.
ExcludeAnyAff	Invalid affinity property. The default value is 0x0.
IncludeAllAff	The affinity property needs to be included. The default value is 0x0.
LspConstraint	Sequence number of the constraint used by an LSP.
ER-Hop Table Index	Index of an explicit routing table.
AR-Hop Table Index	Index of the actual explicit routing table.
C-Hop Table Index	Routing table index that is calculated by CSPF.
PrevTunnelIndexInSession	Index of the previous tunnel entry in the same session.
NextTunnelIndexInSession	Index of the next tunnel entry in the same session.
PSB Handle	Handle of the PSB.
Created Time	Amount of time an MPLS TE tunnel is created for.
RSVP LSP Type	LSP type. ● Primary: indicates that the LSP is a primary LSP. ● Hot-Standby: indicates that the LSP is a hot-standby LSP. **NOTE** This field is displayed as "-" because the device does not support the error code switching function.
Bandwidth Reserved Flag	Bandwidth reservation flag: ● Unreserved: indicates that no bandwidth is reserved for CTs. ● Reserved: indicates that the bandwidth is reserved for one or multiple CTs.
CT0 Bandwidth(Kbit/sec) - CT7 Bandwidth(Kbit/sec)	Value of the bandwidth that is reserved for CT0 to CT7.

Item	Description
Setup-Priority	Setup priority of an MPLS TE tunnel.
Hold-Priority	Holding priority of an MPLS TE tunnel.
Primary LSP Info	Information about the primary LSP.
TE Attribute Flag	Flag of the TE tunnel attribute.
Protected Flag	Flag of the primary tunnel of the protection group.
Bypass In Use	LSP ID of the bypass tunnel. "Not Exists" indicates that the primary tunnel is not bound to a bypass tunnel.
Bypass Tunnel Id	Tunnel ID of the bypass tunnel.
BypassTunnel	Name of the bypass tunnel.
Bypass LSP ID	LSP ID of the bypass tunnel.
FrrNextHop	Next hop of the redirect route.
ReferAutoBypassHandle	Handle of the automatic bypass tunnel.
FrrPrevTunnelTableIndex	Index value of the previous tunnel entry in FRR.
FrrNextTunnelTableIndex	Index value of the next tunnel entry in FRR.
Bypass Attribute	Attributes of a bypass tunnel. "(Not configured)" indicates that no such attribute is configured and the bypass tunnel inherits the attributes of the primary tunnel.
Setup Priority	Setup priority of a bypass tunnel.
Hold Priority	Holding priority of a bypass tunnel.
HopLimit	Maximum number of hops along a bypass tunnel.
Bandwidth	Bandwidth of a bypass tunnel.
IncludeAnyGroup	Valid affinity property of a bypass tunnel.
ExcludeAnyGroup	Invalid affinity property of a bypass tunnel.
IncludeAllGroup	The affinity property of a bypass tunnel needs to be included.
Bypass Unbound Bandwidth Info	Information about the bandwidth that is not bound to a bypass tunnel.

Item	Description
CT0 Unbound Bandwidth - CT7 Unbound Bandwidth	Bandwidth that is able to be reserved, but not for CT0 to CT7.
NextSessionTunnelIndex	Next index of a bypass tunnel entry.
PrevSessionTunnelIndex	Previous index of a bypass tunnel entry.
NextLspId	Value of the next bypass LSP ID.
PrevLspId	Value of the previous bypass LSP ID.

9.3.49 display mpls te tunnel c-hop

Function

The **display mpls te tunnel c-hop** command displays the path computation results of tunnels.

Format

display mpls te tunnel c-hop [*tunnel-name*] [**lsp-id** *ingress-lsr-id session-id lsp-id*]

Parameters

Parameter	Description	Value
tunnel-name	Displays the path computation result of the specified tunnel.	The value is an existing tunnel name.
lsp-id	Displays the path computation result of the specified tunnel based on the LSP ID.	-
ingress-lsr-id	Specifies the ingress LSR ID.	The value is in dotted decimal notation.
session-id	Specifies the session ID.	The value is an integer that ranges from 0 to 65535.
lsp-id	Specifies the LSP ID.	The value is an integer that ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Tunnels are established based on path computation results. When a tunnel cannot be established successfully, run the **display mpls te tunnel c-hop** command to view the path computation results for locating causes on a per-hop basis.

Example

# Display the path computation result of a tunnel.

```
<HUAWEI> display mpls te tunnel c-hop
 Tunnel Interface Name : Tunnel1
 Lsp ID : 10.2.2.2 :1 :10958
 CHop Information:
  Hop 0   10.3.0.2
  Hop 1   10.3.0.3
```

# Display the path computation result of the specified tunnel based on the LSP ID.

```
<HUAWEI> display mpls te tunnel c-hop lsp-id 10.2.2.2 1 10958
 Tunnel Interface Name : Tunnel1
 Lsp ID : 10.2.2.2 :1 :10958
 CHop Information:
  Hop 0   10.3.0.2
  Hop 1   10.3.0.3
```

Table 9-98 Description of the display mpls te tunnel c-hop command output

Item	Description
Tunnel Interface Name	Interface name of a tunnel.
Lsp ID	LSP ID of a tunnel, in the Ingress-Lsr-Id:Tunnel-Id:LSP-Id format.
CHop Information	Information about CSPF path computation. **Hop** specifies the IPv4 address of each hop in the path computation result.

9.3.50 display mpls te tunnel path

Function

The **display mpls te tunnel path** command displays the path of an MPLS TE tunnel.

Format

display mpls te tunnel path [[[**tunnel-name**] *tunnel-name*] [**lsp-id** *ingress-lsr-id session-id lsp-id*] | **fast-reroute** { **local-protection-available** | **local-protection-inuse** } | **lsr-role** { **ingress** | **transit** | **egress** }]

display mpls te tunnel path expanded tunnel-name *tunnel-name* [**lsp-id** *ingress-lsr-id session-id lsp-id*]

display mpls te tunnel path expanded lsp-id *ingress-lsr-id session-id lsp-id*

Parameters

Parameter	Description	Value
tunnel-name *tunnel-name*	Specifies the name of an MPLS TE tunnel. If the **mpls te signalled tunnel-name** command has been used to configure a tunnel name, this specified name is used.	The value is an existing tunnel name.
ingress-lsr-id	Specifies the LSR ID of the ingress.	The value is in dotted decimal notation.
session-id	Specifies the ID of a session.	The value is an integer that ranges from 0 to 65535.
lsp-id	Specifies the LSP ID.	The value is an integer that ranges from 0 to 65535.
fast-reroute local-protection-available	Specifies the available path for local protection of FRR.	-
fast-reroute local-protection-inuse	Specifies the path in use for local protection of FRR.	-
lsr-role { **ingress** | **transit** | **egress** }	Indicates the role of an LSR. ● **ingress**: indicates the ingress LSR. ● **transit**: indicates the transit LSR. ● **egress**: indicates the egress LSR.	-
expanded	Displays the expanded LSP path information by completing the RRO information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display mpls te tunnel path** command displays information about the path of an MPLS TE tunnel.

If no tunnel name is specified, information about all MPLS TE tunnels' path attributes is displayed.

When a Huawei device is interconnected with a non-Huawei device and the RRO information carried in the packet sent by the non-Huawei device is incomplete, the RRO information can be complemented using the **display mpls te tunnel path expanded** command on the Huawei device to display the information about the entire LSP path.

Precautions

The system can record and display the paths only after the **mpls te record-route** command is configured.

Example

# Display information about path attributes of all MPLS TE tunnels.

```
<HUAWEI> display mpls te tunnel path
Tunnel Interface Name : Tunnel1
 Lsp ID : 10.1.1.9 :100 :34
 Hop Information
  Hop 0   172.16.1.1 Local-Protection available | node
  Hop 1   172.16.1.2  Label 1055
  Hop 2   10.2.2.9  Label 1055
  Hop 3   172.20.1.1 Local-Protection available
  Hop 4   172.20.1.2  Label 1063
  Hop 5   10.3.3.9  Label 1063
  Hop 6   172.30.1.1
  Hop 7   172.30.1.2  Label 3
  Hop 8   10.4.4.9  Label 3
```

# Display path attributes of the MPLS TE tunnel with the ingress IP address being 10.1.1.9, the session ID being 300, and the LSP ID being 4.

```
<HUAWEI> display mpls te tunnel path lsp-id 10.1.1.9 300 4
 Tunnel Interface Name : Tunnel1
 Lsp ID : 10.1.1.9 :300 :4
 Hop Information
  Hop 0   172.16.1.1
  Hop 1   172.16.1.2  Label 1043
  Hop 2   10.2.2.9  Label 1043
  Hop 3   172.20.1.1
  Hop 4   172.20.1.2  Label 4
  Hop 5   10.3.3.9  Label 4
```

# Display path attributes of a tunnel named **LSRAtoLSRC**.

```
<HUAWEI> display mpls te tunnel path tunnel-name LSRAtoLSRC
 Tunnel Interface Name : LSRAtoLSRC
 Lsp ID : 10.1.1.9 :1 :2
 Hop Information
  Hop 0   10.11.1.1  Local-Protection in use
  Hop 1   10.11.1.2  Label 3
  Hop 2   10.2.2.9
```

# Display path attributes of a tunnel named **A2** using the command which expanded the information about the path.

```
<HUAWEI> display mpls te tunnel path expanded tunnel-name A2
 Tunnel Interface Name : A2
 Lsp ID : 10.1.1.9 :300 :4
```

```
Hop Information
 Hop 0   10.1.1.9   Local-Protection available | bandwidth
 Hop 1   172.16.1.1
 Hop 2   172.16.1.2  Label 1042
 Hop 3   10.2.2.9  Label 1042
 Hop 4   172.20.1.1
 Hop 5   172.20.1.2  Label 3
 Hop 6   10.3.3.9  Label 3
```

Table 9-99 Description of the display mpls te tunnel path command output

Item	Description
Tunnel Interface Name	Name of a tunnel interface.
Lsp ID	LSP ID on the ingress.
Hop Information	Number, IP address, and label of each hop.
Local-Protection available	Link protection provided by the bypass tunnel.
Local-Protection available | bandwidth	Bandwidth protection provided by the bypass tunnel.
Local-Protection available | node	Node protection provided by the bypass tunnel.
Local-Protection in use	The bypass tunnel in use.

9.3.51 display mpls te tunnel statistics

Function

The **display mpls te tunnel statistics** command displays the number and status of MPLS TE tunnels.

Format

display mpls te tunnel statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the number and status of MPLS TE tunnels, run the **display mpls te tunnel statistics** command.

Example

# Display the number and status of MPLS TE tunnels.

```
<HUAWEI> display mpls te tunnel statistics
Ingress:    84 Tunnels     83 Up,     83 CRLSPs Up
           0 Modified,    0 In-Progress,    1 Failed
Transit:     2 Up
Egress :     3 Up
```

Table 9-100 Description of the display mpls te tunnel statistics command output

Item	Description
Ingress	Number and status of MPLS TE tunnels on the local LSR functioning as the ingress node: ● Tunnel: indicates the number of primary tunnels. ● Up: indicates the number of MPLS TE tunnels in the Up state. ● CRLSPs Up: indicates the number of CR-LSPs in the Up state. ● Modified: indicates the number of tunnels in the reestablishing state. **NOTE** The possible causes that an MPLS TE tunnel is in the Modified state are as follows: Configurations of the MPLS TE tunnel are manually modified. The MPLS TE tunnel is being re-optimized. The MPLS TE tunnel is in the FRR inuse state. The MPLS TE tunnel is in the Backup state. ● In-Progress: indicates the number of MPLS TE tunnels in the establishing process. At the moment, these tunnels do not go Up. ● Failed: indicates the number of MPLS TE tunnels in the Down state.
Transit	Number of MPLS TE tunnels, which are in the Up state, on the local LSR functioning as a transit node.
Egress	Number of MPLS TE tunnels, which are in the Up state, on the local LSR functioning as the egress node.

9.3.52 display ospf mpls-te

Function

The **display ospf mpls-te** command displays information about TE LSAs in an LSDB.

Format

display ospf [*process-id*] **mpls-te** [**area** *area-id*] [**self-originated**]

Parameters

Parameter	Description	Value
process-id	Specifies the OSPF process ID.	The value ranges from 1 to 65535.
area *area-id*	Displays information about the area with a specified ID. The value can be a decimal integer or in the IP address format.	The integer value ranges from 0 to 4294967295.
self-originated	Displays information about the self originated TE LSAs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can view information about LSAs of a specific process or area by specifying parameters.

Example

# Display information about all TE LSAs in the LSDB.

```
<HUAWEI> display ospf mpls-te
        OSPF Process 1 with Router ID 172.16.1.2

 Area ID                  : 0.0.0.0

 Traffic Engineering LSAs of the database

 ------------------------------------------------

 LSA [ 1 ]

 ------------------------------------------------
   Lsa  Type               : Opq-Area
```

```
  Opaque Type              : 1
  Opaque Id                : 2
  Advertising Router Id    : 172.16.1.2
  Lsa  age                 : 36
  Length                   : 200
  Lsa  Options             : E
  LS Seq Number            : 80000001
  CheckSum                 : 7130

  Link Type                : MultiAccess
  Link ID                  : 172.20.1.1
  Local Interface Address  : 172.20.1.1
  Remote Interface Address : 0.0.0.0
  TE Metric                : 1
  Maximum Bandwidth        : 0 bytes/sec
  Maximum Reservable BW    : 0 bytes/sec
  Admin Group              : 0X0

 Global Pool               :
  Unreserved BW [ 0] =   0  bytes/sec
  Unreserved BW [ 1] =   0  bytes/sec
  Unreserved BW [ 2] =   0  bytes/sec
  Unreserved BW [ 3] =   0  bytes/sec
  Unreserved BW [ 4] =   0  bytes/sec
  Unreserved BW [ 5] =   0  bytes/sec
  Unreserved BW [ 6] =   0  bytes/sec
  Unreserved BW [ 7] =   0  bytes/sec
  Sub Pool                 :
  Unreserved BW [ 8] =   0  bytes/sec
  Unreserved BW [ 9] =   0  bytes/sec
  Unreserved BW [10] =   0  bytes/sec
  Unreserved BW [11] =   0  bytes/sec
  Unreserved BW [12] =   0  bytes/sec
  Unreserved BW [13] =   0  bytes/sec
  Unreserved BW [14] =   0  bytes/sec
  Unreserved BW [15] =   0  bytes/sec

  DS-TE Mode: Non-Standard IETF Mode

  Bandwidth Constraint Model: RDM

 Bandwidth Constraints

            BC [ 0] =   0  bytes/sec             BC [ 1] =   0  bytes/sec

 Local OverBooking Multipliers

           LOM [ 0] =   1                  LOM [ 1] =   1


------------------------------------------------

 LSA [ 2 ]

 ------------------------------------------------
  Lsa  Type                : Opq-Area
  Opaque Type              : 1
  Opaque Id                : 1
  Advertising Router Id    : 172.16.1.2
  Lsa  age                 : 1681
  Length                   : 200
  Lsa  Options             : E
  LS Seq Number            : 80000033
  CheckSum                 : 77F4

  Link Type                : MultiAccess
  Link ID                  : 172.17.1.1
  Local Interface Address  : 172.17.1.1
  Remote Interface Address : 0.0.0.0
  TE Metric                : 1
  Maximum Bandwidth        : 0 bytes/sec
  Maximum Reservable BW    : 0 bytes/sec
  Admin Group              : 0X0

Global Pool                :
  Unreserved BW [ 0] =   0  bytes/sec
  Unreserved BW [ 1] =   0  bytes/sec
  Unreserved BW [ 2] =   0  bytes/sec
  Unreserved BW [ 3] =   0  bytes/sec
  Unreserved BW [ 4] =   0  bytes/sec
  Unreserved BW [ 5] =   0  bytes/sec
  Unreserved BW [ 6] =   0  bytes/sec
  Unreserved BW [ 7] =   0  bytes/sec
  Sub Pool                 :
  Unreserved BW [ 8] =   0  bytes/sec
  Unreserved BW [ 9] =   0  bytes/sec
  Unreserved BW [10] =   0  bytes/sec
  Unreserved BW [11] =   0  bytes/sec
  Unreserved BW [12] =   0  bytes/sec
  Unreserved BW [13] =   0  bytes/sec
  Unreserved BW [14] =   0  bytes/sec
  Unreserved BW [15] =   0  bytes/sec

  DS-TE Mode: Non-Standard IETF Mode

  Bandwidth Constraint Model: RDM

Bandwidth Constraints

            BC [ 0] =   0  bytes/sec             BC [ 1] =   0  bytes/sec

Local OverBooking Multipliers

            LOM [ 0] =   1                  LOM [ 1] =   1
...
```

Table 9-101 Description of the display ospf mpls-te command output

Item	Description
OSPF Process 1 with Router ID 172.16.1.2	OSPF process 1 with Router ID being 172.16.1.2.
Area ID	ID of the OSPF area enabled with TE.
Traffic Engineering LSAs of the database	TE LSAs in an LSDB.
Lsa Type	LSA type: ● Opq-Link: indicates Type 9 LSAs that can only be spread on a specified interface. ● Opq-Area: indicates Type 10 LSAs that can only be spread within a specified area. ● Opq-As: indicates Type 11 LSAs that can be spread the same as Type 5 LSAs in the entire AS, except for the stub and NSSA areas.

Item	Description
Opaque Type	Application type of LSAs. For example, when LSAs are applied to traffic engineering, the value of the LSA type is 1. When LSAs are applied to the OSPF graceful restart, the value of the LSA type is 3.
Opaque Id	LSAs that are applied to the same application type. Opaque type and Opaque ID in an LSA header together specify the link status ID.
Advertising Router Id	Device that generates the LSA.
Lsa age	Aging time of the LSA. It is in the header of Opaque LSA, in seconds.
Length	Length of the Opaque LSA, including the LSA header, in bytes.
Lsa Options	LSA options: ● E: floods AS-external-LSAs. ● MC: forwards IP multicast packets. ● N/P: processes Type 7 LSAs. ● DC: processes required links.
LS Seq Number	LSA sequence, according to which other devices can identify the latest LSAs.
CheckSum	Checksum of LSA fields except for the LS age field.
Link Type	Link type: ● Point-to-point ● Point-to-multi-point (P2MP) ● Broadcast
Link ID	Link ID in the IP address format: ● Point-to-point: indicates the router ID of an OSPF neighbor. ● P2MP or broadcast: indicates the IP address of the DR interface.
Local Interface Address	IP address of the local interface.
Remote Interface Address	IP address of the peer interface: ● Point-to-point: indicates that the IP address of the peer is used. ● P2MP or broadcast: indicates that 0.0.0.0 is used or the IP address is omitted.
TE Metric	TE metric.

Item	Description
Maximum Bandwidth	Maximum bandwidth.
Maximum Reservable BW	Maximum capacity of reserved bandwidth.
Admin Group	Administration group.
Global Pool	Global address pool.
Unreserved BW [0] to [7]	Available bandwidth of eight levels.
Sub Pool	Sub-address pool. It is only applied to DS-TE LSAs.
Unreserved BW [8] to [15]	Available bandwidth of eight levels in the sub-address pool.
DS-TE Mode	DS-TE mode: ● Standard IETF mode ● Non-standard IETF mode
Bandwidth Constraint Model	Bandwidth Constraints model of LSAs: ● RDM ● MAM ● Extended-MAM
Bandwidth Constraints	Bandwidth constraints, which are only applied to DS-TE LSAs.
BC [0] - [7]	Eight bandwidth constraints, which are only applied to DS-TE LSAs.
Local OverBooking Multipliers	Local overbooking multiplier.
LOM [0] LOM [1]	Local overbooking multipliers for BC0 or BC1. It is applied only to DS-TE LSAs.

9.3.53 display ospf traffic-adjustment

Function

The **display ospf traffic-adjustment** command displays OSPF process-specific tunnel information relevant to traffic adjustment (through IGP shortcut and forwarding adjacency).

Format

display ospf [*process-id*] **traffic-adjustment**

Parameters

Parameter	Description	Value
process-id	Specifies the OSPF process ID. If you do not specify a process ID, information about all OSPF processes is displayed.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you want to look up the OSPF process-specific tunnel information relevant to traffic adjustment, you can run this command.

Example

# Display tunnel information, which is relevant to traffic adjustment, of OSPF process 100.

```
<HUAWEI> display ospf 100 traffic-adjustment

          OSPF Process 100 with Router ID 1.1.1.9
                   Traffic adjustment

 Interface: 1.1.1.9 (Tunnel1)
 Type: Forwarding Adjacency
 Neighbor ID: 3.3.3.9            Cost: 1
 Configuration:
  Neighbor ip address: 3.3.3.9
  Cost      :1
  Cost Type: Absolute
  Hold Time: 0
```

Table 9-102 Description of the display ospf traffic-adjustment command output

Item	Description
Interface	Name and IP address of a tunnel interface
Type	Whether a tunnel is applied to IGP shortcut or forwarding adjacency
Neighbor ID	Router ID of a neighbor device
Cost	Actual cost
Neighbor ip address	IP address of a neighbor device
Cost	Configured cost

Item	Description
Cost Type	Cost type: ● Relative: Relative cost ● Absolute: Absolute cost
Hold Time	Time elapsed since the tunnel has been created

9.3.54 enable traffic-adjustment

Function

The **enable traffic-adjustment** command enables the IGP shortcut function.

The **enable traffic-adjustment advertise** command enables the forwarding adjacency function.

The **undo enable traffic-adjustment** command disables the IGP shortcut function.

The **undo enable traffic-adjustment advertise** command disables the forwarding adjacency function.

By default, the IGP shortcut function and the forwarding adjacency function are disabled.

Format

enable traffic-adjustment [**advertise**]

undo enable traffic-adjustment [**advertise**]

Parameters

None.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

After the configuration of a command, all TE tunnels are involved in the SPF calculation and flooding.

Example

# Enable the forwarding adjacency function of the OSPF process.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] enable traffic-adjustment advertise
```

9.3.55 explicit-path

Function

The **explicit-path** command configures an explicit path of a tunnel.

The **undo explicit-path** command deletes a configured explicit path.

By default, no explicit path of a tunnel is configured.

Format

explicit-path *path-name*

undo explicit-path *path-name*

Parameters

Parameter	Description	Value
path-name	Indicates the name of an explicit path.	The value is a string of 1 to 31 case-insensitive characters, spaces not supported.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You must enable MPLS TE before running the **explicit-path** command.

The addresses of the hops along the explicit path must be different, without loops. If a loop exists, CSPF detects the loop and fails to compute a path.

If the explicit path is in use, the **undo explicit-path** command cannot be run to delete the explicit path.

Example

# Create an explicit path named path1.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] quit
[HUAWEI] explicit-path path1
[HUAWEI-explicit-path-path1] quit
```

9.3.56 explicit-path (LSP attribute view)

Function

The **explicit-path** command configures an explicit path in a CR-LSP attribute template.

The **undo explicit-path** command deletes an explicit path from a CR-LSP attribute template.

No explicit path is configured in a CR-LSP attribute template by default.

Format

explicit-path *path-name*

undo explicit-path

Parameters

Parameter	Description	Value
path-name	Specifies the name of an explicit path.	The value is an existing explicit path name.

Views

LSP attribute view

Default Level

2: Configuration level

Usage Guidelines

To specify an explicit path in a CR-LSP attribute template, you must configure the explicit path in the system view and ensure that its hop list is not null.

Example

# Configure an explicit path in the CR-LSP attribute template.

```
<HUAWEI> system-view
[HUAWEI] lsp-attribute lsp-attribute-name
[HUAWEI-lsp-attribute-lsp-attribute-name] explicit-path path-name
```

9.3.57 fast-reroute

Function

The **fast-reroute** command enables the Fast Reroute (FRR) function in a CR-LSP attribute template.

The **undo fast-reroute** command disables the FRR function in the CR-LSP attribute template.

The FRR function is disabled in the CR-LSP attribute template by default.

Format

fast-reroute [**bandwidth**]

undo fast-reroute

Parameters

Parameter	Description	Value
bandwidth	Indicates that bandwidth protection is needed during fast rerouting.	-

Views

LSP attribute view

Default Level

2: Configuration level

Usage Guidelines

After the FRR function is enabled, the route storing function is automatically enabled. After the FRR function is disabled, the bypass tunnel configurations are automatically deleted.

Example

# Enable the FRR function in the CR-LSP attribute template.

```
<HUAWEI> system-view
[HUAWEI] lsp-attribute lsp-attribute-name
[HUAWEI-lsp-attribute-lsp-attribute-name] fast-reroute
```

9.3.58 hop-limit

Function

The **hop-limit** command sets the hop limit in a CR-LSP attribute template.

The **undo hop-limit** command restores the default hop limit from a CR-LSP attribute template.

By default, the hop limit in a CR-LSP attribute template is 32.

Format

hop-limit *hop-limit*

undo hop-limit

Parameters

Parameter	Description	Value
hop-limit	Specifies the value of the hop limit.	The value is an integer that ranges from 1 to 32. The hop limit is 32 by default.

Views

LSP attribute view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To limit the maximum number of hops supported by each CR-LSP established using the CR-LSP attribute template, run the **hop-limit** command in the LSP attribute view. This hop limit restricts CR-LSP path selection.

Prerequisites

A CR-LSP attribute template has been created and the LSP attribute view has been entered using the **lsp-attribute** command.

