MPLS Command Reference for Cisco NCS 6000 Series Routers

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
    800 553-NETS (6387)
Fax: 408 527-0883

C O N T E N T S

C H A P T E R 4 **RSVP Infrastructure Commands** **425**

Preface

The preface contains these sections:

Changes to This Document

This table lists the technical changes made to this document since it was first printed.

Table 1: Changes to This Document

Revision	Date	Change Summary
OL-30983-01	November 2013	Initial release of this document.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

MPLS Label Distribution Protocol Commands

This module describes the commands used to configure Label Distribution Protocol (LDP) in a Multiprotocol Label Switching (MPLS) network on the .

LDP provides a standard methodology for hop-by-hop (or dynamic label) distribution in an MPLS network by assigning labels to routes that have been chosen by the underlying Interior Gateway Protocol (IGP) routing protocols. The resulting labeled paths, called *label switch paths* (LSPs), forward labeled traffic across an MPLS backbone.

LDP also provides the means for label switching routers (LSRs) to request, distribute, and release label prefix binding information to peer routers in a network. LDP enables LSRs to discover potential peers and establish LDP sessions with those peers to exchange label binding information.

For detailed information about MPLS concepts, configuration tasks, and examples, see *MPLS Configuration Guide for Cisco NCS 6000 Series Routers*.

backoff

To configure the parameters for the Label Distribution Protocol (LDP) backoff mechanism, use the **backoff** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

backoff *initial maximum*

no backoff

Syntax Description

initial	Initial backoff delay, in seconds. Range is 5 to 50331.
maximum	Maximum backoff delay, in seconds. Range is 5 to 50331.

Command Default

initial : 15

maximum : 120

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The LDP backoff mechanism prevents two incompatibly configured label switch routers from engaging in an unthrottled sequence of session setup failures. If a session setup attempt fails (due to incompatibility), each Label Switching Router (LSR) delays the next attempt, increasing the delay exponentially with each successive failure until the maximum backoff delay is reached.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples   The following example shows how to configure the initial backoff delay to 30 seconds and the maximum backoff delay to 240 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls ldp
RP/0/RP0/CPU0:router(config-ldp)# backoff 30 240
```

Related Commands

Command	Description
show mpls ldp backoff, on page 63	Displays information about the configured session setup backoff parameters and LDP peers.
show mpls ldp parameters, on page 95	Displays current LDP parameter settings.

clear mpls ldp msg-counters neighbor

To clear the Label Distribution Protocol (LDP) message counters, use the **clear mpls ldp msg-counters neighbor** command in XR EXEC mode.

clear mpls ldp msg-counters neighbor {*ip-address* | **all**}

Syntax Description	

ip-address	LSR or LDP ID of the neighbor.
all	Clears LDP message counters for all neighbors.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **clear mpls ldp msg-counters neighbor**command to clear the statistics on message counters for a specific neighbor (IP address) or for all neighbors. These message counters count the number of LDP protocol messages sent to and received from LDP neighbors.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples   The following example shows how to clear message counters for neighbor 10.20.20.20:

```
RP/0/RP0/CPU0:router# clear mpls ldp msg-counters neighbor 10.20.20.20
```

Related Commands

Command	Description
show mpls ldp statistics msg-counters, on page 98	Displays statistics about the type and count of the messages sent and received from neighbors.

clear mpls ldp neighbor

To force Label Distribution Protocol (LDP) session restart, use the **clear mpls ldp neighbor** command in XR EXEC mode.

clear mpls ldp neighbor [*ip-address*]

Syntax Description

ip-address	(Optional) Neighbor IP address or LDP ID.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **clear mpls ldp neighbor** command to restart a single LDP session or all LDP sessions (without restarting the LDP process itself).

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples

The following example shows how to force an unconditional LDP session restart:

```
RP/0/RP0/CPU0:router# clear mpls ldp neighbor 10.20.20.20
```

Related Commands

Command	Description
show mpls ldp neighbor, on page 89	Displays information about LDP neighbors.

clear mpls ldp forwarding

To clear (or reset) the MPLS Label Distribution Protocol (LDP) forwarding rewrites, use the **clear mpls ldp forwarding** command in EXEC mode.

clear mpls ldp forwarding [*IP -address*]

Syntax Description

IP-address	(Optional) IPv4 address, specified in four-part, dotted-decimal notation.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 4.0.1	This command was introduced.
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command resets LDP installed forwarding state for all prefixes or a given prefix. It is useful when installed LDP forwarding state needs to be reprogrammed in LSD and MPLS forwarding.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples

This is a sample output from the **clear mpls ldp forwarding** command:

```
RP/0/RP0/CPU0:router# clear mpls ldp forwarding
```

Related Commands

Command	Description
show mpls ldp forwarding	Displays the LDP forwarding state installed in MPLS forwarding.
show mpls forwarding	Displays the contents of the MPLS Label Forwarding Information Base (LFIB).
graceful-restart (MPLS LDP), on page 23	Configures the LDP graceful restart feature.
show mpls ldp bindings, on page 65	Displays the contents of LDP LIB.

default-route

To enable Multiprotocol Label Switching (MPLS) switching for IP default route by allocating and advertising non-null label, use the **default-route** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

default-route

no default-route

Syntax Description   This command has no arguments or keywords.

Command Default   Allocates null (implicit or explicit) local label for IP default route prefix 0.0.0.0/0.

Command Modes   MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When the IP default route 0.0.0.0/0 is configured on an egress router, it is advertised through Interior Gateway Protocol (IGP) to other routers to enable default IP forwarding. When MPLS LDP is configured and establishing label switch paths (LSPs) for other prefixes, you can emulate default forwarding and switching for MPLS in the same way as IP forwarding. To do so, allocate a non-null local label and advertise this label to its peers.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples   The following example shows how to enable default MPLS switching for default prefix:

```
RP/0/RP0/CPU0:router(config-ldp)# default-route
```

Related Commands

Command	Description
show mpls ldp bindings, on page 65	Displays LDP label bindings.
show mpls ldp forwarding, on page 76	Displays LDP installed forwarding state.

discovery hello

To configure the interval between transmission of consecutive Label Distribution Protocol (LDP) discovery hello messages and the holdtime for a discovered LDP neighbor, use the **discovery hello** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

discovery hello {**holdtime** *seconds*| **interval** *seconds*}

no discovery hello {**holdtime | interval**}

Syntax Description

holdtime	Sets the time, in seconds, a discovered LDP neighbor is remembered without receipt of an LDP hello message from the neighbor. Default is 15.
interval	Sets the time, in seconds, between consecutive hello messages. Default is 5.
seconds	Time value, in seconds. Range is 1 to 65535 (65535 means infinite).

Command Default

holdtime: 15

interval: 5

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples

The following example shows how to configure the link hello holdtime to 30 seconds:

```
RP/0/RP0/CPU0:router(config-ldp)# discovery hello holdtime 30
```

The following example shows how to configure the link hello interval to 10 seconds:

```
RP/0/RP0/CPU0:router(config-ldp)# discovery hello interval 10
```

Related Commands

Command	Description
discovery targeted-hello, on page 15	Configures targeted-hello messages.

discovery instance-tlv disable

To disable transmit and receive processing for Type-Length-Value (TLV), use the **discovery instance-tlv disable** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

discovery instance-tlv disable

no discovery instance-tlv disable

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values

Command Modes   MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples   The following example shows how to disable transmit and receive processing for TLV:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls ldp
RP/0/RP0/CPU0:router(config-ldp)# discovery instance-tlv disable
```

Related Commands

Command	Description
discovery targeted-hello, on page 15	Configures targeted-hello messages.

discovery targeted-hello

To configure the interval between transmission of consecutive Label Distribution Protocol (LDP) discovery targeted-hello messages, the hold time for a discovered targeted LDP neighbor, and to accept targeted hello from peers, use the **discovery targeted-hello** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

discovery targeted-hello {**accept**| [**from** *acl*]| **holdtime** *seconds*| **interval** *seconds*}

no discovery targeted-hello {**accept** | **holdtime** | **interval**}

Syntax Description

accept	Accepts targeted hellos from any source.
from *acl*	(Optional) Accepts targeted hellos from LDP peers as permitted by the access-list.
holdtime	Configures the time a discovered LDP neighbor is remembered without receipt of an LDP hello message from a neighbor.
interval	Displays time between consecutive hello messages.
seconds	Time value, in seconds. Range is 1 to 65535.

Command Default

accept : Targeted hello messages are not accepted from any source (neighbor).

holdtime : 90

interval : 10

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

LDP supports IPv4 standard access lists only.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples

The following example shows how to configure the targeted-hello holdtime to 45 seconds:

```
RP/0/RP0/CPU0:router(config-ldp)# discovery targeted-hello holdtime 45
```

The following example shows how to configure the targeted-hello interval to 5 seconds:

```
RP/0/RP0/CPU0:router(config-ldp)# discovery targeted-hello interval 5
```

The following example shows how to configure acceptance of targeted hellos from all peers:

```
RP/0/RP0/CPU0:router(config-ldp)# discovery targeted-hello accept
```

The following example shows how to configure acceptance of targeted hello from peers 10.1.1.1 and 10.2.2.2 only:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list peer_acl_10
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 10.1.1.1
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 10.2.2.2
RP/0/RP0/CPU0:router(config-ldp)# discovery targeted-hello accept from peer_acl_10
```

Related Commands

Command	Description
show mpls ldp discovery, on page 71	Displays LDP discovery information.
show mpls ldp parameters, on page 95	Displays LDP parameters information.

discovery transport-address

To provide an alternative address for a TCP connection, use the **discovery transport-address** command in MPLS LDP interface configuration mode. To return to the default behavior, use the **no** form of this command.

discovery transport-address {*ip-address* | **interface**}

no discovery transport-address {*ip-address* | **interface**}

Syntax Description

ip-address	IP address to be advertised as the transport address in discovery hello messages.
interface	Advertises the IP address of the interface as the transport address in discovery hello messages.

Command Default   LDP advertises its LDP router ID as the transport address in LDP discovery hello messages.

Command Modes   MPLS LDP interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Establishing an LDP session between two routers requires a session TCP connection. To establish the session TCP connection, each router must know the transport address (IP address) of the other router.

The LDP discovery mechanism provides the means for a router to advertise transport addresses. Transport address is implicit or explicit. Implicit addresses do not appear as part of the contents of the discovery hello messages sent to the peer. If explicit, the advertisement appears as part of the contents of discovery hello messages sent to the peer.

The **discovery transport-address** command modifies the default behavior described above. Using the **interface** keyword, LDP advertises the IP address of the interface in LDP discovery hello messages sent from the interface. Using the *ip-address* argument, LDP advertises the IP address in LDP discovery hello messages sent from the interface.

Note   When a router has multiple links connecting it to its peer device, the router must advertise the same transport address in the LDP discovery hello messages it sends on all such interfaces.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples

The following example shows how to specify an exiting address (10.10.3.1) as the transport address on an interface POS 0/1/0/0:

```
RP/0/RP0/CPU0:router(config-ldp)# interface POS 0/1/0/0
RP/0/RP0/CPU0:router(config-ldp-if)# discovery transport-address 10.10.3.1

RP/0/RP0/CPU0:router# show mpls ldp neighbor

  Peer LDP Identifier: 10.44.44.44:0
    TCP connection: 10.44.44.44:65520 - 10.10.3.1:646
    Graceful Restart: Yes (Reconnect Timeout: 15 sec, Recovery: 180 sec)
    State: Oper; Msgs sent/rcvd: 13/9
    Up time: 00:00:11
    LDP Discovery Sources:
        POS 0/1/0/0
    Addresses bound to this peer:
      10.10.3.2        10.44.44.44
```

Related Commands

Command	Description
show mpls ldp discovery, on page 71	Displays the status of the LDP discovery process.
show mpls ldp neighbor, on page 89	Displays information about LDP neighbors.

downstream-on-demand

To configure MPLS Label Distribution Protocol (LDP) downstream-on-demand mode, use the **downstream-on-demand** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

downstream-on-demand with *access-list*

nodownstream-on-demand with *access-list*

Syntax Description

with	Displays access list of LDP peers.
access-list	IP access-list name.

Command Default   No default behavior or values

Command Modes   MPLS LDP configuration

Command History

Release	Modification
Release 4.0.1	This command was introduced.
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
mpls-ldp	read, write

Examples   This is a sample output from the **downstream-on-demand** command:

```
RP/0/RP0/CPU0:router(config-ldp)# downstream-on-demand with access-list
```

Related Commands

Command	Description
graceful-restart (MPLS LDP), on page 23	Configures the LDP graceful restart feature.
show mpls ldp bindings, on page 65	Displays the contents of LDP LIB.

explicit-null

To configure a router to advertise explicit null labels instead of implicit null labels, use the **explicit-null** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

explicit-null [**to** *peer-acl*| **for** *prefix-acl* [**to** *peer-acl*]]

no explicit-null

Syntax Description

to *peer-acl*	(Optional) Specifies LDP peers for which explicit-null is advertised instead of implicit-null. Range is 1 to 99.
for *prefix-acl*	(Optional) Specifies prefixes for which explicit-null is advertised instead of implicit-null. Range is 1 to 99.

Command Default

Implicit null is advertised as default null label for routes, such as directly connected routes.

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Normally, LDP advertises an implicit null label for directly connected routes. The implicit null label causes the previous hop router to perform next to last router hop popping.

The **explicit-null** command advertises the explicit-null labels in place of implicit null labels for directly connected prefixes.

LDP supports IPv4 standard access lists only.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples   The following command shows how to advertise explicit null for all directly connected routes to all LDP peers:

```
RP/0/RP0/CPU0:router(config-ldp)# explicit-null
```

The following command sequence shows how to advertise explicit-null for directly connected route 192.168.0.0 to all LDP peers and implicit-null for all other directly connected routes:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list pfx_acl_192_168
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 192.168.0.0
RP/0/RP0/CPU0:router(config-ldp)# explicit-null for pfx_acl_192_168
```

The following command sequence shows how to send explicit-null for all directly connected routes to peers 10.1.1.1 and 10.2.2.2 and implicit-null to all other peers:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list peer_acl_10
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 10.1.1.1
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 10.2.2.2

RP/0/RP0/CPU0:router(config-ldp)# explicit-null to peer_acl_10
```

The following command shows how to advertise explicit-null for prefix 192.168.0.0 to peers 10.1.1.1 and 10.2.2.2 and advertise implicit-null for all other applicable routes to all other peers:

```
RP/0/RP0/CPU0:router(config-ldp)# explicit-null for pfx_acl_192_168 to peer_acl_10
```

Related Commands

Command	Description
show mpls ldp bindings, on page 65	Displays the contents of LDP LIB.
show mpls ldp forwarding, on page 76	Displays the contents of the LDP forwarding database.
show mpls ldp parameters, on page 95	Displays current LDP parameter settings.

graceful-restart (MPLS LDP)

To configure graceful restart, use the **graceful-restart** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

graceful-restart [**reconnect-timeout** *seconds*| **forwarding-state-holdtime** *seconds*]

no graceful-restart [**reconnect-timeout**| **forwarding-state-holdtime**]

Syntax Description

reconnect-timeout *seconds*	(Optional) Configures the time that the local LDP sends to its graceful restartable peer, indicating how long its neighbor should wait for reconnection in the event of a LDP session failure, in seconds. Range is 60 to 1800.
forwarding-state-holdtime *seconds*	(Optional) Configures the time the local forwarding state is preserved (without being reclaimed) after the local LDP control plane restarts, in seconds. Range is 60 to 1800.

Command Default

By default, graceful restart is disabled.

reconnect-timeout: 120

forwarding-state-holdtime: 180

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 3.9.0	The maximum value for the seconds argument is 1800.
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the LDP graceful restart capability to achieve nonstop forwarding (NSF) during an LDP control plane communication failure or restart. To configure graceful restart between two peers, enable LDP graceful restart on both label switch routers (LSRs).

When an LDP graceful restart session is established and there is control plane failure, the peer LSR starts graceful restart procedures, initially keeps the forwarding state information pertaining to the restarting peer, and marks this state as stale. If the restarting peer does not reconnect within the reconnect timeout, the stale forwarding state is removed. If the restarting peer reconnects within the reconnect time period, it is provided recovery time to resynchronize with its peer. After this time, any unsynchronized state is removed.

The value of the forwarding state hold time keeps the forwarding plane state associated with the LDP control-plane in case of a control-plane restart or failure. If the control plane fails, the forwarding plane retains the LDP forwarding state for twice the forwarding state hold time. The value of the forwarding state hold time is also used to start the local LDP forwarding state hold timer after the LDP control plane restarts. When the LDP graceful restart sessions are renegotiated with its peers, the restarting LSR sends the remaining value of this timer as the recovery time to its peers. Upon local LDP restart with graceful restart enabled, LDP does not replay forwarding updates to MPLS forwarding until the forwarding state hold timer expires.

Note In the presence of a peer relationship, any change to the LDP graceful restart configuration will restart LDP sessions. If LDP configuration changes from nongraceful restart to graceful restart, all the sessions are restarted. Only graceful restart sessions are restarted upon graceful restart to nongraceful restart configuration changes.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples The following example shows how to configure an existing session for graceful restart:

```
RP/0/RP0/CPU0:router(config-ldp)# graceful-restart

RP/0/RP0/CPU0:router:Apr  3 10:56:05.392 : mpls_ldp[336]: %ROUTING-LDP-5-NBR_CHANGE : Nbr
2.2.2.2:0, DOWN
RP/0/RP0/CPU0:router:Apr  3 10:56:05.392 : mpls_ldp[336]: %ROUTING-LDP-5-NBR_CHANGE : Nbr
3.3.3.3:0, DOWN
RP/0/RP0/CPU0:router:Apr  3 10:56:09.525 : mpls_ldp[336]: %ROUTING-LDP-5-NBR_CHANGE : Nbr
3.3.3.3:0, UP
RP/0/RP0/CPU0:router:Apr  3 10:56:11.114 : mpls_ldp[336]: %ROUTING-LDP-5-NBR_CHANGE : Nbr
2.2.2.2:0, UP

RP/0/RP0/CPU0:router# show mpls ldp neighbor brief

  Peer              GR Up Time         Discovery Address
  ----------------- -- --------------- --------- -------
  3.3.3.3:0         Y  00:01:04               3       8
  2.2.2.2:0         N  00:01:02               2       5

RP/0/RP0/CPU0:router# show mpls ldp graceful-restart

   Forwarding State Hold timer : Not Running
   GR Neighbors               : 1

   Neighbor ID     Up  Connect Count  Liveness Timer     Recovery Timer
   --------------- --  -------------  ------------------ ------------------
   3.3.3.3         Y        1               -                  -
```

Related Commands

Command	Description
show mpls ldp forwarding, on page 76	Displays the contents of the LDP forwarding database.
show mpls ldp graceful-restart, on page 81	Displays information related to graceful restart.
show mpls ldp neighbor, on page 89	Displays information about LDP neighbors.
show mpls ldp parameters, on page 95	Displays current LDP parameter settings.
show mpls ldp summary, on page 100	Displays summarized information regarding the LDP process.

holdtime (MPLS LDP)

To change the time for which an Label Distribution Protocol (LDP) session is maintained in the absence of LDP messages from the session peer, use the **holdtime** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

holdtime *seconds*

no holdtime

Syntax Description

seconds	Time, in seconds, that an LDP session is maintained in the absence of LDP messages from the session peer. Range is 15 to 65535.

Command Default

seconds: 180

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples

The following example shows how to change the hold time of LDP sessions to 30 seconds:

```
RP/0/RP0/CPU0:router(config-ldp)# holdtime 30
```

Related Commands

Command	Description
show mpls ldp parameters, on page 95	Displays current LDP parameter settings.

igp auto-config disable

To disable Label Distribution Protocol (LDP) auto-configuration, use the **igp auto-config disable** command in MPLS LDP interface configuration mode. To return to the default behavior, use the **no** form of this command.

igp auto-config disable

no igp auto-config disable

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values

Command Modes   MPLS LDP interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

IGP auto-configuration can be enabled on ISIS and OSPF. Configuration details are described in .

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples   The following example shows how to disable LDP auto-configuration on POS 0/1/0/3:

```
RP/0/RP0/CPU0:router(config)# mpls ldp
RP/0/RP0/CPU0:router(config-ldp)# interface pos 0/1/0/3
RP/0/RP0/CPU0:router(config-ldp-if)# igp auto-config disable
```

Related Commands

Command	Description
show mpls ldp interface, on page 86	Displays information about LDP-enabled interfaces.

igp sync delay

To enable Label Distribution Protocol (LDP) Interior Gateway Protocol (IGP) sync delay timer feature, use the **igp sync delay** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

igp sync delay *seconds*

no igp sync delay

Syntax Description

seconds	Time, in seconds, that declaration of LDP sync state being up is delayed after session establishment upon link coming up. Range is 5 to 300.

Command Default LDP does not delay declaration of sync up and notifies IGP as soon as sync up conditions are met for a link.

Command Modes MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

- By default, LDP declares LDP sync up as soon as all the requisite conditions are met, namely:

  ◦ LDP session is up.

  ◦ LDP has sent all its label bindings to at least one peer.

  ◦ LDP has received at least one label binding from a peer.

  This minimizes traffic loss on link up but can still lead to substantial traffic loss under certain circumstances (for example, when interoperating with an LSR with ordered mode operation). It may be necessary to delay declaration of sync up after the session comes up by configuring a timeout period.

- When the graceful-restart event is configured, the IGP sync delay timer does not take effect.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples   The following example shows how to configure LDP to delay declaration of sync-up to 30 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls ldp
RP/0/RP0/CPU0:router(config-ldp)# igp sync delay 30
```

Related Commands

Command	Description
show mpls ldp igp sync, on page 83	Displays LDP IGP sync information for link(s).

igp sync delay on-proc-restart

To delay the declaration of synchronization events to the Interior Gateway Protocol (IGP) when the label distribution protocol (LDP) fails or restarts, use the **igp sync delay on-proc restart** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

igp sync delay on-proc restart *seconds*

no igp sync delay on-proc restart *seconds*

Syntax Description

seconds	Time, in seconds, duration of process-level delay for synchronization events when the LDP fails or restarts. Range is from 60 to 600.

Command Default

This command is disabled by default.

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **igp sync delay on-proc restart** command enables a process-level delay for synchronization events when the LDP fails or restarts. This delay defers the sending of sync-up events to the IGP until most or all the LDP sessions converge and also allows the LDP to stabilize. This allows the LDP process failure to be less stressful because IGPs receive all the sync-up events in bulk. This means that the IGP is required to run the shortest path first (SPF) and link-state advertisements (LSAs) only one time with an overall view of the sync-up events.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples

The following example shows how to configure LDP to delay the declaration of synchronization events to IGP by 60 seconds:

```
RP/0/RP0/CPU0:router# configure
```

```
RP/0/RP0/CPU0:router(config)# mpls ldp
RP/0/RP0/CPU0:router(config-ldp)# igp sync delay on-proc restart 60
```

The following example shows the status following execution of the command:

```
RP/0/RP0/CPU0:router# show mpls ldp igp sync

  Process Restart Sync Delay: 60 sec, Gloal timer running (15 sec remaining)
  GigabitEthernet0/3/0/2:
  Sync status: Deferred
  ....
```

When the timer is not running, the output displays the following:

```
Process Restart Sync Delay: 60 sec, Global timer not running
```

Related Commands

Command	Description
show mpls ldp igp sync, on page 83	Displays LDP IGP sync information for link(s).

interface (MPLS LDP)

To configure or enable Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) on an interface, use the **interface** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

interface *type interface-path-id*

no interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default   No default behavior or values

Command Modes   MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When you configure LDP on an interface, the LDP process begins neighbor discovery, sending link hello messages on the interface. This can result in a session setup with discovered neighbors. When LDP is enabled on tunnel-te interfaces, targeted discovery procedures apply.

LDP interface configuration supports forward reference; accordingly, it is possible to configure a nonexisting interface under LDP.

Note   You cannot enable LDP on loopback interfaces.

MPLS LDP is supported over Generic Route Encapsulation (GRE) tunnels by configuring the tunnel-ip interface. LDP establishes a link session (as opposed to a targeted LDP session) over the GRE tunnel.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples

The following example shows how to configure LDP on POS interface 0/1/0/0:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls ldp
RP/0/RP0/CPU0:router(config-ldp)# interface POS 0/1/0/0
RP/0/RP0/CPU0:router(config-ldp-if)#
```

The following example shows how to configure LDP on an MPLS TE tunnel:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls ldp
RP/0/RP0/CPU0:router(config-ldp)# interface tunnel-te 123
RP/0/RP0/CPU0:router(config-ldp-if)#
```

Related Commands

Command	Description
show mpls ldp parameters, on page 95	Displays current LDP parameter settings.
show mpls ldp neighbor, on page 89	Displays LDP neighbor session parameters.

label accept

To control the receipt of labels (remote bindings) for a set of prefixes from a peer, use the **label accept** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

label accept for *prefix-acl* **from** *ip-address*

no label accept for *prefix-acl* **from** *ip-address*

Syntax Description		
for *prefix-acl*		Accepts and retains remote bindings for prefixes that are permitted by the prefix access list *prefix-acl* argument.
from *ip-address*		Displays the peer IP address.

Command Default   LDP accepts and retains label bindings for all prefixes from all peers.

Command Modes   MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

By default, LDP accepts labels (as remote bindings) for all prefixes from all its peers. To save resources (such as memory) configure the access list to specify label and binding acceptance for a set of prefixes from a peer.

If the inbound label filtering policy changes such that it now allows previously denied prefixes from a peer, you must reset the LDP session with the peer using the **clear mpls ldp neighbor** command.

LDP supports IPv4 standard access lists only.

Note   Label acceptance control is also referred to as LDP inbound label filtering.

Task ID

Task ID	Operations
mpls-ldp	read, write

label accept

Examples   The following example shows how to configure inbound label filtering policy. In this example, an LSR is configured to accept and retain label bindings for prefixes 192.168.1.1 (pfx_acl_1) from peer 1.1.1.1, prefix 192.168.2.2 (pfx_acl_2) from peer 2.2.2.2, and prefixes 192.168.1.1, 192.168.2.2, 192.168.3.3 (pfx_acl_3) from peer 3.3.3.3:

```
RP/0/RP0/CPU0:router(config-ldp)# label accept
RP/0/RP0/CPU0:router(config-ldp-lbl-acpt)# for pfx_acl_1 from 1.1.1.1
RP/0/RP0/CPU0:router(config-ldp-lbl-acpt)# for pfx_acl_2 from 2.2.2.2
RP/0/RP0/CPU0:router(config-ldp-lbl-acpt)# for pfx_acl_3 from 3.3.3.3
```

Related Commands

Command	Description
label advertise, on page 37	Controls advertisement of LDP local label bindings (outbound label filtering).
clear mpls ldp neighbor, on page 7	Resets LDP neighbor sessions.
show mpls ldp bindings, on page 65	Displays LDP binding information.

label advertise

To control the advertisement of local labels, use the **label advertise** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

label advertise [**disable**| **for** *prefix-acl* [**to** *peer-acl*]| **interface** *type interface-path-id*]

no label advertise [**disable**| **for** *prefix-acl* [**to** *peer-acl*]| **interface** *type interface-path-id*]

Syntax Description

disable	(Optional) Disables label advertisement to all peers for all prefixes.
for *prefix-acl*	(Optional) Specifies prefix destinations for which labels will be advertised.
to *peer-acl*	(Optional) Specifies which LDP neighbors will receive label advertisements.
interface	(Optional) Specifies an interface for label allocation and advertisement of its interface IP address.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default   LDP advertises labels for all known prefixes to all peers. LDP does not advertise labels for local interfaces addresses other than Loopback interfaces.

Command Modes   MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **label advertise** command determines how the label switch router (LSR) advertises local labels. The following rules describe the effects of running multiple commands:

- Every command has a prefix-acl or peer-acl pair associated with it, as follows:

  ◦ In the absence of the **for** or **to** keywords, the access list pair is (none, none).

  ◦ When using the **for** keyword without the **to** keyword, the access list is (prefix-acl, none).

- A prefix can have a maximum of one (prefix-acl, peer-acl) pair, as follows:

  ◦ A (prefix-acl, peer-acl) pair applies to a prefix only if the prefix-acl matches the prefix. A match occurs if the prefix-acl permits the prefix.

  ◦ If more than one (prefix-acl, peer-acl) pair from multiple **label advertise** commands matches a prefix, the (prefix-acl, peer-acl) pair in the first command applies to the prefix.

- When an LSR is ready to advertise a label for a prefix, the LSR determines whether a (prefix-acl, peer-acl) pair applies to the prefix.

  ◦ If none applies, and if the **disable** keyword has been configured for the command, the label for the prefix is not advertised to any peer; otherwise, the label is advertised to all peers.

  ◦ If a (prefix-acl, peer-acl) pair applies to the prefix, and if the prefix-acl denies the prefix, the label is not advertised to any peer.

  ◦ If the prefix-acl permits the prefix and the peer-acl is none (that is, the command that applies to the prefix is an **label advertise for** *prefix-acl* command without the **to** keyword), the label is advertised to all peers.

  ◦ If the prefix-acl permits the prefix and there is a peer-acl, the label is advertised to all peers permitted by the peer-acl.

Normally, LDP advertises labels for non-BGP routes present in the routing table. Additionally, LDP advertises labels from /32 IP addresses on Loopback interfaces and does not advertise /32 addresses for other non-Loopback interfaces. To control advertisement of labels for /32 IP addresses on these interfaces, use the **label advertise interface** command.

LDP supports IPv4 standard access lists only.

Note   Label advertisement control is also referred to as LDP outbound label filtering.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples   The following example shows how to disable advertisement of all locally assigned labels to all peers:

```
RP/0/RP0/CPU0:router(config-ldp)# label advertise
RP/0/RP0/CPU0:router(config-ldp-lbl-advt)# disable
```

The following example shows how to send labels only for prefixes 10.1.1.0 and 20.1.1.0 to all peers:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list pfx_acl_1
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 10.1.1.0
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 20.1.1.0

RP/0/RP0/CPU0:router(config-ldp)# label advertise
RP/0/RP0/CPU0:router(config-ldp-lbl-advt)# disable
RP/0/RP0/CPU0:router(config-ldp-lbl-advt)# for pfx_acl_1
```

The following example shows how to send labels for prefix 10.0.0.0 to peers 10.1.1.1 and 10.2.2.2, labels for prefix 20.0.0.0 to peer 20.1.1.1, and labels for all other prefixes to all other peers:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list pfx_acl_10
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 10.0.0.0

RP/0/RP0/CPU0:router(config)# ipv4 access-list pfx_acl_20
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 20.0.0.0

RP/0/RP0/CPU0:router(config)# ipv4 access-list peer_acl_10
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 10.1.1.1
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 10.2.2.2

RP/0/RP0/CPU0:router(config)# ipv4 access-list peer_acl_20
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 20.1.1.1

RP/0/RP0/CPU0:router(config-ldp)# label advertise
RP/0/RP0/CPU0:router(config-ldp-lbl-advt)# for pfx_acl_10 to peer_acl_10
RP/0/RP0/CPU0:router(config-ldp-lbl-advt)# for pfx_acl_20 to peer_acl_20
```

Note   To advertise pfx_acl_10 to peer_acl_10 and pfx_acl_20 to peer_acl_20 and disable all other advertisements to all other peers, include the **disable** keyword with the **label advertise** command.

The following example shows how to use the **interface** keyword to advertise /32 IP address for POS 0/1/0/0:

```
RP/0/RP0/CPU0:router(config-ldp)# label advertise
RP/0/RP0/CPU0:router(config-ldp-lbl-advt)# interface POS 0/1/0/0
```

Related Commands

Command	Description
show mpls ldp neighbor, on page 89	Displays information about LDP neighbors.
show mpls ldp bindings, on page 65	Displays information about LDP label bindings.

label allocate

To control allocation of local label only for a set of prefixes, use the **label allocate** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

label allocate for {*prefix-acl* | **host-routes**}

no label allocate

Syntax Description

for	Specifies set of prefixes for which local label needs to be allocated.
prefix-acl	IP access-list name or number. Range is from 1 to 99.
host-routes	Allocates the label for host routes only.

Command Default   LDP allocates local label for all learned routes (prefixes).

Command Modes   MPLS LDP configuration

Command History

Release	Modification
Release 3.9.0	The **host-routes** keyword was added.
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Local label allocation control lets you override the default label allocation policy and provides many benefits, including reduced memory usage and fewer forwarding and network updates.

By default, LDP allocates local labels for all learned routes. There are times when you may want to limit label allocation for a given set of prefixes; for example, when using LDP in the core network to provide MPLS transport from one edge to another edge. In such cases, it is necessary to set up label switch packets (LSPs) for Loopback /32 addresses for provider edge (PE) routers (rendering it unnecessary to allocate and advertise local labels for other Interior Gateway Protocol (IGP) prefixes).

LDP supports IPv4 standard access lists only.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples   The following example shows how to configure LDP to limit allocation of local labels to prefixes 192.168.1.1, 192.168.2.2, and 192.168.3.3 only:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list pfx_acl_1
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 192.168.1.1
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 192.168.2.2
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 192.168.3.3

RP/0/RP0/CPU0:router(config-ldp)# label allocate for pfx_acl_1
```

Related Commands

Command	Description
show mpls ldp bindings, on page 65	Displays information about LDP label bindings.
show mpls ldp forwarding, on page 76	Displays the contents of the LDP forwarding database.

log graceful-restart

To set up notification describing graceful-restart (GR) session events, use the **log graceful-restart** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

log graceful-restart

no log graceful-restart

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values

Command Modes   MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **log graceful-restart** command to receive a syslog/console message when a graceful restart-related session event occurs, including LDP graceful restart session disconnection, reconnection, and timeout.

Note   A logging message is issued upon graceful restart session events.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples   The following example shows how to enable logging messages for graceful restart session events:

```
RP/0/RP0/CPU0:router(config-ldp)# log graceful-restart
```

The following sample output shows the logging events that can be displayed on the console:

```
RP/0/RP0/CPU0:router: mpls_ldp[340]: %ROUTING-LDP-5-GR : GR session 4.4.4.4:0 (instance 1)
```

```
 disconnected

RP/0/RP0/CPU0:router: mpls_ldp[340]: %ROUTING-LDP-5-GR : GR session 4.4.4.4:0 (instance 2)
 reconnected

RP/0/RP0/CPU0:router: mpls_ldp[340]: %ROUTING-LDP-5-GR : GR session 5.5.5.5:0 (instance 3)
 timed out

RP/0/RP0/CPU0:router: mpls_ldp[336]: %ROUTING-LDP-5-GR_RESTART_COMPLETE : GR forwarding
state hold timer has expired
```

Related Commands

Command	Description
show mpls ldp neighbor, on page 89	Displays information about LDP neighbors.
show mpls ldp graceful-restart, on page 81	Displays information about LDP GR sessions.

log neighbor

To enable logging of notices describing session changes, use the **log neighbor** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

log neighbor

no log neighbor

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values

Command Modes   MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **log neighbor** command to receive a syslog or console message when a neighbor goes up or down.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples   The following example shows how to enable logging messages for neighbor session up and down events:

```
RP/0/RP0/CPU0:router(config-ldp)# log neighbor
```

Note   A logging message is issued when an LDP session state changes from up to down (and down to up).

The following shows sample output of logging events that can be displayed on the console:

```
RP/0/RP0/CPU0:router:10 21:11:32.111:mpls_ldp[113]:%LDP-5-NBR_CHANGE: Nbr 10.44.44.44:0,
DOWN
```

Related Commands

Command	Description
show mpls ldp neighbor, on page 89	Displays information about LDP neighbors.

log nsr

To enable logging of nonstop routing (NSR) synchronization events, use the **log nsr** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

log nsr

no log nsr

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values

Command Modes   MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples   The following example shows how to enable logging of NSR synchronization events:

```
RP/0/RP0/CPU0:router(config-ldp)# log nsr
```

log session-protection

To enable logging of notices describing LDP session protection events, use the **log session-protection** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

log session-protection

no log session-protection

| **Syntax Description** | This command has no arguments or keywords. |

Command Default   No default behavior or values

Command Modes   MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **log session-protection** command to receive a syslog or console message when LDP session protection event occurs. These events include LDP session protection initiation, recovery, and timeout.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples   The following example shows how to enable logging messages for session protection events:

```
RP/0/RP0/CPU0:router(config-ldp)# log session-protection
```

Note   Logging messages are issued when session protection events occur.

The following sample output shows the logging events that are displayed on the console:

```
RP/0/RP0/CPU0:router:Apr 21 12:15:01.742: mpls_ldp[315]:%ROUTING-LDP-5-SESSION_PROTECTION:
 Session hold up initiated for peer 4.4.4.4:0
```

```
RP/0/RP0/CPU0:router:Apr 21 12:18:04.987: mpls_ldp[315]:%ROUTING-LDP-5-SESSION_PROTECTION:
 Session recovery succeeded for peer 4.4.4.4:0
```

Related Commands

Command	Description
show mpls ldp neighbor, on page 89	Displays information about LDP neighbors.

mpls ldp

To enter MPLS Label Distribution Protocol (LDP) configuration mode, use the **mpls ldp** command in global configuration mode.

mpls ldp

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values

Command Modes   Global configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples   The following example shows how to MPLS LDP configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls ldp
RP/0/RP0/CPU0:router(config-ldp)
```

neighbor password

To configure password authentication using the TCP Message Digest 5 (MD5) option for a neighbor, use the **neighbor password** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

neighbor *IP-address* **password** {**clear | encrypted**} *password*

no neighbor *IP-address* **password**

Syntax Description

IP-address	Neighbor IP address.
clear	Clears the password for the encyrption parameter to specify that an unencrypted password will follow.
encrypted	Specifies that an encrypted password will follow.
password	Clear text or encrypted password string.