Example

# Set the maximum number of hops in the CR-LSP attribute template to 20.

```
<HUAWEI> system-view
[HUAWEI] lsp-attribute lsp-attribute-name
[HUAWEI-lsp-attribute-lsp-attribute-name] hop-limit 20
```

9.3.59 hotstandby-switch

Function

The **hotstandby-switch force** command forcibly switches traffic from a primary CR-LSP to a hot-standby CR-LSP.

The **hotstandby-switch clear** command disables the forcible switchover function and switches traffic from a hot-standby CR-LSP to the primary CR-LSP.

Format

hotstandby-switch { **force** | **clear** }

Parameters

None.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a hot-standby CR-LSP is established and a primary CR-LSP needs to be adjusted, run the **hotstandby-switch force** command to switch traffic forcibly to the hot-standby CR-LSP. After the primary CR-LSP has been adjusted, run the **hotstandby-switch clear** command to disable the forcible switchover function and switch traffic back to the primary CR-LSP.

Precautions

A hot-standby CR-LSP must have been established before the **hotstandby-switch force** command is used. If this command is run but no hot-standby CR-LSP is established, traffic will be dropped.

Example

# Forcibly switch traffic from a primary CR-LSP to a hot-standby CR-LSP.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] hotstandby-switch force
```

9.3.60 list hop

Function

The **list hop** command displays information about nodes along an explicit path of an MPLS TE tunnel.

Format

list hop [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a node.	The value is in dotted decimal notation.

Views

Explicit path view

Default Level

2: Configuration level

Usage Guidelines

To view the information about nodes along an explicit path of an MPLS TE tunnel, run the **list hop** command.

Example

# Display information about nodes along an explicit path of an MPLS TE tunnel.

```
<HUAWEI> system-view
[HUAWEI] explicit-path path1
[HUAWEI-explicit-path-path1] list hop
 Path Name : path1      Path Status : Enabled
 1       10.1.1.1           Strict      Include
 2       10.2.2.2           Strict      Exclude
 3       10.3.3.3           Loose        Include              Outgoing
 4       10.4.4.4           Strict      Include              Incoming
```

9.3.61 lsp-attribute

Function

The **lsp-attribute** command creates a CR-LSP attribute template and displays the LSP attribute view.

The **undo lsp-attribute** command deletes a specified CR-LSP attribute template.

By default, no CR-LSP attribute template is created.

Format

lsp-attribute *lsp-attribute-name*

undo lsp-attribute *lsp-attribute-name*

Parameters

Parameter	Description	Value
lsp-attribute-name	Specifies the name of the CR-LSP attribute template.	The value is a string of 1 to 31 case-insensitive characters, spaces not supported.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To simplify configurations of TE tunnel interfaces and enhance their flexibility, you can reference CR-LSP attribute templates to set up TE tunnels. The CR-LSP attribute template contains the attributes relevant to a TE tunnel, including the bandwidth, affinity property, explicit path, hop limit, route storing, setup priority, holding priority, FRR, and bypass tunnel attribute.

Prerequisites

Before configuring a CR-LSP attribute template, you must enable the MPLS TE function in the system view.

Precautions

When deleting a CR-LSP attribute template, ensure that the CR-LSP attribute template is not referenced by any tunnel interface.

Example

# Create the CR-LSP attribute template named **lsp-attribute-name**.

```
<HUAWEI> system-view
[HUAWEI] lsp-attribute lsp-attribute-name
[HUAWEI-lsp-attribute-lsp-attribute-name]
```

9.3.62 modify hop

Function

The **modify hop** command modifies the IP address of a hop on an explicit path.

Format

modify hop *ip-address1 ip-address2* [**include** [[**loose** | **strict**] | [**incoming** | **outgoing**]] * | **exclude**]

Parameters

Parameter	Description	Value
ip-address1 ip-address2	Changes *ip-address1* to *ip-address2* on an explicit path.	The value is in dotted decimal notation.

Parameter	Description	Value
include [[**loose** | **strict**] | [**incoming** | **outgoing**]] *	Indicates that the explicit path must pass through the modified node on the explicit path. ● **strict**: indicates the strict explicit path. The modified node must be directly connected to the previous node. ● **loose**: indicates the loose explicit path. The modified node can be not directly connected to the previous node. ● **incoming**: indicates that the *ip-address2* is the IP address of an inbound interface of the modified node. ● **outgoing**: indicates that the *ip-address2* is the IP address of an outbound interface of the modified node.	By default, a node is added to an explicit path in **include strict** mode.
exclude	Indicates that the LSP set up along an explicit path excludes the modified link or node.	-

Views

Explicit path view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following commands are used to adjust nodes on a created explicit path:

- The **add hop** command is used to add a node to the explicit path.
- The **modify hop** command is used to delete a node from the explicit path and replace the node with a specified node.
- The **delete hop** command is used to delete a node from the explicit path.

Prerequisites

A next-hop IP address has been configured using the **next hop** command.

Follow-up Procedure

Run the **display explicit-path** command to view information about the explicit path.

Precautions

A node can be modified on an explicit path using the **modify hop** command only when the following conditions are met:

- *ip-address2* must not be a next-hop IP address of an existing node on the explicit path.
- If an explicit path over which a TE tunnel has been established is modified, the make-before-break mechanism is triggered, and a CR-LSP is reestablished without traffic loss.

Example

# Modify IP address of a node along the explicit path from 10.1.1.9 to 10.2.2.9.

```
<HUAWEI> system-view
[HUAWEI] explicit-path p1
[HUAWEI-explicit-path-p1] next hop 10.1.1.9
[HUAWEI-explicit-path-p1] modify hop 10.1.1.9 10.2.2.9
```

9.3.63 mpls-te enable

Function

The **mpls-te enable** command enables the MPLS TE feature in the current OSPF area.

The **undo mpls-te** command disables the MPLS TE feature in the current OSPF area.

OSPF area does not support MPLS TE by default.

Format

mpls-te enable [**standard-complying**]

undo mpls-te

Parameters

Parameter	Description	Value
standard-complying	Accepts only LSAs in the standard format. This means that an LSA is rejected if it has more than one Top level TLV.	-

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

MPLS TE can only be enabled in an OSPF area after the OSPF process is enabled with the Opaque LSA function.

Example

# Enable TE in OSPF area 1.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] opaque-capability enable
[HUAWEI-ospf-100] area 1
[HUAWEI-ospf-100-area-0.0.0.1] mpls-te enable
```

9.3.64 mpls autobypass-tunnel-number threshold-alarm

Function

The **mpls autobypass-tunnel-number threshold-alarm** command configures the conditions that trigger the threshold-reaching alarm and its clear alarm for Auto bypass tunnel interfaces.

The **undo mpls autobypass-tunnel-number threshold-alarm** command restores the default settings.

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

Format

mpls autobypass-tunnel-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls autobypass-tunnel-number threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper alarm threshold for the proportion of configured Auto bypass tunnel interfaces to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold for the proportion of configured Auto bypass tunnel interfaces to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of Auto bypass tunnel interfaces reaches a specified upper limit, new Auto bypass tunnel interfaces cannot be configured due to insufficient resources. To alert the administrator in operation and maintenance, enable a device to generate an alarm when the proportion of configured Auto bypass tunnel interfaces to all supported ones reaches a specified upper alarm threshold. The following parameters can be configured in the **mpls autobypass-tunnel-number threshold-alarm** command:

- *upper-limit-value*: upper alarm threshold. If the proportion of configured Auto bypass tunnel interfaces to all supported ones reaches the upper alarm threshold, an alarm can be generated.
- *lower-limit-value*: lower alarm threshold. If the proportion of configured Auto bypass tunnel interfaces to all supported ones falls below the lower alarm threshold, a clear alarm can be generated.

Precautions

- If the **mpls autobypass-tunnel-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- The **mpls autobypass-tunnel-number threshold-alarm** command only configures the trigger conditions for an alarm and its clear alarm. Although trigger conditions are met, the alarm and its clear alarm can be generated only after the **snmp-agent trap enable feature-name mpls_lspm trap-name** { **hwmplsresourcethresholdexceed** | **hwmplsresourcethresholdexceedclear** } command is run to enable the device to generate an MPLS resource insufficiency alarm and its clear alarm.

Example

# Configure conditions that trigger the threshold-reaching alarm and its clear alarm for Auto bypass tunnel interfaces.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls autobypass-tunnel-number threshold-alarm upper-limit 90 lower-limit 60
```

9.3.65 mpls bfd-te-number threshold-alarm

Function

The **mpls bfd-te-number threshold-alarm** command configures the conditions that trigger the threshold-reaching alarm and its clear alarm for dynamic BFD sessions for TE.

The **undo mpls bfd-te-number threshold-alarm** command restores the default settings.

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

Format

mpls bfd-te-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls bfd-te-number threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Sets the upper alarm threshold for the proportion of established dynamic BFD sessions for TE to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Sets the lower alarm threshold for the proportion of established dynamic BFD sessions for TE to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of dynamic BFD sessions for TE reaches a specified upper limit, new dynamic BFD sessions for TE cannot be configured due to insufficient resources. To alert the administrator in operation and maintenance, enable a device to generate an alarm when the proportion of established dynamic BFD sessions for TE to all supported ones reaches a specified upper alarm threshold. The following parameters can be configured in the **mpls bfd-te-number threshold-alarm** command:

- *upper-limit-value*: upper alarm threshold. If the proportion of established dynamic BFD sessions for TE to all supported ones reaches the upper alarm threshold, an alarm can be generated.
- *lower-limit-value*: lower alarm threshold. If the proportion of established dynamic BFD sessions for TE to all supported ones falls below the lower alarm threshold, a clear alarm can be generated.

Precautions

- If the **mpls bfd-te-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- The **mpls bfd-te-number threshold-alarm** command only configures the trigger conditions for an alarm and its clear alarm. Although trigger conditions are met, the alarm and its clear alarm can be generated only after the **snmp-agent trap enable feature-name mpls_lspm trap-name** { **hwmplsresourcethresholdexceed** | **hwmplsresourcethresholdexceedclear** } command is run to enable the device to generate an MPLS resource insufficiency alarm and its clear alarm.

Example

# Configure conditions that trigger the threshold-reaching alarm and its clear alarm for dynamic BFD sessions for TE.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls bfd-te-number threshold-alarm upper-limit 90 lower-limit 60
```

9.3.66 mpls cspf threshold-alarm

Function

The **mpls** { **cspf-link-number** | **cspf-node-number** | **cspf-nlsa-number** | **cspf-srlg-number** } **threshold-alarm** command sets the upper and lower alarm thresholds for the proportion of the number of existing CSPF resources of a specified type to the maximum number of CSPF resources that a device supports. The CSPF resources can be CSPF links, nodes, network LSAs, or SRLGs.

The **undo mpls** { **cspf-link-number** | **cspf-node-number** | **cspf-nlsa-number** | **cspf-srlg-number** } **threshold-alarm** command restores the default the upper and lower alarm thresholds.

By default, the upper threshold for alarms is 80 (percent), and the lower threshold for clear alarms is 75 (percent).

Format

mpls { **cspf-link-number** | **cspf-node-number** | **cspf-nlsa-number** | **cspf-srlg-number** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls { **cspf-link-number** | **cspf-node-number** | **cspf-nlsa-number** | **cspf-srlg-number** } **threshold-alarm**

Parameters

Parameter	Description	Value
cspf-link-number	Indicates the upper and lower alarm thresholds of the proportion of the existing CSPF links to the maximum number of CSPF links that a device supports.	-
cspf-node-number	Indicates the upper and lower alarm thresholds of the proportion of the existing CSPF nodes to the maximum number of CSPF nodes that a device supports.	-
cspf-nlsa-number	Indicates the upper and lower alarm thresholds of the proportion of the existing CSPF network LSAs to the maximum number of CSPF network LSAs that a device supports.	-
cspf-srlg-number	Indicates the upper and lower alarm thresholds of the proportion of the existing CSPF SRLGs to the maximum number of CSPF SRLGs that a device supports.	-
upper-limit *upper-limit-value*	Specifies a percent for the upper alarm threshold.	The value is a percent integer ranging from 1 to 100. Set the value less than or equal to 95. Default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies a percent for the lower alarm threshold.	The value is a percent integer ranging from 1 to 100. *lower-limit-value* must be less than *upper-limit-value*. Default value 75 is recommended.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the following example, the alarm thresholds for CSPF links are used. If the number of CSPF links reaches the maximum number of CSPF links that a device supports, new CSPF links fail to be established. To alert the administrator in operation and maintenance, enable a device to generate an alarm when the proportion of configured CSPF links to all supported ones reaches a specified upper alarm threshold. To enable this function, run the **mpls cspf-link-number threshold-alarm** command to set the upper and lower alarm thresholds with the following parameters configured:

- *upper-limit-value*: An alarm is generated if the proportion of the number of existing CSPF links to the maximum number reaches *upper-limit-value*.
- *lower-limit-value*: The alarm is cleared if the proportion of the number of existing CSPF links to the maximum number falls to *lower-limit-value*.

Precautions

- If the **mpls** { **cspf-link-number** | **cspf-node-number** | **cspf-nlsa-number** | **cspf-srlg-number** } **threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- The **mpls** { **cspf-link-number** | **cspf-node-number** | **cspf-nlsa-number** | **cspf-srlg-number** } **threshold-alarm** command only configures trigger conditions for alarms and clear alarms. Although trigger conditions are met, an alarm and its clear alarm can be generated only after the **snmp-agent trap enable feature-name mpls_lspm trap-name** { **hwmplsresourcethresholdexceed** | **hwmplsresourcethresholdexceedclear** } command is run to enable the device to generate an MPLS resource insufficiency alarm and its clear alarm.

Example

# Set the upper and lower alarm thresholds to 90% and 60%, respectively, for the proportion of existing CSPF links to the maximum number of CSPF links that a device supports.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls cspf-link-number threshold-alarm upper-limit 90 lower-limit 60
```

9.3.67 mpls rsvp-lsp-number threshold-alarm

Function

The **mpls rsvp-lsp-number threshold-alarm** command configures the alarm threshold for Resource Reservation Protocol (RSVP) label switched path (LSP) usage.

The **undo mpls rsvp-lsp-number threshold-alarm** command restores the default settings.

The default upper limit of the alarm threshold for RSVP LSP usage is 80%. The default lower limit of the clear alarm threshold for RSVP LSP usage is 75%.

Format

mpls rsvp-lsp-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

mpls rsvp-lsp-number { **ingress** | **transit** | **egress** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls rsvp-lsp-number threshold-alarm

undo mpls rsvp-lsp-number { **ingress** | **transit** | **egress** } **threshold-alarm**

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper limit of the alarm threshold for RSVP LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies the lower limit of the clear alarm threshold for RSVP LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.
ingress	The alarm that the number of ingress RSVP LSPs reached the upper threshold is generated.	-
transit	The alarm that the number of transit RSVP LSPs reached the upper threshold is generated.	-
egress	The alarm that the number of egress RSVP LSPs reached the upper threshold is generated.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of RSVP LSPs in the system reaches a specific limit, establishing subsequent RSVP LSPs may fail because of insufficient resources. To facilitate user operation and maintenance, enable an alarm to be generated when the number of RSVP LSPs reaches the specific limit. To configure the alarm threshold for RSVP LSP usage, run the **mpls rsvp-lsp-number threshold-alarm** command. The parameters in this command are described as follows:

- When the RSVP LSP usage increases to the value of *upper-limit-value*, an alarm for RSVP LSPs is generated.
- When the RSVP LSP usage falls below the value of *lower-limit-value*, a clear alarm for RSVP LSPs is generated.

If you want to set the alarm threshold for ingress RSVP LSPs, transit RSVP LSPs or egress RSVP LSPs, run **mpls rsvp-lsp-number** { **ingress** | **transit** | **egress** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*.

Precautions

- If the **mpls rsvp-lsp-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- This command configures the alarm threshold for RSVP LSP usage. The alarm that the number of LSPs exceeded the upper threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceed** is configured, and the actual RSVP LSP usage reaches the upper limit of the alarm threshold. The alarm that the number of LSPs fell below the lower threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceedclear** is configured, and the actual RSVP LSP usage falls below the lower limit of the clear alarm threshold.

Example

# Configure the upper limit and the lower limit of the alarm threshold for RSVP LSP usage.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-lsp-number threshold-alarm upper-limit 90 lower-limit 60
```

9.3.68 mpls rsvp-peer-number threshold-alarm

Function

The **mpls rsvp-peer-number threshold-alarm** command configures the conditions that trigger the threshold-reaching alarm and its clear alarm for RSVP neighbors.

The **undo mpls rsvp-peer-number threshold-alarm** command restores the default settings.

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

Format

mpls rsvp-peer-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls rsvp-peer-number threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper alarm threshold for the proportion of configured RSVP neighbors to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold for the proportion of configured RSVP neighbors to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of RSVP neighbors reaches a specified upper limit, new RSVP neighbors cannot be configured due to insufficient resources. To alert the administrator in operation and maintenance, enable a device to generate an alarm when the proportion of configured RSVP neighbors to all supported ones reaches a specified upper alarm threshold. The following parameters can be configured in the **mpls rsvp-peer-number threshold-alarm** command:

- *upper-limit-value*: upper alarm threshold. If the proportion of configured RSVP neighbors to all supported ones reaches the upper alarm threshold, an alarm can be generated.
- *lower-limit-value*: lower alarm threshold. If the proportion of configured RSVP neighbors to all supported ones falls below the lower alarm threshold, a clear alarm can be generated.

Precautions

- If the **mpls rsvp-peer-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.

- The **mpls rsvp-peer-number threshold-alarm** command only configures the trigger conditions for an alarm and its clear alarm. Although trigger conditions are met, the alarm and its clear alarm can be generated only after the **snmp-agent trap enable feature-name mpls_rsvp trap-name** { **hwrsvpteifnbrthresholdexceed** | **hwrsvpteifnbrthresholdexceedclear** } command is run to enable the device to generate an MPLS resource insufficiency alarm and its clear alarm.

Example

# Configure conditions that trigger the threshold-reaching alarm and its clear alarm for RSVP neighbors.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-peer-number threshold-alarm upper-limit 90 lower-limit 60
```

9.3.69 mpls rsvp-te

Function

The **mpls rsvp-te** command enables the RSVP-TE function on an interface or globally.

The **undo mpls rsvp-te** command disables the RSVP-TE function.

RSVP-TE is disabled by default.

Format

mpls rsvp-te

undo mpls rsvp-te

Parameters

None

Views

MPLS view, VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Prerequisites

You must run the **mpls (system view)** and **mpls te** commands to enable MPLS and MPLS TE before running the **mpls rsvp-te** command in the MPLS view.

You must run the **mpls (interface view)** and **mpls te** commands to enable MPLS and MPLS TE before running the **mpls rsvp-te** command in the interface view.

Precautions

Before enabling the RSVP-TE function on an interface, you need to run this command in the MPLS view to enable the RSVP-TE function globally.

NOTICE

After the **undo mpls rsvp-te** command is run in the MPLS view, MPLS RSVP-TE services may be interrupted and all MPLS RSVP-TE configurations are deleted. To restore the MPLS RSVP-TE services, reconfigure these commands.

Example

# Enable RSVP-TE globally.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls rsvp-te
```

# Enable RSVP-TE on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
```

# Enable RSVP-TE on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
```

9.3.70 mpls rsvp-te authentication

Function

The **mpls rsvp-te authentication** command run in the interface or neighbor view enables authentication and sets an authentication key.

The **undo mpls rsvp-te authentication** command run in the interface or neighbor view disables authentication.

Authentication is disabled by default.

Format

mpls rsvp-te authentication { { **cipher** | **plain** } *auth-key* | **keychain** *keychain-name* [**sha256-compatible**] }

undo mpls rsvp-te authentication

Parameters

Parameter	Description	Value
cipher	Indicates that the key is displayed in cipher text.	-
plain	Indicates that the key is displayed in plain text. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. In this case, users at a lower level can easily obtain the password by viewing the configuration file. This brings security risks. Therefore, it is recommended that you select **cipher** to save the password in cipher text.	-
auth-key	Specifies the password.	A string of case-sensitive characters, spaces not supported. When the key is displayed in plaintext, its length ranges from 1 to 255; when the key is displayed in MD5 cipher text, its length ranges from 20 to 392. When double quotation marks are used around the string, spaces are allowed in the string.
keychain *keychain-name*	Specifies the keychain name, which is configured by running the **keychain** command.	The value is the name of an existing keychain.
sha256-compatible	Indicates that the calculated digest includes the authentication key when the SHA-256 algorithm is used for Keychain authentication. If this parameter is not specified, the calculated digest does not include the authentication key.	-

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, RSVP-TE neighbor view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

RSVP authentication can be configured to improve network reliability and security and prevent attacks initiated using messages modified or forged by unauthorized users.

RSVP authentication can prevent the setup of an illegal RSVP neighbor relationship using the following methods and protect the local node against attacks (such as malicious reservation of a larger number of bandwidth resources):

- An unauthorized node attempts to set up an RSVP 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.

Prerequisites

The **mpls rsvp-te** command is run to enable RSVP-TE in the MPLS view and interface view.

Precautions

The **mpls rsvp-te authentication** command run in either of the following views produces a specific result:

- If this command is run in the interface view, RSVP authentication takes effect on packets received by the interface. The interface sends RSVP-TE packets all carrying authentication information that is calculated using the key of the configured authentication mode, and authenticates all received RSVP-TE packets based on the configured key.
- If this command is run in the MPLS RSVP-TE neighbor view, RSVP authentication takes effect on packets received by the local RSVP-TE neighbor. The RSVP-TE packets sending by neighbor node all carry authentication information that is calculated using the key of the configured authentication mode, and authenticates all RSVP-TE packets sending to the neighbor node based on the configured key.

Parameters are optional for configuring HMAC-MD5 or keychain authentication:

- **cipher**: indicates HMAC-MD5 authentication with the key displayed in cipher text.
- **plain**: indicates HMAC-MD5 authentication with the key displayed in plain text.
- **keychain**: indicates keychain authentication with a globally configured keychain.
  - If the **sha256-compatible** parameter is specified and the SHA-256 algorithm is used for Keychain authentication, the calculated digest includes the authentication key.
  - If the **sha256-compatible** parameter is not specified and the SHA-256 algorithm is used for Keychain authentication, the digest is calculated using only original packets.

– If the SHA-256 algorithm is not used for Keychain authentication, the **sha256-compatible** parameter does not need to be specified.

Note that HMAC-MD5 encryption algorithm cannot ensure security. Keychain authentication is recommended.

Example

# Configure keychain authentication for the peer. The referenced keychain name is **kc1**.

```
<HUAWEI> system-view
[HUAWEI] keychain kc1 mode absolute
[HUAWEI-keychain-kc1] quit
[HUAWEI] mpls rsvp-te peer 10.0.0.1
[HUAWEI-mpls-rsvp-te-peer-10.0.0.1] mpls rsvp-te authentication keychain kc1
```

# Configure keychain authentication for the peer. The referenced keychain name is **kc1**.

```
<HUAWEI> system-view
[HUAWEI] keychain kc1 mode absolute
[HUAWEI-keychain-kc1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
[HUAWEI-Vlanif100] mpls rsvp-te authentication keychain kc1
```

# Configure keychain authentication for the peer. The referenced keychain name is **kc1**.

```
<HUAWEI> system-view
[HUAWEI] keychain kc1 mode absolute
[HUAWEI-keychain-kc1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te authentication keychain kc1
```

9.3.71 mpls rsvp-te authentication handshake

Function

The **mpls rsvp-te authentication handshake** command configures the RSVP-TE handshake mechanism.

The **undo mpls rsvp-te authentication handshake** command deletes the RSVP-TE handshake mechanism configuration.

By default, no RSVP-TE handshake mechanism is configured.

Format

mpls rsvp-te authentication handshake

undo mpls rsvp-te authentication handshake

Parameters

None

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, RSVP-TE neighbor view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Enhanced RSVP authentication can be configured to improve the system security and the capability to authenticate users in the unfavorable environment such as network congestion. Enhanced RSVP authentication functions are as follows:

- Sets the sliding window size for RSVP authentication messages.
- Configures the RSVP-TE handshake mechanism.

Traditional RSVP authentication is used to prevent an unauthorized remote node from setting up a neighbor relationship with the local node. It also prevents attacks (such as maliciously reserving a large number of bandwidth resources) initiated by a remote node after the remote node constructs pseudo RSVP messages to set up an RSVP neighbor relationship with the local node. Traditional RSVP authentication, however, cannot prevent anti-replay attacks or prevent the problem of neighbor relationship termination due to RSVP message disorder.

In an unfavorable environment, the **mpls rsvp-te authentication handshake** command can be used to configure the RSVP-TE handshake mechanism to prevent anti-replay and improve network security.

Prerequisites

The RSVP authentication function must have been enabled by running the **mpls rsvp-te authentication** { { **cipher** | **plain** } *auth-key* | **keychain** *keychain-name* [**sha256-compatible**] } command in the interface view or the MPLS RSVP-TE neighbor view.

Example

# Configure the RSVP-TE handshake mechanism.

```
<HUAWEI> system-view
[HUAWEI] mpls rsvp-te peer 172.16.1.1
[HUAWEI-mpls-rsvp-te-peer-172.16.1.1] mpls rsvp-te authentication cipher beijing123
[HUAWEI-mpls-rsvp-te-peer-172.16.1.1] mpls rsvp-te authentication handshake
```

# Configure the RSVP-TE handshake mechanism.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
```

```
[HUAWEI-Vlanif100] mpls rsvp-te authentication cipher beijing123
[HUAWEI-Vlanif100] mpls rsvp-te authentication handshake
```

# Configure the RSVP-TE handshake mechanism.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te authentication cipher beijing123
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te authentication handshake
```

9.3.72 mpls rsvp-te authentication lifetime

Function

The **mpls rsvp-te authentication lifetime** command sets the RSVP-TE authentication lifetime.