Command Default   LDP sessions are negotiated without any password (and MD5).

Command Modes   MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This security feature is enabled per neighbor, so that a session establishment attempt is allowed only when a password match has been configured. This option must be configured so that both peer passwords match.

To override the default password for a specific neighbor, use the **neighbor** *IP-address* **password** command, where the *IP-address* argument is the IP address of the neighbor.

> **Note**   The global default password must be configured before being able to override the default password for a specific neighbor.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples

The following example shows how to configure the password *abc* for neighbor 10.20.20.20:

```
RP/0/RP0/CPU0:router(config-ldp)# neighbor 10.20.20.20 password clear abc
```

Related Commands

Command	Description
neighbor targeted, on page 53	Configures transmission of targeted hellos towards a neighbor.

neighbor password disable

To override an individual neighbor which requires no password, use the **neighbor password disable** command in MPLS LDP configuration mode.

neighbor *IP-address* **password disable**

Syntax Description

IP-address	Neighbor IP address.

Command Default

LDP sessions are negotiated without any password (and MD5).

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The system uses the global password to compute each neighbor's effective password and overrides the global password with the individual neighbor password, if configured. The session remains stable if you shift from an individual neighbor password to an equal global password. However, if the effective password changes during configuration, the session might be rendered unstable.

Note   You must configure the password for an individual neighbor using the neighbor's LSR ID.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples

The following example shows how to override the individual password *abc*, for the neighbor:

```
RP/0/RP0/CPU0:router(config-ldp)# neighbor 10.20.20.20 password disable abc
RP/0/RP0/CPU0:router(config-ldp)#
```

neighbor targeted

To configure transmission of targeted hellos toward a neighbor for setting up an LDP session, use the **neighbor targeted** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

neighbor *IP address* **targeted**

no neighbor *IP address* **targeted**

Syntax Description

IP address	Neighbor IP address.

Command Default   No default behavior or values

Command Modes   MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples   The following example shows how to set up a targeted discovery session for neighbor 200.1.1.1:

```
RP/0//CPU0:router(config-ldp)# neighbor 200.1.1.1 targeted
```

Related Commands

Command	Description
neighbor password, on page 50	Configures password authentication using MD5.
show mpls ldp neighbor, on page 89	Displays information about LDP neighbors.

Command	Description
show mpls ldp discovery, on page 71	Displays information about LDP discovery sources.

nsr (MPLS-LDP)

To configure nonstop routing for LDP protocols in the event of a disruption in service, use the **nsr** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

nsr

no nsr

Syntax Description   This command has no arguments or keywords.

Command Default   By default, MPLS LDP NSR is disabled.

Command Modes   MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

A disruption in service may include any of the following events:

- LDP process restart

- In-service system upgrade (ISSU)

- Minimum disruption restart (MDR)

Enabling NSR causes events such as these to be invisible to the routing peers and provide minimal service disruption.

Note   The LDP Process restart is supported by NSR only if the NSR process-failures switchover is configured, else the process restart causes the session to be unstable.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples   The following example shows how to enable MPLS LDP NSR:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls ldp
RP/0/RP0/CPU0:router(config-ldp)# nsr
```

Related Commands

Command	Description
nsr process-failures switchover	Configures switchover as a recovery action for active instances to switch over to a standby RP or a DRP, to maintain NSR. For more information, see *IP Addresses and Services Command Reference* .
show mpls ldp neighbor, on page 89	Displays standby node specific information.

redistribute (MPLS LDP)

To redistribute routes from a Border Gateway Protocol (BGP) autonomous system into an MPLS LDP, use the **redistribute** command in MPLS LDP configuration mode. To disable route redistribution, use the **no** form of this command.

redistribute bgp {**as** *as-number*| **advertise-to** *access-list-name*}

no redistribute bgp {**as** *as-number*| **advertise-to** *access-list-name*}

Syntax Description

bgp	Redistributes information from BGP protocols.
as *as-number*	Specifies the BGP autonomous system number.
advertise-to *access-list*	Advertise the redistributed route information.

Command Default   No default behavior or values

Command Modes   MPLS LDP configuration

Command History

Release	Modification
Release 4.1.0	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
MPLS LDP	read, write

Examples   The following example shows how to redistribute BGP information to MPLS LDP peers:

```
RP/0/RP0/CPU0:router(config)# mpls ldp
RP/0/RP0/CPU0:router(config-ldp)# redistribute bgp ?
  advertise-to  IP access list specifying LDP peers to advertise
  as            BGP AS-number
  <cr>
RP/0/RP0/CPU0:router(config-ldp)# redistribute bgp as 10000
RP/0/RP0/CPU0:router(config-ldp)# commit

RP/0/RP0/CPU0:router# show run mpls ldp | b bgp
 bgp
```

```
 as 10000
!
```

router-id (MPLS LDP)

To specify the IP address of a preferred interface or a specific IP address as the LDP router ID, use the **router-id** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

router-id *IP-address*

no router-id

Syntax Description

IP-address	32-bit router ID value specified in four-part, dotted-decimal notation.

Command Default

LDP uses router ID as determined by global router ID agent, IP Address Repository Manager (IP ARM).

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **router-id** command lets you specify an interface with an IP address to be used as the LDP router ID (which is necessary when an IP address selected as the LDP router ID might not be advertisable by the routing protocol to a neighboring router). In such cases, use the **router-id** command to select the IP address of the specified loopback interface (if the interface is operational) or a specific IP address.

LDP uses the router ID from different sources in the following order:

1 Configured LDP router ID.
2 Global router ID (if configured).
3 Calculated (computed) using the primary IPv4 address of the highest numbered configured loopback address. We recommend configuring at least one loopback address.

Note   We recommend that you configure an IP address for the LDP router-id to avoid unnecessary session flaps.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples

The following example shows how to specify an IP address as the LDP router ID:

```
RP/0/RP0/CPU0:router(config-ldp)#router-id 10.0.0.1
```

Related Commands

Command	Description
show mpls ldp discovery, on page 71	Displays the status of the LDP discovery process.
show mpls ldp neighbor, on page 89	Displays information about LDP neighbors.
show mpls ldp parameters, on page 95	Displays current LDP parameter settings.

session protection

To enable the LDP session protection feature for keeping LDP peer session up by means of targeted discovery following the loss of link discovery with a peer, use the **session protection** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

session protection [**duration** *seconds*| **infinite**] [**for** *peer-acl*]

no session protection

Syntax Description		
duration *seconds*	(Optional) Specifies the protection duration, that is, the number of seconds that targeted discovery should continue following the loss of link discovery to a neighbor. Range is 30 to 2147483.	
infinite	(Optional) Specifies session protection to last forever after loss of link discovery.	
for *peer-acl*	(Optional) Specifies set of LDP peers for which session protection is to be enabled.	

Command Default

By default, session protection is disabled. When enabled without peer-acl and duration, session protection is provided for all LDP peers and continues for 24 hours after a link discovery loss.

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

LDP session protection feature allows you to enable the automatic setup of targeted hello adjacencies with all or a set of peers and specify the duration for which session needs to be maintained using targeted hellos after loss of link discovery.

LDP supports only IPv4 standard access lists.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples   The following example shows how to enable session protection for all discovered peers with unlimited duration to maintain the session after link discovery loss:

```
RP/0/RP0/CPU0:router(config-ldp)# session protection
```

The following example shows how to enable session protection for a set of peers (as permitted by a peer ACL) with duration of 30 seconds to maintain the session after link discovery loss:

```
RP/0/RP0/CPU0:router(config-ldp)# session protection for peer_acl duration 30
```

Related Commands

Command	Description
show mpls ldp neighbor, on page 89	Displays information about LDP neighbors.

show mpls ldp backoff

To display information about the configured session setup backoff parameters and any potential LDP peers with which session setup attempts are being throttled, use the **show mpls ldp backoff** command in EXEC mode.

show mpls ldp backoff [**location** *node-id* | **standby**]

Syntax Description

location *node-id*	(Optional) Displays location information for the specified node ID.
standby	(Optional) Displays standby-node-specific information.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You must enable the MPLS LDP application to use the **show mpls ldp backoff** command.

Task ID

Task ID	Operations
mpls-ldp	read

Examples

The following shows a sample output from the **show mpls ldp backoff** command:

```
RP/0/RP0/CPU0:router# show mpls ldp backoff

Backoff Time:
  Initial:15 sec, Maximum:120 sec

Backoff Table: (2 entries)

  LDP Id              Backoff (sec)  Waiting (sec)
  -------------------- -------------- ----------------
```

```
33.33.33.33:0              15                  15
11.11.11.11:0              30                  30
```

This table describes the significant fields shown in the display.

Table 2: show mpls ldp backoff Command Field Descriptions

Field	Description
Backoff Time	Initial and maximum backoff time parameters, in seconds.
Backoff Table	List of discovered LDP neighbors for which session setup is being delayed because of previous failures to establish a session due to incompatible configuration. The backoff table incorporates the following information: **LDP Id** Identifies the LDP neighbors. **Backoff (sec)** Specifies the time that the session setup is delayed. **Waiting (sec)** Specifies an approximate time the session setup has been delayed.

Related Commands

Command	Description
backoff, on page 3	Configures LDP backoff parameters.
show mpls ldp forwarding, on page 76	Displays the contents of MPLS forwarding table.
show mpls ldp bindings, on page 65	Displays the contents of LDP LIB.

show mpls ldp bindings

To display the contents of the Label Information Base (LIB), use the **show mpls ldp bindings** command in EXEC command.

show mpls ldp bindings [*IP-address* /*prefix* {*mask*| *length*}] **[advertisement-acls] [brief] [detail] [local]** [**local-label** *label* [**to** *label*]] **[local-only]** [**neighbor** *address*] **[remote-only]**[**remote-label** *label* [**to** *label*]] **[summary]** [**location** *node-id*| **standby**]

Syntax Description

IP-address /*prefix*	(Optional) Destination prefix/mask length, written in A.B.C.D format.
mask	Network mask, written in A.B.C.D format.
length	Mask length, in bits. Range is 0 to 32.
advertisement-acls	(Optional) Displays the label bindings as applied for (advertisement) outbound label filtering ACLs.
brief	(Optional) Displays all the prefixes in the LDP database.
detail	(Optional) Displays the total counts of advertised-to and remote-binding peers in IP address sort order, with remote bindings in tabular format.
local	(Optional) Displays the local label bindings.
local-label *label* [**to** *label*]	(Optional) Displays entries matching local label values. Add the *label* **to** *label* argument to indicate the label range.
local-only	(Optional) Displays binding matches with a local label only.
neighbor *address*	(Optional) Displays the label bindings assigned by the selected neighbor.
remote-only	(Optional) Displays bindings matches with a remote label only.
remote-label *label* [**to** *label*]	(Optional) Displays entries matching the label values assigned by a neighbor router. Add the *label* **to***label* argument to indicate the label range. Range is from 0 to 2147483647.
summary	(Optional) Displays a summary of the contents of the Label Information Base (LIB).
location *node-id*	(Optional) Displays location information for the specified node ID.
standby	(Optional) Displays standby-node-specific information.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show mpls ldp bindings** command displays local and remote label bindings learned from neighbors for non-BGP routes (such as IGP prefixes and static routes).

You can choose to view the entire database or a subset of entries according to the following criteria:

- Prefix
- Input or output label values or ranges
- Neighbor advertising the label

Note   The **show mpls ldp bindings summary** command displays summarized information from the LIB and is used when testing scalability or when deployed in a large scale network.

Task ID

Task ID	Operations
mpls-ldp	read

Examples   The following sample output displays the contents of the LIB for the default routing domain:

```
RP/0/RP0/CPU0:router# show mpls ldp bindings

    5.41.0.0/16 , rev 4
        local binding: label:IMP-NULL
        No remote bindings
  5.43.9.98/32 , rev 6
        local binding: label:IMP-NULL
        No remote bindings
  10.10.2.0/24 , rev 12
        local binding: label:IMP-NULL
        remote bindings :
            lsr:10.255.255.255:0, label:16
            lsr:10.256.256.256:0, label:IMP-NULL
  10.10.3.0/24 , rev 10
        local binding: label:IMP-NULL
        remote bindings :
            lsr:10.255.255.255:0, label:IMP-NULL
```

```
            lsr:10.256.256.256:0, label:22
 22.22.22.22/32 , rev 14
        local binding: label:16
        remote bindings :
            lsr:10.255.255.255:0, label:17
            lsr:10.256.256.256:0, label:IMP-NULL
 33.33.33.33/32 , rev 2
        local binding: label:IMP-NULL
        remote bindings :
            lsr:10.255.255.255:0, label:18
            lsr:10.256.256.256:0, label:23
```

The following sample output shows detailed information for the total counts of advertised-to and remote-binding peers in IP address sort order, with remote bindings for 150.150.150.150/32:

```
RP/0/RP0/CPU0:router# show mpls ldp bindings 150.150.150.150/32 detail

  150.150.150.150/32, rev 2
      Local binding: label: IMP-NULL
        Advertised to: (6 peers)
          120.120.120.120:0  130.130.130.130:0  150.150.150.1:0  150.150.150.2:0
          150.150.150.3:0    150.150.150.4:0
      Remote bindings:    (3 peers)
        Peer              Label
      -----------------  --------
          120.120.120.120:0    27018
          130.130.130.130:0    26017
          160.160.160.160:0    27274
```

The following sample output specifies a network number and displays labels learned from label switched router (LSR) 10.255.255.255 for all networks. The **neighbor** keyword is used to suppress the output of remote labels learned from other neighbors:

```
RP/0/RP0/CPU0:router# show mpls ldp bindings neighbor 10.255.255.255

 10.10.2.0/24 , rev 12
        local binding: label:IMP-NULL
        remote bindings :
            lsr:10.255.255.255, label:16
 10.10.3.0/24 , rev 10
        local binding: label:IMP-NULL
        remote bindings :
            lsr:10.255.255.255:0, label:IMP-NULL
 22.22.22.22/32 , rev 14
        local binding: label:16
        remote bindings :
            lsr:10.255.255.255:0, label:17
 33.33.33.33/32 , rev 2
        local binding: label:IMP-NULL
        remote bindings :
            lsr:10.255.255.255:0, label:18
 44.44.44.44/32 , rev 16
        local binding: label:17
        remote bindings :
            lsr:10.255.255.255:0, label:IMP-NULL
```

This table describes the significant fields shown in the display.

Table 3: show mpls ldp bindings and show mpls ldp bindings neighbor Command Field Descriptions

Field	Description
a.b.c.d/n	IP prefix and mask for a particular destination (network/mask).

Field	Description
rev	Revision number (rev) that is used internally to manage label distribution for this destination.
local binding	Locally assigned label for a prefix.
remote bindings	Outgoing labels for this destination learned from other LSRs.[1] Each item in this list identifies the LSR from which the outgoing label was learned and reflects the label associated with that LSR. Each LSR in the transmission path is identified by its LDP identifier.

[1] Label switched routers.

The following sample output summarizes the content by using the **summary** keyword:

```
RP/0/RP0/CPU0:router# show mpls ldp bindings summary

  LIB Summary:
    Total Prefix   : 20
    Revision No    : Current:34, Advertised:34
    Local Bindings : 14
        NULL    : 10 (implicit:10, explicit:0)
        Non-NULL: 4 (lowest:48, highest:51)
    Remote Bindings: 24
```

This table describes the significant fields shown in the display.

Table 4: show mpls ldp bindings summary Command Field Descriptions

Field	Description
Total Prefix	Number of prefixes (routes) known to LDP LIB. All invalid and timed-out routes display as no-routes.
Revision No	Current revision number of LIB entries as well as the minimum revision number that has been advertised to all peers.
Local Bindings	Total number of local bindings, with information on how many of them are Null, non-null, and lowest/highest label assigned or allocated by LDP.
Remote Bindings	Number of remote bindings.

The following sample output shows the access-list advertisement:

```
RP/0/RP0/CPU0:router# show mpls ldp bindings advertisement-acls

  Advertisement Spec:
        Prefix ACL = 'pfx_11'
        Prefix ACL = 'pfx_22'
        Prefix ACL = 'pfx_40_1'; Peer ACL = 'peer_11'

  5.41.0.0/16 , rev 82
  11.11.11.11/32 , rev 69
        Advert ACL(s): Prefix ACL 'pfx_11'
  20.20.20.20/32 , rev 83
  22.22.22.22/32 , rev 78
        Advert ACL(s): Prefix ACL 'pfx_22'
  40.1.1.0/24 , rev 79
        Advert ACL(s): Prefix ACL 'pfx_40_1'; Peer ACL 'peer_11'
```

This table describes the significant fields shown in the display.

Table 5: show mpls ldp bindings advertisement-acls Command Field Descriptions

Field	Description
Advertisement Spec	Lists all prefix and peer access-lists used as outbound label advertisement control.
Advert ACL(s)	Lists the first matching rule (if any) for the prefix entry for outbound label advertisement control (for prefix-acl).

The following sample output shows all the prefixes in the LDP database using the **brief** keyword:

```
RP/0/RP0/CPU0:router# show mpls ldp bindings brief

  Prefix            Local Advertised Remote Bindings
                    Label (peers)        (peers)
  ----------------- -------- ---------- ---------------
  1.1.2.2/32         -          0          1
  1.2.3.4/32        16010      396         0
  4.4.4.4/32        16004      396         3
  10.0.0.0/24       19226      396         395
```

The following sample output shows that the binding matches with a local label:

```
RP/0/RP0/CPU0:router# show mpls ldp bindings local-only

  10.12.32.2/32, rev 4
        Local binding: label: IMP-NULL
        No remote bindings
```

The following sample output shows that the binding matches with a remote label:

```
RP/0/RP0/CPU0:router# show mpls ldp bindings remote-only

  10.26.4.0/24, rev 0
        No local binding
        Remote bindings: (1 peers)
            Peer              Label
            ----------------- --------
            10.6.6.6:0        IMP-NULL
  10.43.4.0/24, rev 0
```

```
        No local binding
        Remote bindings: (1 peers)
               Peer              Label
               ----------------  --------
               10.4.4.4:0        IMP-NULL
 10.46.4.0/24, rev 0
        No local binding
        Remote bindings: (2 peers)
               Peer              Label
               ----------------  --------
               10.4.4.4:0        IMP-NULL
               10.6.6.6:0        IMP-NULL
```

Related Commands

Command	Description
label accept, on page 35	Configures the LDP remote label acceptance.
label advertise, on page 37	Configures the LDP local label advertisement control.
show mpls ldp neighbor, on page 89	Displays information on the LDP neighbors.
show mpls ldp forwarding, on page 76	Displays the contents of the LDP forwarding database.

show mpls ldp discovery

To display the status of the LDP discovery process, use the **show mpls ldp discovery** command in EXEC mode.

show mpls ldp discovery [*IP-address type interface-path-id*| **brief | link | targeted | summary**] **[detail]** [**location** *node-id*| **standby**]

Syntax Description		
	IP-address	(Optional) Neighbor IP address.
	type	(Optional) Interface type. For more information, use the question mark (?) online help function.
	interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
	brief	(Optional) Displays concise information about a specified LDP-enabled interface.
	link	(Optional) Displays link information for LDP discovery.
	targeted	(Optional) Displays targeted information for LDP discovery.
	summary	(Optional) Displays summarized information for LDP discovery.
	detail	(Optional) Displays detailed information (including, inbound label filtering, session KAs, and session protection state) for an LDP session.
	location *node-id*	(Optional) Displays location information for the specified node ID.
	standby	(Optional) Displays standby node-specific information.

Command Default No default behavior or values

Command Modes EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show mpls ldp discovery command** shows both link discovery and targeted discovery. When no interface filter is specified, this command generates a list of interfaces running the LDP discovery process. This command also displays neighbor discovery information for the default routing domain.

Task ID

Task ID	Operations
mpls-ldp	read

Examples

The following sample output is from the **show mpls ldp discovery** command:

```
RP/0/RP0/CPU0:router# show mpls ldp discovery

  Local LDP Identifier: 10.44.44.44:0
  Discovery Sources:
    Interfaces:
       POS 0/1/0/0 : xmit/recv
        LDP Id: 10.33.33.33:0, Transport address: 10.33.33.33
            Hold time: 15 sec (local:15 sec, peer:15 sec)
```

This table describes the significant fields shown in the display.

Table 6: show mpls ldp discovery Command Field Descriptions

Field	Description
Local LDP Identifier	LDP identifier for the local router. An LDP identifier is a 6-byte construct displayed in the form IP address:number. By convention, the first 4 bytes of the LDP identifier constitute the router ID; integers, starting with 0, constitute the final two bytes of the IP address:number construct.

Field	Description
Interfaces	Interfaces engaged in LDP discovery activity, as follows: **xmit field** Indicates that the interface is transmitting LDP discovery hello packets. **recv field** indicates that the interface is receiving LDP discovery hello packets. The LDP identifiers indicate the LDP neighbors discovered on the interface.
Transport Address	Address associated with this LDP peer (advertised in hello messages).
LDP Id	LDP identifier of the LDP peer.
Hold time	State of the forwarding hold timer and its current value.

The following sample output summarizes information for LDP discovery by using the **summary** keyword:

```
RP/0/RP0/CPU0:router# show mpls ldp discovery summary

  LDP Identifier: 139.0.0.1:0
  Interfaces:
    Configured: 2
    Enabled   : 1
  Discovery:
    Hello xmit: 1 (1 link)
    Hello recv: 1 (1 link)
```

This table describes the significant fields shown in the display.

Table 7: show mpls ldp discovery summary Command Field Descriptions

Field	Description
LDP Identifier	The LDP identifier for the local router.

Field	Description
Interfaces	Summary of interfaces engaged in LDP activity. **Configured** Number of interfaces configured for LDP. **Enabled** Number of interfaces on which LDP is actively enabled and is thus sending LDP hellos. An interface configured for LDP is enabled only if running IP and not in the down state.
Discovery	Summary of LDP discovery process. **Hello xmit** Number of local LDP discovery sources (including link and targeted hellos) emitting LDP hellos. **Hello recv** Number of discovered hello sources via link or targeted hello mechanics.

The following sample output MPLS LDP discovery hello information in brief form:

```
RP/0/RP0/CPU0:router# show mpls ldp discovery brief

  Local LDP Identifier: 150.150.150.150:0

  Discovery Source       Peer LDP Id          Holdtime Session
  ---------------------- -------------------- -------- -------
  BE35                   130.130.130.130:0    15       Y
  Gi0/6/0/6              160.160.160.160:0    15       Y
  Gi0/6/2/7.1            174.1.1.2:0          45       Y
  Target: 120.120.120.120  120.120.120.120:0  90       Y
  Target: 150.150.150.1  150.150.150.1:0      120      Y
```

Related Commands

Command	Description
discovery hello, on page 12	Configures LDP link hello parameters.
discovery targeted-hello, on page 15	Configures LDP targeted-hello parameters.
neighbor targeted, on page 53	Configures LDP targeted neighbor.
session protection, on page 61	Configures LDP session protection.

Command	Description
interface (MPLS LDP), on page 33	Configures LDP on an interface.
show mpls ldp neighbor, on page 89	Displays information about LDP neighbors.

show mpls ldp forwarding

To display the Label Distribution Protocol (LDP) forwarding state installed in MPLS forwarding, use the **show mpls ldp forwarding** command in EXEC mode.

show mpls ldp forwarding [*IP -address*] {*mask*| *length*} **[fast-reroute] [detail]** [**next-hop**| **address** *IP-address*| **interface***interface-path-id*| **label** *label-value* | **neigbor** *IP -address* | **unlabelled**] [**local-label** *label-value*] [**location** *node-id*| **summary**| **standby**]

Syntax Description

IP-address	(Optional) IP address, specified in four-part, dotted-decimal notation.
mask	Network mask.
length	Mask length, in bits. Range is 0 to 32.
detail	(Optional) Displays detailed information for the LDP timestamp that is used for the routing and forwarding update.
fast-reroute	(Optional) Displays the prefix that is LFA FRR protected in nature.
next-hop	Matches prefixes by next-hop IP address.
local-label *label-value*	(Optional) Displays the prefix with the specified local label. Range is from 0 to 1048575.
neighbor	Matches prefixes with a path through specified LDP neighbor.
unlabelled	Matches prefixes containing unlabelled paths.
location *node-id*	(Optional) Displays location information for the specified node ID.
summary	(Optional) Displays the summary information for the LDP forwarding information base (LFIB).
standby	(Optional) Displays standby-node specific information.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 3.9.0	The following items were added: • The **detail** keyword. • Sample output for the **detail** keyword. • The **local-label** keyword. • The **location** keyword. • The **standby** keyword.
Release 4.0.1	These items were added: • The **fast-reroute** keyword. • The **summary** keyword. • The **next-hop** keyword. • The **neighbor** keyword. • The **unlabelled** keyword.
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show mpls ldp forwarding** command displays the LDP forwarding entries and provides LDP view of its installed forwarding entries.

Task ID

Task ID	Operations
mpls-ldp	read

Examples   This is a sample output from the **show mpls ldp forwarding** command:

```
RP/0/RP0/CPU0:router# show mpls ldp forwarding

  Prefix            Label Label     Outgoing      Next Hop         GR Stale
                    In    Out       Interface
  ----------------- ----- --------- ----------- --------------- -- -----
  2.2.2.2/32        22    ImpNull   PO0/2/0/1      12.0.0.2         N  N
  3.0.0.1/32        24    20        PO0/2/0/1      12.0.0.2         N  N
  3.0.0.2/32        25    21        PO0/2/0/1      12.0.0.2         N  N
  3.0.0.3/32        26    22        PO0/2/0/1      12.0.0.2         N  N
  4.4.4.4/32        20    ExpNullv4 tt10           4.4.4.4          N  N
  4.4.4.5/32        21    ExpNullv4 tt10           4.4.4.4          N  N
  123.0.0.0/24      23    ImpNull   PO0/2/0/1      12.0.0.2         N  N
  3.3.3.3/32        16000 16001     PO0/2/0/3.1  131.1.1.4         Y  N
                          16002     PO0/2/0/3.2  131.1.2.4         Y  N
                          16003     PO0/2/0/3.3  131.1.3.4         N  N
                          16002     PO0/2/0/1    192.11.1.1 (!)    Y  N
                          Unlabelled PO0/2/0/2   192.11.2.1 (!)    N  N
```

✎

Note   The (!) symbol referes to a non-primary LFA backup path.

This sample output shows detailed information for the LDP timestamp that is used for routing and forwarding update from the **detail** keyword:

```
RP/0/RP0/CPU0:router# show mpls ldp forwarding 1.1.1.1/32 detail

  Prefix            Label   Label     Outgoing      Next Hop         GR Stale
                    In      Out       Interface
  ---------------- ------- --------- ----------- --------------- -- -----
  3.3.3.3/32        16000   16001     PO0/2/0/3.1  131.1.1.4         N  N
                    [ Protected; path-id 1 backup-path-id 33;
                    [peer 13.13.13.1:0 ]
                            16002     PO0/2/0/3.2  131.1.2.4         Y  N
                    [ Protected; path-id 2 backup-path-id 33;
                    peer 13.13.13.1:0 ]
                            16003     PO0/2/0/3.3  131.1.3.4         N  N
                    [ Protected; path-id 3 backup-path-id 34;
                    peer 13.13.13.2:0 ]
                            16002     PO0/2/0/1    192.11.1.1 (!)    Y  N
                    [ Backup; path-id 33; peer 14.14.14.1:0 ]
                            Unlabelled PO0/2/0/2   192.11.2.1 (!)    N  N
                    [ Backup; path-id 34 ]


    Routing update   : Mar 31 13:35:25.348 (00:55:32 ago)
    Forwarding update: Mar 31 13:35:25.349 (00:55:32 ago)
```

✎

Note   The (!) symbol referes to a non-primary LFA backup path.

This sample output shows only LDP prefixes with protection (ECMP or secondary LFA backups) update from the **fast-reroute** keyword:

This sample output shows the statistics of protected prefixes and protected paths from the **summary** keyword:

```
RP/0/RP0/CPU0:router# show mpls ldp forwarding summary
Forwarding Server (LSD):
  Connected: Yes
```

```
      Forwarding State Holdtime: 360 sec
Forwarding States:
  Interfaces: 10
  Local labels: 8
  Rewrites:
    Prefix:
      Total: 8 (0 with ECMP, 8 FRR protected)
      Labelled:
        Primary pathset : 8 labelled (0 partial), 0 unlabelled
        Backup pathset  : 8 labelled (0 partial), 0 unlabelled
        Complete pathset: 8 labelled (0 partial), 0 unlabelled
    Paths:
      Total: 16 (8 backup, 8 FRR protected)
      Labelled: 16 (8 backup)
```

This table describes the significant fields shown in the display.

Table 8: show mpls ldp forwarding Command Field Descriptions

Field	Description
Prefix/mask	Prefix on the FEC[2] for an MPLS forwarding entry.
Label In	Local label assigned to the prefix/mask.
Label Out	Outgoing label for the prefix/mask.
Outgoing Interface	Outgoing physical interface.
Next Hop	Next Hop address.
GR	Graceful restart status (Y or N).
Stale	Status of the entry, stale or not stale. An entry is marked stale when the next-hop graceful restart neighbor disconnects and is unmarked when neighbor reconnects and refreshes the label.
Chkpt	Status of the entry, checkpointed or not checkpointed.
path-id	Primary Path-id.
Backup-path-id	The backup path-id is the path-id of the path protecting a given primary path. A protecting path can be primary path or a non-primary path.
Peer	Displays next-hop LDP peer's LDP identifier.
Connected	Displays LDP connection state with LSD forwarding server.
Forwarding State Holdtime	Displays time that LDP has registered with LSD server to keep LDP forwarding state intact upon LDP disconnect event.

Field	Description
Interfaces	Number of LDP enabled MPLS interfaces.
Local Labels	Number of LDP allocated local labels from LSD.
Rewrites	Counts of Forwarding rewrites. Displays total number of known IPv4 prefixes alongwith information on number of prefixes with more than one ECMP path. This also displays number of prefixes with LFA-FRR protection. The labelled set prints the counts related to prefixes with none, all, partial labelled paths as shown by unlabeled, labelled, and partial keywords. This information is available for primary, backup, and complete path set.
Paths	Forwarding path counts. Displays count of total number of known forwarding paths, along with number of backup paths and number of FRR protected paths. It also displays the count of labelled paths indicating how many of non-primary paths are labelled.

2 Forwarding Equivalence Class.

Related Commands

Command	Description
graceful-restart (MPLS LDP), on page 23	Configures the LDP graceful restart feature.
show mpls ldp bindings, on page 65	Displays the contents of LDP LIB.

show mpls ldp graceful-restart

To display the status of the Label Distribution Protocol (LDP) graceful restart, use the **show mpls ldp graceful-restart** command in EXEC mode.

show mpls ldp graceful-restart [**location** *node-id* | **standby**]

Syntax Description

location *node-id*	(Optional) Displays location information for the specified node ID.
standby	(Optional) Displays standby-node-specific information.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show mpls ldp graceful-restart** command displays LDP graceful-restart-related information when the **graceful-restart** command is enabled.

Task ID

Task ID	Operations
mpls-ldp	read

Examples

The following shows a sample output from the **show mpls ldp graceful-restart** command:

```
RP/0/RP0/CPU0:router# show mpls ldp graceful-restart

    Forwarding State Hold timer : Not Running
    GR Neighbors                : 1

    Neighbor ID     Up  Connect Count  Liveness Timer      Recovery Timer
    --------------- --  -------------  ------------------  ------------------
    10.0.0.2            Y       1              -                   -
```

This table describes the significant fields shown in the display.

Table 9: show mpls ldp graceful-restart Command Field Descriptions

Field	Description
Forwarding State Hold timer	State of the hold timer—running or not running.
GR Neighbors	Number of graceful restartable neighbors.
Neighbor ID	Router ID of each neighbor.
Up	Neighbor up or down.
Connect Count	Number of times the same neighbor has reconnected.
Liveness Timer	State of the liveness timer (running or not running) and its expiration time, if running.
Recovery Timer	State of the recovery timer (running or not running) and its expiration time, if running.

Related Commands

Command	Description
graceful-restart (MPLS LDP), on page 23	Configures the LDP graceful restart feature.
show mpls ldp neighbor, on page 89	Displays information about LDP neighbors.

show mpls ldp igp sync

To display Label Distribution Protocol (LDP) Interior Gateway Protocol (IGP) synchronization information on interface(s), use the **show mpls ldp igp sync** command in EXEC mode.

show mpls ldp igp sync [**interface** *type interface-path-id*] [**location** *node-id* | **standby**]

Syntax Description

interface	(Optional) Displays the interface type.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	(Optional) Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	(Optional) Displays location information for the specified node ID.
standby	(Optional) Displays standby-node-specific information.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

LDP IGP synchronization addresses traffic loss issues as a result of synchronization between MPLS LDP and IP (IGP). For instance, upon a link up, IGP can advertise a link before MPLS converges on the link. Also, the IGP link is still used even when MPLS session goes down and MPLS LSP is broken on this link. The use of IGP link is determined based on MPLS LDP convergence synchronization status on the link.

Use the **show mpls ldp igp sync** command to display MPLS convergence status. The configuration for LDP IGP synchronization resides in IGPs (OSPF, ISIS); accordingly, LDP displays and advertises this information for all LDP-enabled interfaces (regardless if the interface is configured for LDP IGP).

Task ID

Task ID	Operations
mpls-ldp	read

Examples

The following shows a sample output from the **show mpls ldp igp sync** command:

```
RP/0/RP0/CPU0:router# show mpls ldp igp sync

  GigabitEthernet0/3/0/0:
    Sync status: Ready
    Peers:
      2.2.2.2:0
      3.3.3.3:0 (GR)
    GR-only Reachability:
      4.4.4.4:0 (Chkpt-created)

  POS0/2/0/0:
    Sync status: Not ready
                 (Deferred; 24 sec remaining)

  POS0/2/0/1:
    Sync status: Not ready
```

This table describes the significant fields shown in the display.

Table 10: show mpls ldp igp sync Command Field Descriptions

Field	Description
Sync status	MPLS LDP convergence status on a given link. Ready indicates that the link is converged and is ready to be used by IGP. Not Ready with Deferred means that the link fulfills LDP IGP synchronization requirements but is deferred by LDP IGP synchronization delay timeout configuration setting. Not Ready means that the link is not ready to be used by IGP.
Peers	List of peers converged on the given link. If the peer session is GR[3]-enabled, output is tagged as GR. If GR-only reachability is indicated due to a GR neighbor record recovered from checkpoint after local start, then Chkpt-created flag is also set.
GR-only Reachability	List of GR[4] peers which are not currently converged on a given link but still in the forwarding state.

[3] Graceful Restart.
[4] Graceful Restart.

Related Commands

Command	Description
igp sync delay, on page 29	Configures LDP IGP sync delay timeout.

show mpls ldp interface

To display information about LDP-enabled interfaces, use the **show mpls ldp interfaces** command in EXEC mode.

show mpls ldp interface [*type interface-path-id* | **summary**] **[brief]** [**location** *node-id* | **standby**]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
summary	(Optional) Displays summary information about a specified LDP-enabled interface.
brief	(Optional) Displays concise information about a specified LDP-enabled interface.
detail	(Optional) Displays detailed information about a specified LDP-enabled interface.
location *node-id*	(Optional) Displays location information for the specified node ID.
standby	(Optional) Displays standby-node-specific information.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	The **location** and **standby** keywords were added.
Release 4.2.0	The **detail** keyword was added.
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-ldp	read

Examples

The following shows a sample output from the **show mpls ldp interface** command:

```
RP/0/RP0/CPU0:router# show mpls ldp interface

  Interface GigabitEthernet0/3/0/3
     No LDP config
  Interface POS0/2/0/0
     No LDP config
     Auto-config items:
        ospf/100/0
  Interface POS0/2/0/1
     No LDP config
     Auto-config items:
        ospf/100/0
  Interface POS0/2/0/2
     No LDP config
     Auto-config items:
        ospf/100/0
  Interface POS0/2/0/3
     No LDP config
     Auto-config items:
        ospf/100/0
```

This table describes the significant fields shown in the display.

Table 11: show mpls ldp interface Command Field Descriptions

Field	Description
Auto-config items	Lists IGPs that specify an interface for MPLS LDP auto-configuration: **OSPF** *ospf instance area* **ISIS** *isis instance*

The following shows a sample output from the **show mpls ldp interface detail** command for the mesh groups:

```
RP/0/RP0/CPU0:router# show mpls ldp interface detail
```

```
Interface GigabitEthernet0/2/0/0 (0x20200040)
 Enabled via config: LDP interface
Interface GigabitEthernet0/2/0/1 (0x20200060)
 Disabled via config: IGP Auto-config disable
    Ignoring: LDP interface
Interface GigabitEthernet0/2/0/2 (0x20200080)
 Disabled via config: IGP Auto-config disable
    Ignoring: LDP interface
Interface tunnel-te1 (0x200000f0)
 Disabled
Interface tunnel-te100 (0x20000110)
 Enabled via config: TE Mesh-group 123, TE Mesh-group all
Interface tunnel-te101 (0x20000130)
 Enabled via config: TE Mesh-group 123, TE Mesh-group all
```

Related Commands

Command	Description
igp auto-config disable, on page 28	Disables LDP auto-configuration.

show mpls ldp neighbor

To display the status of Label Distribution Protocol (LDP) sessions, use the **show mpls ldp neighbor** command in EXEC mode.

show mpls ldp neighbor [*IP-address*] [*type interface-path-id*] **[brief] [detail] [gr]** [**location** *node-id*] **[non-gr] [sp] [standby]**

Syntax Description

IP-address	(Optional) Neighbor IP address.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
brief	(Optional) Displays the existing LDP sessions in brief format.
detail	(Optional) Displays detailed information (including, inbound label filtering, session KAs, and session protection state) for an LDP session.
gr	(Optional) Displays graceful restartable neighbors.
location *node-id*	(Optional) Displays location information for the specified node ID.
non-gr	(Optional) Displays non-graceful restartable neighbors.
sp	(Optional) Displays neighbors with session protection.
standby	(Optional) Displays standby-node-specific information.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show mpls ldp neighbor** command provides information about all LDP neighbors in the entire routing domain—conversely, the show output is filtered to display:

- LDP neighbors with specific IP addresses

- LDP neighbors on a specific interface

- LDP neighbors that are graceful restartable

- LDP neighbors that are nongraceful restartable

- LDP neighbors enabled with session protection

Task ID

Task ID	Operations
mpls-ldp	read

Examples   The following shows a sample output from the **show mpls ldp neighbor** command using an IP address:

```
RP/0/RP0/CPU0:router# show mpls ldp neighbor 10.22.22.22

  Peer LDP Identifier: 10.22.22.22:0
    TCP connection: 10.22.22.22:646 - 10.33.33.33:65530
    Graceful Restart: No
    State: Oper; Msgs sent/rcvd: 46/43
    Up time: 00:31:21
    LDP Discovery Sources:
  POS 0/2/0/0
    Addresses bound to this peer:
      10.22.22.22     10.10.2.1
```

The following shows a sample output from the **show mpls ldp neighbor** command using the **non-gr** keyword:

```
RP/0/RP0/CPU0:router# show mpls ldp neighbor non-gr

  Peer LDP Identifier: 10.44.44.44:0
    TCP connection: 10.44.44.44:65535 - 10.33.33.33:646
    Graceful Restart: No
    State: Oper; Msgs sent/rcvd: 49/46
    Up time: 00:33:33
    LDP Discovery Sources:
      POS 0/1/0/0
    Addresses bound to this peer:
      10.44.44.44     10.10.3.2
  Peer LDP Identifier: 10.22.22.22:0
    TCP connection: 10.22.22.22:646 - 10.33.33.33:65530
    Graceful Restart: No
    State: Oper; Msgs sent/rcvd: 48/45
    Up time: 00:33:11
    LDP Discovery Sources:
      POS 0/2/0/0
    Addresses bound to this peer:
      10.22.22.22     10.10.2.1
```

This table describes the significant fields shown in the display.

Table 12: show mpls ldp neighbor Command Field Descriptions

Field	Description
Peer LDP Identifier	LDP identifier of the neighbor (peer) for this session.

TCP connection	TCP connection used to support the LDP session, shown in the following format:
	
	neighbor IP address
	
	   peer port
	
	local IP address
	
	   local port

Graceful Restart	Graceful-restart status (Y or N).
State	State of the LDP session. Generally this is Oper (operational), but transient is another possible state.
Msgs sent/rcvd	Number of LDP messages sent to and received from the session peer. The count includes the transmission and receipt of periodic keepalive messages, which are required for maintenance of the LDP session.
Up time	The length of time that this session has been up for (in *hh:mm:ss* format).
LDP Discovery Sources	The source(s) of LDP discovery activity leading to the establishment of the LDP session.
Addresses bound to this peer	The known interface addresses of the LDP session peer. These are addresses that might appear as "next hop" addresses in the local routing table. They are used to maintain the LFIB[5].

5 LFIB = Label Forwarding Information Base.

The following shows a sample output from the **show mpls ldp neighbor** command using the **brief** keyword:

```
RP/0/RP0/CPU0:router# show mpls ldp neighbor brief

 Peer              GR  NSR  Up Time     Discovery  Address  IPv4 Label
 ----------------- --  ---  ----------  ---------  -------  ----------
 2.2.2.2:0         N   Y    01:39:50            1        4          19
 3.3.3.3:0         N   N    01:38:04            1        3           5
```

This table describes the significant fields shown in the display.

Table 13: show mpls ldp neighbor brief Command Field Descriptions

Field	Description
Peer	LDP identifier of the neighbor (peer) for this session.
GR	Graceful-restart status (Y or N).
Up Time	Time the session has been up (in hh:mm:ss format).
Discovery	Number of LDP discovery sources corresponding to the neighbor.
Address	Number of addresses bound to this peer.

The following shows a sample output from the **show mpls ldp neighbor** command using the **detail** keyword:

```
RP/0/RP0/CPU0:router# show mpls ldp neighbor detail

  Peer LDP Identifier: 2.2.2.2:0
    TCP connection: 2.2.2.2:11707 - 1.1.1.1:646
    Graceful Restart: No
    Session Holdtime: 180 sec
    State: Oper; Msgs sent/rcvd: 33/29
    Up time: 00:13:37
    LDP Discovery Sources:
       POS0/2/0/1
      Targeted Hello (1.1.1.1 ->2.2.2.2, active)
    Addresses bound to this peer:
      23.0.0.2 2.0.0.2        123.0.4.2        10.42.37.119
      10.2.2.2
    Peer holdtime: 180 sec; KA interval: 60 sec; Peer state: Estab
    Clients: Dir Adj Client
    Inbound label filtering: accept acl 'pfx_acl2'
    Session Protection:
      Enabled, state: Ready
      Duration: 30 seconds
```

This table describes the significant fields shown in the display.

Table 14: show mpls ldp neighbor detail Command Field Descriptions

Field	Description
Peer LDP Identifier	LDP identifier of the neighbor (peer) for this session.

TCP connection	TCP connection used to support the LDP session, shown in the following format:
	
	neighbor IP address
	
	    peer port
	
	local IP address
	
	    local port

Field	Description
Graceful Restart	Graceful-restart status (Y or N).
Session Holdtime	Session hold time, in seconds.
State	State of the LDP session (operational or transient).
Msgs sent/rcvd	Number of LDP messages sent to and received from the session peer. The count includes the transmission and receipt of periodic keepalive messages, which are required for maintenance of the LDP session.
Up time	Time the session has been up for (in *hh:mm:ss* format).
Peer holdtime	Time to keep LDP peer session up without receipt of LDP protocol message from a peer.
Peer state	Peer session state.
Peer holdtime	Time to keep LDP peer session up without receipt of LDP protocol message from a peer.
Clients	LDP (internal) clients requesting session with a neighbor.
Inbound label filtering	LDP neighbor inbound filtering policy.
Session Protection	State of the session protection: **Incomplete** Targeted discovery requested but not yet up. **Ready** Targeted discovery and at least one link hello adjacency to the peer are up. **Protecting** Targeted discovery is up and there is no link hello adjacency to the peer. Targeted discovery is protecting and backing up link discoveries.
Duration	Maximum time to maintain session through targeted discovery upon loss of primary link discovery.
Holdtimer	When in "protecting" state, time to keep LDP peer session up without receipt of LDP protocol message from a peer.

Related Commands

Command	Description
graceful-restart (MPLS LDP), on page 23	Configures the LDP graceful restart feature.
label accept, on page 35	Configures the LDP inbound label filtering feature.
session protection, on page 61	Configures the LDP session protection feature.
show mpls ldp discovery, on page 71	Displays the status of the LDP discovery process.

show mpls ldp parameters

To display current LDP parameters, use the **show mpls ldp parameters** command in EXEC mode.

show mpls ldp parameters [**location** *node-id* | **standby**]

Syntax Description

location *node-id*	(Optional) Displays location information for the specified node ID.
standby	(Optional) Displays standby-node-specific information.

Command Default No default behavior or values

Command Modes EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show mpls ldp parameters** command displays all LDP operational and configuration parameters.

Task ID

Task ID	Operations
mpls-ldp	read
network	read

Examples The following shows a sample output from the **show mpls ldp parameters** command:

```
RP/0/RP0/CPU0:router# show mpls ldp parameters

  LDP Parameters:
    Protocol Version: 1
    Router ID: 10.11.11.11
    Null Label: Implicit
    Session:
      Hold time: 180 sec
      Keepalive interval: 60 sec
```

```
      Backoff: Initial:15 sec, Maximum:120 sec
Discovery:
  Link Hellos:     Holdtime:15 sec, Interval:5 sec
  Targeted Hellos: Holdtime:90 sec, Interval:10 sec
                   (Accepting peer ACL 'peer_acl_10')
Graceful Restart:
  Enabled (Configured)
  Reconnect Timeout:120 sec, Forwarding State Holdtime:180 sec
Timeouts:
  Binding with no-route: 300 sec
  LDP application recovery (with LSD): 360 sec
OOR state
  Memory: Normal
```

This table describes the significant fields shown in the display.

Table 15: show mpls ldp parameters Command Field Descriptions

Field	Description
Protocol Version	Version of LDP running on the platform.
Router ID	Currently used router ID.
Null Label	LDP use of implicit-null or explicit-null as label for prefixes where it has to use a null label.
Session Hold time	Time LDP session is to be maintained with an LDP peer without receiving LDP traffic or an LDP keepalive message from the peer.
Session Keepalive interval	Time interval between consecutive transmissions of LDP keepalive messages to an LDP peer.
Session Backoff	Initial maximum backoff time for sessions.
Discovery Link Hellos	Time to remember that a neighbor platform wants an LDP session without receiving an LDP hello message from the neighbor (hold time), and the time interval between the transmission of consecutive LDP hello messages to neighbors (interval).
Discovery Targeted Hellos	Indicates the time: • To remember that a neighbor platform wants an LDP session when the neighbor platform is not directly connected to the router or the neighbor platform has not sent an LDP hello message. This intervening interval is known as *hold time*. • Interval between the transmission of consecutive hello messages to a neighbor not directly connected to the router and if targeted hellos are being accepted, displaying peer-acl (if any).
Graceful Restart	Status of graceful-restart status (Y or N).

Field	Description
Timeouts	Various timeouts (of interest) that the LDP is using. One timeout is *binding no route*, which indicates how long the LDP waits for an invalid route before deleting it. It also shows restart recovery time for LSD and LDP.
OOR state	Out of resource memory state: Normal, Major, or Critical.

Related Commands

Command	Description
backoff, on page 3	Configures the parameters for the LDP backoff mechanism.
discovery hello, on page 12	Configures the interval between transmission of LDP discovery messages.
explicit-null, on page 21	Configures a router to advertise an explicit-null label.
graceful-restart (MPLS LDP), on page 23	Configures the LDP graceful restart feature.
holdtime (MPLS LDP), on page 26	Configures keepalive message hold time for LDP sessions.
neighbor targeted, on page 53	Specifies the preferred interface or IP address of a Loopback interface for determining the LDP router ID.

show mpls ldp statistics msg-counters

To display statistics of the messages exchanged between neighbors, use the **show mpls ldp statistics msg-counters** command in EXEC mode.

show mpls ldp statistics msg-counters [*IP-address*] [**location** *node-id* | **standby**]

Syntax Description

IP-address	(Optional) Neighbor IP address.
location *node-id*	(Optional) Displays location information for the specified node ID.
standby	(Optional) Displays standby-node-specific information.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show mpls ldp statistics msg-counters** command can provide counter information about different types of messages sent and received between neighbors.

Task ID

Task ID	Operations
mpls-ldp	read

Examples

The following shows a sample output from the **show mpls ldp statistics msg-counters** command:

```
RP/0/RP0/CPU0:router# show mpls ldp statistics msg-counters

  Peer LDP Identifier: 10.33.33.33:0
    Msg Sent: (80)
      Init            : 1
      Address         : 1
```

```
              Address_Withdraw : 0
              Label_Mapping    : 5
              Label_Withdraw   : 0
              Label_Release    : 0
              Notification     : 0
              KeepAlive        : 73

          Msg Rcvd: (81)
              Init             : 1
              Address          : 1
              Address_Withdraw : 0
              Label_Mapping    : 8
              Label_Withdraw   : 0
              Label_Release    : 0
              Notification     : 0
              KeepAlive        : 71
```

Table 16: show mpls ldp statistics msg-counters Command Field Descriptions, on page 99 describes the significant fields shown in the display.

Table 16: show mpls ldp statistics msg-counters Command Field Descriptions

Field	Description
Peer LDP Identifier	LDP identifier of the neighbor (peer).
Msg Sent	Summary of messages sent to the LDP peer.
Msg Rcvd	Summary of messages received from the LDP peer.

Related Commands

Command	Description
clear mpls ldp msg-counters neighbor, on page 5	Clears MPLS LDP message counter values.
show mpls ldp bindings, on page 65	Displays the contents of LDP LIB.
show mpls ldp neighbor, on page 89	Displays LDP neighbor information.

show mpls ldp summary

To display a summary of LDP information, use the **show mpls ldp summary** command in EXEC mode.

show mpls ldp summary [**location** *node-id* | **standby**]

Syntax Description

location *node-id*	(Optional) Displays location information for the specified node ID.
standby	(Optional) Displays standby-node-specific information.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show mpls ldp summary** command can provide information about the number of LDP neighbors, interfaces, forwarding state (rewrites), servers connection/registration, and graceful-restart information.

Task ID

Task ID	Operations
mpls-ldp	read

Examples

The following shows a sample output from the **show mpls ldp summary** command:

```
RP/0/RP0/CPU0:router# show mpls ldp summary

  Routes   : 4
  Neighbors : 1 (1 GR)
  Hello Adj : 1
  Interfaces: 4 (1 forward reference, 2 LDP configured)
  Addresses : 3
  Clients   : 0
  Servers   :
              Connected  Registered
              ---------  ----------
```

```
SysDB           Y          Y
IM              Y          Y
IPv4 ARM        Y          -
LSD             Y          Y
RIBv4           Y          Y
```

This table describes the significant fields shown in the display.

Table 17: show mpls ldp summary Command Field Descriptions

Field	Description
Routes	Number of known IP routes (prefixes).
Neighbors	Number of LDP neighbors, including targeted and graceful restartable neighbors.
Hello Adj	Number of discovered LDP discovery sources.
Interfaces	Number of known IP interfaces and number of LDP configured interfaces. LDP is configured on a forward-referenced interface which may not exist or for which no IP address is configured.
Addresses	Number of known local IP addresses.
Clients	Number of external LDP clients. This number is always zero.
Servers	Connection and registration status with servers: SysDB[6], IM[7], IPv4 ARM[8], LSD[9], and IPv4 RIBv4[10].

[6] SysDB = System Database.

[7] IM = Interface Manager.

[8] IPv4 ARM = IPv4 Address Resource Manager.

[9] LSD = Label Switching Database.

[10] RIBv4 = Routing Information Base.

Related Commands

Command	Description
show mpls ldp bindings, on page 65	Displays the contents of LDP LIB.
show mpls ldp discovery, on page 71	Displays the status of the LDP discovery process.
show mpls ldp forwarding, on page 76	Displays the contents of the LDP forwarding database.
show mpls ldp graceful-restart, on page 81	Displays the status of the LDP graceful restart.
show mpls ldp parameters, on page 95	Displays current LDP parameter settings.

show lcc

To display label consistency checker (LCC) information, use the **show lcc** command in EXEC mode.

show lcc {**ipv4**| **ipv6**} **unicast** {**all**| **label**| **tunnel-interface**| **statistics** | [**summary**| **scan-id** *scan-id*]} [**vrf** *vrfname*]

Syntax Description

ipv4	Specifies IP version 4 address prefixes.
ipv6	Specifies IP version 6 address prefixes.
unicast	Specifies unicast address prefixes.
all	Scans all routes.
label	Scans all labels.
tunnel-interface	Specifies the interface of a tunnel.
statistics	Displays route consistency check statistics information.
scan-id	Specifies the value of scan-id. Range is from 0 to 100000.
summary	Displays background route consistency check statistics summary information.
vrf *vrfname*	(Optional) Specifies a particular VPN routing and forwarding (VRF) instance or all VRF instances.

Command Default None

Command Modes IPv4 address family configuration

IPv6 address family configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
IPv4	read
IPv6	read

Examples

The following example shows an outcome of the label consistency checker information:

```
RP/0/RP0/CPU0:router# show lcc ipv4 unicast all

Sending scan initiation request to IPv4 LSD ... done
Waiting for scan to complete (max time 600 seconds).....................
Scan Completed
Collecting scan results from FIBs (max time 30 seconds)... done
Number of nodes involved in the scan: 2
Number of nodes replying to the scan: 2

Legend:
        ? - Currently Inactive Node, ! - Non-standard SVD Role
        * - Node did not reply

    Node               Checks Performed              Errors

    0/2/CPU0                  6                           0
    0/0/CPU0                  6                           0
```

Related Commands

Command	Description
show rcc	Displays route consistency checker related information.

signalling dscp (LDP)

To assign label distribution protocol (LDP) signaling packets a differentiated service code point (DSCP) to assign higher priority to the control packets while traversing the network, use the **signalling dscp** command in MPLS LDP configuration mode. To return to the default behavior, use the **no** form of this command.

signalling dscp *dscp*

no signalling dscp

Syntax Description

dscp	DSCP priority value. Range is 0 to 63.

Command Default   LDP control packets are sent with precedence 6 (*dscp*: 48)

Command Modes   MPLS LDP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

DSCP marking improves signaling setup and teardown times.

Ordinarily, when LDP sends hello discovery or protocol control messages, these are marked using the default control packet precedence value (6, or *dscp* 48). You can use the **signalling dscp** command to override that DSCP value to ensure that all control messages sent are marked with a specified DSCP.

Note   While the **signalling dscp** command controls LDP signaling packets (Discovery hellos and protocol messages), it has no effect on ordinary IP or MPLS data packets.

Task ID

Task ID	Operations
mpls-ldp	read, write

Examples   The following example shows how to assign LDP packets a DSCP value of 56:

```
RP/0/RP0/CPU0:router(config-ldp)# signalling dscp 56
```

snmp-server traps mpls ldp

To inform a network management system of session and threshold cross changes, use the **snmp-server traps mpls ldp** command in global configuration mode.

snmp-server traps mpls ldp {**up | down | threshold**}

Syntax Description

up	Displays the session-up notification.
down	Displays the session-down notification.
threshold	Displays the session-backoff-threshold crossed notification.

Command Default

LDP does not send SNMP traps.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **snmp-server traps mpls ldp** command sends notifications to the SNMP server. There are three types of traps sent by LDP:

Session up

Generated when sessions go up.

Session down

Generated when sessions go down.

Threshold

Generated when attempts to establish a session fails. The predefined value is 8.

Task ID	Operations
mpls-ldp	read, write
mpls-te	read, write
snmp	read, write

Examples

The following example shows how to enable LDP SNMP trap notifications for Session up:

```
RP/0/RP0/CPU0:router(config)# snmp-server traps mpls ldp up
```

MPLS Forwarding Commands

This module describes the commands used to configure and use Multiprotocol Label Switching (MPLS) forwarding.

For detailed information about MPLS concepts, configuration tasks, and examples, see *MPLS Configuration Guide for Cisco NCS 6000 Series Routers*.

mpls ip-ttl-propagate

To configure the behavior controlling the propagation of the IP Time-To-Live (TTL) field to and from the MPLS header, use the **mpls ip-ttl-propagate** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

mpls ip-ttl-propagate disable [**forwarded** | **local**]

no mpls ip-ttl-propagate

Syntax Description

disable	Disables the propagation of IP TTL to and from the MPLS header for both forwarded and local packets.
forwarded	(Optional) Disables the propagation of IP TTL to and from the MPLS headed for only the forwarded packets. This prevents the **traceroute** command from displaying the MPLS-enabled nodes beyond the device under the configuration.
local	(Optional) Disables the propagation of IP TTL to the MPLS header for only locally generated packets. This prevents the **traceroute** command from displaying the MPLS-enabled nodes beyond the device under the configuration.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

By default, the IP TTL is propagated to the MPLS header when IP packets enter the MPLS domain. Within the MPLS domain, the MPLS TTL is decremented at each MPLS hop. When an MPLS encapsulated IP packet exits the MPLS domain, the MPLS TTL is propagated to the IP header. When propagation is disabled, the MPLS TTL is set to 255 during the label imposition phase and the IP TTL is not altered.

Task ID

Task ID	Operations
mpls-te	read, write

Task ID	Operations
mpls-ldp	read, write

Examples   The following example shows how to disable IP TTL propagation:

```
RP/0/RP0/CPU0:router(config)# mpls ip-ttl-propagate disable
```

The following example shows how to disable IP TTL propagation for forwarded MPLS packets:

```
RP/0/RP0/CPU0:router(config)# mpls ip-ttl-propagate disable forwarded
```

The following example shows how to disable IP TTL propagation for locally generated MPLS packets:

```
RP/0/RP0/CPU0:router(config)# mpls ip-ttl-propagate disable local
```

mpls label range

To configure the dynamic range of local labels available for use on packet interfaces, use the **mpls label range** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

mpls label range table *table-id minimum maximum*

no mpls label range table *table-id minimum maximum*

Syntax Description

table *table-id*	Identifies a specific label table; the global label table has table-id = 0. If no table is specified, the global table is assumed. Currently, you can specify table 0 only.
minimum	Smallest allowed label in the label space. Default is 16000.
maximum	Largest allowed label in the label space. Default is 1048575.

Command Default

table-id: 0

minimum: 16000

maximum: 1048575

Command Modes

Global configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

After configuring the **mpls label range** command, restart the router for the configuration to take effect.

The label range defined by the **mpls label range** command is used by all MPLS applications that allocate local labels (for dynamic label switching Label Distribution Protocol [LDP], MPLS traffic engineering, and so on).

Labels 0 through 15 are reserved by the Internet Engineering Task Force (IETF) (see the draft-ietf-mpls-label-encaps-07.txt for details) and cannot be included in the range using the **mpls label range** command.

Labels 16 through 15999 are reserved for Layer 2 VPN static pseudowires. You should not configure Layer 2 VPN static pseudowires which fall within the dynamic range. If more Layer 2 VPN static pseudowires are required, restrict the dynamic label range using this configuration.

Note
- Labels outside the current range and which are allocated by MPLS applications remain in circulation until released.

- You must understand the maximum labels that are supported for each platform versus the labels that are supported for the CLI.

Task ID

Task ID	Operations
mpls-te	read, write
mpls-ldp	read, write

Examples

The following example shows how to configure the size of the local label space using a *minimum* of 16200 and a *maximum* of 120000:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls label range 16200 120000
```

Related Commands

Command	Description
show mpls label range, on page 125	Displays the range of the MPLS local label space.

show mpls forwarding

To display the contents of the MPLS Label Forwarding Information Base (LFIB), use the **show mpls forwarding**command in EXEC mode.

show mpls forwarding [**detail**] [**hardware**{**ingress | egress**}] [**interface** *type interface-path-id*] [**location** *node-id*] [**labels** *low-value* [*high-value*]] [**prefix**{*network*/*mask*| **ipv4 unicast** *network*/*mask*}] [**private**] [**summary**] [**tunnels** *tunnel-id*] [**vrf** *vrf-name*]

Syntax Description		
detail	(Optional) Displays information in long form (includes length of encapsulation, length of Media Access Control [MAC] string, maximum transmission unit [MTU], Packet switched, and label stack).
hardware	(Optional) Displays the hardware location entry.
ingress	(Optional) Reads information from the ingress PSE.
egress	(Optional) Reads information from the egress PSE.
interface	(Optional) Displays information for the specified interface.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
labels *low-value* [*high-value*]	(Optional) Entries with a local labels range. Ranges for both *low-value* and *high-value* are 0 to 1048575.
location *node-id*	(Optional) Displays hardware resource counters on the designated node.
prefix *network*/*mask* /*length*	(Optional) Displays the destination address and mask/prefix length. **Note** The forward slash (/) between *network* and *mask* is required.
ipv4 unicast	(Optional) Displays the IPv4 unicast address.
private	(Optional) Displays private information.
summary	(Optional) Displays summarized information.
tunnels *tunnel-id*	(Optional) Displays entries either for a specified label switch path (LSP) tunnel or all LSP tunnel entries.

vrf *vrf-name*	(Optional) Displays entries for VPN routing and forwarding (VRF).

Command Modes EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines The optional keywords and arguments described allow specification of a subset of the entire MPLS forwarding table.

The *node-id* argument is entered in the *rack/slot/module* notation.

Task ID

Task ID	Operations
mpls-te	read, write
mpls-ldp	read, write
mpls-static	read, write

Examples The following sample output is from the **show mpls forwarding** command using the **location** keyword and a specific node ID:

```
RP/0/RP0/CPU0:router# show mpls forwarding location 0/2/CPU0

 Local  Outgoing    Outgoing     Next Hop                     Bytes
 Label  Label       Interface                                 Switched
 ------ ----------- ------------ --------------- ---------------------------
 16000  Unlabelled  ce01::ce01/128[V]  Gi0/1/0/0    ce01:10::2      0
 16001  Aggregate   router: Per-VRF Aggr[V]   \
                                     router 0
 16021  16020       P2MP TE:10   Gi0/2/0/3    172.99.1.2     13912344
        16040       P2MP TE:10   Gi0/2/0/3    172.99.2.2     13912344
        16045       P2MP TE:10   PO0/1/0/4    172.16.1.2     13912344
```

The following sample output shows detailed information for the LSP tunnels:

```
RP/0/RP0/CPU0:router#  show mpls forwarding prefix 10.241.4.0/24 detail

 Local  Outgoing    Prefix            Outgoing     Next Hop        Bytes
 Label  Label       or ID             Interface                    Switched
 ------ ----------- ----------------- ------------ --------------- ------------
 16057  16058       10.241.4.0/24     Gi0/1/0/23   10.114.4.11     0
     Updated May 10 20:00:15.983
     MAC/Encaps: 14/18, MTU: 9202
     Label Stack (Top -> Bottom): { 16058 }
     Packets Switched: 0
```

```
      16058       10.241.4.0/24     Te0/4/0/0    10.114.8.11     0
   Updated May 10 20:00:15.983
   MAC/Encaps: 14/18, MTU: 9086
   Label Stack (Top -> Bottom): { 16058 }
   Packets Switched: 0
```

The following sample output shows the number of P2MP TE heads and midpoints and the number of P2MP route updates that are received from the MRIB from the **summary** keyword:

```
RP/0/RP0/CPU0:router# show mpls forwarding summary

 Forwarding entries:
   Label switching: 91647
   MPLS TE tunnel head: 1351, protected: 1
   MPLS TE midpoint: 0, protected: 0
   MPLS TE internal: 1351, protected: 1
   MPLS P2MP TE tunnel head: 499
   MPLS P2MP TE tunnel midpoint/tail: 999 Forwarding updates:
   messages: 3925
      p2p updates: 229115
      p2mp updates: 13519
         add/modify:12020, deletes:1499,
         dropped:0 (iir trigger drops:0)) Labels in use:
   Reserved: 3
   Lowest: 0
   Highest: 112979
   Deleted stale label entries: 0
```

This table describes the significant fields shown in the display.

Table 18: show mpls forwarding Field Descriptions

Field	Description
Local Label	Label assigned by this router.
Outgoing Label	Label assigned by the next hop or downstream peer. Some of the entries that display in this column are: **Unlabeled** No label for the destination from the next hop, or label switching is not enabled on the outgoing interface. **Pop Label** Next hop advertised an implicit-null label for the destination.
Prefix or Tunnel ID	Address or tunnel to which packets with this label are going.
Outgoing Interface	Interface through which packets with this label are sent.
Next Hop	IP address of neighbor that assigned the outgoing label.
Bytes Switched	Number of bytes switched with this incoming label.

Field	Description
TO	Timeout: Indicated by an "*" if entry is being timed out in forwarding.
Mac/Encaps	Length in bytes of Layer 2 header, and length in bytes of packet encapsulation, including Layer 2 header and label header.
MTU	MTU[11] of labeled packet.
Label Stack	All the outgoing labels on the forwarded packet.
Packets Switched	Number of packets switched with this incoming label.
Label switching	Number of Label switching LFIB[12] forwarding entries.
IPv4 label imposition	Number of IPv4 label imposition forwarding entries (installed at ingress LSR).
MPLS TE tunnel head	Number of forwarding entries (installed at ingress LSR) on MPLS TE tunnel head.
MPLS TE fast-reroute	Number of forwarding entries (installed at PLR) for MPLS-TE fast reroute.
Forwarding updates	Number of forwarding updates sent from LSD (RP/DRP) to LFIB/MPLS (RP/DRP/LC) using BCDL mechanism, indicating the total number of updates and total number of BCDL messages.
Labels in use	Local labels in use (installed in LFIB). These usually indicate the lowest and highest label in use (allocated by applications). Furthermore, some reserved labels, such as explicit-nullv4, explicit-nullv6, are installed in the forwarding plane. The label range is 0 to 15.

[11] MTU = Maximum Transmission Unit.
[12] LFIB = Label Forwarding Information Base.

Related Commands

Command	Description
show mpls forwarding exact-route, on page 118	Displays the exact path for the source and destination address pair.

show mpls forwarding exact-route

To display the exact path for the source and destination address pair, use the **show mpls forwarding exact-route** command in EXEC mode.

show mpls forwarding exact-route label *label-number* {**bottom-label** *value*| **ipv4** *source-address destination-address*| **ipv6***source-addressdestination-address*} [**detail**] [**protocol** *protocol* **source-port** *source-port* **destination-port** *destination-port* **ingress-interface** *type interface-path-id*] [**location** *node-id*] [**policy-class** *value*] [**hardware** {**ingress** | **egress**}]

Syntax Description

label *label-number*	Displays the exact path for a source and destination address pair.
bottom-label *value*	Displays the bottom label value. Range is 0 to 1048575.
ipv4 *source-address destination-address*	Displays the exact path for IPv4 payload. The IPv4 source address in x.x.x.x format. The IPv4 destination address in x.x.x.x format.
ipv6 *source-address destination-address*	Displays the exact path for IPv6 payload. The IPv6 source address in x:x::x format. The IPv6 destination address in x:x::x format.
detail	(Optional) Displays detailed information.
protocol *protocol*	(Optional) Displays the specified protocol for the route.
source-port *source-port*	Sets the UDP source port. The range is from 0 to 65535.
destination-port *destination-port*	Sets the UDP destination port. The range is from 0 to 65535.
ingress-interface	Sets the ingress interface.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	(Optional) Displays hardware resource counters on the designated node.
policy-class *value*	(Optional) Displays the policy-based tunnel selection (PBTS) to direct traffic into specific TE tunnels. The policy-class attribute maps the correct traffic class to this policy. The range for the policy-class value is from 1 to 7.
hardware	(Optional) Displays the hardware location entry.

| ingress | (Optional) Reads information from the ingress PSE. |
| egress | (Optional) Reads information from the egress PSE. |

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show mpls forwarding exact-route** command displays information in long form and includes the following information:

- Encapsulation length
- Media Access Control (MAC) string length
- Maximum transmission unit (MTU)
- Packet switching information
- Label stacking information

Task ID

Task ID	Operations
mpls-te	read, write
mpls-ldp	read, write
mpls-static	read, write

Examples   The following shows a sample output from the **show mpls forwarding exact-route** command:

```
RP/0/RP0/CPU0:router# show mpls forwarding exact-route label 16000 ipv4 10.74.1.6 127.0.0.15
 protocol tcp source-port 3503 destination-port 3503 ingress-interface pos 0/3/4/3

 Local   Outgoing   Prefix          Outgoing      Next Hop      Bytes
 Label   Label      or ID           Interface                   Switched
```

```
       ------ ----------- ------------------ ----------- --------------- ------------
       16000  16001       5.5.5.5/32         PO0/1/5/1   1.24.1.192      N/A
              Via: PO0/1/5/1, Next Hop: point2point
              MAC/Encaps: 4/8, MTU: 1500
              Label Stack (Top -> Bottom): { 16001 }
```

This table describes the significant fields shown in the display.

Table 19: show mpls forwarding exact-route Field Descriptions

Field	Description
Local Label	Label assigned by this router.
Outgoing Label	Label assigned by the next hop or downstream peer. Some of the entries that display in this column are: **Unlabeled** No label for the destination from the next hop, or label switching is not enabled on the outgoing interface. **Pop Label** Next hop advertised an implicit-null label for the destination.
Prefix or Tunnel ID	Address or tunnel to which packets with this label are going.
Outgoing Interface	Interface through which packets with this label are sent.
Next Hop	IP address of neighbor that assigned the outgoing label.
Bytes Switched	Number of bytes switched with this incoming label.
TO	Timeout: Indicated by an "*" if entry is being timed out in forwarding.
MAC/Encaps	Length in bytes of Layer 2 header, and length in bytes of packet encapsulation, including Layer 2 header and label header.
MTU	MTU[13] of labeled packet.
Label Stack	All the outgoing labels on the forwarded packet.
Packets Switched	Number of packets switched with this incoming label.

Field	Description
Label switching	Number of Label switching LFIB[14] forwarding entries.
IPv4 label imposition	Number of IPv4 label imposition forwarding entries (installed at ingress LSR).
MPLS TE tunnel head	Number of forwarding entries (installed at ingress LSR) on MPLS TE tunnel head.
MPLS TE fast-reroute	Number of forwarding entries (installed at PLR) for MPLS-TE fast reroute.
Forwarding updates	Number of forwarding updates sent from LSD (RP/DRP) to LFIB/MPLS (RP/DRP/LC) using BCDL mechanism, indicating the total number of updates and total number of BCDL messages.
Labels in use	Local labels in use (installed in LFIB). These usually indicate the lowest and highest label in use (allocated by applications). Furthermore, some reserved labels, such as explicit-nullv4, explicit-nullv6, are installed in the forwarding plane. The label range is 0 to 15.

[13] MTU = Maximum Transmission Unit.
[14] LFIB = Label Forwarding Information Base.

Related Commands

Command	Description
show mpls forwarding, on page 114	Displays the contents of the MPLS LFIB.

show mpls interfaces

To display information about one or more interfaces that have been configured for MPLS, use the **show mpls interfaces** command in EXEC mode.

show mpls interfaces [*type interface-path-id*] [**location** *node-id*] [**detail**]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	(Optional) Displays hardware resource counters on the designated node.
detail	(Optional) Displays detailed information for the designated node.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command displays MPLS information about a specific interface or about all interfaces where MPLS is configured.