The **undo mpls rsvp-te authentication lifetime** command restores the default RSVP-TE authentication lifetime.

By default, the RSVP-TE authentication lifetime is 30 minutes.

Format

mpls rsvp-te authentication lifetime *lifetime*

undo mpls rsvp-te authentication lifetime

Parameters

Parameter	Description	Value
lifetime	Specifies the authentication lifetime.	The value ranges from 00:00:01 to 23:59:59 in the format of HH:MM:SS. The default value is 00:30:00.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, RSVP-TE neighbor view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The RSVP lifetime functions are as follows:

- When no CR-LSP exists between RSVP neighbors, the RSVP adjacency remains until the RSVP authentication lifetime expires. The configuration of the RSVP authentication time does not affect the status of existing CR-LSPs.
- This function can avoid continuous RSVP authentication. For example, when RSVP authentication is enabled between RTA and RTB, but the key is damaged because the RSVP messages sent from RTA to RTB are incorrect, RTB receives and discards the messages. This can cause RTA to continuously send RTB the faulty RSVP messages and RTB to continuously discard these RSVP messages. The authentication relationship between the neighbors, however, cannot be torn down. In this case, the authentication lifetime needs to be configured. When a neighbor is able to receive a valid RSVP message within the lifetime, the RSVP authentication lifetime resets. Otherwise, the authentication relationship between RSVP-TE neighbors is deleted after the authentication lifetime expires.

Prerequisites

The RSVP authentication function must have been enabled by running the **mpls rsvp-te authentication** { { **cipher** | **plain** } *auth-key* | **keychain** *keychain-name* [**sha256-compatible**] } command in the interface view or the MPLS RSVP-TE neighbor view.

Example

# Set the authentication lifetime to 40 minutes.

```
<HUAWEI> system-view
[HUAWEI] mpls rsvp-te peer 10.0.0.1
[HUAWEI-mpls-rsvp-te-peer-10.0.0.1] mpls rsvp-te authentication cipher beijing123
[HUAWEI-mpls-rsvp-te-peer-10.0.0.1] mpls rsvp-te authentication lifetime 00:40:00
```

# Set the authentication lifetime to 20 minutes.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
[HUAWEI-Vlanif100] mpls rsvp-te authentication cipher beijing123
[HUAWEI-Vlanif100] mpls rsvp-te authentication lifetime 00:20:00
```

# Set the authentication lifetime to 20 minutes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te authentication cipher beijing123
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te authentication lifetime 00:20:00
```

9.3.73 mpls rsvp-te authentication window-size

Function

The **mpls rsvp-te authentication window-size** command specifies the maximum number of RSVP authentication messages that can be received out of sequence.

The **undo mpls rsvp-te authentication window-size** command restores the default configuration.

By default, the maximum number of RSVP authentication messages that can be received out of sequence is 1.

Format

mpls rsvp-te authentication window-size *window-size*

undo mpls rsvp-te authentication window-size

Parameters

Parameter	Description	Value
window-size	Specifies the size of a message window.	The value is an integer that ranges from 1 to 64. The default size is 1.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, RSVP-TE neighbor view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Enhanced RSVP authentication can be configured to improve the system security and the capability to authenticate users in the unfavorable environment such as network congestion. Enhanced RSVP authentication functions are as follows:

- Sets the sliding window size for RSVP authentication messages.
- Configures the RSVP-TE handshake mechanism and sets the local password.

Traditional RSVP authentication is used to prevent an unauthorized remote node from setting up a neighbor relationship with the local node. It also prevents attacks (such as maliciously reserving a large number of bandwidth resources) initiated by a remote node after the remote node constructs pseudo RSVP messages to set up an RSVP neighbor relationship with the local node. Traditional RSVP authentication, however, cannot prevent anti-replay attacks or prevent the problem of neighbor relationship termination due to RSVP message disorder.

In an unfavorable environment, the **mpls rsvp-te authentication window-size** command can be used to set the maximum number of RSVP authentication messages that can be received. This setting prevents authentication termination due to RSVP message disorder.

Prerequisites

The RSVP authentication function must have been enabled by running the **mpls rsvp-te authentication** { { **cipher** | **plain** } *auth-key* | **keychain** *keychain-name*

[**sha256-compatible**] } command in the interface view or the MPLS RSVP-TE neighbor view.

Precautions

Setting the window size to a value greater than 32 is recommended. If the size of a sliding window is small, the RSVP messages may be dropped and the RSVP neighbor relationship may be terminated. If the size of a sliding window is set to 1, all the RSVP authentication messages that are received out of sequence are dropped.

Example

# Set the size of the message window to 64.

```
<HUAWEI> system-view
[HUAWEI] mpls rsvp-te peer 172.16.1.1
[HUAWEI-mpls-rsvp-te-peer-172.16.1.1] mpls rsvp-te authentication cipher beijing123
[HUAWEI-mpls-rsvp-te-peer-172.16.1.1] mpls rsvp-te authentication window-size 64
```

# Set the size of the message window to 1.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
[HUAWEI-Vlanif100] mpls rsvp-te authentication cipher beijing123
[HUAWEI-Vlanif100] mpls rsvp-te authentication window-size 1
```

# Set the size of the message window to 1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te authentication cipher beijing123
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te authentication window-size 1
```

9.3.74 mpls rsvp-te bfd

Function

The **mpls rsvp-te bfd** command sets parameters of a BFD session for RSVP on a specified interface.

The **undo mpls rsvp-te bfd** command restores the default configuration.

By default, no parameter of a BFD session for RSVP on a specified interface is set.

Format

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

undo mpls rsvp-te bfd { **min-tx-interval** | **min-rx-interval** | **detect-multiplier** } *

undo mpls rsvp-te bfd { **min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier* } *

Parameters

Parameter	Description	Value
min-tx-interval *tx-interval*	Specifies the interval at which BFD packets are sent.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
min-rx-interval *rx-interval*	Specifies the interval at which BFD packets are received.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
detect-multiplier *multiplier*	Specifies the local detection multiplier value of a BFD session.	An integer ranging from 3 to 50. The value is 3 by default.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Actual local interval at which BFD packets are sent = MAX { Local interval at which BFD packets are sent, Remote interval at which BFD packets are received }; Actual local interval at which BFD packets are received = MAX { Remote interval at which BFD packets are sent, Local interval at which BFD packets are received }; Local detection period = Actual interval at which BFD packets are received x Remote BFD detection multiplier.

For example:

- The local sending interval is 200 ms, while the local receiving interval is 300 ms, and the detection multiplier is 4.
- The remote sending interval is 100 ms, while the remote receiving interval is 600 ms, and the detection multiplier is 5.

Then,

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

Example

# Set the parameters for the BFD session on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
[HUAWEI-Vlanif100] mpls rsvp-te bfd min-tx-interval 50 detect-multiplier 5
```

# Set the parameters for the BFD session on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te bfd min-tx-interval 50 detect-multiplier 5
```

9.3.75 mpls rsvp-te bfd all-interfaces

Function

The **mpls rsvp-te bfd all-interfaces** command sets session parameters on all RSVP-TE interfaces.

The **undo mpls rsvp-te bfd all-interfaces** command restores the default configuration.

By default, no session parameters on all RSVP-TE interfaces are set.

Format

mpls rsvp-te bfd all-interfaces { **min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier* } *

undo mpls rsvp-te bfd all-interfaces { **min-tx-interval** | **min-rx-interval** | **detect-multiplier** } *

undo mpls rsvp-te bfd all-interfaces { **min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier* } *

Parameters

Parameter	Description	Value
min-tx-interval *tx-interval*	Specifies the interval at which BFD packets are sent.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.

Parameter	Description	Value
min-rx-interval *rx-interval*	Specifies the interval at which BFD packets are received.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
detect-multiplier *multiplier*	Specifies the local detection multiplier value of a BFD session.	An integer ranging from 3 to 50. The value is 3 by default.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Actual local interval at which BFD packets are sent = MAX { Local interval at which BFD packets are sent, Remote interval at which BFD packets are received }; Actual local interval at which BFD packets are received = MAX { Remote interval at which BFD packets are sent, Local interval at which BFD packets are received }; Local detection period = Actual interval at which BFD packets are received x Remote BFD detection multiplier.

For example:

- The local sending interval is 200 ms, while the local receiving interval is 300 ms, and the detection multiplier is 4.
- The remote sending interval is 100 ms, while the remote receiving interval is 600 ms, and the detection multiplier is 5.

Then,

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

Example

# Set the session parameters of all RSVP-TE interfaces.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te bfd all-interfaces min-tx-interval 500 min-rx-interval 400
```

9.3.76 mpls rsvp-te bfd all-interfaces enable

Function

The **mpls rsvp-te bfd all-interfaces enable** command globally enables BFD for RSVP.

The **undo mpls rsvp-te bfd all-interfaces enable** command restores the default configuration.

By default, BFD for RSVP is disabled.

Format

mpls rsvp-te bfd all-interfaces enable

undo mpls rsvp-te bfd all-interfaces enable

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

The **mpls rsvp-te bfd all-interfaces enable** command enables the capability of creating BFD sessions on all interfaces that are not blocked from BFD for RSVP.

Example

# Enable BFD for RSVP globally.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te bfd all-interfaces enable
```

9.3.77 mpls rsvp-te bfd block

Function

The **mpls rsvp-te bfd block** command blocks the BFD for RSVP capability on an interface.

The **undo mpls rsvp-te bfd block** command restores the default configuration.

By default, the BFD for RSVP capability on an interface is not blocked.

Format

mpls rsvp-te bfd block

undo mpls rsvp-te bfd block

Parameters

None

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls rsvp-te bfd block** command and the **mpls rsvp-te bfd enable** command are mutually exclusive.

The **mpls rsvp-te bfd block** command is similar to the **undo mpls rsvp-te bfd enable** command. Their differences are as follows:

- When the **undo mpls rsvp-te bfd enable** command is run to disable BFD for RSVP on an RSVP interface, the interface can obtain the BFD for RSVP capability after you configure the **mpls rsvp-te bfd all-interfaces enable** command in the MPLS view.
- When the **mpls rsvp-te bfd block** command is run on an interface, the interface cannot obtain the BFD for RSVP capability even if the **mpls rsvp-te bfd all-interfaces enable** command is run in the MPLS view.

NOTE

- To enable the BFD for RSVP capability on a majority of interfaces, you can run the **mpls rsvp-te bfd block** command on a minority of interfaces that do not need to be enabled with BFD for RSVP. Then, you can run the **mpls rsvp-te bfd all-interfaces enable** command in the MPLS view to enable the BFD for RSVP capability for the desired majority.
- To enable BFD for RSVP capability on a few interfaces, you can run the **mpls rsvp-te bfd enable** command on these specific interfaces. In addition, you can run the **undo mpls rsvp-te bfd enable** command or the **mpls rsvp-te bfd block** command to disable BFD for RSVP on these interfaces.

Example

# Disable BFD for RSVP on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
[HUAWEI-Vlanif100] mpls rsvp-te bfd block
```

# Disable BFD for RSVP on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te bfd block
```

9.3.78 mpls rsvp-te bfd enable

Function

The **mpls rsvp-te bfd enable** command enables the BFD for RSVP capability on an interface.

The **undo mpls rsvp-te bfd enable** command restores the default configuration.

By default, the BFD for RSVP capability on an interface is disabled.

Format

mpls rsvp-te bfd enable

undo mpls rsvp-te bfd enable

Parameters

None

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls rsvp-te bfd enable** command and the **mpls rsvp-te bfd block** command are mutually exclusive. When using these commands, note the following:

- If the **undo mpls rsvp-te bfd enable** command is run to disable BFD for RSVP on an RSVP interface, the interface can still obtain the BFD for RSVP capability after you configure the **mpls rsvp-te bfd all-interfaces enable** command in the MPLS view.
- If the **mpls rsvp-te bfd block** command is run on an interface, the interface cannot obtain the BFD for RSVP capability even if the **mpls rsvp-te bfd all-interfaces enable** command is run in the MPLS view.

NOTE

- To enable the BFD for RSVP capability on a majority of interfaces, you can run the **mpls rsvp-te bfd block** command on a minority of interfaces that do not need to be enabled with BFD for RSVP. Then, you can run the **mpls rsvp-te bfd all-interfaces enable** command in the MPLS view to enable the BFD for RSVP capability for the desired majority.
- To enable BFD for RSVP capability on a few interfaces, you can run the **mpls rsvp-te bfd enable** command on these specific interfaces. In addition, you can run the **undo mpls rsvp-te bfd enable** command or the **mpls rsvp-te bfd block** command to disable BFD for RSVP on these interfaces.

Example

# Enable the BFD for RSVP capability on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
[HUAWEI-Vlanif100] mpls rsvp-te bfd enable
```

# Enable the BFD for RSVP capability on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te bfd enable
```

9.3.79 mpls rsvp-te challenge-lost

Function

The **mpls rsvp-te challenge-lost** command sets the maximum number of times that the authenticator allows itself to retransmit Challenge messages during RSVP authentication.

The **undo mpls rsvp-te challenge-lost** command restores the default setting.

By default, the number of times for retransmitting Challenge messages is 3.

Format

mpls rsvp-te challenge-lost *max-miss-times*

undo mpls rsvp-te challenge-lost

Parameters

Parameter	Description	Value
max-miss-times	Specifies the number of times for retransmitting Challenge messages.	The value is an integer that ranges from 1 to 10. The default value is 3.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Assume node A and node B are RSVP neighbors and they need to authenticate each other. Node A authenticates node B as follows:

- Node A sends an RSVP message carrying an Integrity object to node B.
- When node B receives the message and detects that the key ID of node A is different from that in the Integrity object, node B sends a Challenge message to node A and starts a timer determining the time interval at which the Challenge message will be periodically retransmitted, and records the number of retries.
- When node A receives the Challenge message from node B, it directly copies the Challenge object in a message and adds its Integrity object to the message to generate a Response message to be sent to node B.
- When node B receives the Response message from node A, it checks whether the Challenge object in the Response message is consistent with the local Challenge object.
  - If the Challenge objects are consistent, node B stops and resets the timer for sending Challenge messages. Then, the authentication is successful.
  - If the Challenge message timer expires before node B receives the Response message, the authentication fails.

You can run the **mpls rsvp-te challenge-lost** command to change the maximum number of times for sending Challenge messages. In addition, you can use the **mpls rsvp-te retrans-timer challenge** command to change the interval for retransmitting Challenge messages.

Example

# Set the number of times for retransmitting Challenge messages to 5.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te challenge-lost 5
```

9.3.80 mpls rsvp-te fast-reroute-bandwidth compatible

Function

The **mpls rsvp-te fast-reroute-bandwidth compatible** command configures the bandwidth of FRR objects to be saved in the integer mode.

The **undo mpls rsvp-te fast-reroute-bandwidth compatible** command restores the default configuration.

By default, the bandwidth of FRR objects is saved in the float point mode.

Format

mpls rsvp-te fast-reroute-bandwidth compatible

undo mpls rsvp-te fast-reroute-bandwidth compatible

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

When Huawei devices communicate with devices from other vendors whose saving mode of the bandwidth of FRR objects is set to the integer mode, you need to run this command to set the saving mode of the bandwidth of FRR objects to the integer mode.

Example

# Configure the saving mode of the bandwidth of FRR objects as the integer mode.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te fast-reroute-bandwidth compatible
```

9.3.81 mpls rsvp-te hello-lost

Function

The **mpls rsvp-te hello-lost** command sets the maximum number of times for the consecutively lost Hello messages.

The **undo mpls rsvp-te hello-lost** command restores the default configuration.

By default, a maximum of three Hello messages can be lost consecutively.

Format

mpls rsvp-te hello-lost *times*

undo mpls rsvp-te hello-lost

Parameters

Parameter	Description	Value
times	Specifies the maximum number of times for the consecutively lost Hello messages.	The value is an integer that ranges from 3 to 10. The default value is 3.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the RSVP Hello extension function is enabled, you can run this command to set the maximum number of times for the consecutively lost Hello messages. If the number of times a node does not receive Hello messages consecutively exceeds the maximum value, it is considered that the link fails.

Prerequisites

The RSVP Hello extension function has been enabled by running the **mpls rsvp-te hello** command in the MPLS view.

Example

# Set the maximum number of times for the consecutively lost Hello messages to 5.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te hello
[HUAWEI-mpls] mpls rsvp-te hello-lost 5
```

9.3.82 mpls rsvp-te hello

Function

The **mpls rsvp-te hello** command enables the RSVP Hello extension function globally or on an interface.

The **undo mpls rsvp-te hello** command disables the RSVP Hello extension function globally or on an interface.

By default, the RSVP Hello extension function is disabled.

Format

mpls rsvp-te hello

undo mpls rsvp-te hello

Parameters

None

Views

MPLS view, VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The RSVP Hello extension mechanism provides fast detection on the reachability between RSVP nodes. The function increases network costs. Therefore, you need to determine whether to enable this function based on network requirements.

Prerequisites

RSVP-TE has been enabled by running the **mpls rsvp-te** command.

Precautions

The **undo mpls rsvp-te hello** command in the MPLS view disables the Hello function from all interfaces and disables GR on the local node.

You can run the **mpls rsvp-te hello** command in the MPLS view to enable the Hello function globally. After that, you can run the **mpls rsvp-te hello** command in the interface view to enable the Hello function on an interface.

The **undo mpls rsvp-te hello** command in the interface view is used to disable the Hello function on the interface. The **undo mpls rsvp-te hello** command in the MPLS view is used to disable the Hello function globally.

Example

# Enable the RSVP Hello extension function globally.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls rsvp-te
[HUAWEI-mpls] mpls rsvp-te hello
```

# Enable the RSVP Hello extension function on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
[HUAWEI-Vlanif100] mpls rsvp-te hello
```

# Enable the RSVP Hello extension function on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te hello
```

9.3.83 mpls rsvp-te hello basic-restart-time

Function

The **mpls rsvp-te hello basic-restart-time** command changes the basic time of RSVP GR.

The **undo mpls rsvp-te hello basic-restart-time** command restores the default setting.

By default, the basic time of RSVP GR is 90 seconds.

Format

mpls rsvp-te hello basic-restart-time *basic-restart-time*

undo mpls rsvp-te hello basic-restart-time

Parameters

Parameter	Description	Value
basic-restart-time	Specifies the basic time of RSVP GR.	The value is an integer that ranges from 30 to 1200, in seconds.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

At the beginning of the AMB/SMB switchover, an RSVP-TE GR node enters a period during which the data plane can forward data but the control plane is not restored. A Restart timer starts following this phase. The restart time is relevant to the basic time, the number of ingress LSPs and the number of non-ingress LSPs. The default basic time is 90 seconds. You can use the **mpls rsvp-te hello basic-restart-time** command to change the value of the basic time.

After the Restart timer expires, the node starts a Recovery timer. The recovery time is relevant to the restart time and total number of LSPs.

Prerequisites

RSVP GR has been enabled by running the **mpls rsvp-te hello full-gr** command in the MPLS view.

Example

# Set the basic time of RSVP GR to 39 seconds.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te hello basic-restart-time 39
```

9.3.84 mpls rsvp-te hello full-gr

Function

The **mpls rsvp-te hello full-gr** command enables RSVP GR and RSVP GR Helper.

The **undo mpls rsvp-te hello full-gr** command restores the default configurations.

By default, RSVP GR and RSVP GR Helper are disabled.

Format

mpls rsvp-te hello full-gr

undo mpls rsvp-te hello full-gr

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

The RSVP Hello extension function has been enabled by running the **mpls rsvp-te hello** command.

Example

# Enable RSVP GR and RSVP GR Helper.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te
[HUAWEI-mpls] mpls rsvp-te hello
[HUAWEI-mpls] mpls rsvp-te hello full-gr
```

9.3.85 mpls rsvp-te hello nodeid-session

Function

The **mpls rsvp-te hello nodeid-session** command establishes a Hello session between a PLR node and an MP node and specifies the ID of a single-hop or multi-hop node.

The **undo mpls rsvp-te hello nodeid-session** command restores the default configuration.

By default, no Hello session is established between a PLR node and an MP node.

Format

mpls rsvp-te hello nodeid-session *ip-address*

undo mpls rsvp-te hello nodeid-session [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the LSR ID of a neighbor.	The value is in dotted decimal notation.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

On a TE FRR network, to ensure the protection of the primary tunnel when FRR and RSVP GR simultaneously occur, run the **mpls rsvp-te hello nodeid-session** command to establish a Hello session between a PLR node and an MP node.

Example

# Establish a Hello session between the PLR and MP along the bypass tunnel.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te hello
[HUAWEI-mpls] mpls rsvp-te hello nodeid-session 10.0.0.1
```

9.3.86 mpls rsvp-te hello support-peer-gr

Function

The **mpls rsvp-te hello support-peer-gr** command enables RSVP GR Helper.

The **undo mpls rsvp-te hello support-peer-gr** command restores the default configuration.

By default, RSVP GR Helper is disabled.

Format

mpls rsvp-te hello support-peer-gr

undo mpls rsvp-te hello support-peer-gr

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Prerequisites

The RSVP Hello extension function has been enabled by running the **mpls rsvp-te hello** command.

Precautions

If the **mpls rsvp-te hello full-gr** command is run on an RSVP node, this node has the capability of RSVP GR Helper. If a node is a GR supporter rather than a GR node, run the **mpls rsvp-te hello support-peer-gr** command.

To change a node from a GR node to a GR supporter, you must run the **undo mpls rsvp-te hello full-gr** command, then run the **mpls rsvp-te hello support-peer-gr** command.

Example

# Enable RSVP GR Helper.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te
[HUAWEI-mpls] mpls rsvp-te hello
[HUAWEI-mpls] mpls rsvp-te hello support-peer-gr
```

9.3.87 mpls rsvp-te keep-multiplier

Function

The **mpls rsvp-te keep-multiplier** command sets the number of retry times allowed for RSVP Refresh messages.

The **undo mpls rsvp-te keep-multiplier** command restores the default settings.

The number of retry times allowed for RSVP Refresh messages is 3 by default.

Format

mpls rsvp-te keep-multiplier *keep-multiplier-number*

undo mpls rsvp-te keep-multiplier

Parameters

Parameter	Description	Value
keep-multiplier-number	Specifies the number of retry times allowed for RSVP Refresh messages.	The value is an integer that ranges from 3 to 255. The default value is 3.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a node does not receive any Refresh message about PSB or RSB within a specified time period, the node deletes the state. You can run this command to modify the number of retry times for Refresh messages to change of the timeout period.

Prerequisites

RSVP-TE has been enabled by running the **mpls rsvp-te** command.

Precautions

The timeout period is calculated by using the following formula:

Timeout period = (*keep-multiplier-number* + 0.5) x 1.5 x *refresh-interval*.

In the formula, *keep-multiplier-number* specifies the number of retry times allowed for RSVP Refresh messages; *refresh-interval* specifies the interval at which RSVP Refresh messages are sent. To set these two parameters, run the **mpls rsvp-te timer refresh** command.

Example

# Set the number of retry times for RSVP Refresh messages to 5.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te keep-multiplier 5
```

9.3.88 mpls rsvp-te peer

Function

The **mpls rsvp-te peer** command sets up an RSVP neighbor node and displays the MPLS RSVP-TE neighbor view.

The **undo mpls rsvp-te peer** command deletes an RSVP neighbor node.

No RSVP neighbor node is set up by default.

Format

mpls rsvp-te peer *ip-address*

undo mpls rsvp-te peer *ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a neighbor interface or the LSR ID. The LSR ID is specified in the **mpls lsr-id** command.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Prerequisites

RSVP-TE has been enabled by running the **mpls rsvp-te** command in the MPLS view.

Precautions

You can run this command on two neighboring devices to configure neighbor nodes. Then you can configure these neighbors with other functions such as authentication and handshake. The command functions differ according to the values of *ip-address*.

- When *ip-address* is the LSR-ID of a neighbor, the command takes effect on an entire device.
- When *ip-address* is the IP address of a neighbor interface, the command takes effect only on the single interface.

NOTE

If a neighbor node is identified by its LSR-ID, CSPF must be enabled on two neighboring devices where RSVP authentication is required.

Example

# Set up an RSVP neighbor node and displays the MPLS RSVP-TE neighbor view.

```
<HUAWEI> system-view
[HUAWEI] mpls rsvp-te peer 10.0.0.1
[HUAWEI-mpls-rsvp-te-peer-10.0.0.1]
```

9.3.89 mpls rsvp-te resv-rro

Function

The **mpls rsvp-te resv-rro** command configures record route objects (RROs) carried in Resv messages.

The **undo mpls rsvp-te resv-rro** command restores the default setting.

By default, the labels carried in the transit LSP RRO in turn are inbound interface address with upstream label, LSR ID with upstream label, and outbound interface address. The labels carried in the egress LSP RRO in turn are inbound interface address with upstream label, LSR ID with upstream label.

Format

mpls rsvp-te resv-rro transit { { **incoming** | **incoming-with-label** } | { **routerid** | **routerid-with-label** } | { **outgoing** | **outgoing-with-label** } } *

mpls rsvp-te resv-rro egress { { **incoming** | **incoming-with-label** } | { **routerid** | **routerid-with-label** } } *

undo mpls rsvp-te resv-rro transit

undo mpls rsvp-te resv-rro egress

Parameters

Parameter	Description	Value
transit	Indicates a transit node.	-
incoming	Indicates an inbound interface address.	-
incoming-with-label	Indicates an inbound interface address and upstream label.	-
routerid	Indicates an LSR ID.	-
routerid-with-label	Indicates an LSR ID and an upstream label.	-
outgoing	Indicates an outbound interface address.	-
outgoing-with-label	Indicates an outbound interface address and a downstream label.	-
egress	Indicates an egress.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Two devices of different types must have the same RRO configuration to ensure that they can communicate with each other. You can run the **mpls rsvp-te resv-rro** command to configure RROs carried in Resv messages.

Precautions

The modification takes effect only for new LSPs.

Example

# Configure the transit LSP RRO to carry the following labels: LSR ID with upstream label, inbound interface address, and outbound interface address with downstream label.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te resv-rro transit routerid-with-label incoming outgoing-with-label
```

# Configure the egress LSP RRO to carry the following labels: LSR ID with upstream label, and inbound interface address.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te resv-rro egress routerid-with-label incoming
```

9.3.90 mpls rsvp-te resvconfirm

Function

The **mpls rsvp-te resvconfirm** command enables the reservation confirmation mechanism on a node.

The **undo mpls rsvp-te resvconfirm** command disables the reservation confirmation mechanism.

The mechanism is disabled on a node by default.

Format

mpls rsvp-te resvconfirm

undo mpls rsvp-te resvconfirm

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

The **mpls rsvp-te resvconfirm** command is configured on the egress of the TE tunnel.

Example

# Enable the reservation confirmation mechanism on the local node.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te resvconfirm
```

9.3.91 mpls rsvp-te retrans-timer challenge

Function

The **mpls rsvp-te retrans-timer challenge** command configures the interval at which a Challenge message is retransmitted.

The **undo mpls rsvp-te retrans-timer challenge** command restores the default value.

The interval at which a Challenge message is retransmitted is set to 1000 milliseconds by default.

Format

mpls rsvp-te retrans-timer challenge *retransmission-interval*

undo mpls rsvp-te retrans-timer challenge

Parameters

Parameter	Description	Value
retransmission-interval	Specifies the interval at which a Challenge message is retransmitted.	An integer ranging from 500 to 10000 in milliseconds. The value is 1000 milliseconds by default.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Assume node A and node B are RSVP neighbors and they need to authenticate each other. Node A authenticates node B as follows:

- Node A sends an RSVP message carrying an Integrity object to node B.
- When node B receives the message and detects that the key ID of node A is different from that in the Integrity object, node B sends a Challenge message to node A and starts a timer determining the time interval at which the Challenge message will be periodically retransmitted, and records the number of retries.
- When node A receives the Challenge message from node B, it directly copies the Challenge object in a message and adds its Integrity object to the message to generate a Response message to be sent to node B.
- When node B receives the Response message from node A, it checks whether the Challenge object in the Response message is consistent with the local Challenge object.
  - If the Challenge objects are consistent, node B stops and resets the timer for sending Challenge messages. Then, the authentication is successful.
  - If the Challenge message timer expires before node B receives the Response message, the authentication fails.

You can run the **mpls rsvp-te challenge-lost** command to change the maximum number of attempts to send Challenge messages. In addition, you can use the

mpls rsvp-te retrans-timer challenge command to change the interval at which a Challenge message is retransmitted.

Example

# Set the interval for retransmitting a Challenge message to 800 ms.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te retrans-timer challenge 800
```

9.3.92 mpls rsvp-te send-message

Function

The **mpls rsvp-te send-message** command configures the formats of objects in a sent message.

The **undo mpls rsvp-te send-message** command restores the default configuration.

By default, the formats of objects in the sent message are not configured.

Format

mpls rsvp-te send-message { **suggest-label** | **extend-class-type value-length-type** | **session-attribute without-affinity** | **down-reason** }

undo mpls rsvp-te send-message { **suggest-label** | **extend-class-type value-length-type** | **session-attribute without-affinity** | **down-reason** }

Parameters

Parameter	Description	Value
suggest-label	Indicates that an RSVP message carries the suggest-label object.	-
extend-class-type value-length-type	Indicates that the encoding format of the extend-class-type object in an RSVP message is value-length-type.	-
session-attribute without-affinity	Indicates that the session-attribute in an RSVP message does not carry the affinity attribute.	-
down-reason	Indicates that RSVP messages carry the down-reason object.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **mpls rsvp-te send-message** command controls the formats of objects in the messages sent by nodes. If required, you can use this command to adjust the transmission of messages so that downstream nodes can use the carried object format in processing.

When a Huawei device attempts to communicate with a non-Huawei device, RSVP messages sent by the non-Huawei device may not support the affinity attribute, causing a communication failure. To allow successful communication, run the **mpls rsvp-te send-message session-attribute without-affinity** command to allow the Huawei device to receive RSVP messages without the affinity attribute.

If you want an ingress to learn RSVP-TE tunnel Down causes of the transit and egress nodes, run the **mpls rsvp-te send-message down-reason** command on the transit and egress nodes, facilitating fault locating.

Precautions

The modification takes effect only for new LSPs.

Configurations of the four formats of objects in a sent message can take effect simultaneously.

Example

# Include the suggest-label object from a message.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te send-message suggest-label
```

# Set the encoding format of the extend-class-type object in an RSVP message to value-length-type.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te send-message extend-class-type value-length-type
```

# Allow a message to carry the session-attribute object without the affinity attribute.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te send-message session-attribute without-affinity
```

# Configure RSVP messages to carry the down-reason object.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te send-message down-reason
```

9.3.93 mpls rsvp-te srefresh

Function

The **mpls rsvp-te srefresh** command enables the summary refresh (Srefresh) function on an interface or globally.

The **undo mpls rsvp-te srefresh** command disables the Srefresh function.

The Srefresh function is disabled by default.

Format

mpls rsvp-te srefresh

undo mpls rsvp-te srefresh

Parameters

None

Views

MPLS view, VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Each RSVP session needs to generate, send, receive, and process RSVP Path messages and Resv message within the refresh period. With an increasing number of RSVP sessions, a large number of Refresh messages are generated to maintain the RSVP soft state. When an RSVP message, not an RSVP Refresh message, is dropped, reliability is deteriorated and causes delay. The Srefresh extension can solve the preceding problems. The summary refresh mechanism reduces the required number of Refresh messages and improves reliability of RSVP messages and efficiency of resource usage.

After the Srefresh function is enabled in the MPLS view, the Srefresh function is enabled globally. In addition, the interface enabled with the Srefresh function can refresh the path status and the reservation status by sending Srefresh messages, rather than Path or Resv messages.

Example

# Enable the Srefresh function globally.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls rsvp-te
[HUAWEI-mpls] mpls rsvp-te srefresh
```

# Enable the Srefresh function on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
[HUAWEI-Vlanif100] mpls rsvp-te srefresh
```

# Enable the Srefresh function on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te srefresh
```

9.3.94 mpls rsvp-te timer hello

Function

The **mpls rsvp-te timer hello** command sets an interval at which Hello messages are sent.

The **undo mpls rsvp-te timer hello** command restores the default setting.

The interval at which Hello messages are sent is 3 seconds by default.

Format

mpls rsvp-te timer hello *interval*

undo mpls rsvp-te timer hello

Parameters

Parameter	Description	Value
interval	Specifies the interval at which Hello messages are sent.	The value is an integer that ranges from 1 to 25, in seconds. The default value is 3s.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

The RSVP Hello extension function has been enabled by running the **mpls rsvp-te hello** command in the MPLS view.

NOTE

If the interval at which Hello messages are sent is changed, the new interval can only take effect after the previous Hello timer expires.

Example

# Set the interval at which Hello messages are sent to 5s.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls rsvp-te
[HUAWEI-mpls] mpls rsvp-te hello
[HUAWEI-mpls] mpls rsvp-te timer hello 5
```

9.3.95 mpls rsvp-te timer refresh

Function

The **mpls rsvp-te timer refresh** command sets an interval at which RSVP Refresh messages are sent.

The **undo mpls rsvp-te timer refresh** command restores the default setting.

The time interval is 30 seconds by default.

Format

mpls rsvp-te timer refresh *refresh-interval*

undo mpls rsvp-te timer refresh

Parameters

Parameter	Description	Value
refresh-interval	Specifies the interval at which RSVP Refresh messages are sent.	An integer ranging from 10 to 65535 in seconds.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

RSVP-TE has been enabled by running the **mpls rsvp-te** command.

NOTE

If the interval at which RSVP Refresh messages are sent is changed, the new interval can only take effect after the previous refreshing timer expires. Therefore, you are not recommended to set an excessively long refreshing interval, or frequently change a refreshing interval.

Example

# Set the interval at which RSVP Refresh messages are sent to 60s.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls rsvp-te
[HUAWEI-mpls] mpls rsvp-te timer refresh 60
```

9.3.96 mpls rsvp-te timer retransmission

Function

The **mpls rsvp-te timer retransmission** command adjusts retransmission-related parameters on an interface.

The **undo mpls rsvp-te timer retransmission** command restores the default settings.

By default, the retransmission incremental is 1 and the timeout period of a retransmission timer is 5000 ms.

Format

mpls rsvp-te timer retransmission { **increment-value** *increment* | **retransmit-value** *interval* } *

undo mpls rsvp-te timer retransmission [**increment-value** [*increment*] | **retransmit-value** [*interval*]] *

Parameters

Parameter	Description	Value
increment-value *increment*	Specifies the retransmission incremental value.	The value is an integer that ranges from 1 to 10. The default value is 1.
retransmit-value *interval*	Specifies the timeout period of a retransmission timer.	The value is an integer that ranges from 500 to 5000, in milliseconds. The default value is 5000 ms.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The relationship between *increment* and *interval*: Next retransmission *interval* = Current retransmission *interval* x (1 + *increment*)

Prerequisites

The Srefresh function has been enabled by running the **mpls rsvp-te srefresh** command in the MPLS view.

Example

# Set the timeout period of the retransmission timer to 500 ms and the increment to 2 on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
[HUAWEI-Vlanif100] mpls rsvp-te timer retransmission retransmit-value 500 increment-value 2
```

# Set the timeout period of the retransmission timer to 500 ms and the increment to 2 on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te timer retransmission retransmit-value 500 increment-value 2
```

9.3.97 mpls te

Function

The **mpls te** command enables MPLS TE.

The **undo mpls te** command disables MPLS TE.

MPLS TE is disabled by default.

Format

mpls te

undo mpls te

Parameters

None

Views

MPLS view, VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When running the **mpls te** command in the MPLS view, you can globally enable MPLS TE. When running the **mpls te** command in the interface view, you can enable MPLS TE on a specified interface. MPLS TE can only be enabled on interfaces after the function is enabled globally.

Precautions

NOTICE

When the MPLS TE is disabled in the interface view, all the CR-LSPs on the current interface change to Down.

After the **undo mpls te** command is run in the MPLS view, MPLS TE services may be interrupted and all MPLS TE configurations are deleted. To restore the MPLS TE services, reconfigure these commands.

Example

# Enable MPLS TE globally.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 1.1.1.9
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
```

# Enable MPLS TE on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
```

# Enable MPLS TE on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
```

9.3.98 mpls te affinity property

Function

The **mpls te affinity property** command configures the affinity property for an MPLS TE tunnel.

The **undo mpls te affinity property** command restores the default settings.

By default, both the affinity value and the affinity mask are 0x0 for an MPLS TE tunnel.

Format

mpls te affinity property *properties* [**mask** *mask-value*] [**secondary** | **best-effort**]

undo mpls te affinity property [**secondary** | **best-effort**]

undo mpls te affinity property *properties* [**mask** *mask-value*] { **secondary** | **best-effort** }

Parameters

Parameter	Description	Value
properties	Specifies the affinity property of links that carry a tunnel.	The value is in hexadecimal notation and is of 32 bits with each bit representing an attribute. The value ranges from 0x0 to 0xFFFFFFFF. The default value is 0x0.
mask *mask-value*	Specifies the link property to be checked.	The value is in hexadecimal notation and is of 32 bits with each bit representing an attribute. The value ranges from 0x0 to 0xFFFFFFFF. The default value is 0x0.
secondary	Indicates the affinity property of a backup CR-LSP.	-
best-effort	Indicates the affinity property of the best-effort path.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Affinity property masks determine the link properties that should be checked by a device.

To ensure that a link can be used by a tunnel, for the bits that are 1 in a mask, it is required that at least one bit in the administrative group and the corresponding bit in the affinity property be 1. In addition, if the bits in the affinity property are 0, the corresponding bits in the administrative group cannot be 1.

After an affinity property for the MPLS TE tunnel is changed and the new configuration is committed, the established LSPs can be affected, and the path of the TE tunnel is recalculated.

Example

# Set the affinity property of Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te affinity property a04 mask e0c
[HUAWEI-Tunnel1] mpls te commit
```

# Set the affinity property of the backup CR-LSP and the best-effort path.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te backup hot-standby
[HUAWEI-Tunnel1] mpls te backup ordinary best-effort
[HUAWEI-Tunnel1] mpls te affinity property a04 mask e0c secondary
[HUAWEI-Tunnel1] mpls te affinity property a04 mask e0c best-effort
[HUAWEI-Tunnel1] mpls te commit
```

9.3.99 mpls te auto-bandwidth

Function

The **mpls te auto-bandwidth** command configures automatic bandwidth adjustment of a tunnel.

The **undo mpls te auto-bandwidth** command disables automatic bandwidth adjustment.

Automatic bandwidth adjustment is disabled by default.

NOTE

Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730-H, and S6730S-H support this command.

Format

mpls te auto-bandwidth { **adjustment** [**threshold** *percent*] | **collect-bw** } [**frequency** *interval*] [**max-bw** *max-bandwidth* **min-bw** *min-bandwidth*]

undo mpls te auto-bandwidth

Parameters

Parameter	Description	Value
adjustment	Enables automatic bandwidth adjustment.	-
threshold *percent*	Specifies the threshold of the difference between the new and existing bandwidth. The value is expressed in percentage.	An integer ranging from 0 to 100. The default value is 0.
collect-bw	Collects output rate information of a tunnel without adjusting the bandwidth.	-
frequency *interval*	Specifies the time interval for automatic bandwidth adjustment.	An integer ranging from 300 to 604800 in seconds. The default value is 86400. The recommended value is not less than the interval for sampling the output rate of a tunnel specified in the **mpls te timer auto-bandwidth** command.
max-bw *max-bandwidth*	Specifies the maximum allowable bandwidth.	An integer ranging from 0 to 4000000000 in kbit/s. The default value is 4294901760.
min-bw *min-bandwidth*	Specifies the minimum allowable bandwidth.	An integer ranging from 0 to 4000000000 in kbit/s. The default value is 0.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The bandwidth of a tunnel can be set manually, but is not adaptable to changeable traffic on the tunnel. To ensure continuity of traffic, reserve enough bandwidth for the maximum volume of traffic. This provides enough bandwidth for traffic, but wastes bandwidth resources. To save bandwidth, configure automatic bandwidth adjustment by running the **mpls te auto-bandwidth** command.

After automatic bandwidth adjustment is enabled, run the **mpls te timer auto-bandwidth** command to configure periodic sampling and obtain the average bandwidth of the MPLS TE tunnel during a sampling interval. The system calculates the average bandwidth during the sampling interval and attempts to establish an MPLS TE tunnel based on the average bandwidth.

- After the MPLS TE tunnel is established, traffic switches to the new MPLS TE tunnel, and the original is deleted.
- If a new MPLS TE tunnel fails to be established, traffic is still transmitted along the original MPLS TE tunnel. The bandwidth will be adjusted after the next sampling period expires.

Configuring the parameter **threshold** controls whether the bandwidth of an MPLS TE tunnel should be adjusted. The system compares the average bandwidth D within a sampling period with the actual bandwidth C. If the percentage of the bandwidth change in comparison to the actual bandwidth is greater than the **threshold** value, that is, (|D-C|÷C)×100 > **threshold**, the system adjusts the bandwidth.

If traffic volume fluctuates on a network but the bandwidth does not need to be adjusted accordingly, set the value of **threshold** to a larger value.

Precautions

The **mpls te auto-bandwidth** command cannot be configured with the following commands on the same tunnel interface:

- **mpls te route-pinning**
- **mpls te resv-style ff**
- **mpls te bandwidth** (tunnel interface view) with the multi-CT specified

Example

# Set the interval for automatic bandwidth adjustment to **1** hour.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te auto-bandwidth adjustment frequency 3600
```

9.3.100 mpls te auto-frr (MPLS view)

Function

The **mpls te auto-frr** command globally enables the TE Auto FRR function.

The **undo mpls te auto-frr** command globally disables the TE Auto FRR function.

TE Auto FRR is disabled by default.

Format

mpls te auto-frr

undo mpls te auto-frr

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **mpls te auto-frr** command to globally enable the TE Auto FRR function.

Precautions

After the TE Auto FRR function is enabled globally, all MPLS TE-enabled interfaces use node protection by default.

If TE Auto FRR is enabled globally, all interfaces that are enabled with MPLS TE on the device are automatically configured with the **mpls te auto-frr default** command by default. To disable TE Auto FRR on certain interfaces, run the **mpls te auto-frr block** command on these interfaces.

Example

# Enable the TE Auto FRR function.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te auto-frr
```

# Disable the TE Auto FRR function.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] undo mpls te auto-frr
```

9.3.101 mpls te auto-frr (interface view)

Function

The **mpls te auto-frr** command configures the TE Auto FRR function in the interface view.

The **undo mpls te auto-frr** command restores the default configuration.

The TE Auto FRR function is disabled on an interface by default.

Format

mpls te auto-frr { **default** | **link** | **node** | **block** }

undo mpls te auto-frr { **block** | **link** | **node** }

Parameters

Parameter	Description	Value
default	Indicates that the configuration of the TE Auto FRR function in the MPLS view is used by default. Only node protection is provided.	-
link	Indicates that only link protection is provided.	-
node	Indicates that node protection is provided. When the topology does not meet the requirement to set up a bypass CR-LSP for node protection, the penultimate hop (but not other hops) on the primary CR-LSP attempts to set up a bypass CR-LSP for link protection.	-
block	Disables the TE Auto FRR function in the interface view.	-

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the TE Auto FRR function is enabled globally, all MPLS TE-enabled interfaces can use the TE Auto FRR configuration configured in the MPLS view.

To disable the TE Auto FRR function on a specified interface, you must run the **mpls te auto-frr block** command. To enable link protection on a specified interface, you must run the **mpls te auto-frr link** command.

Prerequisites

MPLS TE has been enabled by running the **mpls te** command in the interface view.

Precautions

After the **mpls te auto-frr block** command is run on an interface, the interface does not have the TE Auto FRR capability, regardless of whether TE Auto FRR is already enabled or reenabled globally.

After the command **mpls te auto-frr** is configured in the MPLS view, the device provides only node protection when you run the **mpls te auto-frr default** or **mpls te auto-frr node** command on an interface. When the topology does not meet the requirement to set up a bypass CR-LSP for node protection, the penultimate hop (but not other hops) on the primary CR-LSP attempts to set up a bypass CR-LSP for link protection.

Example

# Enable TE Auto FRR that provides link protection on the interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls te auto-frr link
```

# Disable the TE Auto FRR function in the interface view.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls te auto-frr block
```

# Enable TE Auto FRR that provides node protection on the interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls te auto-frr node
```

9.3.102 mpls te auto-frr reoptimization

Function

The **mpls te auto-frr reoptimization** command enables auto bypass tunnel re-optimization.

The **undo mpls te auto-frr reoptimization** command disables auto bypass tunnel re-optimization.

By default, auto bypass tunnel re-optimization is disabled.

Format

mpls te auto-frr reoptimization [**frequency** *interval*]

undo mpls te auto-frr reoptimization

Parameters

Parameter	Description	Value
frequency *interval*	Indicates the re-optimization interval. Paths are recalculated at the *interval* based on auto bypass tunnel constraints. If an optimal path to the same destination is available, the system re-optimizes the auto bypass tunnel.	The value is an integer ranging from 60 to 604800, in seconds. The default value is 3600s (one hour).

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Network changes often cause the changes in optimal paths. Run the **mpls te auto-frr reoptimization** to allow paths to be recalculated at certain intervals for an auto bypass tunnel. If an optimal path to the same destination is found due to some reasons, such as the changes in the cost, a new auto bypass tunnel will be set up over this optimal path. In this manner, network resources are optimized.

Auto bypass tunnel re-optimization can be classified into the following modes:

- Automatic re-optimization: Auto bypass tunnels are re-optimized at intervals, requiring no manual intervention. The **mpls te auto-frr reoptimization** command can be used to implement the function, and this command takes effect on the auto bypass tunnels that have been already set up successfully.
- Manual re-optimization: After the **mpls te auto-frr reoptimization** command is run, run the **mpls te reoptimization (user view)** command to re-optimize auto bypass tunnels manually.

Prerequisites

MPLS TE has been enabled using the **mpls te** command.

Example

# Configure auto bypass tunnel re-optimization at 8939-second intervals.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls te auto-frr reoptimization frequency 8939
```

9.3.103 mpls te backup

Function

The **mpls te backup** command specifies the backup mode of an existing tunnel.

The **undo mpls te backup** command restores the default configuration.

By default, no tunnel is backed up.

Format

mpls te backup ordinary [**best-effort**]

mpls te backup hot-standby [**mode** { **revertive** [**wtr** *interval*] | **non-revertive** } | **dynamic-bandwidth**] *

mpls te backup hot-standby wtr *interval* [**dynamic-bandwidth**]

mpls te backup hot-standby dynamic-bandwidth wtr *interval*

undo mpls te backup { **hot-standby** [**mode** { **revertive** [**wtr** [*interval*]] | **non-revertive** } | **dynamic-bandwidth**] * | **ordinary** }

Parameters

Parameter	Description	Value
ordinary	Enables the ordinary backup mode. In ordinary backup mode, an ordinary backup CR-LSP is created only after the primary CR-LSP fails.	-
hot-standby	Enables the hot-standby mode. In hot-standby mode, both the primary and backup CR-LSP are set up. If the primary CR-LSP fails, traffic is immediately switched to the hot-standby CR-LSP.	-
dynamic-bandwidth	Enables the dynamic bandwidth function for a hot-standby CR-LSP.	-
wtr *interval*	Specifies the wait-to-restore (WTR) time in hot standby.	The value is an integer that ranges from 0 to 2592000, in seconds. The default value is 10 seconds.
best-effort	Enables the best-effort path mode. When both the primary and backup CR-LSPs fail, the system triggers the establishment of a best-effort path.	-

Parameter	Description	Value
mode { **revertive** | **non-revertive** }	Specifies the revertive mode. ● **revertive**: The current mode can be switched to the original mode. ● **non-revertive**: The current mode cannot be switched to the original mode.	The default mode is **revertive**.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To help enhance the reliability of a CR-LSP, you are recommended to set up a backup CR-LSP to protect traffic on the primary CR-LSP.

You can select the following CR-LSP backup modes as required:

- Hot-standby mode: A hot-standby backup CR-LSP is set up over a separate path immediately after the primary CR-LSP is set up. When the CR-LSP transmitting services fails, traffic can be immediately switched to the other CR-LSP. However, additional bandwidth is needed in hot-standby mode.
- Ordinary backup mode: The system attempts to set up an ordinary backup CR-LSP over a new explicit path, only when the primary CR-LSP fails. No additional bandwidth is needed in ordinary backup mode. In the case that the primary CR-LSP fails, this mode provides a traffic switchover slower than that of the hot-standby mode.
- Best-effort path mode: When both the primary and backup CR-LSP fail, the system establishes a best-effort path. There are few constraints on the establishment of best-effort path; therefore, it is easy to set up. In best-effort path mode, packet loss is decreased, and certain QoS requirements may not be guaranteed.

Prerequisites

A tunnel ID has been configured by running the **mpls te tunnel-id** command.

Precautions

After tunnel backup is enabled, the route storing function is automatically enabled, regardless of whether the **mpls te record-route** command is run.

Tunnel backup and the function configured by running the **mpls te resv-style ff** command are mutually exclusive.

The **mpls te backup ordinary** command and the **mpls te backup ordinary best-effort** command cannot be configured together; otherwise, the previous configuration overrides the later one.

After initiating the dynamic bandwidth function for a hot-standby CR-LSP, the hot-standby CR-LSP does not occupy any bandwidth when bearing no traffic. If the primary CR-LSP fails, the system re-establishes a hot-standby CR-LSP with the expected bandwidth according to the Make-Before-Break mechanism. The new hot-standby CR-LSP now transmits traffic. The system then deletes the hot-standby CR-LSP with the bandwidth being 0 bit/s.