Task ID

Task ID	Operations
mpls-te	read, write
mpls-ldp	read, write

Task ID	Operations
mpls-static	read, write

Examples

The following shows a sample output from the **show mpls interfaces** command:

```
RP/0/RP0/CPU0:router# show mpls interfaces

  Interface              LDP       Tunnel    Enabled
  ------------------------ -------- -------- --------
  POS0/4/0/0              Yes       Yes       Yes
  POS0/4/0/1              Yes       Yes       Yes
  POS0/4/0/2              Yes       Yes       Yes
```

The following shows a sample output from the **show mpls interfaces** command using the **detail** keyword:

```
RP/0/RP0/CPU0:router# show mpls interfaces detail

  Interface POS0/4/0/0:
        LDP labelling enabled
        LSP labelling enabled (TE-Control)
        MPLS enabled
        MTU = 4474
  Interface POS0/4/0/1:
        LDP labelling enabled
        LSP labelling enabled (TE-Control)
        MPLS enabled
        MTU = 4474
  Interface POS0/4/0/2:
        LDP labelling enabled
        LSP labelling enabled (TE-Control)
        MPLS enabled
        MTU = 4474
```

The following shows a sample output from the **show mpls interfaces** command using the **location** keyword:

```
RP/0/RP0/CPU0:router# show mpls interfaces location pos 0/4/0/0

  Interface              LDP       Tunnel    Enabled
  ------------------------ -------- -------- --------
  POS0/4/0/0             Yes       Yes       Yes

RP/0/RP0/CPU0:router# show mpls interfaces pos 0/4/0/0 detail

  Interface POS0/4/0/0:
        LDP labelling enabled
        LSP labelling enabled (TE-Control)
        MPLS enabled
        MTU = 4474
```

This table describes the significant fields in the sample display.

Table 20: show mpls interfaces Command Field Descriptions

Field	Description
LDP	State of LDP labelling.
Tunnel	State of LSP Tunnel labelling.

Field	Description
MTU	MTU[15] of labeled packet.
Caps	Capsulation switching chains installed on an interface.
M	MPLS switching capsulation/switching chains are installed on the interface and are ready to switch MPLS traffic.

15 MTU = Maximum Transmission Unit.

show mpls label range

To display the range of local labels available for use on packet interfaces, use the **show mpls label range** command in EXEC mode.

show mpls label range

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You can use the **show mpls label range** command to configure a range for local labels that is different from the default range.

Task ID

Task ID	Operations
mpls-te	read, write
mpls-ldp	read, write
mpls-static	read, write

Examples   The following shows a sample output from the **show mpls label range** command:

```
RP/0/RP0/CPU0:router# show mpls label range
  Range for dynamic labels: Min/Max: 16000/144000
```

This table describes the significant fields shown in the display.

Table 21: show mpls label range Command Field Descriptions

Field	Description
Range for dynamic labels	Minimum and maximum allowable range for local labels (which differs from the default range).

Related Commands

Command	Description
mpls label range, on page 112	Configures a range of values for use as local labels.

show mpls label table

To display the local labels contained in the MPLS label table, use the **show mpls label table** command in EXEC mode.

show mpls label table *table-index* [**application** *application*] [**label** *label-value*] [**summary**] [**detail**]

Syntax Description

table-index	Index of the label table to display. The global label table is 0. Currently, you can specify table 0 only.
application *application*	(Optional) Displays all labels owned by the selected application. Options are: **bgp-ipv4**, **bgp-spkr**, **bgp-vpn-ipv4**, **internal**, **ldp**, **none**, **l2vpn**, **static**, **te-control**, **te-link**, and **test**.
label *label-value*	(Optional) Displays a selected label based on the label value. Range is 0 to 1048575.
summary	(Optional) Displays a summary of local labels.
detail	(Optional) Displays detailed information for the MPLS label table.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	The **detail** keyword was added.
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note   Labels 16 to 15999 are reserved for static Layer 2 VPN pseudowires.

Task ID

Task ID	Operations
mpls-te	read, write
mpls-ldp	read, write
mpls-static	read, write

Examples

The following shows a sample output from the **show mpls label table** command:

```
RP/0/RP0/CPU0:router# show mpls label table 0

 Table Label   Owner      State  Rewrite
 ----- ------- ---------- ------ -------
 0     0       LSD        InUse  Yes
 0     1       LSD        InUse  Yes
 0     2       LSD        InUse  Yes
 0     3       LSD        InUse  Yes
 0     16      TE-Link    InUse  Yes
```

This table describes the significant fields shown in the display.

Table 22: show mpls label table Command Field Descriptions

Field	Description
Table	Table ID.
Label	Label index.
Owner	Application that allocated the label. All labels displaying "InUse" state have an owner.

Field	Description
State	**InUse** Label allocated and in use by an application. **Alloc** Label allocated but is not yet in use by an application. **Pend** Label was in use by an application that has terminated unexpectedly, and the application has not reclaimed the label. **Pend-S** Label was in use by an application, but the MPLS LSD (Label Switching Database) server has recently restarted and the application has not reclaimed the label.
Rewrite	Number of initiated rewrites.

Related Commands

Command	Description
show mpls forwarding, on page 114	Displays entries in the MPLS forwarding table. Label switching entries are indexed by their local label.
show mpls lsd applications, on page 130	Displays MPLS applications that are registered with the MPLS LSD server.

show mpls lsd applications

To display the MPLS applications registered with the MPLS Label Switching Database (LSD) server, use the **show mpls lsd applications** command in EXEC mode.

show mpls lsd applications [**application** *application*]

Syntax Description

application *application*	(Optional) Displays all labels owned by the selected application. Options are: **bgp-ipv4**, **bgp-spkr**, **bgp-vpn-ipv4**, **internal**, **ldp**, **none**, **l2vpn**, **static**, **te-control**, **te-link**, and **test**.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	The **application** keyword was added.
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

MPLS applications include Traffic Engineering (TE) control, TE Link Management, and label distribution protocol (LDP). The application must be registered with MPLS LSD for its features to operate correctly. All applications are clients (see the show mpls lsd clients, on page 132 command), but not all clients are applications.

Task ID

Task ID	Operations
mpls-te	read, write
mpls-ldp	read, write
mpls-static	read, write

Examples   The following shows a sample output from the **show mpls lsd applications** command:

```
RP/0/RP0/CPU0:router# show mpls lsd applications

  Type          State     RecoveryTime Node
  ------------  --------  ------------ ------------
  LDP           Active    300          0/0/CPU0
  TE-Control    Active    100          0/0/CPU0
  TE-Link       Active    600          0/0/CPU0
```

This table describes the significant fields shown in the display.

Table 23: show mpls lsd applications Command Field Descriptions

Field	Description
Type	LSD application type.
State	**Active** Application registered with MPLS LSD and is functioning correctly. **Recover** Application registered with MPLS LSD and is recovering after recently restarting. In this state, the RecoveryTime value indicates how many seconds are left before the application becomes active. **Zombie** Application not reregistered after an unexpected termination. In this case, RecoveryTime indicates how many seconds are left before MPLS LSD gives up on the application.
RecoveryTime	Seconds remaining before MPLS LSD gives up or resumes the application.
Node	Node expressed in standard *rack*/*slot*/*module* notation.

Related Commands

Command	Description
show mpls lsd clients, on page 132	Displays MPLS clients connected to the MPLS LSD server.

show mpls lsd clients

To display the MPLS clients connected to the MPLS Label Switching Database (LSD) server, use the **show mpls lsd clients** command in EXEC mode.

show mpls lsd clients

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

MPLS clients include Traffic Engineering (TE) Control, TE Link Management, Label Distribution Protocol (LDP), and Bulk Content Downloader (BCDL) Agent. Not all clients are applications (see the **show mpls lsd applications** command), but all applications are clients.

Task ID

Task ID	Operations
mpls-te	read, write
mpls-ldp	read, write
mpls-static	read, write

Examples   The following shows a sample output from the **show mpls lsd clients** command:

```
RP/0/RP0/CPU0:router# show mpls lsd clients

 Id Services            Node
 -- ------------------- ------------
 0  BA(p=none)          0/0/CPU0
 1  A(TE-Link)          0/0/CPU0
 2  A(LDP)              0/0/CPU0
```

```
   3  A(TE-Control)         0/0/CPU0
```

The following table describes the significant fields shown in the display.

Table 24: show mpls lsd clients Command Field Descriptions

Field	Description
Id	Client identification number.
Services	A(xxx) means that this client is an application and xxx is the application name, BA(yyy) means that this client is a BCDL Agent and yyy is expert data. Depending on system conditions, there can be multiple BCDL Agent clients (this is normal).
Node	Node expressed in standard rack/slot/module notation.

Related Commands

Command	Description
show mpls lsd applications	Displays MPLS applications registered with the MPLS LSD server.

show mpls traffic-eng fast-reroute database

To display the contents of the fast reroute (FRR) database, use the **show mpls traffic-eng fast-reroute database** command in EXEC mode.

show mpls traffic-eng fast-reroute database [*ip-address*] [*ip-address* /*length*] [**afi-all** { **safi-all**| **unicast**}{*ip-address* | *ip-address/length*}] [**backup-interface**] [**tunnel** *tunnel -id*] [**unresolved**] [**interface** *type interface-path-id*] [**ipv4** { **safi-all**| **unicast**}{*ip-address* | *ip-address/length*}] [**labels** *low-number high-number*] [**state** {**active** | **complete** | **partial** | **ready**}] [**role** {**head** | **midpoint**}] [**summary**] [**location** *node-id*]

Syntax Description

ip-address	(Optional) IP address of the destination network.
ip-address/*length*	(Optional) Bit combination indicating the portion of the IP address that is being used for the subnet address.
afi-all	(Optional) Returns data for all specified address family identifiers.
safi-all	(Optional) Returns data for all sub-address family identifiers.
unicast	(Optional) Returns unicast data only.
backup-interface	(Optional) Displays entries with the specified backup interface.
tunnel *tunnel-id*	(Optional) Tunnel and tunnel ID to which packets with this label are going. The **summary** suboption is available.
unresolved	(Optional) Displays entries whose backup interface has not yet been fully resolved.
interface	(Optional) Displays entries with this primary outgoing interface. The **summary** keyword is available.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
ipv4	(Optional) Displays only IPv4 data.
labels	(Optional) Displays database entries that possess in-labels assigned by this router (local labels). Specify either a starting value or a range of values. The **state** suboption is available.

state	(Optional) Filters the database according to the state of the entry:	
	active	
		FRR rewrite is in the forwarding active database (where it can be placed onto appropriate incoming packets).
	complete	
		FRR rewrite is assembled, ready or active.
	partial	
		FRR rewrite is fully created; its backup routing information is still incomplete.
	ready	
		FRR rewrite was created but is not in the forwarding active state.
role	(Optional) Displays entries associated either with the tunnel **head** or tunnel **midpoint**. The **summary** suboption is available.	
summary	(Optional) Displays summarized information about the FRR database.	
location *node-id*	(Optional) Displays hardware resource counters on the designated node.	

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

For fast reroute (FRR) information in regards to multicast label forwarding, see *Multicast Command Reference*.

If the location is specified, Fast-Reroute (FRR) entries for both Point-to-Point (P2P) and P2MP tunnels are available. If the location is not specified, only P2P tunnel entries are available.

Task ID

Task ID	Operations
mpls-te	read

Examples

The following shows a sample output from the **show mpls traffic-eng fast-reroute database** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng fast-reroute database

Tunnel head FRR information:
Tunnel      Out intf/label    FRR intf/label   Status
----------  ----------------  ---------------- -------
tt4000       PO0/3/0/0:34      tt1000:34        Ready
tt4001       PO0/3/0/0:35      tt1001:35        Ready
tt4002       PO0/3/0/0:36      tt1001:36        Ready
```

Note   The Prefix field indicates the IP address where packets with this label are headed.

The following sample output displays filtering of the FRR database using the **backup-interface** keyword:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng fast database backup-interface

LSP midpoint FRR information:
LSP Identifier                  Out Intf/       FRR Intf/        Status
                                Label           Label
------------------------------  --------------- ---------------- -------
10.10.10.10 1006 [54]           Gi0/6/5/2:Pop   tt1060:Pop       Ready
```

The following sample output displays the FRR database filtered by the primary outgoing interface:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng fast-reroute database interface pos0/3/0/0

  Tunnel head FRR information:
  Tunnel      Out intf/label    FRR intf/label   Status
  ----------  ----------------  ---------------- -------
  tt4000       PO0/3/0/0:34      tt1000:34        Ready
  tt4001       PO0/3/0/0:35      tt1001:35        Ready
  tt4002       PO0/3/0/0:36      tt1001:36        Ready
```

The following sample output displays a summary of the FRR database with the role as head:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng fast-reroute database role head summary

  Status     Count
  ---------- ----------
  Active     0
  Ready      3
  Partial    0
```

The following sample output displays summarized information for the FRR database with the role as midpoint:

```
RP/0/RP0/CPU0:routerr# show mpls traffic-eng fast-reroute database role midpoint summary

  Status     Count
  -------    -----
  Active     0
  Ready      2
```

```
Partial    0
```

This table describes the significant fields shown in the display.

Table 25: show mpls traffic-eng fast-reroute database Command Field Descriptions

Field	Description
Tunnel	Short form of tunnel interface name.
Out intf/label	**Out interface** Short name of the physical interface through which traffic goes to the protected link. **Out label** At a tunnel head, this is the label that the tunnel destination device advertises. The value "Unlabeled" indicates that no such label is advertised. At a tunnel midpoint, this is the label selected by the next hop device. The value "Pop Label" indicates that the next hop is the final hop for the tunnel.
FRR intf/label	**Fast reroute interface** Backup tunnel interface. **Fast reroute label** At a tunnel head, this is the label that the tunnel tail selected to indicate the destination network. The value "Unlabeled" indicates that no label is advertised. At a tunnel midpoint, this has the same value as the Out label.

Field	Description
Status	State of the rewrite: partial, ready, or active.

Related Commands

Command	Description
show mpls traffic-eng fast-reroute log, on page 139	Displays the contents of the FRR event log.

show mpls traffic-eng fast-reroute log

To display a history of fast reroute (FRR) events, use the **show mpls traffic-eng fast-reroute log** command in EXEC mode.

show mpls traffic-eng fast-reroute log [**interface***typeinterface-path-id* | **location** *node-id*]

Syntax Description

interface	(Optional) Displays all FRR events for the selected protected interface.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface.
	Note Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router.
	For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	(Optional) Displays all FRR events that occurred on the selected node.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	Sample output was modified.
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read

Examples   The following shows a sample output from the **show mpls traffic-eng fast-reroute log** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng fast-reroute log

 Node     Protected LSPs  Rewrites When                  Switching Time
          Interface                                           (usec)
 -------- --------- ----- -------- --------------------- --------------
 0/0/CPU0 PO0/1/0/1 1     1        Feb 27 19:12:29.064000     147
```

This table describes the significant fields shown in the display.

Table 26: show mpls traffic-eng fast-reroute log Field Descriptions

Field	Description
Node	Node address.
Protected Interface	Type and interface-path-id that is being protected.
LSPs	LSP[16] associated with each interface being protected.
Rewrites	Number of rewrites initiated on the LSP.
When	Date the interface was protected.
Switching Time	Time required to switch the protected interface in microseconds.

[16] LSP = Link-state Packet.

Related Commands

Command	Description
show mpls traffic-eng fast-reroute database, on page 134	Displays the contents of the FRR database.

MPLS Traffic Engineering Commands

This module describes the commands used to configure Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) on .

Your network must support the following Cisco features before you can enable MPLS-TE:

- MPLS

- IP Cisco Express Forwarding (CEF)

- Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF) routing protocol

- Resource Reservation Protocol (RSVP)

MPLS Label Distribution Protocol (LDP), Resource Reservation Protocol (RSVP), and Universal Control Plane (UCP) command descriptions are documented separately.

For detailed information about MPLS concepts, configuration tasks, and examples, see .

adjustment-threshold (MPLS-TE)

To configure the tunnel bandwidth change threshold to trigger an adjustment, use the **adjustment-threshold** command in MPLS-TE automatic bandwidth interface configuration mode. To disable this feature, use the **no** form of this command.

adjustment-threshold *percentage* [**min** *minimum bandwidth*]

no adjustment-threshold *percentage* [**min** *minimum bandwidth*]

Syntax Description

percentage	Bandwidth change percent threshold to trigger an adjustment if the largest sample percentage is higher or lower than the current tunnel bandwidth. The range is from 1 to 100. The default is 5.
min *minimum bandwidth*	(Optional) Configures the bandwidth change value to trigger an adjustment. The tunnel bandwidth is changed only if the largest sample is higher or lower than the current tunnel bandwidth, in kbps. The range is from 10 to 4294967295. The default is 10.

Command Default

percentage: 5

minimum bandwidth: 10

Command Modes

MPLS-TE automatic bandwidth interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If you configure or modify the adjustment threshold while the automatic bandwidth is already running, the next band-aids application is impacted for that tunnel. The new adjustment threshold determines if an actual bandwidth takes place.

Examples

The following example configures the tunnel bandwidth change threshold to trigger an adjustment:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# auto-bw
```

```
RP/0/RP0/CPU0:router(config-if-tunte-autobw)# adjustment-threshold 20 min 500
```

Related Commands

Command	Description
application (MPLS-TE), on page 156	Configures the application frequency, in minutes, for the applicable tunnel.
auto-bw (MPLS-TE), on page 166	Configures automatic bandwidth on a tunnel interface and enters MPLS-TE automatic bandwidth interface configuration mode.
bw-limit (MPLS-TE), on page 181	Configures the minimum and maximum automatic bandwidth to set on a tunnel.
collect-bw-only (MPLS-TE), on page 198	Enables only the bandwidth collection without adjusting the automatic bandwidth.
overflow threshold (MPLS-TE), on page 265	Configures tunnel overflow detection.
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.

admin-weight

To override the Interior Gateway Protocol (IGP) administrative weight (cost) of the link, use the **admin-weight** command in MPLS-TE interface configuration mode. To return to the default behavior, use the **no** form of this command.

admin-weight *weight*

no admin-weight *weight*

Syntax Description

weight	Administrative weight (cost) of the link. Range is 0 to 4294967295.

Command Default

weight: IGP Weight (default OSPF 1, ISIS 10)

Command Modes

MPLS-TE interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

To use MPLS the **admin-weight** command for MPLS LSP path computations, path-selection metric must be configured to TE.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to override the IGP cost of the link and set the cost to 20:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# interface POS 0/7/0/0
RP/0/RP0/CPU0:router(config-mpls-te-if)# admin-weight 20
```

Related Commands

Command	Description
interface (MPLS-TE), on page 231	Enables MPLS-TE on an interface and enters MPLS-TE interface configuration mode.
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.
path-selection metric (interface), on page 280	Specifies an MPLS-TE tunnel path-selection metric type.

affinity

To configure an affinity (the properties the tunnel requires in its links) for an MPLS-TE tunnel, use the **affinity** command in interface configuration mode. To disable this behavior, use the **no** form of this command.

affinity {*affinity-value* **mask** *mask-value* | **exclude** *name* | **exclude-all** | **include** *name* | **include-strict** *name*}

no affinity {*affinity-value* **mask** *mask-value* | **exclude** *name* | **exclude-all** | **include** *name* | **include-strict** *name*}

Syntax Description

affinity-value	Attribute values that are required for links to carry this tunnel. A 32-bit decimal number. Range is from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.
mask *mask-value*	Checks the link attribute. A 32-bit decimal number. Range is 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute mask is 0 or 1.
exclude *name*	Configures a particular affinity to exclude.
exclude-all	Excludes all affinities.
include *name*	Configures the affinity to include in the loose sense.
include-strict *name*	Configures the affinity to include in the strict sense.

Command Default

affinity-value: 0X00000000

mask-value: 0x0000FFFF

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Affinity determines the link attributes of the tunnel (that is, the attributes for which the tunnel has an affinity). The attribute mask determines which link attribute the router should check. If a bit in the mask is 0, the attribute

value of a link or that bit is irrelevant. If a bit in the mask is 1, the attribute value of that link and the required affinity of the tunnel for that bit must match.

A tunnel can use a link if the tunnel affinity equals the link attributes and the tunnel affinity mask.

Any properties set to 1 in the affinity should be 1 in the mask. The affinity and mask should be set as follows:

```
tunnel_affinity=tunnel_affinity and tunnel_affinity_mask
```

You can configure up to 16 affinity constraints under a given tunnel. These constraints are used to configure affinity constraints for the tunnel:

Include constraint

Specifies that a link is considered for CSPF if it contains all affinities associated with the include constraint. An acceptable link contains more affinity attributes than those associated with the include statement. You can have multiple include statements under a tunnel configuration.

Include-strict constraint

Specifies that a link is considered for CSPF if it contains only the colors associated with the include-strict statement. The link cannot have any additional colors. In addition, a link without a color is rejected.

Exclude constraint

Specifies that a link satisfies an exclude constraint if it does not have all the colors associated with the constraint. In addition, a link that does not have any attribute satisfies an exclude constraint.

Exclude-all constraint

Specifies that only the links without any attribute are considered for CSPF. An exclude-all constraint is not associated with any color; whereas, all other constraint types are associated with up to 10 colors.

You set one bit for each color; however, the sample output shows multiple bits at the same time. For example, you can configure red and black colors on GigabitEthernet0/4/1/3 from the **interface** command. The sample output from the show mpls traffic-eng link-management interfaces, on page 348 command shows that the Attributes field is set to 0x21, which means that there are 0x20 and 0x1 bits on the link.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

This example shows how to configure the tunnel affinity and mask:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# affinity 0101 mask 303
```

This example shows that a link is eligible for CSPF if the color is red.. The link can have any additional colors.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# affinity include red
```

This example shows that a link is eligible for CSPF if it has at least red and black colors. The link can have any additional colors.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# affinity include red black
```

This sample output shows that the include constraint from the **show mpls traffic-eng tunnels** command is 0x20 and 0x1:

```
Name: tunnel-te1 Destination: 0.0.0.0
    Status:
      Admin:    up Oper: down   Path: not valid   Signalling: Down
      G-PID: 0x0800 (internally specified)

    Config Parameters:
      Bandwidth:        0 kbps (CT0) Priority:  7  7
      Number of configured name based affinity constraints: 1
      Name based affinity constraints in use:
      Include bit map       : 0x21
      Metric Type: TE (default)
      AutoRoute:  disabled  LockDown: disabled
      Loadshare:         0 equal loadshares
      Auto-bw: disabled(0/0) 0  Bandwidth Requested:       0
      Direction: unidirectional
      Endpoint switching capability: unknown, encoding type: unassigned
      Transit switching capability: unknown, encoding type: unassigned

    Reason for the tunnel being down: No destination is configured
    History:
```

This example shows that a tunnel can go over a link that contains red or black affinity. A link is eligible for CSPF if it has a red color or a black color. Thus, a link with red and any other colors and a link with black and other additional colors must meet the constraint.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# affinity include red
RP/0/RP0/CPU0:router(config-if)# affinity include black
```

This sample output shows that the include constraint from the **show mpls traffic-eng tunnels** command is 0x20 or 0x1:

```
Name: tunnel-te1 Destination: 0.0.0.0
    Status:
      Admin:    up Oper: down   Path: not valid   Signalling: Down
      G-PID: 0x0800 (internally specified)

    Config Parameters:
      Bandwidth:        0 kbps (CT0) Priority:  7  7
      Number of configured name based affinity constraints: 2
      Name based affinity constraints in use:
        Include bit map       : 0x1
        Include bit map       : 0x20
      Metric Type: TE (default)
      AutoRoute:  disabled  LockDown: disabled
      Loadshare:         0 equal loadshares
      Auto-bw: disabled(0/0) 0  Bandwidth Requested:       0
      Direction: unidirectional
      Endpoint switching capability: unknown, encoding type: unassigned
      Transit switching capability: unknown, encoding type: unassigned

    Reason for the tunnel being down: No destination is configured
    History:
```

This example shows that a link is eligible for CSPF if it has only red color. The link must not have any additional colors.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# affinity include-strict red
```

This example shows that a link is eligible for CSPF if it does not have the red attribute:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# affinity exclude red
```

This example shows that a link is eligible for CSPF if it does not have red and blue attributes. Thus, a link that has only a red attribute or only a blue attribute is eligible for CSPF.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# affinity exclude red blue
```

This example shows that a link is eligible for CSPF if it does not have either a red or a blue attribute:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# affinity exclude red
RP/0/RP0/CPU0:router(config-if)# affinity exclude blue
```

Related Commands

Command	Description
affinity-map, on page 154	Assigns a numerical value to each affinity name.
attribute-names, on page 160	Configures attribute names for the interface.
interface tunnel-te, on page 235	Configures an MPLS-TE tunnel interface.
show mpls traffic-eng affinity-map, on page 307	Displays the color name-to-value mappings configured on the router.
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.

affinity-map

To assign a numerical value to each affinity name, use the **affinity-map** command in MPLS-TE configuration mode. To return to the default behavior, use the **no** form of this command.

affinity-map *affinity name* {*affinity value*| **bit-position** *value*}

no affinity-map *affinity name* {*affinity value*| **bit-position** *value*}

Syntax Description

affinity name	Affinity map name-to-value designator (in hexadecimal, *0-ffffffff*).
affinity value	Affinity map value designator. Range is from 1 to 80000000.
bit-position	Configures the value of an affinity map for the bit position of the 32-bit number.
value	Bit position value. Range is from 0 to 31.

Command Default No default behavior or values

Command Modes MPLS-TE configuration

Command History

Release	Modification
Release 3.9.0	The following command syntax was enhanced: • The *affinity value* argument range was changed to 1 to 80000000. • The **bit-position** keyword and *value* argument were added. • Sample output was added to show how to configure the value for the bit position.
Release 5.0.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note The name-to-value mapping must represent a single bit of a 32-bit value.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to assign a numerical value to each affinity name:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# affinity-map red 1
RP/0/RP0/CPU0:router(config-mpls-te)# affinity-map blue 2
```

The following example shows how to configure the value of 15 for an affinity map by bit position:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# affinity-map red2 bit-position 15
```

Related Commands

Command	Description
affinity, on page 150	Configures affinity (the properties that the tunnel requires in its links) for an MPLS-TE tunnel.
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.
show mpls traffic-eng affinity-map, on page 307	Displays the color name-to-value mappings configured on the router.

application (MPLS-TE)

To configure the application frequency, in minutes, for the applicable tunnel, use the **application** command in MPLS-TE automatic bandwidth interface configuration mode. To disable this feature, use the **no** form of this command.

application *minutes*

no application *minutes*

Syntax Description

minutes	Frequency, in minutes, for the automatic bandwidth application. The range is from 5 to 10080 (7 days). The default is 1440.

Command Default

minutes : 1440 (24 hours)

Command Modes

MPLS-TE automatic bandwidth interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If you configure and modify the application frequency, the application period can reset and restart for that tunnel. The next bandwidth application for the tunnel happens within the specified minutes.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to configure application frequency to 1000 minutes for MPLS-TE interface 1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# auto-bw
RP/0/RP0/CPU0:router(config-if-tunte-autobw)# application 1000
```

Related Commands

Command	Description
adjustment-threshold (MPLS-TE), on page 146	Configures the tunnel-bandwidth change threshold to trigger an adjustment.
auto-bw (MPLS-TE), on page 166	Configures automatic bandwidth on a tunnel interface and enters MPLS-TE automatic bandwidth configuration mode.
bw-limit (MPLS-TE), on page 181	Configures the minimum and maximum automatic bandwidth to set on a tunnel.
collect-bw-only (MPLS-TE), on page 198	Enables only the bandwidth collection without adjusting the automatic bandwidth.
interface tunnel-te, on page 235	Configures an MPLS-TE tunnel interface.
overflow threshold (MPLS-TE), on page 265	Configures tunnel overflow detection.
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.

attribute-flags

To configure attribute flags for an interface, use the **attribute-flags** command in MPLS-TE interface configuration mode. To return to the default behavior, use the **no** form of this command.

attribute-flags *attribute-flags*

no attribute-flags *attribute-flags*

Syntax Description

attribute -flags	Links attributes that are compared to the affinity bits of a tunnel during selection of a path. Range is 0x0 to 0xFFFFFFFF, representing 32 attributes (bits) where the value of an attribute is 0 or 1.

Command Default

attributes : 0x0

Command Modes

MPLS-TE interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **attribute-flags** command assigns attributes to a link so that tunnels with matching attributes (represented by their affinity bits) prefer this link instead of others that do not match.

The interface attribute is flooded globally so that it can be used as a tunnel headend path selection criterion.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to set attribute flags to 0x0101:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# interface POS 0/7/0/0
RP/0/RP0/CPU0:router(config-mpls-te-if)# attribute-flags 0x0101
```

Related Commands

Command	Description
admin-weight, on page 148	Overrides the IGP administrative weight of the link.
affinity, on page 150	Configures affinity (the properties that the tunnel requires in its links) for an MPLS-TE tunnel.
attribute-names, on page 160	Configures the attribute names for the interface.
interface (MPLS-TE), on page 231	Enables MPLS-TE on an interface and enters MPLS-TE interface configuration mode.
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.

attribute-names

To configure attributes for the interface, use the **attribute-names** command in MPLS-TE interface configuration mode. To return to the default behavior, use the **no** form of this command.

attribute-names *attribute name*

no attribute-names *attribute name*

Syntax Description

attribute name	Attribute name expressed using alphanumeric or hexidecimal characters.

Command Default   No default behavior or values

Command Modes   MPLS-TE interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note   The name-to-value mapping must represent a single bit of a 32-bit value.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to assign an attribute name (in this case, red) to a TE link:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# interface pos 0/2/0/1
RP/0/RP0/CPU0:router(config-mpls-te-if)# attribute-name red
```

Related Commands

Command	Description
affinity, on page 150	Configures affinity (the properties that the tunnel requires in its links) for an MPLS-TE tunnel.
attribute-flags, on page 158	Configures attribute flags for the interface.
interface (MPLS-TE), on page 231	Enables MPLS-TE on an interface and enters MPLS-TE interface configuration mode.
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.

attribute-set

To configure attribute-set for auto-mesh tunnels, use the **attribute-set** command in MPLS-TE configuration mode.

attribute-set auto-mesh *attribute-set-name* {**affinity** {*affinity-value* **mask** *mask-value*| **exclude** *name*| **exclude-all**| **include** *name*| **include-strict** *name*}| **auto-bw collect-bw-only**| **autoroute announce**| **bandwidth** *bandwidth*| **fast-reroute** [**protect** {**bandwidth node**| **node bandwidth**}]| **logging events lsp-status** {**insufficient-bandwidth**| **reoptimize**| **reroute**| **state**}| **priority** *setup-range hold-range*| **record-route**| **signalled-bandwidth** *bandwidth* [**class-type** *cl*]| **soft-preemption**}

To configure attribute-set for a path-option, use the **attribute-set** command in MPLS-TE configuration mode.

attribute-set path-option *attribute-set-name* {**affinity** {*affinity-value* **mask** *mask-value*| **exclude** *name*| **exclude-all**| **include** *name*| **include-strict** *name*}| **signalled-bandwidth** *bandwidth* [**class-type** *cl*]}

To disable this behavior, use the **no** form of this command.

no attribute-set

Syntax Description

auto-mesh	Specifies the values of an attribute set for the auto-mesh group.
path-option	Specifies the values of an attribute set for the path option.
attribute-set-name	A 32-bit character string, specifies the name of the attribute-set template.
affinity-value	Attribute values that are required for links to carry this tunnel. A 32-bit decimal number, representing 32 attributes (bits), where the value of an attribute is 0 or 1. Range is from 0x0 to 0xFFFF.
mask *mask-value*	Checks the link attribute. A 32-bit decimal number, representing 32 attributes (bits), where the value of an attribute mask is 0 or 1. Range is from 0x0 to 0xFFFF.
exclude *name*	Configures a specific affinity that is to be excluded.
exclude-all	Excludes all affinities.
include *name*	Configures the affinity to include in the loose sense.
include-strict *name*	Configures the affinity to include in the strict sense.

logging	Per-interface logging configuration.
events	Per-interface logging events.
lsp-status	Enables interface LSP state change alarms.
reoptimize	Enables interface LSP REOPT change alarms.
state	Enables interface LSP UP/DOWN change alarms.
priority	Specifies the tunnel priority.
setup-range	Specifies setup priority. Range is 0 to 7.
hold-range	Specifies hold priority. Range is 0 to 7.
record-route	Records the route used by the tunnel.
signalled-bandwidth	Specifies the tunnel bandwidth requirement to be signalled.
bandwidth	Bandwidth required for an MPLS-TE tunnel, specified in kilobits per second. By default, bandwidth is reserved in the global pool. Range is from 0 to 4294967295.
class-type *ct*	(Optional) Configures the class type of the tunnel bandwidth request. Range is 0 to 1. Class-type 0 is equivalent to global-pool. Class-type 1 is equivalent to subpool.
soft-preemption	Enables the soft-preemption feature on this tunnel.

Command Default

affinity-value: 0x0

mask-value: 0xFFFF

Command Modes

MPLS TE configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced. The **sub-pool** keyword is not supported.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The values specified for an attribute within a **path-option attribute-set** does not prevent the configuration of the same attribute at the tunnel level. However, only one level is taken into consideration. The configuration at the **path-option** level is considered more specific than the one at the level of the tunnel, and is therefore used.

Attributes that are **not** specified within an **attribute-set** picks their default values, as usual, from the configuration at the tunnel level, the configuration at the global mpls level, or default values.

An XRO attribute-set can be specified as part of the path-option, if required. An empty XRO attribute set results in the GMPLS tunnel being signaled with no exclusions, and therefore no XRO.

Task ID

Task ID	Operation
mpls-te	read, write

Examples

This example shows how to configure an attribute-set to a TE interface for an auto-mesh tunnel:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)#  mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)#  auto-tunnel mesh
RP/0/RP0/CPU0:router(config-te-auto-mesh)#  group 1
RP/0/RP0/CPU0:router(config-te-mesh-group)#  attribute-set am1
RP/0/RP0/CPU0:router(config-te-mesh-group)#  destination-list dl1
```

This example shows how to configure the tunnel affinity and signalled-bandwidth for a path-option:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)#  mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)#  attribute-set path-option myset
RP/0/RP0/CPU0:router(config-te-attribute-set)# affinity 0x3 mask 0x3
RP/0/RP0/CPU0:router(config-te-attribute-set)# signalled-bandwidth 2000
```

Related Commands

Command	Description
affinity-map, on page 154	Assigns a numerical value to each affinity name.
attribute-names, on page 160	Configures attribute names for the interface.
interface tunnel-te, on page 235	Configures an MPLS-TE tunnel interface.
show mpls traffic-eng affinity-map, on page 307	Displays the color name-to-value mappings configured on the router.

Command	Description
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.

auto-bw (MPLS-TE)

To configure automatic bandwidth on a tunnel interface and to enter MPLS-TE automatic bandwidth interface configuration mode, use the **auto-bw** command in MPLS-TE interface configuration mode. To disable the automatic bandwidth on that tunnel, use the **no** form of this command.

auto-bw

no auto-bw

Syntax Description   This command has no arguments or keywords.

Command Default   By default, automatic bandwidth is not enabled.

Command Modes   MPLS-TE interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **auto-bw** command to enter MPLS-TE automatic bandwidth interface configuration mode.

The **auto-bw** and **load-share unequal** commands should not be used together.

The **load-share unequal**command determines the load-share for a tunnel based on the bandwidth. However, the MPLS-TE automatic bandwidth feature changes the bandwidth around. If you are configuring both the **load-share unequal** command and the MPLS-TE automatic bandwidth feature, we recommend that you specify an explicit load-share value configuration under each MPLS-TE automatic bandwidth tunnel.

The following automatic bandwidth scenarios are described:

- If you configure the automatic bandwidth on a tunnel, the automatic bandwidth is enabled on that tunnel. If no other configuration is specified, defaults for the various parameters are used, the operation stops.

- The automatic operation (for example, output rate collection) starts as soon as the automatic bandwidth is enabled on one tunnel. If automatic bandwidth is disabled from all tunnels, the operation stops.

- If the output rate collection is already active when the automatic bandwidth is configured on a tunnel, the statistics collection for that tunnel starts at the next collection configuration.