Example

# Enable hot standby for the current CR-LSP.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te backup hot-standby
[HUAWEI-Tunnel1] mpls te commit
```

9.3.104 mpls te backup frr-in-use

Function

The **mpls te backup frr-in-use** command allows a device to start a bypass CR-LSP if a primary CR-LSP becomes faulty (when the primary CR-LSP is in the FRR-in-use state), and to attempt to set up a backup CR-LSP while the system is restoring the primary CR-LSP.

The **undo mpls te backup frr-in-use** command restores the default configuration.

If the primary CR-LSP is faulty, the system starts the bypass CR-LSP and attempts to restore the primary CR-LSP, but does not set up a backup CR-LSP by default.

Format

mpls te backup frr-in-use

undo mpls te backup frr-in-use

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the primary CR-LSP is faulty, the system starts the bypass CR-LSP and tries to restore the primary CR-LSP the same time it sets up a backup CR-LSP.

Prerequisites

End-to-end protection in hot standby or ordinary backup mode has been enabled by running the **mpls te backup** { **hot-standby** | **ordinary** } command, and local protection of TE FRR has been enabled by running the **mpls te fast-reroute** command.

Precautions

If only the best-effort path is configured, rather than another end-to-end protection mode, the **mpls te backup frr-in-use** command cannot take effect.

After the **mpls te backup frr-in-use** command is run and if the primary CR-LSP is faulty:

- If ordinary backup is configured, the system tries to set up a backup CR-LSP when the traffic is switched to the bypass CR-LSP and also attempts to restore the primary CR-LSP. If the backup CR-LSP is set up successfully and the primary CR-LSP is not restored, traffic is switched to the backup CR-LSP.
- If hot standby is configured and the backup CR-LSP is in the Up state, the traffic is switched to the bypass CR-LSP and then immediately to the backup CR-LSP while the system attempts to restore the primary CR-LSP.

It is recommended that ordinary backup be configured together with the **mpls te backup frr-in-use** command. This saves bandwidth resources and improves tunnel security.

Example

# Configure the system to set up a backup CR-LSP the same time it starts the bypass CR-LSP and tries to restore the primary CR-LSP after the primary CR-LSP is faulty.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te backup ordinary
[HUAWEI-Tunnel1] mpls te fast-reroute
[HUAWEI-Tunnel1] mpls te backup frr-in-use
[HUAWEI-Tunnel1] mpls te commit
```

9.3.105 mpls te backup hot-standby overlap-path

Function

The **mpls te backup hot-standby overlap-path** command enables the path partially overlapping function for hot-standby CR-LSPs.

The **undo mpls te backup hot-standby overlap-path** command disables the path overlapping function for hot-standby CR-LSPs.

By default, the path partially overlapping function is disabled for hot-standby CR-LSPs.

Format

mpls te backup hot-standby overlap-path

undo mpls te backup hot-standby overlap-path

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

After the path overlapping function is configured, the path of a hot-standby CR-LSP can partially overlap the path of the primary CR-LSP when primary CR-LSP is not excluded by the system in path calculation.

Example

# Enable the path overlapping function for hot-standby CR-LSPs.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te backup hot-standby
[HUAWEI-Tunnel1] mpls te backup hot-standby overlap-path
[HUAWEI-Tunnel1] mpls te commit
```

9.3.106 mpls te backup hotstandby-lsp-constraint

Function

The **mpls te backup hotstandby-lsp-constraint** command sets the WTR time for a switchback, locks an attribute template, and enables the dynamic bandwidth function for a hot-standby CR-LSP.

The **undo mpls te backup hotstandby-lsp-constraint** command restores default settings.

By default, the interval between switchbacks is 10 seconds; no attribute template is locked; the dynamic bandwidth function is disabled for a hot-standby CR-LSP.

Format

mpls te backup hotstandby-lsp-constraint { **wtr** *interval* | **lock** | **dynamic-bandwidth** | **overlap-path** }

mpls te backup hotstandby-lsp-constraint mode { **revertive** [**wtr** *interval*] | **non-revertive** }

undo mpls te backup hotstandby-lsp-constraint { **wtr** | **lock** | **dynamic-bandwidth** | **overlap-path** }

undo mpls te backup hotstandby-lsp-constraint mode { **non-revertive** | **revertive wtr** }

Parameters

Parameter	Description	Value
dynamic-bandwidth	Enables the dynamic bandwidth function for a hot-standby CR-LSP.	-
lock	Enables the function of locking a hot-standby CR-LSP attribute template.	-
wtr *interval*	Specifies the WTR time for a switchback from a hot-standby CR-LSP.	The value is an integer that ranges from 0 to 2592000, in seconds. The default value is 10 seconds.
overlap-path	Indicates that if no other path is available, the hot-standby LSP can overlap the primary LSP.	-
mode { **revertive** | **non-revertive** }	Specifies the revertive mode. ● **revertive**: The current mode can be switched to the original mode. ● **non-revertive**: The current mode cannot be switched to the original mode.	The default mode is **revertive**.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The function of locking a hot-standby CR-LSP attribute template allows the system to lock a lower-priority attribute template that has been used by an exiting hot-standby CR-LSP. The system will not attempt to use a higher-priority template to set up a new hot-standby CR-LSP.

Prerequisites

The following configurations must be completed before the **mpls te backup hotstandby-lsp-constraint** command is run:

- Run the **mpls te primary-lsp-constraint** command to use attribute templates to set up a primary CR-LSP.
- Run the **mpls te hotstandby-lsp-constraint** command to use attribute template to set up a hot-standby CR-LSP.

Precautions

This command is valid only for the hot-standby CR-LSP that is set up using a CR-LSP attribute template. If a hot-standby CR-LSP is set up without a CR-LSP attribute template, the following commands apply:

- The **mpls te backup hot-standby wtr** *interval* command is used to set the WTR time for a switchback.
- The **mpls te backup hot-standby dynamic-bandwidth** command is used to enable the dynamic bandwidth function for the hot-standby CR-LSP.
- The **mpls te backup hot-standby overlap-path** command is used to enable the path overlapping function for hot-standby CR-LSPs that are not established using attribute templates.

The dynamic bandwidth function for the hot-standby CR-LSP prevents a hot-standby CR-LSP transmitting no traffic from using bandwidth resources. If the primary CR-LSP fails, the system attempts to re-establish a new hot-standby CR-LSP with the required bandwidth determined by the Make-Before-Break mechanism. After the new hot-standby CR-LSP takes over traffic, the bandwidth of the failed hot-standby CR-LSP becomes 0 bit/s and is deleted by the system.

Example

# Set the WTR time for a switchback from the hot-standby CR-LSP to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] mpls te primary-lsp-constraint lsp-attribute t1
[HUAWEI-Tunnel1] mpls te hotstandby-lsp-constraint 1 lsp-attribute t2
[HUAWEI-Tunnel1] mpls te backup hotstandby-lsp-constraint wtr 20
[HUAWEI-Tunnel1] mpls te commit
```

9.3.107 mpls te backup ordinary-lsp-constraint

Function

The **mpls te backup ordinary-lsp-constraint** command globally locks an attribute template for ordinary backup CR-LSPs.

The **undo mpls te backup ordinary-lsp-constraint** command restores the default setting.

The attribute template for ordinary backup CR-LSPs is unlocked by default.

Format

mpls te backup ordinary-lsp-constraint lock

undo mpls te backup ordinary-lsp-constraint lock

Parameters

Parameter	Description	Value
lock	Locks an attribute template for ordinary backup CR-LSPs.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Assume that an existing ordinary backup CR-LSP has been set up using a lower-priority attribute template. When the lower-priority attribute template is locked, the system does not attempt to use a higher-priority attribute template to set up a new ordinary backup CR-LSP, avoiding unnecessary traffic switchover.

Prerequisites

An ordinary backup CR-LSP has been set up using a CR-LSP attribute template by running the **mpls te ordinary-lsp-constraint** command.

Precautions

This command is valid only for an ordinary backup CR-LSP that is set up using a CR-LSP attribute template.

Example

# Lock an attribute template for ordinary backup CR-LSPs.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] mpls te primary-lsp-constraint lsp-attribute t1
[HUAWEI-Tunnel1] mpls te ordinary-lsp-constraint 2 lsp-attribute t2
[HUAWEI-Tunnel1] mpls te ordinary-lsp-constraint 3 lsp-attribute t3
[HUAWEI-Tunnel1] mpls te backup ordinary-lsp-constraint lock
[HUAWEI-Tunnel1] mpls te commit
```

9.3.108 mpls te bandwidth (interface view)

Function

The **mpls te bandwidth** command sets the BC bandwidth for a link.

The **undo mpls te bandwidth** command restores the default setting.

By default, no BC bandwidth is configured for a link.

Format

mpls te bandwidth { **bc0** *bc0-bw-value* | **bc1** *bc1-bw-value* } *

undo mpls te bandwidth

Parameters

Parameter	Description	Value
bc0 *bc0-bw-value*	Specifies the bandwidth of BC0.	The value is an integer that ranges from 1 to 4000000000, in kbit/s. The default value is 1.
bc1 *bc1-bw-value*	Specifies the bandwidth of BC1.	The value is an integer that ranges from 1 to 4000000000, in kbit/s. The default value is 1.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In real-world situations, the bandwidth value is set on outbound interfaces along links of a TE tunnel that requires sufficient bandwidth.

NOTE

The configured bandwidth takes effect only during tunnel establishment and protocol negotiation, and does not limit the bandwidth for traffic forwarding.

Precautions

To change bandwidth BC values, reconfigure the **mpls te bandwidth** command. The last configured BC bandwidth value overrides the previous one.

One or more BC bandwidth values can be set in a single command in a random order.

A BC bandwidth value can be changed only to a value greater than or equal to the set one. For example, the BC0 bandwidth of 10 Mbit/s can be changed to 10 or a larger value.

Example

# Set the maximum reservable bandwidth to 10000 kbit/s, the bandwidth of BC0 to 1000 kbit/s on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls te bandwidth max-reservable-bandwidth 10000
[HUAWEI-Vlanif100] mpls te bandwidth bc0 1000
```

# Set the maximum reservable bandwidth to 10000 kbit/s, the bandwidth of BC0 to 1000 kbit/s on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls te bandwidth max-reservable-bandwidth 10000
[HUAWEI-GigabitEthernet0/0/1] mpls te bandwidth bc0 1000
```

9.3.109 mpls te bandwidth (tunnel interface view)

Function

The **mpls te bandwidth** command sets the bandwidth of an MPLS TE tunnel.

The **undo mpls te bandwidth** command restores the default settings.

By default, the bandwidth of an MPLS TE tunnel is not set.

Format

mpls te bandwidth { **ct0** *ct0-bw-value* | **ct1** *ct1-bw-value* }

undo mpls te bandwidth { **all** | **ct0** [*ct0-bw-value*] | **ct1** [*ct1-bw-value*] }

Parameters

Parameter	Description	Value
ct0 *ct0-bw-value*	Specifies the bandwidth reserved for a TE tunnel of CT0.	*ct0-bw-value* is an integer that ranges from 1 to 4000000000, in kbit/s.
ct1 *ct1-bw-value*	Specifies the bandwidth reserved for a TE tunnel of CT1.	*ct1-bw-value* is an integer that ranges from 1 to 4000000000, in kbit/s.
all	Deletes bandwidth for all CTs.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

NOTE

The configured bandwidth takes effect only during tunnel establishment and protocol negotiation, and does not limit the bandwidth for traffic forwarding.

The **undo mpls te bandwidth** command is used to restore the default settings of all CTs or specified CTs:

- **undo mpls te bandwidth all**: deletes all configured bandwidth.
- **undo mpls te bandwidth** { **ct0** | **ct1** }: deletes the bandwidth of the specified CT configured on the current TE tunnel.

Example

# Set the bandwidth required by Tunnel1. The bandwidth of CT0 is 2000 kbit/s.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 10.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te bandwidth ct0 2000
[HUAWEI-Tunnel1] mpls te commit
```

9.3.110 mpls te bandwidth change thresholds

Function

The **mpls te bandwidth change thresholds** command sets the percentage threshold of the physical link bandwidth used by an MPLS TE tunnel for flooding link information.

The **undo mpls te bandwidth change thresholds** command restores the default settings.

If the ratio of the reserved (or released) bandwidth for a tunnel to the remaining bandwidth in a Traffic Engineering Database (TEDB) is equal to or greater than 10%, an IGP floods link information and CSPF updates the TEDB by default.

Format

mpls te bandwidth change thresholds { **down** | **up** } *percent*

undo mpls te bandwidth change thresholds { **down** | **up** }

Parameters

Parameter	Description	Value
down	Indicates the flooding threshold of the bandwidth used by an MPLS TE tunnel. If the ratio of the bandwidth used by an MPLS TE tunnel to the remaining link bandwidth in a TEDB is equal to or greater than the threshold, an IGP floods link information and CSPF updates the TEDB.	-
up	Indicates the flooding threshold of the bandwidth released by an MPLS TE tunnel. If the ratio of the bandwidth released by an MPLS TE tunnel to the remaining link bandwidth in a TEDB is equal to or greater than the threshold, an IGP floods link information and CSPF updates the TEDB.	-
percent	Specifies the threshold as a percentage.	The value is an integer that ranges from 0 to 100. The default value is 10.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

When the bandwidth changes slightly, flooding the bandwidth wastes network resources. For example, the bandwidth of a link is 100 Mbit/s. During the creation of 100 TE tunnels each with the bandwidth being 1 Mbit/s, the bandwidth of all TE tunnels needs to be flooded 100 times. If the flooding threshold is set to 10%, the first nine tunnels are created without flooding. When the tenth tunnel is created, the 10 Mbit/s bandwidth that is used by the preceding 10 tunnels is flooded. The tunnels from the eleventh tunnel to the eighteenth are created without flooding. When the nineteenth tunnel is created, the bandwidth is flooded, and so on.

Example

# On VLANIF100, when the link bandwidth reserved for the MPLS TE tunnel exceeds 10% of the overall bandwidth or the bandwidth released by the MPLS TE tunnel exceeds 25% of the overall bandwidth, the link information is flooded.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls te bandwidth change thresholds up 25
[HUAWEI-Vlanif100] mpls te bandwidth change thresholds down 10
```

# On GE0/0/1, when the link bandwidth released by the MPLS TE tunnel exceeds 25% of the overall bandwidth, the link information is flooded.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls te bandwidth change thresholds up 25
```

9.3.111 mpls te bandwidth max-reservable-bandwidth

Function

The **mpls te bandwidth max-reservable-bandwidth** command sets or modifies the maximum reservable bandwidth of a link.

The **undo mpls te bandwidth max-reservable-bandwidth** command restores the default configuration.

The maximum reservable bandwidth of a link is not configured by default.

Format

mpls te bandwidth max-reservable-bandwidth *bw-value*

undo mpls te bandwidth max-reservable-bandwidth

Parameters

Parameter	Description	Value
bw-value	Specifies the maximum reservable bandwidth of a link.	The value is an integer that ranges from 0 to 4000000000, in kbit/s. The default value is 0.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

In practical applications, the **mpls te bandwidth max-reservable-bandwidth** command can be configured for a TE tunnel on an outgoing interface of the link through which the tunnel passes.

NOTE

The configured bandwidth takes effect only during tunnel establishment and protocol negotiation, and does not limit the bandwidth for traffic forwarding.

Example

# Set the maximum reservable bandwidth of the link to 10000 kbit/s on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls te bandwidth max-reservable-bandwidth 10000
```

# Set the maximum reservable bandwidth of the link to 10000 kbit/s on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls te bandwidth max-reservable-bandwidth 10000
```

9.3.112 mpls te bfd

Function

The **mpls te bfd** command sets the parameters of a BFD session for TE.

The **undo mpls te bfd** command restores the default configuration.

By default, no parameters of a BFD session for TE are set.

Format

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

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

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

Parameters

Parameter	Description	Value
min-tx-interval *tx-interval*	Specifies the interval at which BFD packets are sent.	The value is an integer that ranges from 100 to 1000, in milliseconds. - After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. - After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
min-rx-interval *rx-interval*	Specifies the interval at which BFD packets are received.	The value is an integer that ranges from 100 to 1000, in milliseconds. - After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. - After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
detect-multiplier *multiplier*	Specifies the local detection multiplier value of a BFD session.	An integer ranging from 3 to 50. The value is 3 by default.

Views

MPLS view, tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

If **min-tx-interval** *tx-interval* configured on the local end is different from **min-rx-interval** *rx-interval* configured on the peer, the larger value is used as the actual session parameter.

The used **detect-multiplier** *multiplier* is the value set on the peer.

If the **mpls te bfd** command is configured in the MPLS view, it takes effect globally. If the command is configured in the tunnel interface view, it only takes effect on the current tunnel interface, and the parameters of the BFD session for TE set in the MPLS view are overridden.

Example

# Set the parameters of the BFD session.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te bfd min-tx-interval 200 detect-multiplier 5
[HUAWEI-Tunnel1] mpls te commit
```

9.3.113 mpls te bfd block

Function

The **mpls te bfd block** command blocks the BFD capability on a specified tunnel interface of a CR-LSP.

The **undo mpls te bfd block** command restores the default configuration.

The BFD capability is not blocked on a tunnel interface by default.

Format

mpls te bfd block

undo mpls te bfd block

Parameters

None.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls te bfd block** command and the **mpls te bfd enable** command are mutually exclusive.

The differences between the **mpls te bfd block** command and the **undo mpls te bfd enable** command in the tunnel interface view are as follows:

- When the **undo mpls te bfd enable** command is run on a tunnel interface, the interface can still obtain the BFD for TE capability after you configure the **mpls te bfd enable** command in the MPLS view.
- When the **mpls te bfd block** command is run on a tunnel interface, the interface cannot obtain the BFD for TE capability even if the **mpls te bfd enable** command is run in the MPLS view.

NOTE

To enable the BFD for TE capability on a majority of interfaces, you can run the **mpls te bfd block** command on a minority of interfaces that do not need to be enabled with BFD for TE. Then, you can run the **mpls te bfd enable** command in the MPLS view to enable the BFD for TE capability on the other interfaces.

To enable BFD for TE capability on a few interfaces, you can run the **mpls te bfd enable** command on these interfaces. After, you can run the **undo mpls te bfd enable** command or the **mpls te bfd block** command to disable BFD for TE from these interfaces.

Example

# Block the BFD capability on Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te bfd block
[HUAWEI-Tunnel1] mpls te commit
```

9.3.114 mpls te bfd enable

Function

The **mpls te bfd enable** command enables BFD for TE.

The **undo mpls te bfd enable** command restores the default configuration.

BFD for TE is disabled by default.

Format

mpls te bfd enable

undo mpls te bfd enable

Parameters

None.

Views

MPLS view, tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

If the **mpls te bfd enable** command is configured in the MPLS view, all TE tunnel interfaces are enabled with BFD for TE, except those configured with the **mpls te bfd block** command, blocking BFD for TE.

If this command is configured in the tunnel interface view, it only takes effect on the single tunnel interface.

The differences between the **undo mpls te bfd enable** command and the **mpls te bfd block** command configured in the tunnel interface view are as follows:

- When the **undo mpls te bfd enable** command is run on a tunnel interface, the interface can still obtain the BFD for TE capability after you configure the **mpls te bfd enable** command in the MPLS view.
- When the **mpls te bfd block** command is run on a tunnel interface, the interface cannot obtain the BFD for TE capability even if the **mpls te bfd enable** command is run in the MPLS view.

NOTE

- To enable the BFD for TE capability on a majority of interfaces, you can run the **mpls te bfd block** command on a minority of interfaces that do not need to be enabled with BFD for TE. Then, you can run the **mpls te bfd enable** command in the MPLS view to enable the BFD for TE capability for the other interfaces.
- To enable BFD for TE capability on a few interfaces, you can run the **mpls te bfd enable** command on these interfaces. After, you can run the **undo mpls te bfd enable** command or the **mpls te bfd block** command to disable BFD for TE from these interfaces.

Example

# Enable BFD for TE globally.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls te bfd enable
```

# Enable BFD for TE on the tunnel interface.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te bfd enable
[HUAWEI-Tunnel1] mpls te commit
```

9.3.115 mpls te bypass-attributes

Function

The **mpls te bypass-attributes** command configures the bypass tunnel attributes in the MPLS TE Auto FRR feature.

The **undo mpls te bypass-attributes** command restores the default settings.

By default, no bypass tunnel attributes in the MPLS TE Auto FRR feature are configured.

Format

mpls te bypass-attributes [**bandwidth** *bandwidth*] [**priority** *setup-priority* [*hold-priority*]]

undo mpls te bypass-attributes

Parameters

Parameter	Description	Value
bandwidth *bandwidth*	Specifies the bandwidth.	The value is an integer that ranges from 1 to 4000000000, in kbit/s.
setup-priority	Specifies the setup priority.	The value is an integer that ranges from 0 to 7. The smaller the value, the higher the priority. The value is 7 by default.
hold-priority	Specifies the holding priority.	The value is an integer that ranges from 0 to 7. The smaller the value, the higher the priority. The value is 7 by default.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Prerequisites

Before running the **mpls te bypass-attributes** command, you must run the **mpls te fast-reroute bandwidth** command to enable FRR function. The bandwidth of a bypass tunnel cannot be greater than that of the primary tunnel.

Precautions

The setup priority of a bypass tunnel cannot be higher than the holding priority. Both cannot be higher than the priorities of the primary tunnel.

On the same TE tunnel interface, the **mpls te bypass-attributes** command cannot be configured together with the **mpls te bandwidth (tunnel interface view)** command.

Example

# Set the bandwidth of the bypass tunnel to 2048 kbit/s, the setup priority to 3, and the holding priority to 3.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 1.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te bandwidth ct0 10000
[HUAWEI-Tunnel1] mpls te priority 3 3
[HUAWEI-Tunnel1] mpls te fast-reroute bandwidth
[HUAWEI-Tunnel1] mpls te bypass-attributes bandwidth 2048 priority 3 3
[HUAWEI-Tunnel1] mpls te commit
```

9.3.116 mpls te bypass-tunnel

Function

The **mpls te bypass-tunnel** command specifies the bypass tunnel for MPLS TE Auto FRR.

The **undo mpls te bypass-tunnel** command deletes the bypass tunnel configuration.

By default, no bypass tunnel for MPLS TE Auto FRR is specified.

Format

mpls te bypass-tunnel

undo mpls te bypass-tunnel

Parameters

None.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The total bandwidth of LSPs protected by the bypass tunnel is not more than the bandwidth of the primary tunnel. When multiple bypass tunnels exist, the system selects a single bypass tunnel through the best-fit algorithm.

If global Srefresh or RSVP GR needs to be enabled on the bypass PLR and MP node, configure the MPLS LSR ID of the destination peer FRR MP node as the destination address of the bypass tunnel.

NOTE

The **mpls te bypass-tunnel** command cannot be configured simultaneously with the following commands on the same tunnel interface:

- **mpls te fast-reroute**
- **mpls te backup**
- **mpls te protection tunnel**

Example

# Configure the bypass tunnel on Tunnel1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te bypass-tunnel
[HUAWEI-Tunnel1] mpls te commit
```

9.3.117 mpls te commit

Function

The **mpls te commit** command commits the tunnel configurations to the system for processing.

Format

mpls te commit

Parameters

None.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The configurations of an MPLS TE tunnel can only take effect after the **mpls te commit** command is run. The destination and tunnel ID must be configured;

otherwise, the commitment fails, and you need to configure both of them and then commit the configuration again. If the MPLS TE configuration changes, you must run the **mpls te commit** command to validate the modification.

NOTE

Each time the MPLS TE tunnel configuration is changed, the **mpls te commit** command must be run to make the modification take effect. If this command is not run, the changed configuration can be saved in the configuration file but cannot take effect.

Example

# Configure an MPLS TE tunnel and then commit the configuration.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 10.2.2.9
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te commit
```

9.3.118 mpls te cspf

Function

The **mpls te cspf** command enables CSPF.

The **undo mpls te cspf** command disables CSPF.

CSPF is disabled by default.

Format

mpls te cspf

undo mpls te cspf

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

You must enable MPLS TE in the MPLS view before enabling CSPF.

CSPF provides a mechanism for selecting a path in an MPLS domain. You must enable CSPF before configuring CSPF functions.

Example

# Enable CSPF.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls te cspf
```

9.3.119 mpls te cspf disable

Function

The **mpls te cspf disable** command disables CSPF calculation when an LSP is being established in a TE tunnel.

The **undo mpls te cspf disable** command enables CSPF calculation when an LSP is being established in a TE tunnel.

By default, CSPF calculation is enabled when an LSP is being established in a TE tunnel.

Format

mpls te cspf disable

undo mpls te cspf disable

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After CSPF is enabled globally, CSPF calculation is triggered each time an LSP is being established in a TE tunnel. In the inter-AS VPN-OptionC scenario, no IGP is configured between two ASs, causing the TEDB to fail to be generated. As a result, CSPF calculation fails to be performed, and inter-area TE tunnels fail to be set up. Run the **mpls te cspf disable** command on the configured TE tunnel interface to disable CSPF calculation in the TE tunnel, and set up inter-area TE tunnels using direct routes or static routes.

Precautions

After the **mpls te cspf disable** command is run, CR-LSP selection functions, such as hop limit, CSPF tie-breaking, and SRLG, will become invalid.

Example

# Disable CSPF calculation when an LSP is being established in a TE tunnel.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te cspf disable
[HUAWEI-Tunnel1] mpls te commit
```

9.3.120 mpls te cspf preferred-igp

Function

The **mpls te cspf preferred-igp** command specifies a preferred IGP for the CSPF calculation.

The **undo mpls te cspf preferred-igp** command restores the default settings.

The TEDB generated by OSPF is preferred by default.

Format

mpls te cspf preferred-igp { **isis** [*isis-process-id* [**level-1** | **level-2**]] | **ospf** [*ospf-process-id* [**area** { *area-id-1* | *area-id-2* }]] }

undo mpls te cspf preferred-igp

Parameters

Parameter	Description	Value
isis	Indicates that the TEDB generated by IS-IS is preferred.	-
isis-process-id	Specifies the process ID.	The value is an integer that ranges from 1 to 65535.
level-1	Indicates that the TEDB generated by a Level-1 IS-IS device is preferred.	-
level-2	Indicates that the TEDB generated by a Level-2 IS-IS device is preferred.	-
ospf	Indicates that the TEDB generated by OSPF is preferred.	-
ospf-process-id	Specifies the ID of an OSPF process.	The value is an integer that ranges from 1 to 65535.
area *area-id-1*	Specifies a preferred OSPF area configured in number format.	The value is an integer that ranges from 0 to 4294967295.
area *area-id-2*	Specifies a preferred OSPF area configured in IP address format.	The value is in dotted decimal notation.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When selecting a path, CSPF prefers the TEDB generated by OSPF to calculate a CR-LSP by default. When the OSPF TEDB can be used to calculate a path, the IS-IS TEDB is not used. If the calculation based on the OSPF TEDB fails, recalculation based on the IS-IS TEDB is performed.

You can run the **mpls te cspf preferred-igp** command to configure CSPF to prefer the TEDB generated by IS-IS when calculating a CR-LSR. In this case, the OSPF TEDB is only used to calculate a path when the path calculation based on the IS-IS TEDB fails.

Prerequisites

CSPF has been enabled using the **mpls te cspf** command.

Example

# Configure CSPF to prefer the TEDB generated by OSPF when calculating a CR-LSP.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te cspf
[HUAWEI-mpls] mpls te cspf preferred-igp ospf
```

9.3.121 mpls te cspf timer failed-link

Function

The **mpls te cspf timer failed-link** command sets the timeout period of a failed-link timer.

The **undo mpls te cspf timer failed-link** command restores the default setting.

By default, the timeout period of the failed-link timer is 10 seconds.

Format

mpls te cspf timer failed-link *interval*

undo mpls te cspf timer failed-link

Parameters

Parameter	Description	Value
interval	Specifies the timeout period of a failed-link timer.	The value is an integer that ranges from 1 to 300, in seconds. The default value is 10.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A failed-link timer starts when a link goes Down.

- If an IGP deletes or modifies the link before the timer expires, CSPF is informed of the change. Then CSPF updates the link in the Traffic Engineering DataBase (TEDB) and terminates the timer.
- If IGP does not delete the link after the timer expires, the link goes Up.

Prerequisites

The CSPF function has been enabled by running the **mpls te cspf** command.

Example

# Set the timeout period of the failed-link timer to 50 seconds.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te cspf
[HUAWEI-mpls] mpls te cspf timer failed-link 50
```

9.3.122 mpls te fast-reroute

Function

The **mpls te fast-reroute** command enables FRR.

The **undo mpls te fast-reroute** command disables FRR.

By default, FRR is disabled.

Format

mpls te fast-reroute [**bandwidth**]

undo mpls te fast-reroute

Parameters

Parameter	Description	Value
bandwidth	Indicates that bandwidth protection is needed.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

When FRR is enabled on a tunnel interface, the record route flag is automatically set as "record reroute with label", irrespective of the configuration of the **mpls te record-route label** command.

You must disable FRR If run the **mpls te record-route** or **undo mpls te record-route** command.

NOTE

- The **mpls te fast-reroute** command and the **mpls te resv-style ff** command cannot be configured together.
- The **mpls te fast-reroute** command and the **mpls te bypass-tunnel** command cannot be configured on the same tunnel interface.
- The **mpls te fast-reroute** command and the **mpls te protected-interface** command cannot be configured on the same tunnel interface.
- The **mpls te fast-reroute** command and the **mpls te protection tunnel** command cannot be configured for the protection tunnel in a tunnel protection group, whereas these two commands can be configured on the interface of the primary tunnel in the tunnel protection group.

Example

# Enable FRR on Tunnel1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te fast-reroute
[HUAWEI-Tunnel1] mpls te commit
```

9.3.123 mpls te hop-limit

Function

The **mpls te hop-limit** command limits the maximum number of hops of a CR-LSP.

The **undo mpls te hop-limit** command restores the default setting.

By default, the maximum number of hops of a CR-LSP is 32.

Format

mpls te hop-limit *hop-limit-value* [**best-effort** | **secondary**]

undo mpls te hop-limit [**best-effort** | **secondary**]

undo mpls te hop-limit *hop-limit-value* { **secondary** | **best-effort** }

Parameters

Parameter	Description	Value
hop-limit-value	Specifies the value of the hop limit.	The value is an integer that ranges from 1 to 32. The default value is 32.
best-effort	Indicates the hop limit of a best-effort path.	-
secondary	Indicates the hop limit of a backup CR-LSP.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

After a CR-LSP is configured with a hop limit, the hop limit acts as one of routing conditions such as the link bandwidth and affinity property when the CR-LSP is created. After the hop limit is set, the number of hops of a CR-LSP cannot exceed this limit.

Example

# Set the maximum number of hops of the primary CR-LSP, bypass CR-LSP, and best-effort path in hot-standby to 10.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te hop-limit 10
[HUAWEI-Tunnel1] mpls te hop-limit 10 secondary
[HUAWEI-Tunnel1] mpls te hop-limit 10 best-effort
[HUAWEI-Tunnel1] mpls te commit
```

9.3.124 mpls te hotstandby-lsp-constraint

Function

The **mpls te hotstandby-lsp-constraint** command allows you to use a CR-LSP attribute template to set up a hot-standby CR-LSP.

The **undo mpls te hotstandby-lsp-constraint** command deletes the used CR-LSP attribute template.

No CR-LSP attribute template is used to set up a hot-standby CR-LSP by default.

Format

mpls te hotstandby-lsp-constraint *number* { **dynamic** | **lsp-attribute** *lsp-attribute-name* }

undo mpls te hotstandby-lsp-constraint *number*

Parameters

Parameter	Description	Value
number	Specifies the number of a CR-LSP attribute template. It indicates the sequence of using each CR-LSP attribute template to set up a hot-standby CR-LSPs. The CR-LSP attribute templates are used in ascending order of their number.	The value is an integer ranging from 1 to 3.
dynamic	Indicates that when a hot-standby CR-LSP is being set up, it is assigned the same bandwidth and priority as the primary CR-LSP, but specified with a different path from the primary LSP.	-
lsp-attribute *lsp-attribute-name*	Specifies the name of a CR-LSP attribute template.	The value is an existing CR-LSP attribute template name.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

A maximum number of three CR-LSP attribute templates can be configured to set up hot-standby CR-LSPs. The hot-standby CR-LSPs must be consistent with the primary CR-LSP in the following attributes:

- Setup priority
- Holding priority
- Bandwidth type

In each of the three CR-LSP attribute template types corresponding to the primary CR-LSP, the hot-standby CR-LSP, and the ordinary backup CR-LSP respectively, only one attribute template can be specified with the **dynamic** parameter.

The parameter *number* is used to number each CR-LSP attribute template, which indicates the sequence of using each CR-LSP attribute template to set up a hot-standby CR-LSP. To set up a hot-standby CR-LSP, the system attempts to apply each CR-LSP attribute template by the template number in ascending order until a hot-standby CR-LSP is successfully up.

NOTE

- Before configuring the **mpls te hotstandby-lsp-constraint** command, you must run the **mpls te primary-lsp-constraint** command to use a CR-LSP attribute template to set up a primary CR-LSP.
- When the **mpls te hotstandby-lsp-constraint** command is configured to help set up a hot-standby CR-LSP, the **record-route** function is automatically enabled.

Example

# Use the attribute template named t2 to set up a hot-standby CR-LSP.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] mpls te primary-lsp-constraint lsp-attribute t1
[HUAWEI-Tunnel1] mpls te hotstandby-lsp-constraint 1 lsp-attribute t2
[HUAWEI-Tunnel1] mpls te commit
```

9.3.125 mpls te igp advertise

Function

The **mpls te igp advertise** command configures forwarding adjacency to take an MPLS TE tunnel as a virtual link and advertise the virtual link to an IGP network.

The **undo mpls te igp advertise** command restores the default configuration.

By default, forwarding adjacency to take an MPLS TE tunnel as a virtual link and advertise the virtual link to an IGP network is disabled.

Format

mpls te igp advertise [**hold-time** *interval*]

undo mpls te igp advertise

Parameters

Parameter	Description	Value
hold-time *interval*	Specifies the interval between the time when a TE tunnel goes Down and when the network is notified of the change.	The value is an integer that ranges from 0 to 4294967295 in milliseconds. The default value is 0.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls te igp advertise** command and the **mpls te igp shortcut** command cannot be configured simultaneously.

Example

# Configure the forwarding adjacency and use the default hold time.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te igp advertise
[HUAWEI-Tunnel1] mpls te commit
```

9.3.126 mpls te igp metric

Function

The **mpls te igp metric** command specifies the MPLS TE tunnel metric for the SPF calculation in IGP shortcut or forwarding adjacency mode.

The **undo mpls te igp metric** command restores the default settings.

The TE tunnel metric is equal to the IGP metric of the TE tunnel by default.

Format

mpls te igp metric { **absolute** *absolute-value* | **relative** *relative-value* }

undo mpls te igp metric

Parameters

Parameter	Description	Value
absolute *absolute-value*	Specifies the absolute metric mode.	The value is an integer that ranges from 1 to 65535.
relative *relative-value*	Specifies the relative metric mode, indicating the offset value between the MPLS TE metric and the IGP metric.	The value is an integer that ranges from -10 to 10. The default value is 0.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IGP uses an auto route related to a CR-LSP in a TE tunnel that functions as a logical link to calculate a path. The tunnel interface is used as an outbound interface in the auto route. An auto route can work in IGP shortcut or forwarding adjacency mode. You can set a metric for a TE tunnel in either mode.

When specifying the metric for a TE tunnel in IGP shortcut mode, pay attention to the following points:

- If the **absolute** parameter is used, the metric of the TE tunnel is the set metric.
- If the **relative** parameter is used, the metric of the TE tunnel is the sum of the metric of the corresponding IGP path and relative metric.

A proper IGP metric for the TE tunnel in forwarding adjacency mode can ensure that the LSP be advertised and used correctly. For example, the metric of a TE tunnel should be less than the metric of an IGP route.

Precautions

When specifying an IGP metric for a TE tunnel in forwarding adjacency mode, select the **absolute** parameter if the IGP protocol is IS-IS.

Example

# Set the MPLS TE tunnel metric to the IGP metric minus 1 in the SPF calculation.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te igp metric relative -1
[HUAWEI-Tunnel1] mpls te commit
```

9.3.127 mpls te igp shortcut

Function

The **mpls te igp shortcut** command configures an IGP to use MPLS TE tunnels in the Up state for performing the enhanced SPF calculation.

The **undo mpls te igp shortcut** command restores the default configuration.

By default, an IGP does not use MPLS TE tunnels for performing the enhanced SPF calculation.

Format

mpls te igp shortcut [**isis** | **ospf**]

undo mpls te igp shortcut

Parameters

Parameter	Description	Value
isis	Indicates the IS-IS protocol.	-
ospf	Indicates the OSPF protocol.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls te igp shortcut** command and the **mpls e igp advertise** command cannot be configured simultaneously.

Example

# Configure OSPF or IS-IS to use Tunnel 1 in the enhanced SPF calculation if this tunnel is Up.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te igp shortcut
[HUAWEI-Tunnel1] mpls te commit
```

9.3.128 mpls te link administrative group

Function

The **mpls te link administrative group** command sets the value of the administrative-group attribute for an interface.

The **undo mpls te link administrative group** command restores the default setting.

The default administrative-group attribute is 0x0.

Format

mpls te link administrative group *value*

undo mpls te link administrative group

Parameters

Parameter	Description	Value
value	Specifies the link attributes compared with affinity bits during the selection of a path.	The value is in hexadecimal notation and is of 32 bits with each bit representing an attribute. The value ranges from 0x0 to 0xFFFFFFFF.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

After being advertised globally, interface attributes can work as a standard for the ingress of a tunnel to select a path.

The modification on the administrative-group attributes takes effect only on the LSPs created after the modification and does not affect the established LSPs.

The **mpls te link administrative group** command can be run on the outgoing interface of the link through which a TE tunnel passes.

Example

# Set the administrative-group attribute to 0x0101 on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
```

```
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls te link administrative group 101
```

# Set the administrative-group attribute to 0x0101 on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls te link administrative group 101
```

9.3.129 mpls te loop-detection

Function

The **mpls te loop-detection** command enables the loop detection function while a tunnel is being set up.

The **undo mpls te loop-detection** command disables this function.

The loop detection function is disabled by default.

Format

mpls te loop-detection

undo mpls te loop-detection

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

To prevent loops, you can run the **mpls te loop-detection** command on the ingress of the MPLS TE tunnel to enable the loop detection function.

Example

# Enable the loop detection when an MPLS TE tunnel is being set up.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te loop-detection
[HUAWEI-Tunnel1] mpls te commit
```

9.3.130 mpls te metric

Function

The **mpls te metric** command configures the TE metric value of a link.

The **undo mpls te metric** command restores the default configuration.

The IGP metric value of a link is used as the TE metric value by default.

Format

mpls te metric *value*

undo mpls te metric

Parameters

Parameter	Description	Value
metric *value*	Specifies the TE metric of a link.	An integer ranging from 1 to 16777215.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

If the IGP is OSPF and the current device is a stub router, the **mpls te metric** command does not take effect.

Example

# Set the TE metric of the link to 20 on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls te metric 20
```

# Set the TE metric of the link to 20 on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls te metric 20
```

9.3.131 mpls te ordinary-lsp-constraint

Function

The **mpls te ordinary-lsp-constraint** command allows you to use a CR-LSP attribute template to set up an ordinary backup CR-LSP.

The **undo mpls te ordinary-lsp-constraint** command deletes a used CR-LSP attribute template.

No CR-LSP attribute template is used to set up an ordinary backup CR-LSP by default.

Format

mpls te ordinary-lsp-constraint *number* { **dynamic** | **lsp-attribute** *lsp-attribute-name* }

undo mpls te ordinary-lsp-constraint *number*

Parameters

Parameter	Description	Value
number	Specifies the number of a CR-LSP attribute template. The CR-LSP attribute templates are used to set up ordinary backup CR-LSPs in sequence of ascending number.	An integer ranging from 1 to 3.
dynamic	Indicates that when an ordinary backup CR-LSP is being set up, it is assigned the same bandwidth and priority as the primary CR-LSP.	-
lsp-attribute *lsp-attribute-name*	Specifies the name of a CR-LSP attribute template.	It is a string of 1 to 31 characters.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

A maximum number of three CR-LSP attribute templates can be configured to set up an ordinary backup CR-LSP. The ordinary backup CR-LSPs must be consistent with the primary CR-LSP in the following attributes:

- Setup priority

- Holding priority
- Bandwidth type

Among the three CR-LSP attribute templates corresponding to a primary CR-LSP and ordinary backup CR-LSP, only one CR-LSP attribute template can be specified with the **dynamic** parameter.

The parameter *number* is used to number each CR-LSP attribute template. The CR-LSP attribute templates are each applied by the system in sequence of ascending number until an ordinary backup CR-LSP is set up.

NOTE

- Before running the **mpls te ordinary-lsp-constraint** command, you must run the **mpls te primary-lsp-constraint** command to use a CR-LSP attribute template to set up a primary CR-LSP.
- When the **mpls te ordinary-lsp-constraint** command is run to help set up an ordinary backup CR-LSP, the **record route** function is automatically enabled.

Example

# Use the attribute template named t3 to set up an ordinary backup CR-LSP.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] mpls te primary-lsp-constraint lsp-attribute t1
[HUAWEI-Tunnel1] mpls te ordinary-lsp-constraint 1 lsp-attribute t3
[HUAWEI-Tunnel1] mpls te commit
```

9.3.132 mpls te path explicit-path

Function

The **mpls te path explicit-path** command configures an explicit path for a tunnel.

The **undo mpls te path** command deletes a configured explicit path.

By default, no explicit path for a tunnel is configured.

Format

mpls te path explicit-path *path-name* [**secondary**]

undo mpls te path [**secondary**]

undo mpls te path explicit-path *path-name* **secondary**

Parameters

Parameter	Description	Value
path-name	Specifies the name of the explicit path for a tunnel.	The value is an existing explicit path name.

Parameter	Description	Value
secondary	Indicates that the explicit path is configured for a backup tunnel. The parameter is applied only to configuring a backup CR-LSP using the **mpls te backup** command.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls te path explicit-path** command can be run successfully only after an explicit path is set up by running the **explicit-path** command in the system view, and the nodes on the path are specified.

Example

# Apply the explicit path named path1 to Tunnel1.

```
<HUAWEI> system-view
[HUAWEI] explicit-path path1
[HUAWEI-explicit-path-path1] next hop 10.2.2.9
[HUAWEI-explicit-path-path1] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te path explicit-path path1
[HUAWEI-Tunnel1] mpls te commit
```

9.3.133 mpls te path metric-type

Function

The **mpls te path metric-type** command specifies a link metric type used to select a path for a tunnel without any metric type.

The **undo mpls te path metric-type** command restores the default settings.

The TE metric is used to select a path for a tunnel by default.

Format

mpls te path metric-type { **igp** | **te** }

undo mpls te path metric-type

Parameters

Parameter	Description	Value
igp	Indicates that the IGP metric is used.	-
te	Indicates that the TE metric is used.	-

Views

MPLS view, tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

If the **mpls te path metric-type** command is not configured in the tunnel interface view, the metric type set in the MPLS view is used. Otherwise, the metric type set in the tunnel interface view will be used.

Example

# Adopt the IGP metric that is used to select a path for the tunnel that is not configured with any metric type.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te path metric-type igp
```

# Adopt the TE metric that is used to select a path for Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te path metric-type te
[HUAWEI-Tunnel1] mpls te commit
```

9.3.134 mpls te path-selection overload

Function

The **mpls te path-selection overload** command associates CR-LSP establishment with the IS-IS overload setting. This association allows CSPF to calculate paths excluding overloaded IS-IS nodes.

The **undo mpls te path-selection** command restores the default configuration.

By default, CR-LSP establishment is not associated with the IS-IS overload setting.

Format

mpls te path-selection overload

undo mpls te path-selection

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An administrator can run the **set-overload** command to mark a node overloaded if the node is transmitting a large number of services or its CPU is overburdened. If there are overloaded nodes on an MPLS TE network, associate CR-LSP establishment with the IS-IS overload setting to ensure that CR-LSPs are established over paths excluding overloaded nodes. This configuration prevents overloaded nodes from being further burdened and improves CR-LSP reliability.

Prerequisites

The route record has been enabled using the **mpls te record-route** command.

Precautions

The **mpls te path-selection overload** command has the following influences on the CR-LSP establishment:

- CSPF recalculates paths excluding overloaded nodes for established CR-LSPs.

  NOTE

  Traffic travels through an existing CR-LSP before a new CR-LSP is established. After the new CR-LSP is established, traffic is switched to the new CR-LSP and the original CR-LSP is deleted. This traffic switchover is performed based on the Make-Before-Break mechanism. Traffic is not dropped during the switchover.

- CSPF calculates paths excluding overloaded nodes for new CR-LSPs.

This command does not take effect on bypass tunnels.

If the ingress or egress is marked overloaded, the **mpls te path-selection overload** command does not take effect. The established CR-LSPs associated with the ingress or egress will not be reestablished and new CR-LSPs associated with the ingress or egress will also not be established.

If a TE LSP uses the local device as a transit node before the **set-overload** command is run, the TE LSP is not torn down and re-established and still uses the local device as a transit node after the **set-overload** command is run; if the local device is restarted after the command is run and fast convergence is not configured on the ingress of the RSVP-LSP, TE LSP forwarding fails, and services are affected. Therefore, the **mpls te path-selection overload** command needs to be run on the ingress of the RSVP-LSP before the device is restarted.

Example

# Associate CR-LSP establishment with the IS-IS overload setting.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls te path-selection overload
```

9.3.135 mpls te primary-lsp-constraint

Function

The **mpls te primary-lsp-constraint** command allows you to use a CR-LSP attribute template to set up a primary CR-LSP.

The **undo mpls te primary-lsp-constraint** command restores the default configuration.

No CR-LSP attribute template is used to set up a primary CR-LSP by default.

Format

mpls te primary-lsp-constraint { **dynamic** | **lsp-attribute** *lsp-attribute-name* }

undo mpls te primary-lsp-constraint

Parameters

Parameter	Description	Value
dynamic	Indicates that when a CR-LSP attribute template is used to set up a primary CR-LSP, all attributes in the attribute template use the default values.	-
lsp-attribute *lsp-attribute-name*	Specifies the name of a CR-LSP attribute template.	The value is an existing CR-LSP attribute template name.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

A CR-LSP attribute template already configured with the bandwidth and priority can be referenced to set up CR-LSPs in batches, greatly simplifying configurations of CR-LSPs.

If the TE attribute configured in the tunnel interface view and that configured through a CR-LSP attribute template coexist, the former takes precedence over the latter.

Example

# Use the attribute template named **t1** to set up a primary CR-LSP.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] mpls te primary-lsp-constraint lsp-attribute t1
[HUAWEI-Tunnel1] mpls te commit
```

9.3.136 mpls te priority

Function

The **mpls te priority** command configures the setup priority and holding priority for an MPLS TE tunnel.

The **undo mpls te priority** command restores the default settings.

The default setup and holding priority for an MPLS TE tunnel are both 7.

Format

mpls te priority *setup-priority* [*hold-priority*]

undo mpls te priority

Parameters

Parameter	Description	Value
setup-priority	Specifies the setup priority.	The value is an integer that ranges from 0 to 7. The smaller the value, the higher the priority.
hold-priority	Specifies the holding priority.	The value is an integer that ranges from 0 to 7. The smaller the value, the higher the priority. Its value is the same as the setup priority by default.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If bandwidth resources on a link cannot satisfy the requirements for establishing all CR-LSPs, you can specify the setup and holding priorities for certain CR-LSPs. In this manner, the CR-LSPs with higher priorities can be established by preempting bandwidth resources of CR-LSPs with lower priorities before transmitting certain user services.

Priorities of a CR-LSP consist of the setup priority and holding priority, representing the preemption relationship between a CR-LSP to be established and an established CR-LSP. If the setup priority of a CR-LSP to be established is higher than the holding priority of an established CR-LSP, the CR-LSP to be established can preempt the bandwidth resources of the established one.

The default setup and holding priorities of CR-LSPs are 7, the lowest priority value. Default priorities take effect on all CR-LSPs if no priorities are specified. These CR-LSPs with the default priorities are at the risk of being preempted by those with higher priorities.

Precautions

During the planning of a network, it is recommended that the setup and holding priorities of all CR-LSPs be strictly planned. To preferentially transmit services over a CR-LSP, you can set the higher setup and holding priorities for the CR-LSP, preventing unwanted bandwidth preemption. The same setup and holding priorities are set for CR-LSPs which are transmitting services with the same priority, also preventing bandwidth preemption.

In addition, on one TE tunnel, its setup priority must be less than or equal to its holding priority. This ensures that CR-LSPs in the tunnel can be successfully set up, and prevents CR-LSP flapping caused by bandwidth preemption between CR-LSPs.

NOTICE

After the priorities of an existing CR-LSP have been changed, the existing CR-LSP will be deleted and a new one will be established. Therefore, back up CR-LSPs with lower priorities before setting higher priorities for a certain CR-LSP.

Example

# Set the setup priority and the holding priority to 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te priority 1
[HUAWEI-Tunnel1] mpls te commit
```

9.3.137 mpls te protected-interface

Function

The **mpls te protected-interface** command specifies an interface to be protected by a bypass tunnel.

The **undo mpls te protected-interface** command delete an interface protected by a bypass tunnel.

By default, no interface to be protected by a bypass tunnel is specified.

Format

mpls te protected-interface *interface-type interface-number*

undo mpls te protected-interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface to be protected. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls te protected-interface** command must be configured together with the **mpls te bypass-tunnel** command on the same tunnel interface. Otherwise, the configured **mpls te protected-interface** command cannot take effect.

Currently, a bypass tunnel can protect up to six interfaces that must be enabled with MPLS TE.

NOTE

If a tunnel interface is configured with the **mpls te protected-interface** command, it cannot be configured with the **mpls te backup** or **mpls te fast-reroute** command.