✎

| **Note** | Because the collection timer is already running, the first collection event for that tunnel happens in less than C minutes (for example, on an average of C/2 minutes). |

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to enter MPLS-TE automatic bandwidth interface configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# auto-bw
RP/0/RP0/CPU0:router(config-if-tunte-autobw)#
```

Related Commands

Command	Description
adjustment-threshold (MPLS-TE), on page 146	Configures the tunnel-bandwidth change threshold to trigger an adjustment.
application (MPLS-TE), on page 156	Configures the application frequency, in minutes, for the applicable tunnel.
bw-limit (MPLS-TE), on page 181	Configures the minimum and maximum automatic bandwidth to set on a tunnel.
collect-bw-only (MPLS-TE), on page 198	Enables only the bandwidth collection without adjusting the automatic bandwidth.
interface tunnel-te, on page 235	Configures an MPLS-TE tunnel interface.
overflow threshold (MPLS-TE), on page 265	Configures tunnel overflow detection.
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.

auto-bw collect frequency (MPLS-TE)

To configure the automatic bandwidth collection frequency, use the **auto-bw collect frequency** command in MPLS-TE configuration mode. To reset the automatic bandwidth frequency to its default value, use the **no** form of this command.

auto-bw collect frequency *minutes*

no auto-bw collect frequency *minutes*

Syntax Description

minutes	Interval between automatic bandwidth adjustments, in minutes. The range is from 1 to 10080. The default is 5.

Command Default

minutes: 5

In addition, the **no** form of this command resets to the default.

Command Modes

MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **auto-bw collect frequency** command configures the automatic bandwidth collection frequency for all the tunnels.

Modifying the global collection frequency does not restart the tunnel for the current application period. The application period continues with the modified collection frequency.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example configures a tunnel for an automatic bandwidth adjustment of 100 minutes:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
```

```
RP/0/RP0/CPU0:router(config-mpls-te)# auto-bw collect frequency 100
```

Related Commands

Command	Description
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.
mpls traffic-eng auto-bw apply (MPLS-TE), on page 247	Configures the highest bandwidth available on a tunnel without waiting for the current application period to end.
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.

autoroute announce

To specify that the Interior Gateway Protocol (IGP) should use the tunnel (if the tunnel is up) in its enhanced shortest path first (SPF) calculation, use the **autoroute announce** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

autoroute announce

no autoroute announce

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values

Command Modes   Interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Currently, the only way to forward traffic over a tunnel is to use the **autoroute announce** or **static routes** commands.

When you configure more than one IGP, the tunnel is announced to the IGP used to find the path to the tunnel destination.

By default, the route metric of the tunnel path to the destination equals the route metric of the shortest IGP path to that destination when the **autoroute announce** command is configured.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   This example shows how to configure IGP to use the tunnel in its enhanced SPF calculation when the tunnel is up:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
```

```
RP/0/RP0/CPU0:router(config-if)# autoroute announce
```

Related Commands

Command	Description
interface tunnel-te, on page 235	Configures an MPLS-TE tunnel interface.

autoroute metric

To specify the MPLS-TE tunnel metric that the Interior Gateway Protocol (IGP) enhanced Shortest Path First (SPF) calculation uses, use the **autoroute metric** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

autoroute metric {**absolute**| **relative**} *value*

no autoroute metric {**absolute**| **relative**} *value*

Syntax Description

absolute	Displays the absolute metric mode; you can enter a positive metric value.
relative	Displays the relative metric mode; you can enter a positive, negative, or zero value.
value	Metric that the IGP enhanced SPF calculation uses. Relative value range is −10 to 10. Absolute value is 1 to 2147483647.

Command Default

relative *value* : 0

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.9.0	The absolute value range is from 1 to 2147483647.
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **autoroute metric** command overwrites the default tunnel route metric of the shortest IGP path to the destination.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to configure the IGP enhanced SPF calculation using MPLS-TE tunnel metric as relative negative 1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# autoroute metric relative -1
```

Related Commands

Command	Description
autoroute announce, on page 170	Instructs the IGP to use the tunnel (if it is up) in its enhanced SPF calculation.
interface tunnel-te, on page 235	Configures an MPLS-TE tunnel interface.
show mpls traffic-eng autoroute, on page 311	Displays the tunnels announced to the IGP, including interface, destination, and bandwidth.

auto-tunnel backup (MPLS-TE)

To automatically build next-hop (NHOP) and next-next-hop (NNHOP) backup tunnels, and to enter auto-tunnel backup configuration mode, use the **auto-tunnel backup** command in MPLS-TE configuration mode. To clear the NHOP and NNHOP backup tunnels, use the **no** form of this command.

auto-tunnel backup

no auto-tunnel backup

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values

Command Modes MPLS-TE configuration

Command History

Release	Modification
Release 4.0.0	This command was introduced.
Release 5.0.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The range of *tunnel-ID* is required to be mentioned for the auto-tunnel backup tunnels; otherwise, none of the tunnels are created.

The **no** form of this command deletes both NHOP and NNHOP backup tunnels that are configured using either the **auto-tunnel backup** command or the **nhop-only** command.

Task ID

Task ID	Operation
mpls-te	read, write

Examples The following example automatically builds NHOP and NNHOP backup tunnels:

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# auto-tunnel backup
```

Related Commands

Command	Description
clear mpls traffic-eng auto-tunnel backup unused, on page 185	Clears the unused automatic backup tunnels.
mpls traffic-eng *interface-path-id* auto-tunnel backup	Configures the automatic backup tunnel for a specific interface.
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.
tunnel-id (auto-tunnel backup), on page 423	Configures range of tunnel interface numbers for automatic backup tunnels.

backup-bw

To configure the backup bandwidth for an MPLS-TE backup tunnel (that is used to protect a physical interface), use the **backup-bw** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

backup-bw {*backup bandwidth* {**any-class-type**| **class-type ct**}| **global-pool** {*bandwidth*| **unlimited**}| **sub-pool** {*bandwidth*| **unlimited**}| **unlimited** {**any-class-type**| **class-type ct**}}

no backup-bw {*backup bandwidth* {**any-class-type**| **class-type ct**}| **global-pool** {*bandwidth*| **unlimited**}| **sub-pool** {*bandwidth*| **unlimited**}| **unlimited** {**any-class-type**| **class-type ct**}}

Syntax Description

backup bandwidth	Backup bandwidth in any-pool provided by an MPLS-TE backup tunnel. Bandwidth is specified in kilobits per second (kbps). Range is 1 to 4294967295.
any-class-type	Displays the backup bandwidth assigned to any class-type protected tunnels.
class-type ct	Displays the class type of the backup bandwidth. Range is 0 to 1.
global-pool *bandwidth*	(In Prestandard DS-TE with RDM) Displays the backup bandwidth in global pool provided by an MPLS-TE backup tunnel. Bandwidth is specified in kilobits per second. Range is 1 to 4294967295.
unlimited	Displays the unlimited bandwidth.
sub-pool *bandwidth*	(In Prestandard DS-TE with RDM) Displays the backup bandwidth in sub-pool provided by an MPLS-TE backup tunnel. Bandwidth is specified in kilobits per second. Range bandwidth is 1 to 4294967295. Only label switched paths (LSPs) using bandwidth from the sub-pool can use the backup tunnel.

Command Default   Any class-type unlimited.

Command Modes   Interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Backup bandwidth can be limited or unlimited or specific to a global pool, sub-pool, or non-specific any-pool. Backup with backup-bw in global-pool protects global-pool LSPs only; backup-bw in sub-pool protects sub-pool LSPs only.

Backup tunnels configured with limited backup bandwidth (from any/global/sub pool) are not assigned to protect LSPs configured with zero signaled bandwidth.

Backup bandwidth provides bandwidth protection for fast reroute (FRR). Bandwidth protection for FRR supports DiffServ-TE with two bandwidth pools (class-types).

Class-type 0 is strictly equivalent to global-pool; class-type 1 is strictly equivalent to sub-pool bandwidth using the Russian Doll Model (RDM).

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to configure backup tunnel 1 for use only by LSPs that take their bandwidth from the global pool (class-type 0 tunnels). Backup tunnel 1 does not provide bandwidth protection.

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# backup-bw global-pool unlimited
```

or

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# backup-bw unlimited class-type 0
```

In the following example, backup tunnel 2 is used by LSPs that take their bandwidth from the sub-pool (class-type 1 tunnels) only. Backup tunnel 2 provides bandwidth protection for up to 1000 units.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 2
RP/0/RP0/CPU0:router(config-if)# backup-bw sub-pool 1000
```

or

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 2
RP/0/RP0/CPU0:router(config-if)# backup-bw 1000 class-type 1
```

Related Commands

Commands	Description
backup-path tunnel-te, on page 179	Assigns one or more backup tunnels to a protected interface.
fast-reroute, on page 215	Enables FRR protection for an MPLS-TE tunnel.
interface tunnel-te, on page 235	Configures an MPLS-TE tunnel interface.

backup-path tunnel-te

To set an MPLS-TE tunnel to protect a physical interface against failure, use the **backup-path tunnel-te** command in MPLS-TE interface configuration mode. To return to the default behavior, use the **no** form of this command.

backup-path tunnel-te *tunnel-number*

no backup-path tunnel-te *tunnel-number*

Syntax Description

tunnel-number	Number of the tunnel protecting the interface. Range is 0 to 65535.

Command Default

No default behavior or values

Command Modes

MPLS-TE interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When the protected interface is down (shut down or removed), the traffic it was carrying (for the other label switched paths [LSPs], referred to as the protected LSPs) is rerouted, using fast reroute (FRR) onto the backup tunnels.

The following guidelines pertain to the FRR process:

- Multiple (backup) tunnels can protect the same interface by entering this command multiple times for different tunnels. The same (backup) tunnel can protect multiple interfaces by entering this command for each interface.

- The backup tunnel used to protect a physical interface must have a valid IP address configured.

- The backup tunnel cannot pass through the same interface that it is protecting.

- TE tunnels that are configured with the FRR option, cannot be used as backup tunnels.

- For the backup tunnel to provide protection to the protected LSP, the backup tunnel must have a terminating-end node in the path of a protected LSP.

- The source IP address of the backup tunnel and the merge point (MP) address (the terminating-end address of the backup tunnel) must be reachable.

> **Note**   You must configure record-route on TE tunnels that are protected by multiple backup tunnels merging at a single node.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to protect PoS interface 0/7/0/0 using tunnel 100 and tunnel 150:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# interface POS 0/7/0/0
RP/0/RP0/CPU0:router(config-mpls-te-if)# backup-path tunnel-te 100
RP/0/RP0/CPU0:router(config-mpls-te-if)# backup-path tunnel-te 150
```

Related Commands

Command	Description
backup-bw, on page 176	Configures backup bandwidth for bandwidth protection.
fast-reroute, on page 215	Enables FRR protection for an MPLS-TE tunnel.
interface (MPLS-TE), on page 231	Enables MPLS-TE on an interface and enters MPLS-TE interface configuration mode.
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.

bw-limit (MPLS-TE)

To configure the minimum and maximum automatic bandwidth to be set on a tunnel, use the **bw-limit** command in MPLS-TE automatic bandwidth interface configuration mode. To disable this feature, use the **no** form of this command.

bw-limit min *bandwidth* {**max** *bandwidth*}

no bw-limit

Syntax Description

min *bandwidth*	Configures the minimum automatic bandwidth, in kbps, on a tunnel. The range is from 0 to 4294967295. The default is 0.
max *bandwidth*	Configures the maximum automatic bandwidth, in kbps, on a tunnel. The range is from 0 to 4294967295. The default is 4294967295.

Command Default

min: 0

max: 4294967295

Command Modes

MPLS-TE automatic bandwidth interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Both the **min** and **max** keywords must be configured.

The **bw-limit** command automatically sets the minimum bandwidth to the default value of 0, or the **bw-limit** command automatically sets the maximum to the default value of 4294967295 kbps.

If the value of the **min** keyword is greater than the **max** keyword, the **bw-limit** command is rejected. If you configure and modify the minimum or maximum bandwidth while the automatic bandwidth is already running, the next bandwidth application for that tunnel is impacted. For example, if the current tunnel requested bandwidth is 30 Mbps and the minimum bandwidth is modified to 50 Mbps, the next application sets the tunnel bandwidth to 50 Mbps.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to configure the minimum and maximum bandwidth for the tunnel:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# auto-bw
RP/0/RP0/CPU0:router(config-if-tunte-autobw)# bw-limit min 30 max 80
```

Related Commands

Command	Description
adjustment-threshold (MPLS-TE), on page 146	Configures the tunnel-bandwidth change threshold to trigger an adjustment.
application (MPLS-TE), on page 156	Configures the application frequency, in minutes, for the applicable tunnel.
auto-bw (MPLS-TE), on page 166	Configures automatic bandwidth on a tunnel interface and enters MPLS-TE automatic bandwidth interface configuration mode.
collect-bw-only (MPLS-TE), on page 198	Enables only the bandwidth collection without adjusting the automatic bandwidth.
interface tunnel-te, on page 235	Configures an MPLS-TE tunnel interface.
overflow threshold (MPLS-TE), on page 265	Configures tunnel overflow detection.
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.

clear mpls traffic-eng auto-bw (MPLS-TE EXEC)

To clear automatic bandwidth sampled output rates and to restart the application period for the specified tunnel, use the **clear mpls traffic-eng auto-bw** command in EXEC mode.

clear mpls traffic-eng auto-bw {**all** | **internal** | **tunnel-te** *tunnel-number*}

Syntax Description

all	Clears the automatic bandwidth sampled output rates for all tunnels.
internal	Clears all the automatic bandwidth internal data structures.
tunnel-te *tunnel-number*	Clears the automatic bandwidth sampled output rates for a specific tunnel. The *tunnel-number* argument is the tunnel ID used to clear the sampled output rates.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If no tunnel is specified, the **clear mpls traffic-eng auto-bw** command clears all the automatic bandwidth enabled tunnels.

For each tunnel in which the automatic bandwidth adjustment is enabled, information is maintained about the sampled output rates and the time remaining until the next bandwidth adjustment. The application period is restarted and values such as the largest collected bandwidth get reset. The tunnel continues to use the current bandwidth until the next application.

Task ID

Task ID	Operations
mpls-te	execute

Examples

The following example displays the information for the automatic bandwidth for tunnel number 0 from the **show mpls traffic-eng tunnels auto-bw brief** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels 0 auto-bw brief

  Tunnel    LSP  Last appl  Requested  Signalled   Highest    Application
            Name   ID    BW(kbps)   BW(kbps)   BW(kbps)   BW(kbps)     Time Left
  -------------- ------ ---------- ---------- ---------- ---------- --------------
    tunnel-te0   278     100        100        100        150       12m 38s
```

The following example shows how to clear the automatic bandwidth sampled output rates for tunnel number 0:

```
RP/0/RP0/CPU0:router# clear mpls traffic-eng auto-bw tunnel-te 0

RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels 0 auto-bw brief

  Tunnel    LSP  Last appl  Requested  Signalled   Highest    Application
            Name   ID    BW(kbps)   BW(kbps)   BW(kbps)   BW(kbps)     Time Left
  -------------- ------ ---------- ---------- ---------- ---------- --------------
    tunnel-te0   278     100        100        100         0        24m 0s
```

Related Commands

Command	Description
clear mpls traffic-eng counters signaling, on page 191	Clears the automatic bandwidth configuration in a tunnel.
show mpls traffic-eng tunnels auto-bw brief, on page 399	Displays the list of automatic-bandwidth-enabled tunnels, and indicates if the current signaled bandwidth of the tunnel is identical to the bandwidth that is applied by the automatic bandwidth.

clear mpls traffic-eng auto-tunnel backup unused

To remove unused automatic backup tunnels, use the **clear mpls traffic-eng auto-tunnel backup unused** command in global configuration mode.

clear mpls traffic-eng auto-tunnel backup unused {**all**| **tunnel-te** *tunnel-number*}

Syntax Description

all	Clears all the unused automatic backup tunnels.
tunnel-te *tunnel-number*	Clears a specific unused automatic backup tunnel.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **unused** auto-tunnel backup tunnel is the tunnel that is not assigned to protect any FRR tunnel.

The behavior of this command is the same as the expiration of the **timers removal unused** command in which, when the timeout value is reached, the automatic backup tunnel is removed.

Task ID

Task ID	Operation
mpls-te	execute

Examples

The following example displays the information for the unused backup automatic tunnels from the **show mpls traffic-eng tunnels unused** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels unused
```
The following example shows how to clear the unused backup automatic tunnels:

```
RP/0/RP0/CPU0:router# clear mpls traffic-eng auto-tunnel backup unused all
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels unused
```

Related Commands

Command	Description
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.

clear mpls traffic-eng auto-tunnel mesh

To clear all unused auto-tunnel mesh destinations, use the **clear mpls traffic-eng auto-tunnel mesh**command in EXEC mode.

clear mpls traffic-eng auto-tunnel mesh unused {**all**| **tunnel-te**}

Syntax Description

all	Clears all applicable unused auto-tunnel destinations.
tunnel-te *id*	Clears an unused auto-tunnel destinations identified by a tunnel identifier.

Command Default   None

Command Modes   EXEC

Command History

Release	Modification
Release 4.1.1	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	execute

Examples   This is sample output from the **clear mpls traffic-eng auto-tunnel mesh** command:

```
clear mpls traffic-eng auto-tunnel mesh
```

clear mpls traffic-eng counters auto-tunnel mesh

To clear all auto-tunnel mesh counters, use the **clear mpls traffic-eng counters auto-tunnel mesh** command in EXEC mode.

clear mpls traffic-eng counters auto-tunnel mesh

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	execute

Examples

This is sample output from the **clear mpls traffic-eng counters auto-tunnel mesh** command:

```
RP/0/RP0/CPU0:routerclear mpls traffic-eng counters auto-tunnel mesh
```

clear mpls traffic-eng counters auto-tunnel backup

To clear MPLS-TE automatic tunnel backup counters, use the **clear mpls traffic-eng counters auto-tunnel backup** command in EXEC mode.

clear mpls traffic-eng counters auto-tunnel backup

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
mpls-te	execute

Examples   The following example removes all counters for the automatic backup tunnels:

```
RP/0/RP0/CPU0:router# clear mpls traffic-eng counters auto-tunnel backup
```

Related Commands

Command	Description
show mpls traffic-eng counters auto-tunnel backup	Displays the MPLS-TE automatic tunnel backup counters.
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.

clear mpls traffic-eng counters global

To clear the internal MPLS-TE tunnel counters, use the **clear mpls traffic-eng counters global** command in EXEC mode.

clear mpls traffic-eng counters global

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	execute

Examples   The following example shows how to clear the internal MPLS-TE tunnel counters:

```
RP/0/RP0/CPU0:router# clear mpls traffic-eng counters global
```

clear mpls traffic-eng counters signaling

To clear (set to zero) the MPLS tunnel signaling counters, use the **clear mpls traffic-eng counters signaling** command in EXEC mode.

clear mpls traffic-eng counters signaling{**all**| [**heads** | **mids** | **tails**]| **name** *name* | **summary**}

Syntax Description

all	Clears counters for all MPLS-TE tunnels.
heads	(Optional) Displays tunnels with their heads at this router.
mids	(Optional) Displays tunnels with their midpoints at this router.
tails	(Optional) Displays tunnels with their tails at this router.
name *name*	Clears counters for an MPLS-TE tunnel with the specified name.
summary	Clears the counter's summary.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **clear mpls traffic-eng counters signaling** command to set all MPLS counters to zero so that changes can be seen easily.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to clear all counters:

```
RP/0/RP0/CPU0:router# clear mpls traffic-eng counters signaling all
```

Related Commands

Command	Description
show mpls traffic-eng counters signaling, on page 320	Displays tunnel signaling statistics.

clear mpls traffic-eng counters soft-preemption

To clear (set to zero) the counters for soft-preemption statistics, use the **clear mpls traffic-eng counters soft-preemption** command in EXEC mode.

clear mpls traffic-eng counters {**all**| **soft-preemption**}

Syntax Description

all	Clears counters for all MPLS-TE tunnels.
soft-preemption	Clears the statistics for soft preemption counters.

Command Default None

Command Modes EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When all counters are cleared using the **clear mpls traffic-eng counters all** command, the counters for soft-preemption statistics are automatically cleared.

Task ID

Task ID	Operations
mpls-te	execute

Examples This example shows how to clear all counters:

```
RP/0/RP0/CPU0:router# clear mpls traffic-eng counters signaling all
```

Related Commands

Command	Description
show mpls traffic-eng counters signaling, on page 320	Displays tunnel signaling statistics.

clear mpls traffic-eng fast-reroute log

To clear the log of MPLS fast reroute (FRR) events, use the **clear mpls traffic-eng fast-reroute log** command in EXEC mode.

clear mpls traffic-eng fast-reroute log

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows sample output before clearing the log of FRR events:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng fast-reroute log

  Node      Protected LSPs  Rewrites  When                    Switching Time
            Interface                                          (usec)
--------  ---------  -----  --------  ----------------------  --------------
0/0/CPU0  PO0/1/0/1  1      1         Feb 27 19:12:29.064000       147
0/1/CPU0  PO0/1/0/1  1      1         Feb 27 19:12:29.060093       165
0/2/CPU0  PO0/1/0/1  1      1         Feb 27 19:12:29.063814       129
0/3/CPU0  PO0/1/0/1  1      1         Feb 27 19:12:29.062861       128

RP/0/RP0/CPU0:router# clear mpls traffic-eng fast-reroute log
```

clear mpls traffic-eng link-management statistics

To clear all the MPLS-TE admission control statistics, use the **clear mpls traffic-eng link-management statistics** command in EXEC mode.

clear mpls traffic-eng link-management statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to clear all the MPLS-TE statistics for admission control:

```
RP/0/RP0/CPU0:router# clear mpls traffic-eng link-management statistics
```

clear mpls traffic-eng pce

To clear the path computation element (PCE) statistics, use the **clear mpls traffic-eng pce** command in EXEC mode.

clear mpls traffic-eng pce [**peer ipv4** *address*]

Syntax Description

peer	(Optional) Clears the statistics for one peer.
ipv4 *address*	(Optional) Configures the IPv4 address for PCE.

Command Default

Clears statistics for all the PCE peers.

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	execute

Examples

The following example shows how to clear the statistics for the PCE:

```
RP/0/RP0/CPU0:router# clear mpls traffic-eng pce
```

Related Commands

Command	Description
show mpls traffic-eng pce peer, on page 358	Displays the status of the PCE peer address and state.

collect-bw-only (MPLS-TE)

To configure only the bandwidth collection without adjusting the bandwidth automatically, use the **collect-bw-only** command in MPLS-TE automatic bandwidth interface configuration mode. To disable this feature, use the **no** form of this command.

collect-bw-only

no collect-bw-only

Syntax Description   This command has no arguments or keywords.

Command Default   Bandwidth collection is either enabled or disabled.

Command Modes   MPLS-TE automatic bandwidth interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If you enable the **collect-bw-only** command while the automatic bandwidth is already running on a tunnel, the bandwidth application is disabled from that moment. Before you enable the actual bandwidth application, you can get the status of the automatic bandwidth behavior.

If you disable the **collect-bw-only** command on a tunnel from which the automatic bandwidth is already running, the actual bandwidth application takes place on the tunnel at the next application period.

It is also possible to manually activate a bandwidth application regardless of the collect bandwidth only flag that is being specified on a tunnel. To activate the bandwidth application, use the mpls traffic-eng auto-bw apply (MPLS-TE), on page 247 command in EXEC mode.

Task ID

Task ID	Operations
mpls-te	read, write

Examples
The following example shows how to enable only the bandwidth collection without adjusting the automatic bandwidth:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# auto-bw
RP/0/RP0/CPU0:router(config-if-tunte-autobw)# collect-bw-only
```

Related Commands

Command	Description
adjustment-threshold (MPLS-TE), on page 146	Configures the tunnel-bandwidth change threshold to trigger an adjustment.
application (MPLS-TE), on page 156	Configures the application frequency, in minutes, for the applicable tunnel.
auto-bw (MPLS-TE), on page 166	Configures automatic bandwidth on a tunnel interface and enters MPLS-TE automatic bandwidth interface configuration mode.
bw-limit (MPLS-TE), on page 181	Configures the minimum and maximum automatic bandwidth to set on a tunnel.
interface tunnel-te, on page 235	Configures an MPLS-TE tunnel interface.
overflow threshold (MPLS-TE), on page 265	Configures tunnel overflow detection.
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.

destination (MPLS-TE)

To configure the destination address of a TE tunnel, use the **destination** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

destination *ip-address*

no destination *ip-address*

Syntax Description

ip-address	Destination address of the MPLS-TE router ID.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note

The tunnel destination address must be a unique MPLS-TE router ID; it cannot be an MPLS-TE link address on a node.

For Point-to-Point (P2P) tunnels, the **destination** command is used as a single-line command.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to set the destination address for tunnel-te1 to 10.10.10.10:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te1
RP/0/RP0/CPU0:router(config-if)# destination 10.10.10.10
```

Related Commands

Command	Description
interface tunnel-te, on page 235	Configures an MPLS-TE tunnel interface.
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.

disable (explicit-path)

To prevent the path from being used by MPLS-TE tunnels while it is configured, use the **disable** command in explicit path configuration mode. To return to the default behavior, use the **no** form of this command.

disable

no disable

Syntax Description

This command has no arguments or keywords.

Command Default

Explicit path is enabled.

Command Modes

Explicit path configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to disable explicit path 200:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# explicit-path identifier 200
RP/0/RP0/CPU0:router(config-expl-path)# disable
```

Related Commands

Command	Description
index exclude-address, on page 225	Specifies the next IP address to exclude from the explicit path.
index next-address, on page 229	Specifies path entries at a specific index.

Command	Description
show explicit-paths, on page 305	Displays the configured IP explicit paths.

disable (P2MP TE)

To disable the given destination for the Point-to-Multipoint (P2MP) tunnel interface, use the **disable** command in P2MP destination interface configuration mode. To return to the default behavior, use the **no** form of this command.

disable

no disable

Syntax Description   This command has no arguments or keywords.

Command Default   None

Command Modes   P2MP destination interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If the **disable** command is not configured, the destination is enabled.

We recommend that you disable those destinations about which you have prior knowledge. This is because those destinations do not have valid MPLS-TE paths; therefore these destinations can be excluded from the P2MP tree computation.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to disable destination 140.140.140.140:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-mte 10
RP/0/RP0/CPU0:router(config-if)# destination 140.140.140.140
RP/0/RP0/CPU0:router(config-if-p2mp-dest)# disable
```

Related Commands

Command	Description
destination (MPLS-TE), on page 200	Configures the destination address of a TE tunnel.
interface tunnel-mte	Configures an MPLS-TE P2MP tunnel interface.

ds-te bc-model

To enable a specific bandwidth constraint model (Maximum Allocation Model or Russian Doll Model) on the entire label switched router (LSR), use the **ds-te bc-model** command in MPLS-TE configuration mode. To return to the default behavior, use the **no** form of this command.

ds-te bc-model mam

no ds-te bc-model mam

Syntax Description

mam	Enables the Maximum Allocation Model (MAM) bandwidth constraints model.

Command Default

RDM is the default bandwidth constraint model.

Command Modes

MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You can configure both the MAM and RDM bandwidth values on a single interface before swapping to an alternate global MPLS-TE BC model.

If you configure bandwidth constraints without configuring the corresponding bandwidth constraint values, the router uses default bandwidth constraint values.

MAM is not supported in prestandard DS-TE mode. MAM and RDM are supported in IETF DS-TE mode; RDM is supported in prestandard DS-TE mode.

Note Changing the bandwidth constraints model affects the entire router and may have a major impact on system performance as nonzero-bandwidth tunnels are torn down.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to enable the MAM bandwidth constraints model:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# ds-te bc-model mam
```

Related Commands

Command	Description
ds-te mode, on page 208	Configures standard DS-TE mode.
ds-te te-classes, on page 210	Enters DS-TE te-class map configuration mode.
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.
show mpls traffic-eng ds-te te-class, on page 326	Displays the Diff-Serv TE-class map in use.

ds-te mode

To configure standard differentiated-service TE mode (DS-TE), use the **ds-te mode** command in MPLS-TE configuration mode. To return to the default behavior, use the **no** form of this command.

ds-te mode ietf

no ds-te mode ietf

Syntax Description

ietf	Enables IETF standard mode.

Command Default   Prestandard DS-TE is the default differentiated service mode.

Command Modes   MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The following two DS-TE modes are supported:

- Prestandard mode

   ◦ The Cisco proprietary mechanism for IGPs and RSVP signalling are used and DS-TE does not interoperate with third-party vendor equipment.

- IETF mode

   ◦ Standard defined extensions are used for IGPs and RSVP signalling and DS-TE in this mode interoperates with third-party equipment.

   ◦ IETF mode supports two bandwidth constraint models: the Russian Doll Model (RDM) and Maximum Allocation Model (MAM).

   ◦ RDM is the default model.

   ◦ Router advertises variable-length bandwidth constraints, max-reservable- bandwidth, and unreserved bandwidths in TE-classes.

   ◦ tunnels must have valid class-type and priority configured as per TE-class map in use; otherwise, tunnels remain down.

◦ TE-class map (a set of tunnel priority and class-type values) is enabled to interpret unreserved bandwidth values advertised in IGP; therefore, TE-class map must be identical on all nodes for TE tunnels to be successfully established

For DS-TE to function properly, DS-TE modes must be configured identically on all MPLS-TE nodes.

If you need to change the DS-TE mode, you must bring down all tunnel interfaces and after the change, you should flood the updated bandwidth values through the network.

> **Note** Changing the DS-TE mode affects the entire LSR and can have a major impact on system performance when tunnels are torn down.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to enable IETF standard mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# ds-te mode ietf
```

Related Commands

Command	Description
ds-te bc-model, on page 206	Enables a specific bandwidth constraint model (Maximum Allocation Model or Russian Doll Model) on the LSR.
ds-te te-classes, on page 210	Configures MPLS DS-TE TE-class maps.
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.
mpls traffic-eng fast-reroute promote, on page 249	Configures the router to assign new or more efficient backup MPLS-TE tunnels to protected MPLS-TE tunnels.
show mpls traffic-eng ds-te te-class, on page 326	Displays the Diff-Serv TE-class map in use.

ds-te te-classes

To enter DS-TE te-class map configuration mode, use the **ds-te te-classes** command in MPLS-TE configuration mode. To return to the default behavior, use the **no** form of this command.

ds-te te-classes te-class *te_class_index* {**class-type** *class_type_number* {**priority** *pri_number*}| **unused**}

no ds-te te-classes te-class *te_class_index* {**class-type** *class_type_number* {**priority** *pri_number*}| **unused**}

Syntax Description

te-class	Configures the te-class map.
te_class_index	TE class-map index. Range is 0 to 7.
class-type	Configures the class type.
class_type_number	Class type value in the te-class map. Range is 0 to 1.
priority	Configures the TE tunnel priority.
pri_number	TE tunnel priority value. Range is 0 to 7.
unused	Marks the TE-class as unused.

Command Default

The following default te-class maps are used in IETF DS-TE mode:

te-class index	class-type	priority
0	0	7
1	1	7
2	UNUSED	—
3	UNUSED	—
4	0	0
5	1	0
6	UNUSED	—
7	UNUSED	—

Note   The default mapping has 4 TE-classes used with 2 class-types and, 4 TE-classes are unused. TE-class map is not used in prestandard DS-TE mode.

Command Modes   MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

In IETF DS-TE mode, modified semantic of the unreserved bandwidth TLV is used. Each of the eight available bandwidth values advertised in the IGP corresponds to a TE class. Because IGP advertises only eight bandwidth values, only eight TE-Classes can be supported in a IETF DS-TE network. The TE-Class mapping must be configured the same way on every router in a DS-TE domain. There is, however, no method to automatically detect or enforce this required consistency.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to configure a TE-class 7 parameter:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# ds-te te-classes te-class 7 class-type 0 priority 4
```

Related Commands

Command	Description
ds-te bc-model, on page 206	Enables a specific bandwidth constraint model (Maximum Allocation Model or Russian Doll Model) on the LSR.
ds-te mode, on page 208	Configures standard DS-TE mode.
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.
show mpls traffic-eng ds-te te-class, on page 326	Displays the Diff-Serv TE-class map in use.

exclude srlg (auto-tunnel backup)

To specify that automatic backup tunnels should avoid Shared Risk Link Groups (SRLGs) of protected interface, use the **exclude srlg** command in auto-tunnel backup configuration mode. To disable this feature, use the **no** form of this command.

exclude srlg [preferred]

no exclude srlg [preferred]

Syntax Description

preferred	(Optional) Causes the backup tunnel to avoid SRLGs of its protected interface(s); however, the backup tunnel is created if SRLGs are not avoided.

Command Default

Strict SRLG

Command Modes

Auto-tunnel backup configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Strict SRLG configuration of this command means that the path computed for the backup tunnel that is automatically created, must not contain any links that are part of the excluded SRLG groups. If such a path cannot be found, the backup tunnel does not come up.

Configuration of the preferred option allows the automatic backup tunnel to come up even if a path that excludes SRLGs can not be found.

Task ID

Task ID	Operation
mpls-te	read, write

Examples

In the following example, automatic backup tunnels must avoid SRLGs of the protected interface.

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# interface pos 0/1/0/1
```

```
RP/0/RP0/CPU0:router(config-mpls-te-if)# auto-tunnel backup
RP/0/RP0/CPU0:router(config-mpls-te-if-auto-backup)#  exclude srlg preferred
```

Related Commands

Command	Description
auto-tunnel backup (MPLS-TE), on page 174	Builds automatic next-hop and next-next-hop tunnels, and enters auto-tunnel configuration mode.

fast-reroute

To enable fast-reroute (FRR) protection for an MPLS-TE tunnel, use the **fast-reroute** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

fast-reroute

no fast-reroute

Syntax Description   This command has no arguments or keywords.

Command Default   FRR is disabled.

Command Modes   Interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When a protected link used by the fast-reroutable label switched path (LSP) fails, the traffic is rerouted to a previously assigned backup tunnel. Configuring FRR on the tunnel informs all the nodes that the LSP is traversing that this LSP desires link/node/bandwidth protection.

You must allow sufficient time after an switchover before triggering FRR on standby to synchronize with the active (verified using the **show redundancy** command). All TE tunnels must be in the recovered state and the database must be in the ready state for all ingress and egress line cards. To verify this information, use the **show mpls traffic-eng tunnels** and **show mpls traffic-eng fast-reroute database** commands.

Note   Wait approximately 60 seconds before triggering FRR after verifying the database state.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to enable FRR on an MPLS-TE tunnel:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# fast-reroute
```

Related Commands

Command	Description
fast-reroute protect, on page 217	Configures node and bandwidth protection for an MPLS-TE tunnel.
interface tunnel-te, on page 235	Configures an MPLS-TE tunnel interface.
show mpls traffic-eng forwarding, on page 328	Displays the contents of the FRR database.
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.

fast-reroute protect

To enable node and bandwidth protection for an MPLS-TE tunnel, use the **fast-reroute protect** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

fast-reroute protect {**bandwidth | node**}

no fast-reroute protect

Syntax Description

bandwidth	Enables bandwidth protection request.
node	Enables node protection request.

Command Default

FRR is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to enable bandwidth protection for a specified TE tunnel:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)#interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# fast-reroute protect bandwidth
```

Related Commands

Command	Description
fast-reroute, on page 215	Enables FRR protection for an MPLS-TE tunnel.
interface tunnel-te, on page 235	Configures an MPLS-TE tunnel interface.
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.

fast-reroute timers promotion

To configure how often the router considers switching a protected MPLS-TE tunnel to a new backup tunnel if additional backup-bandwidth or a better backup tunnel becomes available, use the **fast-reroute timers promotion** command in MPLS-TE configuration mode. To return to the default behavior, use the **no** form of this command.

fast-reroute timers promotion *interval*

no fast-reroute timers promotion

Syntax Description

interval	Interval, in seconds, between scans to determine if a label switched path (LSP) should use a new, better backup tunnel. Range is 0 to 604800. A value of 0 disables backup tunnel promotions.

Command Default *interval*: 300

Command Modes MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Setting the interval to a low value puts more load on the CPU because it has to scan all protected LSPs more frequently. It is not recommended that the timer be configured below the default value of 300 seconds.

Pacing mechanisms have been implemented to distribute the load on the CPU when backup promotion is active. Because of this, when a large number of protected LSPs are promoted, some delay is noticeable in backup promotion. If the promotion timer is configured to a very low value (depending on the number of protected LSPs) some protected LSPs may never get promoted.

To disable the timer, set the value to zero.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to specify that LSPs are scanned every 600 seconds (10 minutes) to determine if they should be promoted to a better backup tunnel:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# fast-reroute timers promotion 600
```

Related Commands

Command	Description
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.
mpls traffic-eng fast-reroute promote, on page 249	Configures the router to use a new or more efficient backup MPLS-TE tunnel when a current tunnel is overloaded.

flooding thresholds

To set the reserved bandwidth thresholds for a link, use the **flooding thresholds** command in MPLS-TE interface configuration mode. To return to the default behavior, use the **no** form of this command.

flooding thresholds {**down** | **up**} *percent* [*percent1* | *percent2* | *percent3* | *... percent 15*]

no flooding thresholds {**down** | **up**}

Syntax Description

down	Configures the threshold for decreased resource availability.
up	Configures the threshold for increased resource availability.
percent [percent]	Bandwidth threshold level. Range is 0 to 100 for all 16 levels.

Command Default

down: *100, 99, 98, 97, 96, 95, 90, 85 , 80, 75 , 60, 45, 30, 15*

up: *5, 30, 45, 60, 75, 80, 85, 90, 95, 97 , 98, 99, 100*

Command Modes

MPLS-TE interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You can configure up to 16 flooding threshold values. The first value is mandatory; the next 15 are optional.

When a threshold is crossed, MPLS-TE link management advertises updated link information. If no thresholds are crossed, changes can be flooded periodically unless periodic flooding was disabled.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to set the reserved bandwidth threshold for the link for decreased resource availability (down) and for increased resource availability (up) thresholds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# interface POS 0/7/0/0
RP/0/RP0/CPU0:router(config-mpls-te-if)# flooding thresholds down 100 75 25
RP/0/RP0/CPU0:router(config-mpls-te-if)# flooding thresholds up 25 50 100
```

Related Commands

Command	Description
interface (MPLS-TE), on page 231	Enables MPLS-TE on an interface and enters MPLS-TE interface configuration mode.
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.
link-management timers periodic-flooding, on page 241	Sets the length of the interval used for periodic flooding.
show mpls traffic-eng link-management advertisements, on page 338	Displays local link information currently being flooded by MPLS-TE link management into the global TE topology.
show mpls traffic-eng link-management bandwidth-allocation, on page 341	Displays current local link information.

forwarding-adjacency

To configure an MPLS-TE forwarding adjacency, use the **forwarding-adjacency** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

forwarding-adjacency [**holdtime** *time*]

no forwarding-adjacency [**holdtime** *time*]

Syntax Description

holdtime *time*	(Optional) Configures the holdtime value, in milliseconds, that is associated with each forwarding-adjacency LSP. The default is 0.

Command Default

holdtime *time*: 0

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If you do not specify a **holdtime** *time* value, a delay is introduced with the following results:

- When forwarding-adjacency is configured on a tunnel that is up, TE notifies IGP without any additional delay.

- When forwarding-adjacency is not configured on a tunnel, TE notifies IGP without any additional delay.

- When forwarding-adjacency is configured on a tunnel that is down, TE does not notify IGP.

- When a tunnel on which forwarding-adjacency has been configured comes up, TE holds the notification to IGP for the period of holdtime (assuming nonzero holdtime). When the holdtime elapses, TE notifies IGP if the tunnel is still up.

The paths that traffic is taking to the destination can be manipulated by adjusting the forwarding adjacency link metric. To do that, use the **bandwidth** command. The unit of possible bandwidth values is in kbps.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   This example shows how to configure forwarding adjacency with a holdtime value of 60 milliseconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 888
RP/0/RP0/CPU0:router(config-if)# forwarding-adjacency holdtime 60
```

Related Commands

Command	Description
bandwidth (RSVP), on page 430	Configures RSVP bandwidth on an interface using prestandard DS-TE mode.
interface tunnel-te, on page 235	Configures an MPLS-TE tunnel interface.
show mpls traffic-eng forwarding-adjacency, on page 331	Displays forwarding-adjacency information.

index exclude-address

To exclude an address from a tunnel path entry at a specific index, use the **index exclude-address** command in explicit path configuration mode. To return to the default behavior, use the **no** form of this command.

index *index-id* **exclude-address**{ **ipv4 unicast** *IP address*}

no index *index-id*

Syntax Description

index-id	Index number at which the path entry is inserted or modified. Range is 1 to 65535.
ipv4 unicast *IP address*	Excludes the IPv4 unicast address.

Command Default   No default behavior or values

Command Modes   Explicit path configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You cannot include or exclude addresses from an IP explicit path unless explicitly configured using the **exclude-address** keyword.

Use the **exclude-address**keyword only after entering the explicit path configuration mode.

If you use the **exclude-address** keyword and specify the IP address of a link, the constraint-based routine does not consider that link when it sets up MPLS-TE paths. If the excluded address is a flooded MPLS-TE router ID, the constraint-based shortest path first (SPF) routine does not consider that entire node.

Note   The person who performs the configuration must know the IDs of the routers, as it may not be apparent if the value refers to the link or to the node.

MPLS-TE accepts IP explicit paths composed of all excluded addresses configured using the **exclude-address** keyword.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to exclude address 192.168.3.2 at index 3 of the explicit path 200:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# explicit-path identifier 200
RP/0/RP0/CPU0:router(config-expl-path)# index 3 exclude-address ipv4 unicast 192.168.3.2
```

Related Commands

Command	Description
index next-address, on page 229	Specifies path entries at a specific index.
show explicit-paths, on page 305	Displays the configured IP explicit paths.

index exclude-srlg

To exclude an address to get SRLGs from a tunnel path entry at a specific index, use the **index exclude-srlg** command in explicit path configuration mode. To return to the default behavior, use the **no** form of this command.

index *index-id* **exclude-srlg ipv4 unicast** *IP address*

no index *index-id*

Syntax Description

index-id	Index number at which the path entry is inserted or modified. Range is 1 to 65535.
exclude-srlg	Specifies an IP address to get SRLG values from for exclusion.
ipv4 unicast *IP address*	Excludes the IPv4 unicast address.

Command Default

No default behavior or values

Command Modes

Explicit path configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
mpls-te	read, write

Examples   The following example shows how to exclude the SRLG values from the IP address 192.168.3.2 at index 1
of the explicit path 100:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# explicit-path identifier 100
RP/0/RP0/CPU0:router(config-expl-path)# index 1 exclude-srlg ipv4 unicast 192.168.3.2
```

index next-address

To include a path entry at a specific index, use the **index next-address** command in explicit path configuration mode. To return to the default behavior, use the **no** form of this command.

index *index-id* **next-address** [**loose** | **strict**] **ipv4 unicast** *IP-address*

no index *index-id*

Syntax Description

index-id	Index number at which the path entry is inserted or modified. Range is 1 to 65535.
ipv4 unicast *IP-address*	Includes the IPv4 unicast address (strict address).
loose ipv4 unicast *IP-address*	(Optional) Specifies the next unicast address in the path as a loose hop.
strict ipv4 unicast *IP-address*	(Optional) Specifies the next unicast address in the path as a strict hop.

Command Default   No default behavior or values

Command Modes   Explicit path configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You cannot include addresses from an IP explicit path unless explicitly configured using the **next-address** keyword.

Use the **next-address** keyword only after entering the explicit path configuration mode.

Note   The person who performs the configuration must know the IDs of the routers, as it may not be apparent if the value refers to the link or to the node.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to insert the **next-address** 192.168.3.2 at index 3 of the explicit path 200:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# explicit-path identifier 200
RP/0/RP0/CPU0:router(config-expl-path)# index 3 next-address ipv4 unicast 192.168.3.2
```

Related Commands

Command	Description
index exclude-address, on page 225	Specifies the next IP address to exclude from the explicit path.
show explicit-paths, on page 305	Displays the configured IP explicit paths.

interface (MPLS-TE)

To enable MPLS-TE on an interface and to enter MPLS-TE interface configuration mode, use the **interface** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

interface *type interface-path-id*

no interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface.
	Note Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router.
	For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You must enter MPLS-TE interface mode to configure specific interface parameters on physical interfaces.

Configuring MPLS-TE links or a tunnel TE interface begins the TE-control process on .

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to enter the MPLS-TE interface configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# interface POS 0/7/0/1
```

The following example shows how to remove an interface from the MPLS-TE domain:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# no interface POS 0/7/0/1
```

interface (SRLG)

To enable Shared Risk Link Groups (SRLGs) on an interface and to enter SRLG interface configuration mode, use the **interface** command in SRLG configuration mode. To return to the previous configuration mode, use the **no** form of this command.

interface *type interface-path-id*

no interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default No default behavior or values

Command Modes SRLG configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
mpls-te	read, write

Examples The following example shows how to enter SRLG interface configuration mode:

```
RP/0/RP0/CPU0:router(config)# srlg
RP/0/RP0/CPU0:router(config-srlg)# interface POS 0/1/0/1
```

```
RP/0/RP0/CPU0:router(config-srlg-if)# value 10
RP/0/RP0/CPU0:router(config-srlg-if)#value 50
```

Related Commands

Command	Description
interface (MPLS-TE), on page 231	Enables MPLS-TE on an interface and enters MPLS-TE interface configuration mode.
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.

interface tunnel-te

To configure an MPLS-TE tunnel interface, use the **interface tunnel-te** command in XR Config mode. To return to the default behavior, use the **no** form of this command.

interface tunnel-te *tunnel-id*

no interface tunnel-te *tunnel-id*

Syntax Description

tunnel-id	Tunnel number. Range is 0 to 65535.

Command Default

Tunnel interfaces are disabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You cannot have two tunnels using the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and to use the loopback interface address as the source address of the tunnel.

Configuring MPLS-TE links or Tunnel-TE interface begins the TE-control process on .

The **interface tunnel-te** command indicates that the tunnel interface is for an MPLS-TE tunnel and enables the various tunnel MPLS configuration options.

Note You must configure record-route on TE tunnels that are protected by multiple backup tunnels merging at a single node.

Task ID

Task ID	Operations
interface	read, write

Examples
The following example shows how to configure tunnel interface 1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# ipv4 unnumbered loopback0
```

The following example shows how to set the tunnel-class attribute to map the correct traffic class to the tunnel:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# policy-class 1
```

Related Commands

Command	Description
affinity, on page 150	Configures affinity (the properties that the tunnel requires in its links) for an MPLS-TE tunnel.
autoroute metric, on page 172	Instructs the IGP to use the tunnel in its enhanced SPF calculation, if the tunnel is in an up state.
backup-bw, on page 176	Configures backup bandwidth for FRR.
fast-reroute, on page 215	Enables FRR protection for an MPLS-TE tunnel.
path-option (MPLS-TE), on page 267	Configures a path option for an MPLS tunnel.
path-selection metric (interface), on page 280	Configures a path selection metric—TE or IGP.
policy-class	Configures PBTS to direct traffic into specific TE tunnels.
priority (MPLS-TE), on page 296	Configures setup and reservation priority for an MPLS-TE tunnel.
record-route, on page 298	Configures record-route on an MPLS-TE tunnel.

ipv4 unnumbered (MPLS)

To specify the MPLS-TE tunnel Internet Protocol Version 4 (IPv4) address, use the **ipv4 unnumbered** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

ipv4 unnumbered *type interface-path-id*

no ipv4 unnumbered *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default   No IP address is set.

Command Modes   Interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Tunnel-te is not signaled until an IP address is configured on the tunnel interface; therefore, the tunnel state stays down without IP address configuration.

Loopback is commonly used as the interface type.

Task ID

Task ID	Operations
network	read, write

Examples The following example shows how to configure the MPLS-TE tunnel to use the IPv4 address used on loopback interface 0:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# ipv4 unnumbered loopback0
```

link-management timers bandwidth-hold

To set the length of time that bandwidth is held for a Resource Reservation Protocol (RSVP) Path (setup) message to wait for the corresponding RSVP Resv message to return, use the **link-management timers bandwidth-hold** command in MPLS-TE configuration mode. To return to the default behavior, use the **no** form of this command.

link-management timers bandwidth-hold *holdtime*

no link-management timers bandwidth-hold *holdtime*

Syntax Description

holdtime	Number of seconds that bandwidth can be held. Range is 1 to 300. Default is 15.

Command Default *holdtime*: 15

Command Modes MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **link-management timers bandwidth-hold** command determines the time allowed for an RSVP message to return from a neighbor RSVP node.

Task ID

Task ID	Operations
mpls-te	read, write

Examples The following example shows how to set the bandwidth to be held for 10 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# link-management timers bandwidth-hold 10
```

Related Commands

Command	Description
link-management timers periodic-flooding, on page 241	Sets the length of the interval used for periodic flooding.
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.
show mpls traffic-eng link-management bandwidth-allocation, on page 341	Displays current local link information and bandwidth hold time.

link-management timers periodic-flooding

To set the length of the interval for periodic flooding, use the **link-management timers periodic-flooding** command in MPLS-TE configuration mode. To return to the default behavior, use the **no** form of this command.

link-management timers periodic-flooding *interval*

no link-management timers periodic-flooding

Syntax Description

| *interval* | Length of the interval, in seconds, for periodic flooding. Range is 0 to 3600. A value of 0 turns off periodic flooding. The minimum value is 30. |

Command Default   *interval*: 180

Command Modes   MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **link-management timers periodic-flooding** command advertises the link state information changes that do not trigger immediate action, such as a change to the allocated bandwidth that does not cross a threshold.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to set the interval length for periodic flooding to 120 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# link-management timers periodic-flooding 120
```

Related Commands

Command	Description
flooding thresholds, on page 221	Sets the reserved bandwidth flooding thresholds for a link.
link-management timers bandwidth-hold, on page 239	Sets the length of time that bandwidth is held for a RSVP Path (setup) message to wait for the corresponding RSVP Resv message to return.
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.
show mpls traffic-eng link-management summary, on page 353	Displays the current periodic flooding interval.

link-management timers preemption-delay

To set the length of the interval for delaying LSP preemption, use the **link-management timers preemption-delay** command in MPLS-TE configuration mode. To disable this behavior, use the **no** form of this command.

link-management timers preemption-delay bundle-capacity *sec*

Syntax Description

bundle-capacity *sec*	Specifies the bundle-capacity preemption timer value in seconds.

Command Default   None

Command Modes   MPLS-TE configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The value *0* as bundle-capacity value in the **link-management timers preemption-delay** command disables this timer. This means there is no delay before preemption sets in when the bundle capacity goes down.

Task ID

Task ID	Operation
mpls-te	read, write

Examples   This example shows how to set the interval length for preemption-delay:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# link-management timers preemption-delay bundle-capacity
 180
```

maxabs (MPLS-TE)

To specify the maximum number of MPLS-TE tunnels that can be configured, use the **maxabs** command in MPLS-TE configuration mode. To return to the default behavior, use the **no** form of this command.

maxabs tunnels *tunnel-limit* **destinations** *dest-limit*

no maxabs tunnels *tunnel-limit* **destinations** *dest-limit*

Syntax Description

tunnels	Configures all tunnels for MPLS-TE.
tunnel-limit	Maximum number of tunnel TE interfaces. Range is 1 to 65536.
destinations	Configures all destinations for MPLS-TE.
dest-limit	Maximum total number of destinations that can be configured. Range is 1 to 65536.

Command Default

tunnel-limit: 4096

dest-limit: 4096

Command Modes

MPLS-TE configuration

Command History

Release	Modification
Release 3.9.0	This command was removed.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to set the tunnel-te configuration limit to 1000:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
```

```
RP/0/RP0/CPU0:router(config-mpls-te)# maxabs tunnels 1000 destinations 1000
```

Related Commands

Command	Description
show mpls traffic-eng maximum tunnels, on page 355	Displays the configuration of the maximum tunnel-te interfaces allowed.

mpls traffic-eng

To enter MPLS-TE configuration mode, use the **mpls traffic-eng** command in global configuration mode.

mpls traffic-eng

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to enter MPLS-TE configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)#
```

mpls traffic-eng auto-bw apply (MPLS-TE)

To apply the highest bandwidth collected on a tunnel without waiting for the current application period to end, use the **mpls traffic-eng auto-bw apply** command in EXEC mode.

mpls traffic-eng auto-bw apply {**all**| **tunnel-te** *tunnel-number*}

Syntax Description

all	Applies the highest bandwidth collected instantly on all the automatic bandwidth-enabled tunnels.
tunnel-te *tunnel-number*	Applies the highest bandwidth instantly to the specified tunnel. The range is from 0 to 65535.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **mpls traffic-eng auto-bw apply** command can forcefully expire the current application period on a specified tunnel and immediately apply the highest bandwidth recorded so far instead of waiting for the application period to end on its own.

Note   The predefined threshold check still applies on the configuration, and if the delta is not significant enough, the automatic bandwidth functionality overrides this command.

The bandwidth application is performed only if at least one output rate sample has been collected for the current application period.

To guarantee the application of a specific signaled bandwidth value when triggering a manual bandwidth application, follow these steps:

1   Configure the minimum and maximum automatic bandwidth to the bandwidth value that you want to apply by using the bw-limit (MPLS-TE), on page 181 command.

2   Trigger a manual bandwidth application by using the **mpls traffic-eng auto-bw apply** command.

3   Revert the minimum and maximum automatic bandwidth value back to their original value.

Task ID

Task ID	Operations
mpls-te	execute

Examples

The following example applies the highest bandwidth to a specified tunnel:

```
RP/0/RP0/CPU0:router# mpls traffic-eng auto-bw apply tunnel-te 1
```

Related Commands

Command	Description
auto-bw collect frequency (MPLS-TE), on page 168	Configures the automatic bandwidth collection frequency and controls the manner in which the bandwidth for a tunnel collects output rate information, but does not adjust the tunnel bandwidth.
show mpls traffic-eng tunnels auto-bw brief, on page 399	Displays the list of automatic-bandwidth-enabled tunnels, and indicates if the current signaled bandwidth of the tunnel is identical to the bandwidth that is applied by the automatic bandwidth.

mpls traffic-eng fast-reroute promote

To configure the router to assign new or more efficient backup MPLS-TE tunnels to protected MPLS-TE tunnels, use the **mpls traffic-eng fast-reroute promote** command in EXEC mode. To return to the default behavior, use the **no** form of this command.

mpls traffic-eng fast-reroute promote

no mpls traffic-eng fast-reroute promote

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values

Command Modes EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Examples The following example shows how to initiate backup tunnel promote and assignment:

```
RP/0/RP0/CPU0:router# mpls traffic-eng fast-reroute promote
```

Related Commands

Command	Description
fast-reroute, on page 215	Enables FRR protection for an MPLS-TE tunnel.

mpls traffic-eng level

To configure a router running Intermediate System-to-System (IS-IS) MPLS-TE at IS-IS Level 1 and Level 2, use the **mpls traffic-eng level** command in router configuration mode. To return to the default behavior, use the **no** form of this command.

mpls traffic-eng level *isis-level*

no mpls traffic-eng level *isis-level*

Syntax Description

isis-level	IS-IS level (1, 2, or both) where MPLS-TE is enabled.

Command Default No default behavior or values

Command Modes Router configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **mpls traffic-eng level** command is supported for IS-IS and affects the operation of MPLS-TE only if MPLS-TE is enabled for that routing protocol instance.

Task ID

Task ID	Operations
isis	read, write

Examples The following example shows how to configure a router running IS-IS MPLS to flood TE for IS-IS level 1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router isis 1
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-af)# mpls traffic-eng level 1
RP/0/RP0/CPU0:router(config-isis-af)# metric-style wide
```

Related Commands

Command	Description
mpls traffic-eng router-id (MPLS-TE router), on page 260	Specifies that the TE router identifier for the node is the IP address associated with a given interface.

mpls traffic-eng link-management flood

To enable immediate flooding of all the local MPLS-TE links, use the **mpls traffic-eng link-management flood** command in EXEC mode. To return to the default behavior, use the **no** form of this command.

mpls traffic-eng link-management flood

no mpls traffic-eng link-management flood

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note   If there is no change in the LSA since last flooding, IGP may dampen the advertisement.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to initiate flooding of the local MPLS-TE links:

```
RP/0/RP0/CPU0:router# mpls traffic-eng link-management flood
```

Related Commands

Command	Description
show mpls traffic-eng link-management advertisements, on page 338	Displays MPLS-TE link-management advertisements.

mpls traffic-eng pce activate-pcep

To force idle peers to be reestablished without waiting for a timer, use the **mpls traffic-eng pce activate-pcep** command in EXEC mode. To return to the default behavior, use the **no** form of this command.

mpls traffic-eng pce activate-pcep {*address* | **all**}

no mpls traffic-eng pce activate-pcep {*address* | **all**}

Syntax Description

address	Address of the idle peer.
all	Activates all the idle peers.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write, execute

Examples

The following example shows how to trigger a path computation client (PCC) or PCE to activate an idle path computation element protocol (PCEP) session:

```
RP/0/RP0/CPU0:router# mpls traffic-eng pce activate-pcep all
```

Related Commands

Command	Description
mpls traffic-eng pce reoptimize, on page 256	Triggers reoptimization manually either for all tunnels or a specific PCE-based tunnel.

mpls traffic-eng pce reoptimize

To trigger reoptimization manually either for all or a specific PCE-based tunnel, use the **mpls traffic-eng pce reoptimize** command in EXEC mode. To disable this feature, use the **no** form of this command.

mpls traffic-eng pce reoptimize [*tunnel ID*] **[force]**

no mpls traffic-eng pce reoptimize [*tunnel ID*] **[force]**

Syntax Description

tunnel ID	(Optional) Tunnel ID to be reoptimized. Range is from 0 to 65535.
force	(Optional) Forces the router to start using the newly calculated route even if the used path has a better metric.

Command Default   Reoptimizes all the PCE tunnels.

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If you do not run the **mpls traffic-eng pce reoptimize** command, the system tries to reoptimize at an interval of 3600 seconds.

Task ID

Task ID	Operations
mpls-te	read, write, execute

Examples   The following example shows how to trigger reoptimization for all PCE-based tunnels:

```
RP/0/RP0/CPU0:router# mpls traffic-eng pce reoptimize
```

Related Commands

Command	Description
mpls traffic-eng pce activate-pcep, on page 254	Forces idle peers to be re-established without waiting for a timer.

mpls traffic-eng reoptimize (EXEC)

To trigger the reoptimization interval of all TE tunnels, use the **mpls traffic-eng reoptimize** command in EXEC mode.

mpls traffic-eng reoptimize [*tunnel-id*] [*tunnel-name*] [**p2p**{**all**| *tunnel-id*}]

Syntax Description

tunnel-id	(Optional) MPLS-TE tunnel identification expressed as a number. Range is from 0 to 65535.
tunnel-name	(Optional) TE tunnel identification expressed as a name.
p2p	(Optional) Forces an immediate reoptimization of all P2P TE tunnels.
all	(Optional) Forces an immediate reoptimization for all P2P tunnels.
tunnel-id	P2P TE tunnel identification to be reoptimized. Range is from 0 to 65535.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	execute

Examples

The following example shows how to immediately reoptimize all TE tunnels:

```
RP/0/RP0/CPU0:router# mpls traffic-eng reoptimize
```

The following example shows how to immediately reoptimize TE tunnel-te90:

```
RP/0/RP0/CPU0:router# mpls traffic-eng reoptimize tunnel-te90
```

The following example shows how to immediately reoptimize all P2P TE tunnels:

```
RP/0/RP0/CPU0:router# mpls traffic-eng reoptimize p2p all
```

Related Commands

Command	Description
reoptimize (MPLS-TE)	Forces immediate re-optimization of all TE tunnels.

mpls traffic-eng router-id (MPLS-TE router)

To specify that the TE router identifier for the node is the IP address associated with a given interface, use the **mpls traffic-eng router-id** command in the appropriate mode. To return to the default behavior, use the **no** form of this command.

mpls traffic-eng router-id *type interface-path-id*

no mpls traffic-eng router-id *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default

No default behavior or values

Command Modes

OSPF configuration

IS-IS address family configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

A routers identifier acts as a stable IP address for the TE configuration. This IP address is flooded to all nodes. You must set the destination on the destination node TE router identifier for all affected tunnels. This router ID is the address that the TE topology database at the tunnel head uses for its path calculation.

Note When the **mpls traffic-eng router-id** command is not configured, global router ID is used by MPLS-TE if there is one configured.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following examples show how to specify the TE router identifier as the IP address associated with loopback interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf CORE_AS
RP/0/RP0/CPU0:router(config-ospf)# mpls traffic-eng router-id 7.7.7.7

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router isis 811
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-af)# mpls traffic-eng router-id 8.8.8.8
```

Related Commands

Command	Description
mpls traffic-eng level, on page 250	Configures a router running OSPF MPLS so that it floods TE for the indicated IS-IS level.

mpls traffic-eng repotimize mesh group

To reoptimize all tunnels of a mesh group, use the **mpls traffic-eng repotimize mesh group**command in EXEC mode.

mpls traffic-eng reoptimize auto-tunnel mesh group *group_id*

Syntax Description

group_id	Defines auto-tunnel mesh group ID that is to be reoptimized. Range is 0 to 4294967295.

Command Default   None

Command Modes   MPLS Transport profile configuration

Command History

Release	Modification
Release 4.1.1	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	execute

Examples   This is sample out from the **mpls traffic-eng reoptimize mesh group** command:

```
RP/0/RP0/CPU0:router mpls traffic-eng reoptimize mesh group 10
```

nhop-only (auto-tunnel backup)

To configure only a next-hop automatic backup tunnel with only link protection, use the **nhop-only** command in MPLS-TE auto-tunnel backup interface configuration mode. To return to the default configuration setting for automatic backup tunnels, use the **no** form of this command.

nhop-only

no nhop-only

Syntax Description   This command has no arguments or keywords.

Command Default   Both NHOP and NNHOP protection are enabled.

Command Modes   Auto-tunnel backup configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If you configure the **nhop-only** command, you destroy any next-next-hop (NNHOP) tunnel created to provide node protection for tunnels running over the specified interface.

If you unconfigure the **nhop-only** command, you trigger a backup assignment on primary tunnels running over that link. The automatic backup tunnel feature attempts to create NNHOP backup tunnnels to provide node protection for the specified tunnels.

Task ID

Task ID	Operation
mpls-te	read, write

Examples   In the following example, NNHOP automatic backup tunnels are destroyed and only NHOP tunnels with link protection is configured:

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# interface pos 0/1/0/1
RP/0/RP0/CPU0:router(config-mpls-te-if)# auto-tunnel backup
RP/0/RP0/CPU0:router(config-mpls-te-if-auto-backup)# nhop-only
```

Related Commands

Command	Description
auto-tunnel backup (MPLS-TE), on page 174	Builds automatic NHOP and NNHOP backup tunnels.

overflow threshold (MPLS-TE)

To configure the tunnel overflow detection, use the **overflow threshold** command in MPLS-TE automatic bandwidth interface configuration mode. To disable the overflow detection feature, use the **no** form of this command.

overflow threshold *percentage* [**min** *bandwidth*] **limit** *limit*

no overflow threshold

Syntax Description

percentage	Bandwidth change percent to trigger an overflow. The range is from 1 to 100.
min *bandwidth*	(Optional) Configures the bandwidth change value, in kbps, to trigger an overflow. The range is from 10 to 4294967295. The default is 10.
limit *limit*	Configures the number of consecutive collection intervals that exceeds the threshold. The bandwidth overflow triggers an early tunnel bandwidth update. The range is from 1 to 10. The default is none.

Command Default

The default value is disabled.

Command Modes

MPLS-TE automatic bandwidth interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If you modify the **limit** keyword, the consecutive overflows counter for the tunnel is also reset.

If you enable or modify the minimum value, the current consecutive overflows counter for the tunnel is also reset, which effectively restarts the overflow detection from scratch.

Several number of consecutive bandwidth samples are greater than the overflow threshold (bandwidth percentage) and the minimum bandwidth configured, then a bandwidth application is updated immediately instead of waiting for the end of the application period.

Overflow detection applies only to bandwidth increase. For example, an overflow can not be triggered even if bandwidth decreases by more than the configured overflow threshold.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to configure the tunnel overflow detection for tunnel-te 1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# auto-bw
RP/0/RP0/CPU0:router(config-if-tunte-autobw)# overflow threshold 50 limit 3
```

Related Commands

Command	Description
adjustment-threshold (MPLS-TE), on page 146	Configures the tunnel bandwidth change threshold to trigger an adjustment.
application (MPLS-TE), on page 156	Configures the application frequency in minutes for the applicable tunnel.
auto-bw (MPLS-TE), on page 166	Configures automatic bandwidth on a tunnel interface and enters MPLS-TE automatic bandwidth interface configuration mode.
bw-limit (MPLS-TE), on page 181	Configures the minimum and maximum automatic bandwidth to set on a tunnel.
collect-bw-only (MPLS-TE), on page 198	Enables only the bandwidth collection without adjusting the automatic bandwidth.
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.

path-option (MPLS-TE)

To configure a path option for an MPLS-TE tunnel, use the **path-option** command in tunnel-te interface configuration mode. To return to the default behavior, use the **no** form of this command.

path-option *preference-priority* {**dynamic** [**pce** [**address ipv4** *address*]]| **explicit** {**name** *path-name*| **identifier** *path-number*}} [**attribute-set** *name]* [**isis** *instance-name* **level** *level*] **[lockdown]** [**ospf** *instance-name* **area** {*value* | *address*}] **[verbatim]**

no path-option *preference-priority* {**dynamic** [**pce** [**address ipv4** *address*]]| **explicit** {**name** *path-name*| **identifier** *path-number*}} [**isis** *instance-name* **level** *level*] **[lockdown]** [**ospf** *instance-name* **area** {*value* | *address*}] **[verbatim]**

Syntax Description

preference-priority	Path option number. Range is from 1 to 1000.
dynamic	Specifies that label switched paths (LSP) are dynamically calculated.
pce	(Optional) Specifies that the LSP is computed by a Path Computation Element (PCE).
address	(Optional) Configures the address for the PCE.
ipv4 *address*	Configures the IPv4 address for the PCE.
explicit	Specifies that LSP paths are IP explicit paths.
name *path-name*	Specifies the path name of the IP explicit path.
identifier *path-number*	Specifies a path number of the IP explicit path.
isis *instance-name*	(Optional) Limits CSPF to a single IS-IS instance and area.
attribute-set *name*	(Optional) Specifies the attribute set for the LSP.
level *level*	Configures the level for IS-IS. The range is from 1 to 2.
lockdown	(Optional) Specifies that the LSP cannot be reoptimized.
ospf *instance-name*	(Optional) Limits CSPF to a single OSPF instance and area.
area	Configures the area for OSPF.
value	Decimal value for the OSPF area ID.
address	IP address for the OSPF area ID.
verbatim	(Optional) Bypasses the Topology/CSPF check for explicit paths.

Command Default   No default behavior or values

Command Modes   Tunnel-te interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You can configure several path options for a single tunnel. For example, there can be several explicit path options and a dynamic option for one tunnel. The path setup preference is for lower (not higher) numbers, so option 1 is preferred.

When the lower number path option fails, the next path option is used to set up a tunnel automatically (unless using the lockdown option).

You specify the backup path for the **path-option** command in case of the primary path failure.

CSPF areas are configured on a per-path-option basis.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to configure the tunnel to use a named IPv4 explicit path as verbatim and lockdown options for the tunnel. This tunnel cannot reoptimize when the FRR event goes away, unless you manually reoptimize it:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# path-option 1 explicit name test verbatim lockdown
```

The following example shows how to enable path protection on a tunnel to configure an explicit path:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# path-option 1 explicit name po4
RP/0/RP0/CPU0:router(config-if)# path-option protecting 1 explicit name po6
```

The following example shows how to limit CSPF to a single OSPF instance and area:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# path-option 1 explicit name router1 ospf 3 area 7 verbatim
```

The following example shows how to limit CSPF to a single IS-IS instance and area:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# path-option 1 dynamic isis mtbf level 1 lockdown
```

Related Commands

Command	Description
show explicit-paths, on page 305	Displays the configured IP explicit paths.
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.

path-option (P2MP TE)

To configure the primary or fallback path setup option for a Point-to-Multipoint (P2MP) TE tunnel, use the **path-option** command in P2MP destination interface configuration mode. To return to the default behavior, use the **no** form of this command.

path-option *preference-priority* {**dynamic**| **explicit** {**name** *path-name*| **identifier** *path-number*} } **[verbatim] [lockdown]**

no path-option *preference-priority* {**dynamic**| **explicit** {**name** *path-name*| **identifier** *path-number*} } **[verbatim] [lockdown]**

Syntax Description

preference-priority	Path option number. Range is from 1 to 1000.
dynamic	Specifies that label switched paths (LSP) are dynamically calculated.
explicit	Specifies that LSP paths are IP explicit paths.
name *path-name*	Specifies the path name of the IP explicit path.
identifier *path-number*	Specifies a path number of the IP explicit path.
verbatim	(Optional) Bypasses the Topology/CSPF check for explicit paths.
lockdown	(Optional) Specifies that the LSP cannot be reoptimized.

Command Default   None

Command Modes   P2MP destination interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You can configure several path options for each destination of a P2MP tunnel. For example, for one tunnel, there can be several explicit path options and a dynamic option. The path preference is for lower (not higher) numbers, so option 1 is preferred over higher options.

When the lower number path option fails, the next path option under the destination is attempted.

Several path-options can be configured for each destination under a tunnel.

When configuring multiple path-options under each destination of a P2MP tunnel, the PCALC on the TE tunnel source attempts to generate the P2MP tree starting from the preferred path-options (lower numbers) for each destination. If some destinations use explicit paths that cause remerges with the dynamic generated paths for other destinations in the P2MP tree, the PCALC source modifies the dynamic paths (for example, optimal path); therefore, it follows the explicit path to correct the remerge problem.

The **path-option** command is common for both Point-to-Point (P2P) and P2MP tunnels.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

This example shows how to configure a P2MP tunnel with two destinations and several path-options per destination:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-mte 100
RP/0/RP0/CPU0:router(config-if)#  destination 1.1.1.1
RP/0/RP0/CPU0:router(config-if-p2mp-dest)# path-option 1 explicit name po_dest1
RP/0/RP0/CPU0:router(config-if-p2mp-dest)# path-option 2 dynamic
```

This example shows that the fallback path option is dynamic:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-mte 100
RP/0/RP0/CPU0:router(config-if)# destination 2.2.2.2
RP/0/RP0/CPU0:router(config-if-p2mp-dest)# path-option 1 explicit name po_dest2
RP/0/RP0/CPU0:router(config-if-p2mp-dest)# path-option 2 dynamic
```

Related Commands

Command	Description
destination (MPLS-TE), on page 200	Configures the destination address of a TE tunnel.
mpls traffic-eng path-protection switchover gmpls	Specifies a switchover for path protection.
show explicit-paths, on page 305	Displays the configured IP explicit paths.
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.
show mrib mpls traffic-eng fast-reroute	Displays information about Multicast Routing Information Base (MRIB) MPLS traffic engineering fast reroute.

path-selection ignore overload (MPLS-TE)

To ignore the Intermediate System-to-Intermediate System (IS-IS) overload bit setting for MPLS-TE, use the **path-selection ignore overload** command in MPLS-TE configuration mode. To return to the default behavior, use the **no** form of this command.

path-selection ignore overload {head | mid | tail}

no path-selection ignore overload {head | mid | tail}

Syntax Description

head	The tunnel stays up if **set-overload-bit** is set by ISIS on the head router. Ignores overload node during CSPF for the head node.
mid	The tunnel stays up if **set-overload-bit** is set by ISIS on the mid router. Ignores overload node during CSPF for the mid node.
tail	The tunnel stays up if **set-overload-bit** is set by ISIS on the tail router. Ignores overload node during CSPF for the tail node.

Command Default   None

Command Modes   MPLS-TE configuration

Command History

Release	Modification
Release 4.1.0	The **head, mid,** and **tail** keywords were added.
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **path-selection ignore overload** command to ensure that label switched paths (LSPs) are not broken because of routers that have IS-IS overload bit as enabled.

When the IS-IS overload bit avoidance (OLA) feature is activated, all nodes with the overload bit set, which includes head nodes, mid nodes, and tail nodes, are ignored. This means that they are still available for use with label switched paths (LSPs). This feature allows you to include an overloaded node in constraint-based shortest path first (CSPF).