Example

# Use Tunnel 1 as a bypass tunnel of VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te protected-interface vlanif 100
[HUAWEI-Tunnel1] mpls te commit
```

9.3.138 mpls te protect-switch

Function

The **mpls te protect-switch** command configures the manual switching mode for a specified tunnel.

The **mpls te protect-switch clear** and **undo mpls te protect-switch** commands delete the manual switching mode for a specified tunnel.

By default, no manual switching mode for a specified tunnel is configured.

Format

mpls te protect-switch { **force** | **lock** | **manual** }

mpls te protect-switch clear

undo mpls te protect-switch

Parameters

Parameter	Description	Value
force	Forcibly directs traffic to a protection tunnel.	-
lock	Locks traffic in the working tunnel. Being locked, traffic cannot be switched to a protection tunnel even if the working tunnel fails.	-
manual	Enables manual switching.	-
clear	Deletes the switching request manually configured on the current tunnel.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an LSP fault is detected, traffic switching is automatically triggered in a tunnel protection group. Alternatively, run the **mpls te protect-switch** command to trigger traffic switching.

MPLS OAM supports multiple traffic switching modes. These switching modes are prioritized. A newly configured switching mode takes effect only if its priority is higher than that of the existing switching mode.

The traffic switching modes are prioritized in descending order when the protection tunnel is Up:

- Force switching mode: has the highest priority. If force switching is configured, traffic is forced to switch to a protection tunnel and does not switch back even if the working tunnel recovers. Both the **mpls te protect-switch force** command and the **mpls te protect-switch lock** command can trigger force switching, but force switching triggered by the latter command has a higher priority.

- Signal failure mode: automatically triggers traffic switching if an LSP fault is detected.
- Manual switching mode: manually switches traffic to a protection tunnel.
- WTR mode: switches traffic back to a working tunnel after the WTR time expires. Although the WTR time is set, if a command is run to manually switch traffic, traffic will be switched immediately before the WTR time expires.

If a new local or remote request has a higher priority than an existing request manually configured using the **mpls te protect-switch** command, the APS state machine is changed, and the manual switching command is deleted. In the **mpls te protect-switch** command, the **force** and **manual** parameters, except the **lock** parameter, configure lower priority requests. After the **mpls te protect-switch** command with **force** or **manual** configured is run, the command is lost after a device is restarted. This situation is normal, in compliance with Recommendation G.8131.

Prerequisites

A tunnel protection group has been created by running the **mpls te protection tunnel** command.

Follow-up Procedure

The **mpls te protect-switch clear** command can be used to cancel force or manual switching.

Example

# Switch traffic to the protection tunnel manually on Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] mpls te protect-switch manual
```

# Delete the traffic switching to the protection tunnel on Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] mpls te protect-switch clear
```

9.3.139 mpls te protection tunnel

Function

The **mpls te protection tunnel** command creates a tunnel protection group by binding a configured protection tunnel to a primary tunnel.

The **undo mpls te protection tunnel** command deletes the binding between the protection tunnel and the primary tunnel.

By default, no protection tunnel group is created.

Format

mpls te protection tunnel *tunnel-id* [**holdoff** *holdoff-time*] [**mode** { **non-revertive** | **revertive** [**wtr** *wtr-time*] }]

undo mpls te protection tunnel

Parameters

Parameter	Description	Value
tunnel-id	Specifies the ID of a protection tunnel.	The value is an integer that ranges from 1 to 10000.
holdoff *holdoff-time*	Specifies the delay time. When a fault on a primary tunnel is detected, the switchover is performed after the delay time expires.	The value is an integer that ranges from 0 to 100 with the step of 100 milliseconds. The maximum delay time is 10 seconds. By default, the value is 10, indicating that the switchover is performed immediately after a fault on the primary tunnel is detected.
mode	Specifies the revertive mode. ● **non-revertive**: The current mode cannot be switched to the original mode. ● **revertive**: The current mode can be switched to the original mode.	By default, the revertive mode is used.
wtr *wtr-time*	Specifies the WTR time for the switchback. When a primary tunnel recovers from a fault, the switchback is performed after the WRT time expires.	The value is an integer that ranges from 0 to 60, with the increment of 30 seconds. By default, the value is 24, that is, 12 minutes.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

In addition to configuring a tunnel protection group to protect a working tunnel, you can configure TE FRR on the working tunnel. In this manner, the working tunnel can work under dual protection. The protection tunnel, however, cannot function as the working tunnel that is protected by another tunnel. In addition, the protection tunnel cannot be enabled with TE FRR.

After creating a protection tunnel in the tunnel interface view, you must run the **mpls te commit** command to commit the configuration.

NOTE

Tunnel protection group and TE FRR cannot be configured simultaneously on the ingress of a primary tunnel.

Example

# Configure a protection tunnel for Tunnel1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te protection tunnel 239 holdoff 100 mode revertive wtr 30
[HUAWEI-Tunnel1] mpls te commit
```

9.3.140 mpls te record-route

Function

The **mpls te record-route** command enables the system to record routes and labels during tunnel establishment.

The **undo mpls te record-route** command configures the system not to record routes and labels during tunnel establishment.

By default, the system does not record routes and labels during tunnel establishment.

Format

mpls te record-route [**label**]

undo mpls te record-route

Parameters

Parameter	Description	Value
label	Indicates that a label is also recorded when the system records a route.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an MPLS TE tunnel is not established over an explicit path, the system does not record detailed path information. In this case, to view detailed path information about the tunnel, run this command on a tunnel interface. After the configuration, RROs are carried in Path and Resv messages and record the IP address of each hop along the tunnel. In addition, the keyword **label** can be configured to record the label of each hop along the tunnel.

Precautions

After the **mpls te record-route** command is configured and the MPLS TE tunnel is established, the **display mpls te tunnel path** command can be run to display detailed path information about the tunnel.

Do not run the **mpls te record-route** command on a large-scale network. On such a network, a large number of hops exist along a tunnel. Running this command allows the Path and Resv messages to carry RROs that record the IP address of each hop along the tunnel. As a result, the Path or Resv message will be oversized, lowering the system performance.

NOTE

After the **mpls te fast-reroute**, **mpls te backup**, or **mpls te bypass-tunnel** command has been configured on a tunnel interface, the route record function is automatically enabled.

Example

# Enable the system to record routes and labels during tunnel establishment.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te record-route label
[HUAWEI-Tunnel1] mpls te commit
```

9.3.141 mpls te reoptimization (user view)

Function

The **mpls te reoptimization** command immediately triggers re-optimization for an MPLS TE tunnel.

Format

mpls te reoptimization [**tunnel** *interface-number*]

Parameters

Parameter	Description	Value
tunnel *interface-number*	Specifies a tunnel that needs immediate re-optimization.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The manual re-optimization function is used in either of the following situations:

- After the network topology is modified manually, a new optimal path will be calculated. The new optimal path needs to be immediately used by the TE tunnel.
- TE tunnels need to be immediately optimized in batches, optimizing resources of these TE tunnels in time.

If you run the **mpls te reoptimization** command without specifying the **tunnel** *interface-number* parameter, all TE tunnels are optimized. If you run the **mpls te reoptimization** command and specify the **tunnel** *interface-number* parameter, the specified TE tunnels are optimized.

Re-optimization of a TE tunnel can be performed in either of the following modes:

- Automatic re-optimization: means that the TE tunnel is periodically optimized, saving manpower. To enable automatic re-optimization, run the **mpls te reoptimization (tunnel interface view)** command in the tunnel interface view. In addition, this command takes effect only on an established TE tunnel.
- Manual re-optimization: means that the TE tunnel is immediately optimized. To immediately optimize the TE tunnel, run the **mpls te reoptimization** command in the user view.

Precautions

- If the re-optimization function is configured after an explicit path is configured and a new path fails to meet the explicit path constraints, the re-optimization function will not take effect.
- After a TE tunnel is configured with the re-optimization function, the tie-breaking in most-fill mode will not be supported.
- The **mpls te reoptimization** command cannot be run together with the following commands:
  - **mpls te route-pinning**
  - **mpls te resv-style ff**

Example

# Immediately re-optimize all the TE tunnels on the local device.

```
<HUAWEI> mpls te reoptimization
```

9.3.142 mpls te reoptimization (tunnel interface view)

Function

The **mpls te reoptimization** command enables automatic re-optimization for a TE tunnel.

The **undo mpls te reoptimization** command restores the default setting.

By default, automatic re-optimization for a TE tunnel is disabled.

Format

mpls te reoptimization [**frequency** *interval*]

undo mpls te reoptimization

Parameters

Parameter	Description	Value
frequency *interval*	Specifies the interval for re-optimization. The system calculates the path for a TE tunnel based on constraints at the intervals of *interval*. If a better path to the same destination is calculated, the TE tunnel will be re-established over the better path.	The value is an integer that ranges from 60 to 604800, in seconds. By default, the interval is 3600 seconds.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a better path is calculated, to allow a TE tunnel to be automatically re-established over the better path, the **mpls te reoptimization** command needs to be run in the tunnel interface view. In this manner, after a better path to the same destination has been calculated for a certain reason such as the change of the cost, the TE tunnel can be automatically re-established, optimizing the resources on the network.

Re-optimization of a TE tunnel can be performed in either of the following modes:

- Automatic re-optimization: means that the TE tunnel is periodically optimized, saving manpower. To enable automatic re-optimization, run the **mpls te reoptimization** command in the tunnel interface view. In addition, this command takes effect only on an established TE tunnel.
- Manual re-optimization: means that the TE tunnel is immediately optimized. To immediately optimize the TE tunnel, run the **mpls te reoptimization** command in the user view.

Prerequisites

CSPF has been enabled by running the **mpls te cspf** command.

Precautions

- If the re-optimization function is configured after an explicit path is configured and a new path fails to meet the explicit path constraints, the re-optimization function will not take effect.
- After a TE tunnel is configured with the re-optimization function, the tie-breaking in most-fill mode will not be supported.
- The **mpls te reoptimization** command cannot be run together with the following commands:
  - **mpls te route-pinning**
  - **mpls te resv-style ff**

Example

# Enable periodic re-optimization for a TE tunnel named Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te reoptimization frequency 43200
[HUAWEI-Tunnel1] mpls te commit
```

9.3.143 mpls te resv-style

Function

The **mpls te resv-style** command specifies a reservation style.

The **undo mpls te resv-style** command restores the default setting.

The default reservation style is SE.

Format

mpls te resv-style { **ff** | **se** }

undo mpls te resv-style

Parameters

Parameter	Description	Value
ff	Indicates the style of fixed filter.	-
se	Indicates the style of shared explicit.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

RSVP-TE only supports two resources reservation styles: FF and SE.

NOTE

The **mpls te resv-style ff** command cannot be configured simultaneously with the following commands: **mpls te fast-reroute**, **mpls te backup**, and **mpls te reoptimization (tunnel interface view)**.

Example

# Set up a CR-LSP with the resource reservation style being FF.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te signal-protocol rsvp-te
[HUAWEI-Tunnel1] mpls te resv-style ff
[HUAWEI-Tunnel1] mpls te commit
```

9.3.144 mpls te route-pinning

Function

The **mpls te route-pinning** command enables the route pinning function.

The **undo mpls te route-pinning** command disables this function.

Route pinning is disabled by default.

Format

mpls te route-pinning

undo mpls te route-pinning

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls te route-pinning** command cannot be configured simultaneously the **mpls te reoptimization (tunnel interface view)** command.

Example

# Enable route pinning function.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te route-pinning
[HUAWEI-Tunnel1] mpls te commit
```

9.3.145 mpls te signal-protocol

Function

The **mpls te signal-protocol** command specifies a signaling protocol to set up an LSP.

The **undo mpls te signal-protocol** command deletes the signaling protocol to set up an LSP.

The default signaling protocol used to set up an LSP is RSVP-TE.

Format

mpls te signal-protocol { **cr-static** | **rsvp-te** | **static** }

undo mpls te signal-protocol { **cr-static** | **static** }

Parameters

Parameter	Description	Value
cr-static	Uses static CR-LSPs to establish TE tunnels.	-
rsvp-te	Uses RSVP-TE as the signaling protocol.	-
static	Uses static LSPs to establish TE tunnels.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

When configuring MPLS TE, you can run this command to specify a signaling protocol to set up a tunnel.

- When configuring a static MPLS TE tunnel, the signaling protocol used is **cr-static**.
- When configuring a dynamic MPLS TE tunnel, the signaling protocol used is **rsvp-te**.

Example

# Use RSVP-TE as the signaling protocol for MPLS TE.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te signal-protocol rsvp-te
[HUAWEI-Tunnel1] mpls te commit
```

9.3.146 mpls te signaling-delay-trigger enable

Function

The **mpls te signaling-delay-trigger enable** command enables the RSVP signaling delay-trigger function.

The **undo mpls te signaling-delay-trigger enable** command disables the RSVP signaling delay-trigger function.

The RSVP signaling delay-trigger function is disabled by default.

Format

mpls te signaling-delay-trigger enable

undo mpls te signaling-delay-trigger enable

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a fault occurs on an MPLS network and a large number of RSVP CR-LSPs need to be re-established, a large amount of system resources may be required. In this case, after the RSVP signaling delay-trigger function is configured, the interval between re-establishments of a CR-LSP is prolonged so that system resources are saved.

Prerequisites

Before running the **mpls te signaling-delay-trigger enable** command, the **mpls te** command must be run in the MPLS view.

Precautions

Use caution when configuring the RSVP signaling delay-trigger function because it causes the delay of CR-LSP convergence. The default settings are recommended.

Example

# Enable the RSVP signaling delay-trigger function.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls te signaling-delay-trigger enable
```

9.3.147 mpls te signalled tunnel-name

Function

The **mpls te signalled tunnel-name** command configures the name of a TE tunnel.

The **undo mpls te signalled tunnel-name** command deletes the configured name of the TE tunnel.

By default, the name of a TE tunnel is not configured.

Format

mpls te signalled tunnel-name *tunnel-name*

undo mpls te signalled tunnel-name

Parameters

Parameter	Description	Value
tunnel-name	Specifies the name of a TE tunnel.	A string of 1 to 63 case-sensitive characters, spaces or slashes (/) not supported. The initial character must be an underscore (_) or an English letter, not a digit.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A tunnel interface name is used as a tunnel name by default, for example, Tunnel1. Alternatively, if you want to customize a name for a TE tunnel, the **mpls te signalled tunnel-name** command can be used to configure a TE tunnel name. For example, a TE tunnel from LSR A to LSR C is named LSRAtoLSRC.

Prerequisites

MPLS TE has been enabled using the **mpls te** command.

Precautions

A TE tunnel name must be unique on an entire device.

If a TE tunnel name is specified, RSVP signaling messages will carry the specified name. If a configured TE tunnel name is deleted or no TE tunnel name is specified, RSVP signaling messages will carry the TE tunnel interface name as the TE tunnel name.

The **mpls te signalled tunnel-name** command or its undo form takes effect on a TE tunnel established using only RSVP signaling, not a static route.

Example

# Name a TE tunnel **LSRAtoLSRC**.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te signalled tunnel-name LSRAtoLSRC
[HUAWEI-Tunnel1] mpls te commit
```

9.3.148 mpls te srlg

Function

The **mpls te srlg** command configures an interface as an SRLG member.

The **undo mpls te srlg** command deletes an interface from an SRLG.

No interface is added to any SRLG by default.

Format

mpls te srlg *srlg-number*

undo mpls te srlg { *srlg-number* | **all** }

Parameters

Parameter	Description	Value
srlg-number	Specifies the number of the SRLG to which an interface belongs.	The value is an integer that ranges from 0 to 4294967295.
all	Indicates that all SRLG configurations are deleted from an interface.	-

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SRLG, like the bandwidth and affinity property, is a constraint in path calculation. If SRLG is configured for links, an IGP floods the TE link information along with the SRLG membership information to all devices in an IGP area. The SRLG membership information is also added into the TEDB.

Prerequisites

Before running the **mpls te srlg** command, the **mpls te** command must be run in the interface view.

Precautions

If SRLG is configured for links and the **mpls te srlg path-calculation** command is configured on the ingress of the primary tunnel, when calculating the path of a bypass tunnel or a hot-standby tunnel, CSPF determines whether the SRLG attribute is used as a constraint according to the configured SRLG calculation mode.

One interface can join multiple SRLGs.

Example

# Add VLANIF100 to SRLG 1 and SRLG 2.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls te srlg 1
[HUAWEI-Vlanif100] mpls te srlg 2
```

# Add GE0/0/1 to SRLG 1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls te srlg 1
```

9.3.149 mpls te srlg path-calculation

Function

The **mpls te srlg path-calculation** command configures an SRLG-based path calculation mode.

The **undo mpls te srlg path-calculation** command deletes an SRLG-based path calculation mode.

By default, when calculating a path, CSPF does not consider an SRLG constraint or check whether the primary CR-LSP and a Bypass CR-LSP or a hot-standby CR-LSP are in the same SRLG.

Format

mpls te srlg path-calculation [**strict** | **preferred**]

undo mpls te srlg path-calculation

Parameters

Parameter	Description	Value
strict	Indicates that CSPF must calculate a bypass CR-LSP or a hot-standby CR-LSP according to the SRLG attribute. The link that the primary path uses and the link that the bypass CR-LSP or hot-standby CR-LSP uses cannot be in the same SRLG. **NOTE** After you specify this parameter, all the links on the primary CR-LSP regardless of whether the SRLG attribute is configured cannot be used for calculation of the bypass or hot-standby CR-LSP. However, nodes on the primary CR-LSP can be used in CSPF calculation.	-
preferred	Indicates that CSPF prefers the SRLG attribute the first time it calculates a Bypass CR-LSP or hot-standby CR-LSP. If the initial calculation fails, the CSPF does not use the SRLG attribute as a constraint. **NOTE** If no path calculation mode is specified in the **mpls te srlg path-calculation** command, SRLG-based path calculation is performed in preferred mode by default.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the TE FRR or hot standby scenario, to enable CSPF to calculate a path for a Bypass CR-LSP or a hot-standby CR-LSP based on the SRLG attribute, you must run the **mpls te srlg path-calculation** command on the ingress of the tunnel.

The SRLG, like the bandwidth and affinity property, is a constraint in path calculation. If SRLG is configured for links and the **mpls te srlg path-calculation** command is configured on the ingress of the primary CR-LSP, when calculating the path of a Bypass CR-LSP or a hot-standby tunnel, CSPF determines whether the SRLG attribute is used as a constraint according to the configured SRLG calculation mode.

Precautions

If **strict** is configured, CSPF always considers SRLG as a constraint.

If **preferred** is configured, the first time that CSPF calculates a path is according to the SRLG attribute. If the calculation fails, CSPF tries to calculate again without considering SRLG.

Example

# Enable path calculation in **strict** mode.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te srlg path-calculation strict
```

9.3.150 mpls te switch-delay

Function

The **mpls te switch-delay** command sets the switching and deletion delays for a TE tunnel.

The **undo mpls te switch-delay** command restores the default settings.

By default, the switching delay is 5000 milliseconds and the deletion delay is 7000 milliseconds.

Format

mpls te switch-delay *switch-time* **delete-delay** *delete-time*

undo mpls te switch-delay *switch-time* **delete-delay** *delete-time*

Parameters

Parameter	Description	Value
switch-delay *switch-time*	Specifies the time period that the TE traffic is switched from the primary CR-LSP to the Modified CR-LSP.	The value is an integer that ranges from 0 to 600000, in milliseconds. The default value is 5000.
delete-delay *delete-time*	Specifies the delay for deleting the primary CR-LSP after the TE traffic is switched to a Modified CR-LSP.	The value is an integer that ranges from 0 to 600000, in milliseconds. The default value is 7000.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MPLS TE uses the Make-Before-Break mechanism. When the attributes of an MPLS TE tunnel such as bandwidth and path change, a new CR-LSP with new attributes, also called Modified CR-LSP, must be established.

On the same modified CR-LSP, when a downstream LSR is too busy but the upstream LSR is not as busy, the Modified CR-LSP may go Up earlier on the upstream LSR than on the downstream LSR. The upstream LSR switches traffic to the Modified CR-LSP but the Modified CR-LSP is not Up on the downstream LSR. This causes a momentary traffic interruption. You can set a suitable switching delay time to avoid the traffic interruption.

If a modified CR-LSP fails, the failed node sends PathErr messages to its upstream LSRs and deletes the Modified CR-LSP, and traffic should be switched back to the primary CR-LSP. In applications, when detecting the fault, the upstream LSRs of the failed node are too occupied to forward the PathErr messages. This causes a traffic interruption on the failed node because the primary CR-LSP is deleted on the failed node. You can set a suitable deletion delay time to prevent the traffic interruption.

NOTE

In a VPLS over MPLS TE scenario, you can configure TE FRR to improve network reliability. TE FRR protects links and nodes on an MPLS TE tunnel. If a link or node fails, TE FRR rapidly switches traffic to the protection path. However, traffic loss may occur during a traffic switchback if the delay for deleting the TE FRR protection path is too short. To prevent this situation, run the **delete-delay** *delete-time* command to configure an appropriate delay based on the number of VSIs on the MPLS TE tunnel:

- 30s if there are 2001 to 4000 VSIs
- 20s if there are 1001 to 2000 VSIs
- 10s if there are 501 to 1000 VSIs
- 7s if there are 1 to 500 VSIs

Prerequisites

MPLS TE has been enabled globally by running the **mpls te** command.

Example

# Set the switching delay of the TE tunnel to 3000 milliseconds and the deletion delay of the TE tunnel to 8000 milliseconds.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls te switch-delay 3000 delete-delay 8000
```

9.3.151 mpls te tie-breaking

Function

The **mpls te tie-breaking** command configures a rule for selecting a route among multiple available equal-cost routes to the destination.

The **undo mpls te tie-breaking** command restores the default settings.

By default, tie-breaking policy is random.

Format

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

undo mpls te tie-breaking

Parameters

Parameter	Description	Value
least-fill	Selects the route with the smallest ratio of the occupied bandwidth to the maximum reservable bandwidth.	-
most-fill	Selects the route with the largest ratio of the occupied bandwidth to the maximum reservable bandwidth.	-
random	Selects a route randomly.	-

Views

MPLS view, tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The route is selected based on the ratio of the occupied available bandwidth to the maximum reservable bandwidth. If **least-fill** is configured, the route with the smallest ratio is selected; if **most-fill** is configured, the route with the largest ratio is selected.

Prerequisites

MPLS TE has been enabled by running the **mpls te** command.

Precautions

Note that the link is selected according to a ratio through the tie-breaking mechanism. In the case that the ratios are the same when the reservable bandwidth is not used or the same reservable bandwidth is used on the links, the first found link is used regardless of whether **least-fill** or **most-fill** is configured.

NOTE

A tunnel prefers the route-selecting rule configured in the local tunnel interface view. If no rule is configured in the tunnel interface view, the rule configured in the MPLS view is used.

Example

# Select the path with the smallest ratio of the occupied bandwidth to the maximum reservable bandwidth.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te tie-breaking least-fill
[HUAWEI-Tunnel1] mpls te commit
```

# Select the path with the smallest ratio of the occupied bandwidth to the maximum reservable bandwidth.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te tie-breaking least-fill
```

9.3.152 mpls te timer auto-bandwidth

Function

The **mpls te timer auto-bandwidth** command enables automatic bandwidth adjustment and samples the output rate for tunnels.

The **undo mpls te timer auto-bandwidth** command disables automatic bandwidth adjustment.

By default, automatic bandwidth adjustment is not enabled.

NOTE

Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730-H, and S6730S-H support this command.

Format

mpls te timer auto-bandwidth [*interval*]

undo mpls te timer auto-bandwidth

Parameters

Parameter	Description	Value
interval	Specifies the interval for sampling the output rate of each tunnel configured with automatic bandwidth adjustment.	The value is an integer that ranges from 1 to 604800 in seconds. The default value is 300 seconds, and is a recommended value.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Before a sampling interval is changed, the **undo mpls te timer auto-bandwidth** command must be run. Then the **mpls te timer auto-bandwidth** command is run to set an interval.

Example

# Sample the output rate of the MPLS TE tunnel every 10 minutes.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls te timer auto-bandwidth 600
```

9.3.153 mpls te timer fast-reroute

Function

The **mpls te timer fast-reroute** command sets the interval at which the binding between a bypass CR-LSP and a primary CR-LSP is refreshed.

The **undo mpls te timer fast-reroute** command restores the default configuration.

By default, the time weight used to calculate the interval is 300. And the actual interval at which the binding between a bypass CR-LSP and a primary LSP is refreshed depends on device performance and the maximum number of LSPs that can be established on the device.

Format

mpls te timer fast-reroute [*weight*]

undo mpls te timer fast-reroute

Parameters

Parameter	Description	Value
weight	Specifies the weight value used to calculate the interval at which the binding between a bypass CR-LSP and a primary LSP is refreshed.	The value is an integer that ranges from 0 to 604800. **NOTE** If *weight* is not specified, the default weight value is 300.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After TE FRR is configured, a PLR refreshes the binding between a bypass CR-LSP and a primary CR-LSP at a specified interval. The PLR searches for the optimal bypass CR-LSP and binds it to a primary CR-LSP. To set the interval at which the binding between a bypass CR-LSP and a primary CR-LSP is refreshed, run the **mpls te timer fast-reroute** command.

The PLR calculates the interval using the value of *weight*. And the actual interval depends on device performance and the maximum number of LSPs that can be established on the device

Prerequisites

RSVP-TE has been enabled by running the **mpls rsvp-te** command in the MPLS view.

Example

# Set the weight of the interval at which binding between a bypass CR-LSP and a primary LSP is refreshed to **120**.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te timer fast-reroute 120
```

9.3.154 mpls te timer retry

Function

The **mpls te timer retry** command sets the interval for re-establishing a tunnel.

The **undo mpls te timer retry** command restores the default setting.

The default interval is 30 seconds.

Format

mpls te timer retry *interval*

undo mpls te timer retry [*interval*]

Parameters

Parameter	Description	Value
interval	Specifies the interval for resetting up tunnels.	The value is an integer that ranges from 10 to 65535, in seconds. The default value is 30 seconds.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a TE tunnel has been established, the TE tunnel is kept Up by periodically sending a Path message from the local node to its neighbor and receiving a Resv message from the neighbor. If no Resv message is received after the specified interval at which a tunnel is re-established, the local node considers the tunnel Down and reattempts to establish the tunnel. You can run this command to modify the interval for re-establishing a tunnel.

Precautions

A rather smaller interval imposes heavy burden of message processing on the system, causing network flapping; a rather large interval deteriorates the efficiency of RSVP CR-LSP convergence. Therefore, the default interval, 30 seconds, is recommended.

Example

# Set the interval for setting up tunnels to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te timer retry 20
[HUAWEI-Tunnel1] mpls te commit
```

9.3.155 mpls te tunnel-id

Function

The **mpls te tunnel-id** command specifies the ID for a tunnel.

Format

mpls te tunnel-id *tunnel-id*

Parameters

Parameter	Description	Value
tunnel-id	Specifies the ID for a tunnel.	The value is an integer that ranges from 1 to 10000.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The ID for a tunnel is a number that uniquely identifies an MPLS TE tunnel to facilitate tunnel planning and management.