Task ID

Task ID	Operations
mpls-te	read, write

Examples

This example shows how to use the **path-selection ignore overload head** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# path-selection ignore overload
RP/0/RP0/CPU0:router(config-mpls-te)# path-selection ignore overload head
```

path-selection loose-expansion affinity (MPLS-TE)

To specify the affinity value to be used to expand a path to the next loose hop for a tunnel on an area border router, use the **path-selection loose-expansion affinity** command in MPLS-TE configuration mode. To return to the default behavior, use the **no** form of this command.

path-selection loose-expansion affinity *affinity-value* **mask** *affinity-mask* [**class-type** *type*]

no path-selection loose-expansion affinity *affinity-value* **mask** *affinity-mask* [**class-type** *type*]

Syntax Description

affinity-value	Attribute values required for links carrying this tunnel. A 32-bit decimal number. Range is 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.
mask *affinity-mask*	Checks the link attribute, a 32-bit decimal number. Range is 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute mask is 0 or 1.
class-type *type*	(Optional) Requests the class-type of the tunnel bandwidth. Range is 0 to 1.

Command Default

affinity-value : 0X00000000

mask-value : 0XFFFFFFFF

Command Modes

MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note

The new affinity scheme (based on names) is not supported for loose-hop expansion. New configuration does not affect the already up tunnels.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to configure affinity 0x55 with mask 0xFFFFFFFF:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# path-selection loose-expansion affinity 55 mask
FFFFFFFF
```

Related Commands

Command	Description
path-selection loose-expansion metric (MPLS-TE), on page 276	Configures a metric type to be used to expand a path to the next loose hop for a tunnel on an area border router.
path-selection metric (MPLS-TE), on page 278	Configures the MPLS-TE tunnel path-selection metric.

path-selection loose-expansion metric (MPLS-TE)

To configure a metric type to be used to expand a path to the next loose hop for a tunnel on an area border router, use the **path-selection loose-expansion metric** command in MPLS-TE configuration mode. To return to the default behavior, use the **no** form of this command.

path-selection loose-expansion metric {**igp**| **te**} [**class-type** *type*]

no path-selection loose-expansion metric {**igp**| **te**} [**class-type** *type*]

Syntax Description

igp	Configures an Interior Gateway Protocol (IGP) metric.
te	Configures a TE metric. This is the default.
class-type *type*	(Optional) Requests the class type of the tunnel bandwidth. Range is 0 to 1.

Command Default

The default is TE metric.

Command Modes

MPLS-TE configuration

Command History

| Release | Modification |
| Release 5.0.0 | This command was introduced. |

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note New configurations do not affect tunnels that are already up.

Task ID

| Task ID | Operations |
| mpls-te | read, write |

Examples   The following example shows how to set the path-selection metric to use the IGP metric overwriting default:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# path-selection loose-expansion metric igp
```

Related Commands

Command	Description
path-selection loose-expansion affinity (MPLS-TE), on page 274	Specifies the affinity value to be used to expand a path to the next loose hop for a tunnel on an area border router.

path-selection metric (MPLS-TE)

To specify the MPLS-TE tunnel path-selection metric, use the **path-selection metric** command in MPLS-TE configuration mode. To return to the default behavior, use the **no** form of this command.

path-selection metric {**igp**| **te**}

no path-selection metric {**igp**| **te**}

Syntax Description

igp	Configures an Interior Gateway Protocol (IGP) metric.
te	Configures a TE metric.

Command Default

The default is TE metric.

Command Modes

MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The metric type to be used for path calculation for a given tunnel is determined as follows:

- If the **path-selection metric** command was entered to specify a metric type for the tunnel, use that metric type.

- Otherwise, use the default (TE) metric.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to set the path-selection metric to use the IGP metric overwriting default:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
```

```
RP/0/RP0/CPU0:router(config-mpls-te)# path-selection metric igp
```

Related Commands

Command	Description
path-selection loose-expansion affinity (MPLS-TE), on page 274	Specifies the affinity value to be used to expand a path to the next loose hop for a tunnel on an area border router.

path-selection metric (interface)

To configure an MPLS-TE tunnel path-selection metric type, use the **path-selection metric** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

path-selection metric {**igp** | **te**}

no path-selection metric {**igp** | **te**}

Syntax Description

igp	Configures Interior Gateway Protocol (IGP) metrics.
te	Configures TE metrics. This is the default.

Command Default

The default is TE metrics.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The metric type to be used for path calculation for a given tunnel is determined as follows:

- If the **path-selection metric** command was entered to either a metric type for the tunnel or only a metric type, use that metric type.

- Otherwise, use the default (TE) metric.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to set the path-selection metric to use the IGP metric overwriting default:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
```

```
RP/0/RP0/CPU0:router(config-if)# path-selection metric igp
```

Related Commands

Command	Description
show mpls traffic-eng topology, on page 364	Displays the tunnel path used.

pce address (MPLS-TE)

To configure the IPv4 self address for Path Computation Element (PCE), use the **pce address** command in MPLS-TE configuration mode. To return to the default behavior, use the **no** form of this command.

pce address ipv4 *address*

no pce address ipv4 *address*

Syntax Description

ipv4 *address*	Configures the IPv4 address for PCE.

Command Default

No default behavior or values

Command Modes

MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The IP address is used in the TCP communication with the other PCEs or PCCs. In addition, this address is advertised using IGP.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to configure the IPv4 self address for PCE:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# pce address ipv4 10.10.10.10
```

Related Commands

Command	Description
pce keepalive (MPLS-TE), on page 286	Configures a PCEP keepalive interval.
path-option (MPLS-TE), on page 267	Configures a path option for an MPLS-TE tunnel.
pce peer (MPLS-TE), on page 288	Configures an IPv4 self address for a PCE peer.
pce reoptimize (MPLS-TE), on page 290	Configures a periodic reoptimization timer.
pce request-timeout (MPLS-TE), on page 292	Configures a PCE request-timeout.
pce tolerance keepalive (MPLS-TE), on page 294	Configures a PCE tolerance keepalive (which is the minimum acceptable peer proposed keepalive).

pce deadtimer (MPLS-TE)

To configure a path computation element (PCE) deadtimer, use the **pce deadtimer** command in MPLS-TE configuration mode. To return to the default behavior, use the **no** form of this command.

pce deadtimer *value*

no pce deadtimer *value*

Syntax Description

value	Keepalive dead interval, in seconds. The range is 0 to 255.

Command Default

value: 120

Command Modes

MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When the dead interval is 0, the LSR does not time out a PCEP session to a remote peer.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to configure a PCE deadtimer:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# pce deadtimer 50
```

Related Commands

Command	Description
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.

Command	Description
path-option (MPLS-TE), on page 267	Configures a path option for an MPLS-TE tunnel.
pce address (MPLS-TE), on page 282	Configures the IPv4 self address for a PCE.
pce keepalive (MPLS-TE), on page 286	Configures a PCEP keepalive interval.
pce peer (MPLS-TE), on page 288	Configures an IPv4 self address for a PCE peer.
pce reoptimize (MPLS-TE), on page 290	Configures a periodic reoptimization timer.
pce request-timeout (MPLS-TE), on page 292	Configures a PCE request-timeout.
pce tolerance keepalive (MPLS-TE), on page 294	Configures a PCE tolerance keepalive (which is the minimum acceptable peer proposed keepalive).

pce keepalive (MPLS-TE)

To configure a path computation element protocol (PCEP) keepalive interval, use the **pce keepalive** command in MPLS-TE configuration mode. To disable this command, use the **no** form of this command.

pce keepalive *interval*

no pce keepalive *interval*

Syntax Description

interval	Keepalive interval, in seconds. The range is 0 to 255.

Command Default

interval: 30

Command Modes

MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When the keepalive interval is 0, the LSR does not send keepalive messages.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to configure PCEP keepalive interval for 10 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router#(config-mpls-te) pce keepalive 10
```

Related Commands

Command	Description
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.

Command	Description
path-option (MPLS-TE), on page 267	Configures a path option for an MPLS-TE tunnel.
pce address (MPLS-TE), on page 282	Configures the IPv4 self address for a PCE.
pce deadtimer (MPLS-TE), on page 284	Configures a PCE deadtimer.
pce peer (MPLS-TE), on page 288	Configures an IPv4 self address for a PCE peer.
pce reoptimize (MPLS-TE), on page 290	Configures a periodic reoptimization timer.
pce request-timeout (MPLS-TE), on page 292	Configures a PCE request-timeout.
pce tolerance keepalive (MPLS-TE), on page 294	Configures a PCE tolerance keepalive (which is the minimum acceptable peer proposed keepalive).

pce peer (MPLS-TE)

To configure an IPv4 self address for a path computation element (PCE) peer, use the **pce peer** command in MPLS-TE configuration mode. To return to the default behavior, use the **no** form of this command.

pce peer ipv4 *address*

no pce peer ipv4 *address*

Syntax Description

ipv4 *address*	Configures the IPv4 address for PCE.

Command Default   TE metric

Command Modes   MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to configure an IPv4 self address for a PCE peer:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# pce peer ipv4 11.11.11.11
```

Related Commands

Command	Description
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.

Command	Description
path-option (MPLS-TE), on page 267	Configures a path option for an MPLS-TE tunnel.
pce address (MPLS-TE), on page 282	Configures the IPv4 self address for a PCE.
pce deadtimer (MPLS-TE), on page 284	Configures a PCE deadtimer.
pce keepalive (MPLS-TE), on page 286	Configures a PCEP keepalive interval.
pce reoptimize (MPLS-TE), on page 290	Configures a periodic reoptimization timer.
pce request-timeout (MPLS-TE), on page 292	Configures a PCE request-timeout.
pce tolerance keepalive (MPLS-TE), on page 294	Configures a PCE tolerance keepalive (which is the minimum acceptable peer proposed keepalive).

pce reoptimize (MPLS-TE)

To configure a periodic reoptimization timer, use the **pce reoptimize** command in MPLS-TE configuration mode. To disable this feature, use the **no** form of this command.

pce reoptimize *value*

no pce reoptimize *value*

Syntax Description

value	Periodic reoptimization timer value, in seconds. The range is 60 to 604800.

Command Default

value: 3600

Command Modes

MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When the dead interval is 0, the LSR does not time out a path computation element protocol (PCEP) session to a remote peer.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to configure a periodic reoptimization timer for 200 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# pce reoptimize 200
```

Related Commands

Command	Description
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.
path-option (MPLS-TE), on page 267	Configures a path option for an MPLS-TE tunnel.
pce address (MPLS-TE), on page 282	Configures the IPv4 self address for a PCE.
pce deadtimer (MPLS-TE), on page 284	Configures a PCE deadtimer.
pce keepalive (MPLS-TE), on page 286	Configures a PCEP keepalive interval.
pce peer (MPLS-TE), on page 288	Configures an IPv4 self address for a PCE peer.
pce request-timeout (MPLS-TE), on page 292	Configures a PCE request-timeout.
pce tolerance keepalive (MPLS-TE), on page 294	Configures a PCE tolerance keepalive (which is the minimum acceptable peer proposed keepalive).

pce request-timeout (MPLS-TE)

To configure a path computation element (PCE) request-timeout, use the **pce request-timeout** command in MPLS-TE configuration mode. To disable this feature, use the **no** form of this command.

pce request-timeout *value*

no pce request-timeout *value*

Syntax Description

value	PCE request-timeout, in seconds. The range is 5 to 100.

Command Default

value: 10

Command Modes

MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

PCC or PCE keeps a pending path request only for the request-timeout period.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to configure a PCE request-timeout for 10 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# pce request-timeout 10
```

Related Commands

Command	Description
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.

Command	Description
path-option (MPLS-TE), on page 267	Configures a path option for an MPLS-TE tunnel.
pce address (MPLS-TE), on page 282	Configures the IPv4 self address for a PCE.
pce deadtimer (MPLS-TE), on page 284	Configures a PCE deadtimer.
pce keepalive (MPLS-TE), on page 286	Configures a PCEP keepalive interval.
pce peer (MPLS-TE), on page 288	Configures an IPv4 self address for a PCE peer
pce reoptimize (MPLS-TE), on page 290	Configures a periodic reoptimization timer.
pce tolerance keepalive (MPLS-TE), on page 294	Configures a PCE tolerance keepalive (which is the minimum acceptable peer proposed keepalive).

pce tolerance keepalive (MPLS-TE)

To configure a path computation element (PCE) tolerance keepalive (which is the minimum acceptable peer proposed keepalive), use the **pce tolerance keepalive** command in MPLS-TE configuration mode. To disable this feature, use the **no** form of this command.

pce tolerance keepalive *value*

no pce tolerance keepalive *value*

Syntax Description

value	PCE tolerance keepalive value, in seconds. The range is 0 to 255.

Command Default

value: 10

Command Modes

MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to configure a PCE tolerance keepalive for 10 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# pce tolerance keepalive 10
```

Related Commands

Command	Description
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.

Command	Description
path-option (MPLS-TE), on page 267	Configures a path option for an MPLS-TE tunnel.
pce address (MPLS-TE), on page 282	Configures the IPv4 self-address for a PCE.
pce deadtimer (MPLS-TE), on page 284	Configures a PCE deadtimer.
pce keepalive (MPLS-TE), on page 286	Configures a PCEP keepalive interval.
pce peer (MPLS-TE), on page 288	Configures an IPv4 self address for a PCE peer
pce reoptimize (MPLS-TE), on page 290	Configures a periodic reoptimization timer.
pce request-timeout (MPLS-TE), on page 292	Configures a PCE request-timeout.

priority (MPLS-TE)

To configure the setup and reservation priority for an MPLS-TE tunnel, use the **priority** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

priority *setup-priority hold-priority*

no priority *setup-priority hold-priority*

Syntax Description

setup-priority	Priority used when signaling a label switched path (LSP) for this tunnel to determine which existing tunnels can be preempted. Range is 0 to 7 (in which a lower number indicates a higher priority). Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non-0 priority.
hold-priority	Priority associated with an LSP for this tunnel to determine if it should be preempted by other LSPs that are being signaled. Range is 0 to 7 (in which a lower number indicates a higher priority).

Command Default

setup-priority: 7

hold-priority: 7

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When an LSP is signaled and an interface does not currently have enough bandwidth available for that LSP, the call admission software (if necessary) preempts lower-priority LSPs to admit the new LSP. Accordingly, the new LSP priority is the setup priority and the existing LSP priority is the hold priority. The two priorities make it possible to signal an LSP with a low setup priority (so that the LSP does not preempt other LSPs on setup) and a high hold priority (so that the LSP is not preempted after it is established). Setup priority and hold priority are typically configured to be equal, and setup priority cannot be numerically smaller than the hold priority.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to configure a tunnel with a setup and hold priority of 1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# priority 1 1
```

Related Commands

Command	Description
interface tunnel-te, on page 235	Configures an MPLS-TE tunnel interface.

record-route

To record the route used by a tunnel, use the **record-route** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

record-route

no record-route

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values

Command Modes   Interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

> **Note**   You must configure record-route on TE tunnels that are protected by multiple backup tunnels merging at a single node.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to enable record-route on the TE tunnel:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# record-route
```

Related Commands

Command	Description
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.

reoptimize timers delay (MPLS-TE)

To delay removal or relabeling of the old label switched paths (LSPs) (reoptimized LSP from the forwarding plane) after tunnel reoptimization, use the **reoptimize timers delay** command in MPLS-TE configuration mode. To restore the default value, use the **no** form of this command.

reoptimize timers delay {**after-frr** *seconds*| **cleanup** *delay-time*| **installation** *delay-time*| **path-protection** *seconds*}

no reoptimize timers delay {**after-frr** *seconds*| **cleanup** *delay-time*| **installation** *delay-time*| **path-protection** *seconds*}

Syntax Description

after-frr	Delays the LSP reoptimization in the event of the FRR.
seconds	Reoptimization initiation delay time of the tunnel, in seconds, after an FRR event. Range is from 0 to 120.
cleanup	Delays removal of the old LSPs after tunnel reoptimization.
delay-time	Reoptimization delay time, in seconds. A value of 0 disables delay. The valid range is from 0 to 300 for cleanup time.
installation	Delays installation of a new label after tunnel reoptimization.
delay-time	Reoptimization delay time, in seconds. A value of 0 disables delay. The valid range is 0 to 3600 for installation time.
path-protection	Delays the time between path protection switchover event and tunnel reoptimization.
seconds	Time, in seconds, between path protection switchover event and tunnel reoptimization. A value of 0 disables delay. Range is from 0 to 604800.

Command Default   **after-frr** *delay*: 0

cleanup *delay*: 20

delay-time: 20

installation *delay*: 20

path-protection: 180

Command Modes   MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   A device with Multiprotocol Label Switching traffic engineering (MPLS-TE) tunnels periodically examines tunnels with established LSPs to discover whether more efficient LSPs (paths) are available. If a better LSP is available, the device signals the more efficient LSP; if the signaling is successful, the device replaces the older LSP with the new, more efficient LSP.

Sometimes the slower router-point nodes may not yet utilize the new label's forwarding plane. In this case, if the headend node replaces the labels quickly, it can result in brief packet loss. By delaying the cleanup of the old LSP using the **reoptimize timers delay cleanup** command, packet loss is avoided.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to set the reoptimization cleanup delay time to 1 minute:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# reoptimize timers delay cleanup 60
```

The following example shows how to set the reoptimization installation delay time to 40 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# reoptimize timers delay installation 40
```

The following example shows how to set the reoptimization delay time after the event of the FRR to 50 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# reoptimize timers delay after-frr 50
```

The following example shows how to set the reoptimization delay time between path protection switchover event and tunnel reoptimization to 80:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# reoptimize timers delay path-protection 80
```

Related Commands

Command	Description
reoptimize (MPLS-TE)	Reoptimizes all traffic engineering tunnels immediately.
mpls traffic-eng reoptimize (EXEC), on page 258	Configures the reoptimization interval of all TE tunnels.

router-id secondary (MPLS-TE)

To configure a secondary TE router identifier in MPLS-TE to be used locally (not advertised through IGP), use the **router-id secondary** command in MPLS-TE configuration mode. To return to the default behavior, use the **no** form of this command.

router-id secondary *IP address*

no router-id secondary *IP address*

Syntax Description

IP address	IPv4 address to be used as secondary TE router ID.

Command Default

No default behavior or values

Command Modes

MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **router-id secondary** command on tail end nodes to terminate verbatim tunnels to secondary TE RIDs as destinations.

You can configure up to 32 IPv4 addresses as TE secondary router IDs.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to configure a secondary TE router identifier in MPLS-TE:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# router-id secondary 1.1.1.1
RP/0/RP0/CPU0:router(config-mpls-te)# router-id secondary 2.2.2.2
```

Related Commands

Command	Description
mpls traffic-eng router-id (MPLS-TE router), on page 260	Specifies that the TE router identifier for the node is the IP address associated with a given interface.

show explicit-paths

To display the configured IP explicit paths, use the **show explicit-paths** command in EXEC mode.

show explicit-paths [**name** *path-name*| **identifier** *number*]

Syntax Description		
	name *path-name*	(Optional) Displays the name of the explicit path.
	identifier *number*	(Optional) Displays the number of the explicit path. Range is 1 to 65535.

Command Default
No default behavior or values

Command Modes
EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

An IP explicit path is a list of IP addresses that represent a node or link in the explicit path.

Task ID

Task ID	Operations
mpls-te	read

Examples
The following shows a sample output from the **show explicit-paths** command:

```
RP/0/RP0/CPU0:router# show explicit-paths

  Path ToR2    status enabled
        0x1: next-address 192.168.1.2
        0x2: next-address 10.20.20.20
  Path ToR3    status enabled
        0x1: next-address 192.168.1.2
        0x2: next-address 192.168.2.2
        0x3: next-address 10.30.30.30
  Path 100     status enabled
        0x1: next-address 192.168.1.2
```

```
             0x2: next-address 10.20.20.20
 Path 200     status enabled
             0x1: next-address 192.168.1.2
             0x2: next-address 192.168.2.2
             0x3: next-address 10.30.30.30
```

This table describes the significant fields shown in the display.

Table 27: show explicit-paths Command Field Descriptions

Field	Description
Path	Pathname or number, followed by the path status.
1: next-address	First IP address in the path.
2: next-address	Second IP address in the path.

The following shows a sample output from the **show explicit-paths** command using a specific path name:

```
RP/0/RP0/CPU0:router# show explicit-paths name ToR3

 Path ToR3     status enabled
         0x1:  next-address 192.168.1.2
         0x2:  next-address 192.168.2.2
         0x3:  next-address 10.30.30.30
```

The following shows a sample output from the **show explicit-paths** command using a specific path number:

```
RP/0/RP0/CPU0:router# show explicit-paths identifier 200

 Path 200     status enabled
         0x1:  next-address 192.168.1.2
         0x2:  next-address 192.168.2.2
         0x3:  next-address 10.30.30.30
```

Related Commands

Command	Description
index exclude-address, on page 225	Specifies the next IP address to exclude from the explicit path.
index next-address, on page 229	Specifies path entries at a specific index.

show mpls traffic-eng affinity-map

To display the color name-to-value mappings configured on the router, use the **show mpls traffic-eng affinity-map** command in EXEC mode.

show mpls traffic-eng affinity-map

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	The Bit Position field was added to the sample output.
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If the affinity value of an affinity associated with an affinity constraint is unknown, the **show mpls traffic-eng affinity-map** command output displays: "(refers to undefined affinity name)"

Task ID

Task ID	Operations
mpls-te	read

Examples

The following shows a sample output from the **show mpls traffic-eng affinity-map** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng affinity-map

  Affinity Name                        Bit-position      Affinity Value
  ----------------------------------   --------------    ----------------
    bcdefghabcdefghabcdefghabcdefgha         0                  1
                                red1         1                  2
                                red2         2                  4
                                red3         3                  8
                                red4         4                 10
                                red5         5                 20
                                red6         6                 40
                                red7         7                 80
```

```
                                      red8                   8                  100
                                      red9                   9                  200
                                     red10                  10                  400
                                     red11                  11                  800
                                     red12                  12                 1000
                                     red13                  13                 2000
                                     red14                  14                 4000
                                     red15                  15                 8000
                                     red16                  16                10000
          cdefghabcdefghabcdefghabcdefghab                  17                20000
                                     red18                  18                40000
                                     red19                  19                80000
                                     red20                  20               100000
                                     red21                  21               200000
                                     red22                  22               400000
                                     red23                  23               800000
                                     red24                  24              1000000
                                     red25                  25              2000000
                                     red26                  26              4000000
                                     red27                  27              8000000
                                   black28                  28             10000000
                                     red28                  29             20000000
                                     red30                  30             40000000
          abcdefghabcdefghabcdefghabcdefgh                  31             80000000
```

describes the significant fields shown in the display.

Table 28: show mpls traffic-eng affinity-map Field Descriptions

Field	Description
Affinity Name	Affinity name associated with the tunnel affinity constraints.
Bit-position	Bit position set in the 32-bit affinity value
Affinity Value	Affinity value associated with the affinity name.

Related Commands

Command	Description
affinity, on page 150	Configures an affinity (the properties the tunnel requires in its links) for an MPLS-TE tunnel.
affinity-map, on page 154	Assigns a numerical value to each affinity name.

show mpls traffic-eng attribute-set

To display the attribute set for MPLS-TE, use the **show mpls traffic-eng attribute-set** command in EXEC mode.

show mpls traffic-eng attribute-set [**auto-backup**| **auto-mesh**| **path-option**| [*attribute-set-name*]]

Syntax Description

auto-backup	Displays information for the auto-backup attribute type.
auto-mesh	Displays information for the auto-mesh attribute type.
path-option	Displays information for the path-option attribute type.
attribute-set-name	Specifies the name of the attribute set to be displayed.

Command Default

Displays information about all types of attribute sets.

Command Modes

EXEC mode

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

To use this command, first enable the MPLS-TE application.

Task ID

Task ID	Operation
mpls-te	read

Examples   The following command shows the attribute set for auto-backup attribute type.

```
RP/0/RP0/CPU0:router# show mpls traffic-eng attribute-set auto-backup auto1

Attribute Set Name: auto1 (Type: auto-backup)
  Affinity: 0x0/0xffff  (Default)
  Priority: 7 7 (Default)
  Record-route: Enabled
  Policy-class: 0 (Not configured)
  Logging: None
  List of protected interfaces (count 0)
  List of tunnel IDs (count 0)
```

The following command shows the attribute set for auto-mesh attribute type.

```
RP/0/RP0/CPU0:router# show mpls traffic-eng attribute-set auto-mesh mesh1

Attribute Set Name: mesh1 (Type: auto-mesh)
  Bandwidth: 0 kbps (CT0) (Default)
  Affinity: 0x0/0xffff  (Default)
  Priority: 7 7 (Default)
  Interface Bandwidth: 0 kbps (Default)
  AutoRoute Announce: Disabled
  Auto-bw: Disabled
  Soft Preemption: Disabled
  Fast Reroute: Disabled, Protection Desired: None
  Record-route: Disabled
  Policy-class: 0 (Not configured)
  Logging: None
  List of Mesh Groups (count 0)
```

The following command shows the attribute set for path-option attribute type.

```
RP/0/RP0/CPU0:router# show mpls traffic-eng attribute-set path-option path1

Attribute Set Name: path1 (Type: path option)
  Bandwidth: 0 kbps (CT0) (Default)
  Affinity: 0x0/0xffff  (Default)
  List of tunnel IDs (count 0)
```

show mpls traffic-eng autoroute

To display tunnels that are announced to the Interior Gateway Protocol (IGP), including information about next hop and destinations, use the **show mpls traffic-eng autoroute** command in EXEC mode.

show mpls traffic-eng autoroute [*IP-address*]

Syntax Description

| *IP-address* | (Optional) Tunnel leading to this address. |

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The enhanced shortest path first (SPF) calculation of the IGP has been modified so that it uses traffic-engineering tunnels. The **show mpls traffic-eng autoroute**command displays those tunnels IGP is currently using in its enhanced SPF calculation (that is, which tunnels are up and have autoroute configured).

Tunnels are organized by destination. All tunnels to a destination carry a share of the traffic tunneled to that destination.

Task ID

Task ID	Operations
mpls-te	read

Examples

The following shows a sample output from the **show mpls traffic-eng autoroute** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng autoroute

  Destination 103.0.0.3 has 2 tunnels in OSPF 0 area 0
  tunnel-te1 (traffic share 1, nexthop 103.0.0.3)
  tunnel-te2 (traffic share 1, nexthop 103.0.0.3)
```

This table describes the significant fields shown in the display.

Table 29: show mpls traffic-eng autoroute Command Field Descriptions

Field	Description
Destination	Multiprotocol Label Switching (MPLS) TE tail-end router ID.
traffic share	A factor based on bandwidth, indicating how much traffic this tunnel should carry, relative to other tunnels, to the same destination. If two tunnels go to a single destination, one with a traffic share of 200 and the other with a traffic share of 100, the first tunnel carries two-thirds of the traffic.
Nexthop	Next-hop router ID of the MPLS-TE tunnel.
absolute metric	Metric with mode absolute for the MPLS-TE tunnel.
relative metric	Metric with mode relative for the MPLS-TE tunnel.

Related Commands

Command	Description
autoroute metric, on page 172	Specifies the MPLS-TE tunnel metric that the IGP-enhanced SPF calculation will use.
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.
topology holddown sigerr (MPLS-TE), on page 421	Specifies the time that a router should ignore a link in its TE topology database in tunnel path CSPF computations following a TE tunnel signalling error on the link.

show mpls traffic-eng auto-tunnel backup

To display information about automatically build MPLS-TE backup tunnels, use the **show mpls traffic-eng auto-tunnel backup** command in EXEC mode.

show mpls traffic-eng auto-tunnel {**backup** [**private**| **summary**| **unused**]}

Syntax Description

backup	Displays information about auto-tunnel backup.
private	(Optional) Displays private information about the automatically build MPLS-TE backup tunnels.
summary	(Optional) Displays the automatically build MPLS-TE backup tunnels summary information.
unused	(Optional) Displays only unused MPLS-TE backup tunnels.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 4.0.0	This command was introduced.
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
mpls-te	read

Examples

This is sample output from the **show mpls traffic-eng auto-tunnel backup** command:

```
AutoTunnel Backup Configuration:
    Interfaces count: 4
```

```
        Unused removal timeout: 1h 0m 0s
        Configured tunnel number range: 2000-2500

AutoTunnel Backup Summary:
    AutoTunnel Backups:
            1 created, 1 up, 0 down, 0 unused
            1 NHOP, 0 NNHOP, 0 SRLG strict, 0 SRLG preferred
    Protected LSPs:
            1 NHOP, 0 NHOP+SRLG
            0 NNHOP, 0 NNHOP+SRLG
    Protected S2L Sharing Families:
            0 NHOP, 0 NHOP+SRLG
            0 NNHOP, 0 NNHOP+SRLG
    Protected S2Ls:
            0 NHOP, 0 NHOP+SRLG
            0 NNHOP, 0 NNHOP+SRLG

Cumulative Counters (last cleared 05:17:19 ago):
                        Total   NHOP  NNHOP
    Created:              1       1      0
    Connected:            1       1      0
    Removed (down):       0       0      0
    Removed (unused):     0       0      0
    Removed (in use):     0       0      0
    Range exceeded:       0       0      0

AutoTunnel Backups:
        Tunnel    State   Protection   Prot.       Protected    Protected
         Name             Offered      Flows*      Interface    Node
    -------------- ------- ------------ ------- --------------- ---------------
     tunnel-te2000    up NHOP             1         Gi0/2/0/2     N/A

    *Prot. Flows = Total Protected LSPs, S2Ls and S2L Sharing Families
```

This is sample output from the **show mpls traffic-eng auto-tunnel mesh** command:

```
RP/0/RP0/CPU0:router#show mpls traffic-eng auto-tunnel mesh

Auto-tunnel Mesh Global Configuration:
  Unused removal timeout: 2h
  Configured tunnel number range: 10000-12000

Auto-tunnel Mesh Groups Summary:
  Mesh Groups count: 5
Mesh Groups Destinations count: 50

Mesh Group 40 (2 Destinations, 1 Up, 1 Down):
  Destination-list: dl-40
  Attribute-set: ta_name
  Destination: 40.40.40.40, tunnel-id: 10000, State: Up
  Destination: 10.10.10.10, tunnel-id: 10001, State: Down
Mesh Group 41 (3 Destinations, 2 Up, 1 Down):
  Destination-list: dl-40
  Attribute-set: ta_name
  Destination: 4.4.4.4, tunnel-id: 10005, State: Up
  Destination: 3.3.3.3, tunnel-id: 10006, State: Up
  Destination: 1.1.1.1, tunnel-id: 10007, State: Down
Mesh Group 51 (0 Destinations, 0 Up, 0 Down):
  Destination-list: Not configured
  Attribute-set: Not configured
Mesh Group 52 (0 Destinations, 0 Up, 0 Down):
  Destination-list: NAME1 (Not defined)
  Attribute-set: NAME2 (Not defined)
Mesh Group 53 (2 Destinations, 1 Up, 1 Down):
  Destination-list: dl-53
  Attribute-set: Not configured
  Destination: 40.40.40.40, tunnel-id: 10000, State: Up
  Destination: 10.10.10.10, tunnel-id: 10001, State: Down


Cumulative Counters (last cleared 7h ago):
                  Total
  Created:          100
```

```
   Connected:          50
   Removed (unused):    50
   Removed (in use):     0
   Range exceeded:       0
```

This is sample output from the **show mpls traffic-eng auto-tunnel private** command:

```
Auto-tunnel Mesh Private Information:
  ID allocator overall maximum ID: 4096
  ID allocator last allocated ID: 50999
  ID allocator number IDs allocated: 1000
```

show mpls traffic-eng auto-tunnel mesh

To display information about automatically built MPLS-TE mesh tunnels, use the **show mpls traffic-eng auto-tunnel mesh** command in EXEC mode.

show mpls traffic-eng auto-tunnel mesh {*mesh-value*| **unused**| **summary**| **attribute-set** *name*| **destination** *address*| **destination-list** *name*| **down**| **up**| **tunnel** {**created**| **not-created**}}

Syntax Description

mesh *mesh-value*	Displays the tunnels that belong to the specified auto-tunnel mesh group. The range of mesh group ID is from 0 to 4294967295.
attribute-set *name*	Displays mesh-groups configured with a specific attribute set.
destination *address*	Displays only the destinations with a specified address.
destination-list *name*	Displays mesh-groups configured with a specified prefix-list.
down	Displays only those tunnels that are down.
up	Displays only those tunnels that are up.
summary	Displays auto-tunnel mesh summary information.
unused	Displays only the down tunnels with no destination in the topology.
**tunnel created	not-created**	Specifies either created destinations with tunnels, or not-created destinations without tunnels.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.1.1	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
MPLS-TE	read

Examples

This is sample output from the **show mpls traffic-eng auto-tunnel mesh** command:

```
RP/0/RP0/CPU0:router show mpls traffic-eng auto-tunnel mesh

Auto-tunnel Mesh Global Configuration:
  Unused removal timeout: 1h 0m 0s
  Configured tunnel number range: 1000-1200

Auto-tunnel Mesh Groups Summary:
  Mesh Groups count: 1
  Mesh Groups Destinations count: 3
  Mesh Groups Tunnels count:
    3 created, 0 up, 3 down, 0 FRR enabled

Mesh Group: 65 (3 Destinations)
  Status: Enabled
  Attribute-set: am-65
  Destination-list: dl-65 (Not a prefix-list)
  Recreate timer: Not running
      Destination    Tunnel ID    State  Unused timer
      ----------------  -----------  -------  -----------
      192.168.0.2         1000       up   Not running
      192.168.0.3         1001       up   Not running
      192.168.0.4         1002       up   Not running
  Displayed 3 tunnels, 0 up, 3 down, 0 FRR enabled

Auto-mesh Cumulative Counters:
  Last cleared: Wed Nov  9 12:56:37 2011 (02:39:07 ago)
                    Total
  Created:              3
  Connected:            0
  Removed (unused):     0
  Removed (in use):     0
  Range exceeded:       0
```

This shows how to configure the **auto-tunnel mesh** command with **destination-list** and **attribute-set** keywords:

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# auto-tunnel mesh
RP/0/RP0/CPU0:router(config-te-auto-mesh)# group 65
RP/0/RP0/CPU0:router(config-te-mesh-group)# disable
RP/0/RP0/CPU0:router(config-te-mesh-group)# destination-list dl-65
RP/0/RP0/CPU0:router(config-te-mesh-group)# attribute-set am-65
```

Note This **attribute-set** is an optional configuration. Without this configuration, all tunnels use default tunnel attribute values. If you configure an non-existent attribute-set, this mesh group does not create any tunnel.

Note This **destination-list** configuration is mandatory. If there is no IPv4 prefix-list by this name on the this mesh group create tunnels with all routers in the network.

show mpls traffic-eng collaborator-timers

To display the current status of the MPLS-TE collaborator timers, use the **show mpls traffic-eng collaborator-timers** command in EXEC mode.

show mpls traffic-eng collaborator-timers

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The MPLS-TE process maintains the timers for all of the collaborators such as RSVP, LSD, and so forth. The **show mpls traffic-eng collaborator-timers** command shows the status of these timers.