Prerequisites

MPLS TE has been configured as the tunnel protocol using the **tunnel-protocol mpls te** command in the tunnel interface view.

Precautions

A tunnel ID must be set for a tunnel; otherwise, the tunnel fails to be established.

Example

# Create a tunnel interface, configure MPLS TE as a tunnel protocol, set the tunnel ID to 100, and assign a tunnel destination address 2.2.2.2 to the interface.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te commit
```

9.3.156 mpls total-crlsp-number threshold-alarm

Function

The **mpls total-crlsp-number threshold-alarm** command configures the alarm threshold for total constraint-based routed label switched path (CR-LSP) usage.

The **undo mpls total-crlsp-number threshold-alarm** command restores the default settings.

The default upper limit of the alarm threshold for total CR-LSP usage is 80%. The default lower limit of the clear alarm threshold for total CR-LSP usage is 75%.

Format

mpls total-crlsp-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

mpls total-crlsp-number { **ingress** | **transit** | **egress** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls total-crlsp-number threshold-alarm

undo mpls total-crlsp-number { **ingress** | **transit** | **egress** } **threshold-alarm**

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper limit of the alarm threshold for total CR-LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies the lower limit of the clear alarm threshold for total CR-LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.
ingress	Specifies the alarm threshold for total ingress CR-LSPs.	-
transit	Specifies the alarm threshold for total transit CR-LSPs.	-
egress	Specifies the alarm threshold for total egress CR-LSPs.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of total CR-LSPs (including static CR-LSPs and Resource Reservation Protocol (RSVP) LSPs) in the system reaches a specific limit, establishing subsequent CR-LSPs may fail because of insufficient resources. To facilitate user operation and maintenance, enable an alarm to be generated when the number of total CR-LSPs reaches the specific limit. To configure the alarm threshold for total CR-LSP usage, run the **mpls total-crlsp-number threshold-alarm** command. The parameters in this command are described as follows:

- When the total CR-LSP usage increases to the value of *upper-limit-value*, an alarm for total CR-LSPs is generated.
- When the total CR-LSP usage falls below the value of *lower-limit-value*, a clear alarm for total CR-LSPs is generated.

If you want to set the alarm threshold for total ingress CR-LSPs, total transit CR-LSPs or total egress CR-LSPs, run **mpls total-crlsp-number** { **ingress** | **transit** | **egress** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*.

Precautions

- If the **mpls total-crlsp-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- This command configures the alarm threshold for total CR-LSP usage. The alarm that the number of LSPs exceeded the upper threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceed** is configured, and the actual total CR-LSP usage reaches the upper limit of the alarm threshold. The alarm that the number of LSPs fell below the lower threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceedclear** is configured, and the actual total CR-LSP usage falls below the lower limit of the clear alarm threshold.

Example

# Configure the upper limit and the lower limit of the alarm threshold for total CR-LSP usage.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls total-crlsp-number threshold-alarm upper-limit 90 lower-limit 60
```

9.3.157 next hop

Function

The **next hop** command specifies the next-hop address on an explicit path, and creates an MPLS TE tunnel through nodes in the order in which they are configured.

The **undo next hop** command restores the default configuration.

By default, no next-hop address on an explicit path is specified.

Format

next hop *ip-address* [**include** [[**loose** | **strict**] | [**incoming** | **outgoing**]] * | **exclude**]

undo next hop *ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies the next-hop IP address on an explicit path.	The value is in dotted decimal notation.
include [[**loose** | **strict**] | [**incoming** | **outgoing**]] *	Specifies the IP address of a node included on an explicit path. ● **strict**: indicates that the node is added in **strict** mode. The node of *ip-address* is directly connected to the previous hop. ● **loose**: indicates that the node is added in **loose** mode. The node of *ip-address* may not be directly connected to the previous hop. ● **incoming**: indicates that the *ip-address1* is the IP address of an inbound interface of a next-hop node. ● **outgoing**: indicates that the *ip-address1* is the IP address of an outbound interface of a next-hop node.	By default, a node is added to an explicit path in **include strict** mode.
exclude	Excludes the IP address from an explicit path.	-

Views

Explicit path view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **next hop** command is used to plan nodes for an explicit path.

Precautions

The **include strict** parameter is used by default, meaning the tunnel must pass through a specified node.

Example

# Exclude the IP address 10.0.0.125 from the MPLS TE explicit path.

```
<HUAWEI> system-view
[HUAWEI] explicit-path p1
[HUAWEI-explicit-path-p1] next hop 10.0.0.125 exclude
```

9.3.158 notify neighbor-down

Function

The **notify neighbor-down** command configures a BFD session to notify the upper layer protocol when the BFD session detects a neighbor Down event.

The **undo notify neighbor-down** command restores the default configuration.

By default, when the BFD detection time expires or a BFD session detects a neighbor Down event, the BFD session notifies the upper layer protocol.

Format

notify neighbor-down

undo notify neighbor-down

Parameters

None

Views

BFD-LSP session view

Default Level

2: Configuration level

Usage Guidelines

In most cases, when you use a BFD session to detect link faults, the BFD session notifies the upper layer protocol of a link fault in the following scenarios:

- When the BFD detection time expires, the BFD session notifies the upper layer protocol. BFD sessions must be configured on both ends. If the BFD session on the local end does not receive any BFD packets from the remote end within the detection time, the BFD session on the local end concludes that the link fails and notifies the upper layer protocol of the link fault.
- When a BFD session detects a neighbor Down event, the BFD session notifies the upper layer protocol. If the BFD session on the local end detects a neighbor Down event within the detection time, the BFD session on the local end directly notifies the upper layer protocol of the neighbor Down event.

When you use a BFD session to detect faults on an LSP, you need only be concerned about whether a fault occurs on the link from the local end to remote end. In this situation, run the **notify neighbor-down** command to configure the BFD session to notify the upper layer protocol only when the BFD session detects a neighbor Down event. This configuration prevents the BFD session from notifying the upper layer protocol when the BFD detection time expires and ensures that services are not interrupted.

Example

# Configure the BFD session to notify the upper layer protocol when the BFD session detects a neighbor Down event.

```
<HUAWEI> system-view
[HUAWEI] bfd atob bind ldp-lsp peer-ip 10.1.2.1 nexthop 10.1.1.2 interface vlanif 100
[HUAWEI-bfd-lsp-session-atob] discriminator local 1
[HUAWEI-bfd-lsp-session-atob] discriminator remote 2
[HUAWEI-bfd-lsp-session-atob] notify neighbor-down
[HUAWEI-bfd-lsp-session-atob] commit
```

9.3.159 opaque-capability enable

Function

The **opaque-capability enable** command enables the Opaque-LSA capability so that an OSPF process can generate Opaque LSAs and receive Opaque LSAs from neighbors.

The **undo opaque-capability** command disables the Opaque-LSA capability.

By default, the Opaque-LSA capability is disabled.

Format

opaque-capability enable

undo opaque-capability

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Opaque LSAs provide a generic mechanism for OSPF extension:

- OSPF supports GR using Type 9 LSAs.
- OSPF supports TE using Type 10 LSAs.

Before configuring OSPF GR or OSPF TE, you must enable opaque LSA capability running the **opaque-capability enable** command.

Configuration Impact

Enabling or disabling the opaque LSA function may delete and re-establish all sessions and instances.

Example

# Enable OSPF opaque-lsa.

```
<HUAWEI> system-view
[HUAWEI] ospf
[HUAWEI-ospf-1] opaque-capability enable
```

9.3.160 priority

Function

The **priority** command sets the setup priority and holding priority in a CR-LSP attribute template.

The **undo priority** command restores the default setup priority and holding priority in a CR-LSP attribute template.

The default setup and holding priority for a CR-LSP attribute template are both 7.

Format

priority *setup_priority_value* [*hold_priority_value*]

undo priority

Parameters

Parameter	Description	Value
setup_priority_value	Specifies the setup priority value in a CR-LSP attribute template.	An integer ranging from 0 to 7. The smaller the value, the higher the priority. The default setup priority is 7.
hold_priority_value	Specifies the holding priority value in a CR-LSP attribute template.	An integer ranging from 0 to 7. The smaller the value, the higher the priority. The default holding priority is 7.

Views

LSP attribute view

Default Level

2: Configuration level

Usage Guidelines

When configuring the **priority** command in the LSP attribute view, ensure that the setup priority is greater than or equal to the holding priority.

Example

# Set both the setup priority and holding priority to 4 in the CR-LSP attribute template.

```
<HUAWEI> system-view
[HUAWEI] lsp-attribute lsp-attribute-name
[HUAWEI-lsp-attribute-lsp-attribute-name] priority 4 4
```

9.3.161 record-route

Function

The **record-route** command enables the system to record routes in a CR-LSP attribute template.

The **undo record-route** command configures the system not to record routes in a CR-LSP attribute template.

The system does not record routes in a CR-LSP attribute template.

Format

record-route [**label**]

undo record-route

Parameters

Parameter	Description	Value
label	Indicates that a label is also recorded when the system records a route.	-

Views

LSP attribute view

Default Level

2: Configuration level

Usage Guidelines

If the FRR function is enabled in a CR-LSP attribute template, the route storing function cannot be disabled.

Example

# Enable the system to record routes in the CR-LSP attribute template.

```
<HUAWEI> system-view
[HUAWEI] lsp-attribute lsp-attribute-name
[HUAWEI-lsp-attribute-lsp-attribute-name] record-route
```

9.3.162 reset mpls rsvp-te

Function

The **reset mpls rsvp-te** command resets RSVP-TE process.

Format

reset mpls rsvp-te

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can delete and re-establish a CR-LSP by running the **reset mpls rsvp-te** command. This command is used to verify the working process of RSVP-TE in special cases. Generally, this command is not needed.

NOTE

If this command is run in an attempt to restart RSVP-TE and the interval at which RSVP-TE is restarted is small, the attempt fails. The interval varies according to the number of LSPs. The more the LSPs are established, the longer the interval is. The interval can be set to 30, 60, 90, or 120, in seconds.

Example

# Reset RSVP-TE.

```
<HUAWEI> reset mpls rsvp-te
Warning: The MPLS RSVP-TE services will be reset. Continue? [Y/N]:y
```

9.3.163 reset mpls rsvp-te statistics

Function

The **reset mpls rsvp-te statistics** command clears the operational statistics on RSVP-TE.

Format

reset mpls rsvp-te statistics { **global** | **interface** [*interface-type interface-number*] }

Parameters

Parameter	Description	Value
global	Clears the global operational statistics on RSVP-TE.	-
interface	Clears the operational statistics on RSVP-TE on the interface.	-
interface-type interface-number	Clears the operational statistics on RSVP-TE on the specifies interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	If no type or number of an interface is specified, statistics about all RSVP-TE interfaces are cleared.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

When you run this command to clear the running information about RSVP-TE, the system displays the statistics from after the previous information is cleared.

Example

# Clear the global operational statistics on RSVP-TE.

```
<HUAWEI> reset mpls rsvp-te statistics global
```

9.3.164 reset mpls stale-interface

Function

The **reset mpls stale-interface** command deletes information about MPLS interfaces in the Stale state.

Format

reset mpls stale-interface [*interface-index*]

Parameters

Parameter	Description	Value
interface-index	Specifies the index of a specified stale interface.	A hexadecimal integer ranging from 1 to FFFFFFFE.

Views

User view

Default Level

3: Management level

Usage Guidelines

If the configuration of an interface is deleted, or MPLS is disabled on an interface, the interface status becomes Stale. Run the **reset mpls stale-interface** command to delete information about a stale interface.

Run the **display mpls stale-interface** command without specifying a parameter to view the index of a stale interface.

Example

# Delete information about a specified stale interface.

```
<HUAWEI> reset mpls stale-interface 9d
```

# Delete information about all stale interfaces.

```
<HUAWEI> reset mpls stale-interface
```

9.3.165 reset mpls te auto-bandwidth adjustment timers

Function

The **reset mpls te auto-bandwidth adjustment timers** command initializes automatic bandwidth adjustment.

NOTE

Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730-H, and S6730S-H support this command.

Format

reset mpls te auto-bandwidth adjustment timers

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

After the automatic bandwidth adjustment function runs for a certain period of time, to delete the running information and re-collect information, run the **reset mpls te auto-bandwidth adjustment timers** command in the user view. You do not need to delete this function or reconfigure it.

After the **reset mpls te auto-bandwidth adjustment timers** command is run, the device deletes information about the sampled traffic rate on the outbound interface and resets the automatic bandwidth adjustment timer.

Example

# Initialize automatic bandwidth adjustment for MPLS TE tunnels.

```
<HUAWEI> reset mpls te auto-bandwidth adjustment timers
```

9.3.166 reset mpls te auto-frr

Function

The **reset mpls te auto-frr** command resets a specified auto bypass tunnel.

NOTE

After the Auto FRR function is enabled, you can use this command to recreate a bypass tunnel.

Format

reset mpls te auto-frr { **lsp-id** *ingress-lsr-id tunnel-id* | **name** *bypass-tunnel-name* }

Parameters

Parameter	Description	Value
lsp-id	Specifies the ID of an LSP.	-
ingress-lsr-id	Specifies the LSR ID of the ingress.	The value is in dotted decimal notation.
tunnel-id	Specifies the ID of a tunnel.	The value is an integer and its ranges from 0 to 65535.

Parameter	Description	Value
name *bypass-tunnel-name*	Specifies the name of a bypass tunnel.	The value is a string of 1 to 63 characters.

Views

User view

Default Level

3: Management level

Usage Guidelines

To immediately recreate a specified auto bypass tunnel, run the **reset mpls te auto-frr** command.

Example

# Reset the bypass tunnel with the ingress address being 1.1.1.1 and the tunnel ID being 10.

```
<HUAWEI> reset mpls te auto-frr lsp-id 1.1.1.1 10
```

9.3.167 reset mpls te tunnel-interface tunnel

Function

The **reset mpls te tunnel-interface tunnel** command resets a TE tunnel interface and re-establishes a TE tunnel.

Format

reset mpls te tunnel-interface tunnel *interface-number*

Parameters

Parameter	Description	Value
tunnel *interface-number*	Specifies the number of a TE tunnel.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

To validate the configurations of an MPLS TE tunnel, you can run the **mpls te commit** command in the tunnel interface view, and then run the **reset mpls te tunnel-interface tunnel** command in the user view.

If you do not run the **mpls te commit** command after modifying the configuration of a TE tunnel in the tunnel interface view, the system prompts a fault after the **reset mpls te tunnel-interface tunnel** command is run.

Example

# Reset Tunnel 1.

```
<HUAWEI> reset mpls te tunnel-interface tunnel 1
```

9.3.168 static-cr-lsp egress

Function

The **static-cr-lsp egress** command configures a static CR-LSP on the egress LSR.

The **undo static-cr-lsp egress** command deletes a static CR-LSP from the egress LSR.

By default, no static CR-LSP on the egress LSR is configured.

Format

static-cr-lsp egress *lsp-name* [**incoming-interface** *interface-type interface-number*] **in-label** *in-label*

undo static-cr-lsp egress *lsp-name*

Parameters

Parameter	Description	Value
lsp-name	Specifies the name of a CR-LSP.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
incoming-interface *interface-type interface-number*	Specifies the type and number of an inbound interface.	-
in-label *in-label*	Specifies the value of an incoming label.	The value is an integer that ranges from 16 to 1023.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When configuring the egress of the CR-LSP, you can run the command **static-cr-lsp egress**. Before setting up an MPLS TE tunnel through a static CR-LSP, configure a static route or an IGP to ensure connectivity between LSRs, and enable basic MPLS and MPLS TE functions. After setting up a static CR-LSP, you can run the **display mpls static-cr-lsp** command to ensure that the static CR-LSP is established successfully.

To modify the value of **incoming-interface** *interface-type interface-number* and **in-label** *in-label*, run the **static-cr-lsp egress** command to set a new value. There is no need to run the **undo static-cr-lsp egress** command before changing a configured value.

Example

# Configure the static CR-LSP named tunnel34 with the inbound interface being VLANIF100, and the incoming label being 233 on the egress LSR.

```
<HUAWEI> system-view
[HUAWEI] static-cr-lsp egress tunnel34 incoming-interface vlanif 100 in-label 233
```

9.3.169 static-cr-lsp ingress

Function

The **static-cr-lsp ingress** command configures a static CR-LSP on the ingress LSR.

The **undo static-cr-lsp ingress** command deletes a static CR-LSP from the ingress LSR.

By default, no static CR-LSP on the ingress LSR is configured.

Format

static-cr-lsp ingress { **tunnel-interface tunnel** *interface-number* | *tunnel-name* } **destination** *destination-address* { **nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number* } * **out-label** *out-label* [**bandwidth** [**ct0** | **ct1**] *bandwidth*]

undo static-cr-lsp ingress { **tunnel-interface tunnel** *interface-number* | *tunnel-name* }

Parameters

Parameter	Description	Value
tunnel-interface tunnel *interface-number*	Specifies the tunnel interface of a static CR-LSP. *interface-number* indicates the tunnel interface number.	-
tunnel-name	Specifies the name of a CR-LSP.	The name is a string of 1 to 19 case-sensitive characters, spaces and abbreviation not supported. If you use the **interface Tunnel 1** command to create a tunnel interface for a static CR-LSP, the tunnel name in the **static-cr-lsp ingress** command must be formatted as "Tunnel1", otherwise, the tunnel cannot be created. There is no such a limit for the transit node and egress node.
destination *destination-address*	Specifies the destination IP address of a static CR-LSP.	The value is in dotted decimal notation.
nexthop *next-hop-address*	Specifies the next-hop IP address of a static CR-LSP.	The value is in dotted decimal notation.
outgoing-interface *interface-type interface-number*	Specifies the type and number of an outgoing interface. This parameter is only applicable to a P2P link.	-
out-label *out-label*	Specifies the value of an outgoing label.	The value is an integer that ranges from 16 to 1048575.
bandwidth [**ct0** | **ct1**] *bandwidth*	Specifies the bandwidth values of CR-LSPs of CT0 to CT1.	The value is an integer that ranges from 0 to 4000000000, in kbit/s. The default value is 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run this command on the ingress node to configure a static CR-LSP.

Before setting up an MPLS TE tunnel through a static CR-LSP, configure a static route or an IGP to ensure connectivity between LSRs, and enable basic MPLS and MPLS TE functions. After setting up a static CR-LSP, you can run the **display mpls static-cr-lsp** command to ensure that the static CR-LSP is established successfully.

Precautions

To modify parameters including **destination** *destination-address*, **nexthop** *next-hop-address*, **outgoing-interface** *interface-type interface-number*, and **out-label** *out-label*, run the **static-cr-lsp ingress** command to set a new value. There is no need to run the **undo static-cr-lsp ingress** command before changing a configured value.

When configuring a static CR-LSP ensure that the route of the static CR-LSP exactly matches the routing information. For example:

- If you specify a next hop when configuring a static CR-LSP, specify a next hop when configuring a static IP route. If you do not specify a next hop, the static LSP cannot be set up. For example:

```
[HUAWEI] ip route-static 10.1.3.0 24 10.1.1.2
[HUAWEI] static-cr-lsp ingress Tunnel1 destination 10.1.3.1 nexthop 10.1.1.2 out-label 237
```

- If a dynamic routing protocol applies to the link between LSRs, the next-hop IP address along the LSP must be the same as the IP address of the next hop in the routing table.

NOTE

The configured bandwidth takes effect only during tunnel establishment and protocol negotiation, and does not limit the bandwidth for traffic forwarding.

Example

# Configure the static CR-LSP named Tunnel1, with the destination IP address being 10.1.3.1, the next-hop address being 10.1.1.2, the outgoing label being 237.

```
<HUAWEI> system-view
[HUAWEI] static-cr-lsp ingress Tunnel1 destination 10.1.3.1 nexthop 10.1.1.2 out-label 237
```

9.3.170 static-cr-lsp transit

Function

The **static-cr-lsp transit** command configures a static CR-LSP on a transit LSR.

The **undo static-cr-lsp transit** command deletes a static CR-LSP from the transit LSR.

By default, no static CR-LSP on a transit LSR is configured.

Format

static-cr-lsp transit *lsp-name* [**incoming-interface** *interface-type interface-number*] **in-label** *in-label* { **nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number* } * **out-label** *out-label* [**bandwidth** [**ct0** | **ct1**] *bandwidth*] [**description** *description*]

undo static-cr-lsp transit *lsp-name*

Parameters

Parameter	Description	Value
lsp-name	Specifies the CR-LSP name.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
incoming-interface *interface-type interface-number*	Specifies the incoming interface of the CR-LSP. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
in-label *in-label*	Specifies the value of an incoming label.	The value is an integer that ranges from 16 to 1023.
nexthop *next-hop-address*	Specifies the next-hop address.	The value is in dotted decimal notation.
outgoing-interface *interface-type interface-number*	Specifies the name of an outgoing interface.	-
out-label *out-label*	Specifies the value of an outgoing label.	The value is an integer that ranges from 16 to 1048575.
bandwidth [**ct0** | **ct1**] *bandwidth*	Specifies the bandwidth values of CR-LSPs of CT0 to CT1.	The value is an integer that ranges from 0 to 4000000000, in kbit/s. The default value is 0.
description *description*	Specifies the description information.	The value is a string of 1 to 63 case-sensitive characters with spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before setting up an MPLS TE tunnel through a static CR-LSP, configure a static route or an IGP to ensure connectivity between LSRs, and enable basic MPLS and MPLS TE functions. After setting up a static CR-LSP, you can run the **display mpls static-cr-lsp** command to ensure that the static CR-LSP is established successfully.

To modify parameters including **incoming-interface** *interface-type interface-number*, **in-label** *in-label*, **nexthop** *next-hop-address*, **outgoing-interface** *interface-type interface-number*, and **out-label** *out-label*, run the **static-cr-lsp transit** command to set a new value for each parameter. There is no need to run the **undo static-cr-lsp transit** command before modifying a value.

NOTE

The configured bandwidth takes effect only during tunnel establishment and protocol negotiation, and does not limit the bandwidth for traffic forwarding.

Example

# Configure the static CR-LSP named tunnel39 with the incoming interface being VLANIF100, the incoming label being 123, the outgoing interface being VLANIF200, the outgoing label as 253.

```
<HUAWEI> system-view
[HUAWEI] static-cr-lsp transit tunnel39 incoming-interface vlanif 100 in-label 123 outgoing-interface vlanif 200 out-label 253
```

9.3.171 statistic enable (MPLS TE tunnel interface view)

Function

The **statistic enable** command enables MPLS TE traffic statistics collection.

The **undo statistic enable** command disables MPLS TE traffic statistics collection.

By default, MPLS TE traffic statistics collection is disabled.

NOTE

Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H support this command.

Format

statistic enable

undo statistic enable

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To view MPLS TE traffic statistics collected in the outbound direction of an interface, run the **statistic enable** command in the tunnel interface view to enable MPLS TE traffic statistics collection first. After a period of time, run the **display interface tunnel** or **display counters interface** command to view the MPLS TE traffic statistics.

Prerequisites

The tunneling protocol of the tunnel interface has been set to MPLS TE using the **tunnel-protocol mpls te** command in the tunnel interface view.

Precautions

MPLS TE traffic statistics collection is supported only in the outbound direction of a tunnel interface.

Example

# Enable MPLS TE traffic statistics collection on Tunnel1.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] statistic enable
```

9.3.172 traffic-eng

Function

The **traffic-eng** command enables TE features on a specified level for an IS-IS process.

The **undo traffic-eng** command restores the default settings.

By default, TE features are disabled for an IS-IS process.

Format

traffic-eng [**level-1** | **level-2** | **level-1-2**]

undo traffic-eng [**level-1** | **level-2** | **level-1-2**]

Parameters

Parameter	Description	Value
level-1	Enables IS-IS TE on Level-1.	-
level-2	Enables IS-IS TE on Level-2.	-
level-1-2	Enables IS-IS TE on Level-1-2. **NOTE** If no level is specified, TE is enabled on Level-1-2.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you deploy MPLS TE on the MPLS backbone network where IS-IS is used to advertise routes, run this command to enable TE features on a specified level for an IS-IS process.

Prerequisites

The **cost-style** command has been executed to set the cost type of IS-IS packets to wide, compatible, or wide-compatible.

Precautions

The IS-IS level in this command must be the same as that on the MPLS backbone network.

Example

# Enable TE on level-2 for IS-IS process 1.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] cost-style compatible
[HUAWEI-isis-1] traffic-eng level-2
```

9.3.173 undo mpls te srlg all-config

Function

The **undo mpls te srlg all-config** command deletes the member interfaces of all SRLGs on an MPLS TE node.

Format

undo mpls te srlg all-config

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

If an MPLS TE node is configured with the **undo mpls te srlg all-config** command, the **mpls te srlg** command is deleted from all the interfaces of an MPLS TE node, while the **mpls te srlg path-calculation** command configured in the MPLS view is not deleted.

Example

# Delete the SRLG configuration from all the interfaces of the MPLS TE node.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls te srlg 1
[HUAWEI-Vlanif10] mpls te srlg 2
[HUAWEI-Vlanif10] quit
[HUAWEI] interface vlanif 20
[HUAWEI-Vlanif20] mpls te srlg 1
[HUAWEI-Vlanif20] mpls te srlg 2
[HUAWEI-Vlanif20] quit
[HUAWEI] mpls
[HUAWEI-mpls] undo mpls te srlg all-config
```