Task ID

Task ID	Operations
mpls-te	read

Examples   The following sample output shows the current status of the collaborator timers:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng collaborator-timers

Collaborator Timers
-------------------
Timer Name: [LMRIB Restart] Index:[0]
    Duration: [60] Is running: NO
    Last start time:  02/09/2009 11:57:59
    Last stop time:   02/09/2009 11:58:00
    Last expiry time: Never expired
Timer Name: [LMRIB Recovery] Index:[1]
    Duration: [60] Is running: YES
    Last start time:  02/09/2009 11:58:00
    Last stop time:   Never Stopped
    Last expiry time: 19/08/2009 17:45:24
Timer Name: [RSVP Restart] Index:[2]
```

```
            Duration: [180] Is running: NO
            Last start time:  26/08/2009 18:59:18
            Last stop time:   26/08/2009 18:59:20
            Last expiry time: Never expired
Timer Name: [RSVP Recovery] Index:[3]
            Duration: [1800] Is running: NO
            Last start time:  26/08/2009 18:59:20
            Last stop time:   26/08/2009 19:03:19
            Last expiry time: 19/08/2009 18:12:39
Timer Name: [LSD Restart] Index:[4]
            Duration: [60] Is running: NO
            Last start time:  19/08/2009 17:44:26
            Last stop time:   19/08/2009 17:44:26
            Last expiry time: Never expired
Timer Name: [LSD Recovery] Index:[5]
            Duration: [600] Is running: NO
            Last start time:  19/08/2009 17:44:26
            Last stop time:   Never Stopped
            Last expiry time: 19/08/2009 17:53:44
Timer Name: [Clearing in progress BW for the whole topology] Index:[6]
            Duration: [60] Is running: YES
            Last start time:  02/09/2009 11:57:50
            Last stop time:   Never Stopped
            Last expiry time: 02/09/2009 11:57:50
```

This table describes the significant fields shown in the display.

Table 30: show mpls traffic-eng collaborator-timers Command Field Descriptions

Field	Description
Timer Name	Timer name that is associated to a collaborator.
Index	Identification number of the timer.
Duration	Expiry delay of the timer, in seconds. For example, the duration indicates the timer interval.
Is running	Timer is running low or not.
Last start time	Last time that the collaborator process for MPLS LSD was restarted.
Last stop time	Time TE was able to reconnect to the MPLS LSD process.
Last expiry time	Time that timer expired.

show mpls traffic-eng counters signaling

To display tunnel signaling statistics, use the **show mpls traffic-eng counters signaling** command in EXEC mode.

show mpls traffic-eng counters {**signaling**| **soft-preemption**} {*tunnel -number*| **all**| [**heads** | **mids** | **tails**]| **name** *tunnel-name*| **summary**}

Syntax Description

signaling	Displays signaling counters.
soft-preemption	Displays the statistics for the soft-preemption.
tunnel-number	Statistics for the input tunnel number. The range is from 0 to 65535.
all	Displays statistics for all tunnels.
heads	(Optional) Displays statistics for all tunnel heads.
mids	(Optional) Displays statistics for all tunnel midpoints.
tails	(Optional) Displays statistics for all tunnel tails.
name	Displays statistics for a specified tunnel.
tunnel-name	Name of the specified tunnel.
summary	Displays a summary of signaling statistics.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.2.0	The **soft-preemption** keyword was added.

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read

Examples

This is a sample output from the **show mpls traffic-eng counters signaling** command, using the **all** keyword, which displays tunnel signaling statistics for all tunnels:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng counters signaling all


  Tunnel Head: tunnel-te100
  Cumulative Tunnel Counters:
    Signalling Events      Recv     Xmit                           Recv     Xmit
      PathCreate            1        1      ResvCreate              1        0
      PathChange            0        0      ResvChange              0        0
      PathError             0        0      ResvError               0        0
      PathTear              0        18     ResvTear                0        0
      BackupAssign          0        1      BackupError             0        0
      PathQuery             0        0      Unknown                 0        0

  Destination 100.0.0.4
  Cumulative counters
    Signalling Events      Recv     Xmit                           Recv     Xmit
      PathCreate            1        1      ResvCreate              1        0
      PathChange            0        0      ResvChange              0        0
      PathError             0        0      ResvError               0        0
      PathTear              0        18     ResvTear                0        0
      BackupAssign          0        1      BackupError             0        0
      PathQuery             0        0      Unknown                 0        0
    S2L LSP ID: 2 Sub-Grp ID: 0 Destination: 100.0.0.4
    Signalling Events      Recv     Xmit                           Recv     Xmit
      PathCreate            1        1      ResvCreate              1        0
      PathChange            0        0      ResvChange              0        0
      PathError             0        0      ResvError               0        0
      PathTear              0        0      ResvTear                0        0
      BackupAssign          0        1      BackupError             0        0
      PathQuery             0        0      Unknown                 0        0

  Tunnel Head: tunnel-mte200
  Cumulative Tunnel Counters:
    Signalling Events      Recv     Xmit                           Recv     Xmit
      PathCreate            2        2      ResvCreate              2        0
      PathChange            0        0      ResvChange              0        0
      PathError             0        0      ResvError               0        0
      PathTear              0        20     ResvTear                0        0
      BackupAssign          0        2      BackupError             0        0
      PathQuery             0        0      Unknown                 0        0

  Destination 100.0.0.4
  Cumulative counters
```

Signalling Events	Recv	Xmit		Recv	Xmit
PathCreate	2	2	ResvCreate	2	0
PathChange	0	0	ResvChange	0	0
PathError	0	0	ResvError	0	0
PathTear	0	20	ResvTear	0	0
BackupAssign	0	2	BackupError	0	0
PathQuery	0	0	Unknown	0	0

S2L LSP ID: 10021 Sub-Grp ID: 1 Destination: 100.0.0.4

Signalling Events	Recv	Xmit		Recv	Xmit
PathCreate	1	1	ResvCreate	1	0
PathChange	0	0	ResvChange	0	0
PathError	0	0	ResvError	0	0
PathTear	0	0	ResvTear	0	0
BackupAssign	0	1	BackupError	0	0
PathQuery	0	0	Unknown	0	0

Tunnel Mid/Tail: router Source: 100.0.0.1 P2MP ID: 1677721603 Tunnel ID: 1 LSP ID: 21
Cumulative LSP Counters:

Signalling Events	Recv	Xmit		Recv	Xmit
PathCreate	2	1	ResvCreate	2	1
PathChange	0	0	ResvChange	0	0
PathError	0	0	ResvError	0	0
PathTear	0	0	ResvTear	0	0
BackupAssign	0	0	BackupError	0	0
PathQuery	0	0	Unknown	0	0

S2L LSP ID: 21 Sub-Grp ID: 0 Destination: 100.0.0.3

Signalling Events	Recv	Xmit		Recv	Xmit
PathCreate	2	1	ResvCreate	2	1
PathChange	0	0	ResvChange	0	0
PathError	0	0	ResvError	0	0
PathTear	0	0	ResvTear	0	0
BackupAssign	0	0	BackupError	0	0
PathQuery	0	0	Unknown	0	0

Tunnel Mid/Tail: router Source: 100.0.0.1 P2MP ID: 1677721603 Tunnel ID: 2 LSP ID: 21
Cumulative LSP Counters:

Signalling Events	Recv	Xmit		Recv	Xmit
PathCreate	2	1	ResvCreate	2	1
PathChange	0	0	ResvChange	0	0
PathError	0	0	ResvError	0	0
PathTear	0	0	ResvTear	0	0
BackupAssign	0	0	BackupError	0	0
PathQuery	0	0	Unknown	0	0

S2L LSP ID: 21 Sub-Grp ID: 0 Destination: 100.0.0.3

Signalling Events	Recv	Xmit		Recv	Xmit
PathCreate	2	1	ResvCreate	2	1
PathChange	0	0	ResvChange	0	0
PathError	0	0	ResvError	0	0
PathTear	0	0	ResvTear	0	0
BackupAssign	0	0	BackupError	0	0
PathQuery	0	0	Unknown	0	0

Tunnel Mid/Tail: router-1_t3 Source: 100.0.0.1 P2MP ID: 1677721603 Tunnel ID: 3 LSP ID: 18
Cumulative LSP Counters:

Signalling Events	Recv	Xmit		Recv	Xmit
PathCreate	2	1	ResvCreate	2	1
PathChange	0	0	ResvChange	0	0
PathError	0	0	ResvError	0	0
PathTear	0	0	ResvTear	0	0
BackupAssign	0	0	BackupError	0	0
PathQuery	0	0	Unknown	0	0

S2L LSP ID: 18 Sub-Grp ID: 0 Destination: 100.0.0.3

Signalling Events	Recv	Xmit		Recv	Xmit
PathCreate	2	1	ResvCreate	2	1
PathChange	0	0	ResvChange	0	0
PathError	0	0	ResvError	0	0
PathTear	0	0	ResvTear	0	0
BackupAssign	0	0	BackupError	0	0
PathQuery	0	0	Unknown	0	0

Tunnel Mid/Tail: router-3_t33 Source: 100.0.0.3 P2MP ID: 1677721605 Tunnel ID: 33 LSP ID: 2

```
Cumulative LSP Counters:
  Signalling Events     Recv    Xmit                           Recv    Xmit
    PathCreate            2       1      ResvCreate             2       1
    PathChange            0       0      ResvChange             0       0
    PathError             0       0      ResvError              0       0
    PathTear              0       0      ResvTear               0       0
    BackupAssign          0       0      BackupError            0       0
    PathQuery             0       0      Unknown                0       0
  S2L LSP ID: 2 Sub-Grp ID: 0 Destination: 100.0.0.5
  Signalling Events     Recv    Xmit                           Recv    Xmit
    PathCreate            2       1      ResvCreate             2       1
    PathChange            0       0      ResvChange             0       0
    PathError             0       0      ResvError              0       0
    PathTear              0       0      ResvTear               0       0
    BackupAssign          0       0      BackupError            0       0
    PathQuery             0       0      Unknown                0       0

Signaling Counter Summary:
  Signalling Events     Recv    Xmit                           Recv    Xmit
    PathCreate           11       7      ResvCreate            11       4
    PathChange            0       0      ResvChange             0       0
    PathError             0       0      ResvError              0       0
    PathTear              0      38      ResvTear               0       0
    BackupAssign          0       3      BackupError            0       0
    PathQuery             0       0      Unknown                0       0
```

This is a sample output from the **show mpls traffic-eng counters signaling** command using the *tunnel number* argument, which displays statistics for the input tunnel number:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng counters signaling 200

Tunnel Head: tunnel-te200
Cumulative Tunnel Counters:
  Signalling Events  Recv    Xmit                           Recv    Xmit
    PathCreate          4       4      ResvCreate             4       0
    PathChange          0       0      ResvChange             0       0
    PathError           0       0      ResvError              0       0
    PathTear            0       1      ResvTear               0       0
    BackupAssign        0       4      BackupError            0       0
    PathQuery           0       0      Unknown                0       0

 Destination 3.3.3.3
 Cumulative counters
  Signalling Events  Recv    Xmit                           Recv    Xmit
    PathCreate          4       4      ResvCreate             4       0
    PathChange          0       0      ResvChange             0       0
    PathError           0       0      ResvError              0       0
    PathTear            0       1      ResvTear               0       0
    BackupAssign        0       4      BackupError            0       0
    PathQuery           0       0      Unknown                0       0
 S2L LSP ID: 3 Sub-Grp ID: 0 Destination: 3.3.3.3
  Signalling Events  Recv    Xmit                           Recv    Xmit
    PathCreate          3       3      ResvCreate             3       0
    PathChange          0       0      ResvChange             0       0
    PathError           0       0      ResvError              0       0
    PathTear            0       0      ResvTear               0       0
    BackupAssign        0       3      BackupError            0       0
    PathQuery           0       0      Unknown                0       0
```

This table describes the significant fields shown in the display.

Table 31: show mpls traffic-eng counters signaling Command Field Descriptions

Field	Description
Tunnel Head	Tunnel head identifier.

Field	Description
Match Resv Create	Number of RSVP Reservation create messages received.
Sender Create	Number of Sender Create messages sent by TE to RSVP.
Path Error	Number of RSVP Path Error messages received.
Match Resv Change	Number of RSVP Reservation change messages received.
Sender Modify	Number of Sender Modify messages sent by TE to RSVP.
Path Change	Number of RSVP Path Change messages received.
Match Resv Delete	Number of RSVP Reservation delete messages received.
Sender Delete	Number of Sender Delete messages sent by TE to RSVP.
Path Delete	Number of RSVP Path Delete messages received.
Total	Total signaling messages received from RSVP.
Unknown	Unknown messages include fast reroute events and internal messages related to process restart.

This is sample output from the **show mpls traffic-eng counters soft-preemption** command, which displays statistics for the soft preempted LSPs:

```
RP/0/RP0/CPU0:routershow mpls traffic-eng counters soft-preemption

Soft Preemption Global Counters:
 Last Cleared: Never
 Preemption Node Stats:
   Number of soft preemption events: 1
   Number of soft preempted LSPs: 1
   Number of soft preempted LSPs that timed out: 0
   Number of soft preempted LSPs that were torn down: 0
   Number of soft preempted LSPs that were fast rerouted: 0
   Minimum Time in Soft Preemption Pending State (sec): 0
   Maximum Time in Soft Preemption Pending State (sec): 0
   Average Time in Soft Preemption Pending State (sec): 0
 Headend Stats:
   Number of soft preempted LSPs: 1
   Number of reoptimized soft preempted headend-LSPs: 0
   Number of path protected switchover soft preempted headend-LSPs: 0
   Number of torn down soft preempted headend-LSPs: 0
```

Related Commands

Command	Description
clear mpls traffic-eng counters signaling, on page 191	Clears the counters for MPLS-TE tunnels.
clear mpls traffic-eng fast-reroute log, on page 195	Clears the counters for MPLS-TE tunnels.
soft-preemption	Enables soft-preemption on a head-end for the MPLS TE tunnel.

show mpls traffic-eng ds-te te-class

To display the Diff-Serv TE-class map in use, use the **show mpls traffic-eng ds-te te-class** command in EXEC mode.

show show mpls traffic-eng ds-te te-class

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note   TE-class is used only in IETF DS-TE mode.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following shows a sample output from the **show mpls traffic-eng ds-te te-class** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng ds-te te-class

  te-class 0: class-type 0 priority 7 status default
  te-class 1: class-type 1 priority 7 status default
  te-class 2: unused
  te-class 3: unused
  te-class 4: class-type 0 priority 0 status default
  te-class 5: class-type 1 priority 0 status default
  te-class 6: unused
  te-class 7: unused
```

This table describes the significant fields shown in the display.

Table 32: show mpls traffic-eng ds-te te-class Command Field Descriptions

Field	Description
te-class	TE-class map, pair of class-type, and priority.
class-type	class-type of the tunnel.
status	Source of the TE-class map, either default or user configured.

show mpls traffic-eng forwarding

To display forwarding information on tunnels that were admitted locally, use the **show mpls traffic-eng forwarding** command in EXEC mode.

show mpls traffic-eng forwarding [**backup-name** *tunnel-name*] [**signalled-name** *tunnel-name*] [**source** *source-address*][**tunnel-id** *tunnel-id*] [**interface** {**in** | **inout** | **out**} *type interface-path-id*] **[detail]**

Syntax Description	
backup-name *tunnel-name*	(Optional) Restricts tunnels with this backup tunnel name.
signalled-name *tunnel-name*	(Optional) Restricts tunnels with this signalled tunnel name.
source *source-address*	(Optional) Restricts tunnels for this specified tunnel source IPv4 address.
tunnel-id *tunnel-id*	(Optional) Restricts tunnels for this tunnel identifier. Range for the *tunnel-id* argument is from 0 to 65535.
interface	(Optional) Displays information on the specified interface.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
in	Displays information for the input interface.
inout	Displays information for either the input or output interface.
out	Displays information for the output interface.
p2p	(Optional) Displays only Point-to-Point (P2P) information.
detail	(Optional) Displays detailed forwarding information.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read

Examples   The following shows a sample output from the **show mpls traffic-eng forwarding** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng forwarding

Tue Sep 15 14:22:39.609 UTC P2P tunnels

Tunnel ID            Ingress IF   Egress IF    In lbl   Out lbl  Backup tunnel
-------------------- ------------ ------------ -------- -------- -------------
2.2.2.2 2_2          Gi0/0/0/3    Gi0/0/0/4    16004    16020    unknown
6.6.6.6 1_23         -            Gi0/0/0/3    16000    3        tt1300
6.6.6.6 1100_9       -            Gi0/0/0/3    16002    16001    unknown
6.6.6.6 1200_9       -            Gi0/0/0/3    16001    16000    unknown
6.6.6.6 1300_2       -            Gi0/0/0/4    16005    16021    unknown
6.6.6.6 1400_9       -            Gi0/0/0/3    16003    16002    unknown
```

This table describes the significant fields shown in the display.

Table 33: show mpls traffic-eng forwarding Field Descriptions

Field	Description
TUNNEL ID	Tunnel identification.
Ingress IF	Ingress interface of the tunnel.
Egress IF	Egress interface of the tunnel.
In lbl	Incoming label associated with the tunnel.

Field	Description
Out lbl	Outgoing label associated with the tunnel.
Backup tunnel	Fast Reroute backup tunnel

show mpls traffic-eng forwarding-adjacency

To display forwarding-adjacency information for an IPv4 address, use the **show mpls traffic-eng forwarding-adjacency** command in EXEC mode.

show mpls traffic-eng forwarding-adjacency [*IP-address*]

Syntax Description

IP-address	(Optional) Destination IPv4 address for forwarding adjacency.

Command Default　No default behavior or values

Command Modes　EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines　To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read

Examples　The following shows a sample output from the **show mpls traffic-eng forwarding-adjacency** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng forwarding-adjacency

destination 3.3.3.3 has 1 tunnels
tunnel-te1    (traffic share 0, next-hop 3.3.3.3)
(Adjacency Announced: yes, holdtime 0)
```

Related Commands

Command	Description
forwarding-adjacency, on page 223	Configures an MPLS-TE forwarding adjacency.

show mpls traffic-eng igp-areas

To display MPLS-TE internal area storage, use the **show mpls traffic-eng igp-areas** command in EXEC mode.

show mpls traffic-eng igp-areas [detail]

Syntax Description

detail	(Optional) Displays detailed information about the configured MPLS-TE igp-areas and communication statistics with IGPs.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read

Examples

This table describes the significant fields shown in the display.

Table 34: show mpls traffic-eng igp-areas Command Field Descriptions

Field	Description
Global router-id	Global router ID on this node.
IGP ID	IGP System ID.
area	IGP area.

Field	Description
TE index	Internal index in the IGP area table.
IGP config for TE	Whether the IGP configuration is complete or missing.

show mpls traffic-eng link-management admission-control

To display which tunnels were admitted locally and their parameters, use the **show mpls traffic-eng link-management admission-control** command in EXEC mode.

show mpls traffic-eng link-management admission-control [**interface** *type interface-path-id*]

Syntax Description

interface	(Optional) Displays information on the specified interface.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read

Examples

The following shows a sample output from the **show mpls traffic-eng link-management admission-control** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng link-management admission-control
```

```
    S System Information:
          Tunnels Count     : 2
          Tunnels Selected  : 2
      Bandwidth descriptor legend:
        B0 = bw from pool 0, B1 = bw from pool 1, R = bw locked, H = bw held

    TUNNEL ID               UP IF      DOWN IF    PRI STATE         BW (kbits/sec)
    ----------------------- ---------- ---------- --- ------------- ---------------
    10.10.10.10 1_34          -        PO0/2/0/1  7/7 Resv Admitted 100       RB0
    10.10.10.10 15_2          -        PO0/2/0/2  7/7 Resv Admitted 0          B0
```

This table describes the significant fields shown in the display.

Table 35: show mpls traffic-eng link-management admission-control Command Field Descriptions

Field	Description
Tunnels Count	Total number of tunnels admitted.
Tunnels Selected	Number of tunnels displayed.
Bandwidth descriptor legend	BW pool type and status displayed with the tunnel entry. Shown as RG (Locked BW in global pool) in the preceding sample output.
TUNNEL ID	Tunnel identification.
UP IF	Upstream interface used by the tunnel.
DOWN IF	Downstream interface used by the tunnel.
PRI	Tunnel setup priority and hold priority.
STATE	Tunnel admission status.
BW (kbps)	Tunnel bandwidth in kilobits per second. If an R follows the bandwidth number, the bandwidth is reserved. If an H follows the bandwidth number, the bandwidth is temporarily being held for a Path message. If a G follows the bandwidth number, the bandwidth is from the global pool. If an S follows the bandwidth number the bandwidth is from the sub-pool.

The following shows a sample output from the **show mpls traffic-eng link-management interface** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng link-management interface pos 0/2/0/1

    System Information::
        Links Count       : 1

    Link ID:: POS0/2/0/1 (35.0.0.5)
      Local Intf ID: 7
      Link Status:
```

```
           Link Label Type          : PSC (inactive)
           Physical BW              : 155520 kbits/sec
           BCID                         : RDM
           Max Reservable BW    : 0 kbits/sec (reserved: 100% in, 100% out)
           BC0 (Res. Global BW): 0 kbits/sec (reserved: 100% in, 100% out)
           BC1 (Res. Sub BW)    : 0 kbits/sec (reserved: 100% in, 100% out)
           MPLS-TE Link State   : MPLS-TE on, RSVP on
           Inbound Admission     : allow-all
           Outbound Admission    : allow-if-room
           IGP Neighbor Count    : 0
           Max Res BW (RDM)    : 0 kbits/sec
           BC0 (RDM)                   : 0 kbits/sec
           BC1 (RDM)                   : 0 kbits/sec
           Max Res BW (MAM)   : 0 kbits/sec
           BC0 (MAM)                   : 0 kbits/sec
           BC1 (MAM)                   : 0 kbits/sec
           Admin Weight             : 1 (OSPF), 10 (ISIS)
           Attributes                   : 0x5 (name-based)
           Flooding Status: (1 area)
             IGP Area[1]: ospf 100 area 0, not flooded
                     (Reason: Interface has been administratively disabled)
```

This table describes the significant fields shown in the display.

Table 36: show mpls traffic-eng link-management interface Command Field Descriptions

Field	Description
Links Count	Number of links configured for MPLS-TE.
Link ID	Index of the link described.
Local Intf ID	Local interface ID.
Link Label Type	Label type of the link, for instance: PSC[17], TDM[18], FSC[19].
Physical BW	Link bandwidth capacity (in kilobits per second).
BCID	Bandwidth constraint model ID (RDM or MAM).
Max Reservable BW	Maximum reservable bandwidth on this link.
BC0 (Res. Global BW)	Bandwidth constraint value for class-type 0.
BC1 (Res. Sub BW)	Bandwidth constraint value for class-type 1.
MPLS-TE Link State	Status of the link MPLS-TE-related functions.
Inbound Admission	Link admission policy for incoming tunnels.
Outbound Admission	Link admission policy for outgoing tunnels.
IGP Neighbor Count	IGP neighbors directly reachable over this link.
Max Res BW (RDM)	Maximum reservable bandwidth on this link for RDM.

Field	Description
BC0 (RDM)	Bandwidth constraint value for RDM.
BC1 (RDM)	Bandwidth constraint value for RDM.
Admin Weight	Administrative weight associated with this link.
Attributes	Interface attributes referring to one or more affinity names.
IGP Area[1]	IGP type and area and level used for TE flooding.

17 PSC = Packet switch capable.

18 TDM = Time-division multiplexing.

19 FSC = Fiber switch capable.

show mpls traffic-eng link-management advertisements

To display local link information that MPLS-TE link management is currently flooding into the global TE topology, use the **show mpls traffic-eng link-management advertisements** command in EXEC mode.

show mpls traffic-eng link-management advertisements

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show mpls traffic-eng link-management advertisements** command has two output formats depending on the Diff-Serv TE Mode: one for prestandard mode and one for IETF mode.

The SRLG values are advertised for the link.

Task ID

Task ID	Operations
mpls-te	read

Examples   The following shows a sample output from the **show mpls traffic-eng link-management advertisements** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng link-management advertisements

Link ID:: 0 (GigabitEthernet0/2/0/1)
        Link IP Address      : 12.9.0.1
        O/G Intf ID          : 28
        Designated Router    : 12.9.0.2
        TE Metric            : 1
        IGP Metric           : 1
        Physical BW          : 1000000 kbits/sec
        BCID                 : RDM
        Max Reservable BW    : 10000 kbits/sec
```

```
      Res Global BW        : 10000 kbits/sec
      Res Sub BW           : 0 kbits/sec
      SRLGs                : 10, 20

      Downstream::
                           Global Pool   Sub Pool
                           -----------   -----------
        Reservable BW[0]:      10000            0   kbits/sec
        Reservable BW[1]:      10000            0   kbits/sec
        Reservable BW[2]:       9800            0   kbits/sec
        Reservable BW[3]:       9800            0   kbits/sec
        Reservable BW[4]:       9800            0   kbits/sec
        Reservable BW[5]:       9800            0   kbits/sec
        Reservable BW[6]:       9800            0   kbits/sec
        Reservable BW[7]:       9800            0   kbits/sec

      Attribute Flags: 0x00000004
      Attribute Names: red2

    Link ID:: 1 (GigabitEthernet0/2/0/2)
        Link IP Address    : 14.9.0.1
        O/G Intf ID        : 29
        Designated Router  : 14.9.0.4
        TE Metric          : 1
        IGP Metric         : 1
        Physical BW        : 1000000 kbits/sec
        BCID               : RDM
        Max Reservable BW  : 750000 kbits/sec
        Res Global BW      : 750000 kbits/sec
        Res Sub BW         : 0 kbits/sec

        Downstream::
                           Global Pool   Sub Pool
                           -----------   -----------
          Reservable BW[0]:     750000           0   kbits/sec
          Reservable BW[1]:     750000           0   kbits/sec
          Reservable BW[2]:     750000           0   kbits/sec
          Reservable BW[3]:     750000           0   kbits/sec
          Reservable BW[4]:     750000           0   kbits/sec
          Reservable BW[5]:     750000           0   kbits/sec
          Reservable BW[6]:     750000           0   kbits/sec
          Reservable BW[7]:     750000           0   kbits/sec

      Attribute Flags: 0x00000000
      Attribute Names:
```

This table describes the significant fields shown in the display.

Table 37: show mpls traffic-eng link-management advertisements Command Field Descriptions

Field	Description
Link ID	Index of the link described.
Link IP Address	Local IP address of the link.
TE Metric	Metric value for the TE link configured under MPLS-TE.
IGP Metric	Metric value for the TE link configured under IGP.
Physical BW	Link bandwidth capacity (in kilobits per second).
BCID	Bandwidth constraint model ID (RDM or MAM).

Field	Description
Max Reservable BW	Maximum reservable bandwidth on this link.
Res Global BW	Maximum reservable of global pool/BC0 bandwidth on this link.
Res Sub BW	Reservable sub-bandwidth for sub-pool /BC1 bandwidth on this link.
SRLGs[20]	Links that share a common fiber or a common physical attribute. If one link fails, other links in the group may also fail. Links in the group have a shared risk.
Downstream	Direction of the LSP path message.
Reservable BW[x]	Bandwidth available for reservations in the global TE topology and subpools.
Attribute Flags	Link attribute flags being flooded.
Attribute Names	Name of the affinity attribute of a link.
BC0	Bandwidth constraint value for class-type 0
BC1	Bandwidth constraint value for class-type 1
TE-class [index]	TE-class configured on this router at given index (mapping of class-type and priority), shows available bandwidth in that class.

[20] SRLGs = Shared Risk Link Groups.

show mpls traffic-eng link-management bandwidth-allocation

To display current local link information, use the **show mpls traffic-eng link-management bandwidth-allocation** command in EXEC mode.

show mpls traffic-eng link-management bandwidth-allocation [**interface** *type interface-path-id*]

Syntax Description

interface	(Optional) Displays information on the specified interface.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface.
	Note Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Advertised and current information may differ depending on how flooding is configured.

Task ID

Task ID	Operations
mpls-te	read

Examples   The following shows a sample output from the **show mpls traffic-eng link-management bandwidth-allocation** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng link bandwidth-allocation interface POS 0/2/0/1


System Information::
        Links Count        : 4
        Bandwidth Hold time : 15 seconds

    Link ID:: POS0/2/0/1 (7.2.2.1)
      Local Intf ID: 4
      Link Status:
      Link Label Type      : PSC
      Physical BW          : 155520 kbits/sec
      BCID                 : MAM
      Max Reservable BW    : 1000 kbits/sec (reserved: 0% in, 0% out)
      BC0                  : 600 kbits/sec (reserved: 2% in, 2% out)
      BC1                  : 400 kbits/sec (reserved: 0% in, 0% out)
      MPLS-TE Link State   : MPLS-TE on, RSVP on, admin-up, flooded
      Inbound Admission    : allow-all
      Outbound Admission   : allow-if-room
      IGP Neighbor Count   : 2
      BW Descriptors       : 1 (including 0 BC1 descriptors)
      Admin Weight         : 1 (OSPF), 10 (ISIS)
  Up Thresholds         : 15 30 45 60 75 80 85 90 95 96 97 98 99 100 (default)
  Down Thresholds       : 100 99 98 97 96 95 90 85 80 75 60 45 30 15 (default)

        Bandwidth Information::

        Downstream BC0 (kbits/sec):

        KEEP PRIORITY BW HELD    BW TOTAL HELD BW LOCKED  BW TOTAL LOCKED
        ------------- ---------- ------------- ---------- ---------------
                    0          0             0          0               0
                    1          0             0          0               0
                    2          0             0          0               0
                    3          0             0          0               0
                    4          0             0          0               0
                    5          0             0          0               0
                    6          0             0          0               0
                    7          0             0         10              10

        Downstream BC1 (kbits/sec):

        KEEP PRIORITY BW HELD    BW TOTAL HELD BW LOCKED  BW TOTAL LOCKED
        ------------- ---------- ------------- ---------- ---------------
                    0          0             0          0               0
                    1          0             0          0               0
                    2          0             0          0               0
                    3          0             0          0               0
                    4          0             0          0               0
                    5          0             0          0               0
                    6          0             0          0               0
```

This table describes the significant fields shown in the display.

Table 38: show mpls traffic-eng link-management bandwidth-allocation Command Field Descriptions

Field	Description
Links Count	Number of links configured for MPLS-TE.
Bandwidth Hold Time	Time, in seconds, that bandwidth can be held.

Field	Description
Link ID	Interface name and IP address of the link.
Link Label type	Label type of the link, for example: • PSC[21] • TDM[22] • FSC[23]
Physical BW	Link bandwidth capacity (in bits per second).
BCID	Bandwidth constraint model ID (RDM or MAM).
Max Reservable BW	Maximum reservable bandwidth on this link.
BC0	Maximum RSVP bandwidth in BC0.
BC1	Maximum RSVP bandwidth in BC1.
BW Descriptors	Number of bandwidth allocations on this link.
MPLS-TE Link State	Status of the link MPLS-TE-related functions.
Inbound Admission	Link admission policy for incoming tunnels.
Outbound Admission	Link admission policy for outgoing tunnels.
IGP Neighbor Count	IGP neighbors directly reachable over this link.
BW Descriptors	Internal bandwidth descriptors created when tunnels are admitted.
Admin Weight	Administrative weight associated with this link.
Up Thresholds	Threshold values used to determine link advertisement when available bandwidth increases.
Down Thresholds	Threshold values used to determine link advertisement when available bandwidth decreases.

[21] PSC = Packet switch capable.
[22] TDM = Time-division multiplexing.
[23] FSC = Fiber switch capable.

show mpls traffic-eng link-management bfd-neighbors

To display TE-enabled Bidirectional Forwarding Detection (BFD) neighbors, use the **show mpls traffic-eng link-management bfd-neighbors** command in EXEC mode.

show mpls traffic-eng link-management bfd-neighbors [**interface** *type interface-path-id*]

Syntax Description

interface	(Optional) Displays information about the specified interface.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read

Examples

The following shows a sample output from the **show mpls traffic-eng link-management bfd-neighbors** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng link-management bfd-neighbors
```

```
    Link ID:: POS0/6/0/0
    BFD Neighbor Address: 7.3.3.1, State: Up
    Link ID:: POS0/6/0/1
    No BFD Neighbor
    Link ID:: POS0/6/0/2
    BFD Neighbor Address: 7.4.4.1, State: Down
```

This table describes the significant fields shown in the display.

Table 39: show mpls traffic-eng link-management bfd Command Field Descriptions

Field	Description
Link ID	Link by which the neighbor is reached.
BFD Neighbor Address	Neighbor address and Up/Down state.

Related Commands

Command	Description
bfd fast-detect (MPLS-TE)	Enables BFD for communication failure detection.
bfd minimum-interval (MPLS-TE)	Sets the BFD interval.
bfd multiplier (MPLS-TE)	Sets the BFD multiplier.

show mpls traffic-eng link-management igp-neighbors

To display Interior Gateway Protocol (IGP) neighbors, use the **show mpls traffic-eng link-management igp-neighbors** command in EXEC mode.

show mpls traffic-eng link-management igp-neighbors [**igp-id** {**isis** *isis-address*| **ospf** *ospf-id*} [**interface** *type interface-path-id*| *IP-address*]]

Syntax Description

igp-id	(Optional) Displays the IGP neighbors that are using a specified IGP identification.
isis *isis-address*	Displays the specified Intermediate System-to-Intermediate System (IS-IS) neighbor system ID when neighbors are displayed by IGP ID.
ospf *ospf-id*	Displays the specified Open Shortest Path first (OSPF) neighbor OSPF router ID when neighbors are displayed by IGP ID.
interface	(Optional) Displays information on the specified interface.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
IP-address	(Optional) IGP neighbors that are using a specified IGP IP address.

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read

Examples

The following shows a sample output from the **show mpls traffic-eng link-management igp-neighbors** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng link igp-neighbors

    Link ID: POS0/7/0/0
      No Neighbors

    Link ID: POS0/7/0/1
      Neighbor ID: 10.90.90.90 (area: ospf   area 0, IP: 10.15.12.2)
```

This table describes the significant fields shown in the display.

Table 40: show mpls traffic-eng link-management igp-neighbors Command Field Descriptions

Field	Description
Link ID	Link by which the neighbor is reached.
Neighbor ID	IGP identification information for the neighbor.

show mpls traffic-eng link-management interfaces

To display interface resources, or a summary of link management information, use the **show mpls traffic-eng link-management interfaces** command in EXEC mode.

show mpls traffic-eng link-management interfaces [*type interface-path-id*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface.
	Note Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router.
	For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You cannot configure more than 250 links under MPLS-TE.

Task ID

Task ID	Operations
mpls-te	read

Examples

The following sample output is from the **show mpls traffic-eng link-management interfaces** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng link-management interfaces GigabitEthernet0/2/0/1
```

```
System Information::
     Links Count         : 7 (Maximum Links Supported 250)

  Link ID:: GigabitEthernet0/2/0/1 (12.9.0.1)
    Local Intf ID: 28
    Link Status:

       Link Label Type     : PSC
       Physical BW         : 1000000 kbits/sec
       BCID                : RDM
       Max Reservable BW   : 10000 kbits/sec (reserved: 2% in, 2% out)
       BC0 (Res. Global BW): 10000 kbits/sec (reserved: 2% in, 2% out)
       BC1 (Res. Sub BW)   : 0 kbits/sec (reserved: 100% in, 100% out)
       MPLS TE Link State  : MPLS TE on, RSVP on, admin-up
       Inbound Admission   : reject-huge
       Outbound Admission  : allow-if-room
       IGP Neighbor Count  : 1
       Max Res BW (RDM)    : 10000 kbits/sec
       BC0 (RDM)           : 10000 kbits/sec
       BC1 (RDM)           : 0 kbits/sec
       Max Res BW (MAM)    : 0 kbits/sec
       BC0 (MAM)           : 0 kbits/sec
       BC1 (MAM)           : 0 kbits/sec
       Attributes          : 0x4
       Attribute Names     : red2
       Flooding Status: (1 area)
         IGP Area[1]: OSPF 100 area 0, flooded
           Nbr: ID 12.9.0.2, IP 0.0.0.0 (Up)
           Admin weight: not set (TE), 1 (IGP)
```

This table describes the significant fields shown in the display.

Table 41: show mpls traffic-eng link-management interfaces Command Field Descriptions

Field	Description
Links Count	Number of links configured for MPLS-TE. Maximum number of links supported is 100.
Link ID	Link identification index.
Link Label Type	Label type assigned to the link.
Physical Bandwidth	Link bandwidth capacity (in kilobits per second).
BCID	Bandwidth constraint model ID (RDM or MAM).
Max Reservable BW	Maximum reservable bandwidth on this link.
BC0	Reservable bandwidth (in kbps) on this link in BC0.
BC1	Reservable bandwidth (in kbps) on this link in BC1.
Attributes	TE link attribute in hexadecimal.
Attribute Names	Name of the affinity attribute of a link.
MPLS-TE Link State	Status of the MPLS link.
Inbound Admission	Link admission policy for inbound tunnels.

Field	Description
Outbound Admission	Link admission policy for outbound tunnels.
IGP Neighbor Count	IGP[24] neighbors directly reachable over this link.
Admin. Weight	Administrative weight associated with this link.
Flooding Status	Status for each configured area or Flooding status for the configured area.
IGP Area	IGP type and area and level used for TE flooding.

24 IGP = Interior Gateway Protocol .

show mpls traffic-eng link-management statistics

To display interface resources or a summary of link management information, use the **show mpls traffic-eng link-management statistics** command in EXEC mode.

show mpls traffic-eng link-management statistics [**summary** | **interface** *type interface-path-id*]

Syntax Description

summary	(Optional) Displays the statistics summary.
interface	(Optional) Displays the interface for which information is requested.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show mpls traffic-eng link-management statistics** command displays resource and configuration information for all configured interfaces.

Task ID

Task ID	Operations
mpls-te	read

Examples

The following shows a sample output from the **show mpls traffic-eng link-management statistics** command using the **summary** keyword:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng link-management statistics summary

  LSP Admission Statistics:

          Setup    Setup    Setup    Setup    Tear     Tear     Tear
          Requests Admits   Rejects  Errors   Requests Preempts Errors
          -------- -------- -------- -------- -------- -------- --------
    Path       13       12        1        0       10        0        0
    Resv        8        8        0        0        5        0        0
```

Table 42: show mpls traffic-eng link-management statistics summary Command Field Descriptions, on page 352 describes the significant fields shown in the display.

Table 42: show mpls traffic-eng link-management statistics summary Command Field Descriptions

Field	Description
Path	Path information.
Resv	Reservation information.
Setup Requests	Number of requests for a setup.
Setup Admits	Number of admitted setups.
Setup Rejects	Number of rejected setups.
Setup Errors	Number of setup errors.
Tear Requests	Number of tear requests.
Tear Preempts	Number of paths torn down due to preemption.
Tear Errors	Number of tear errors.

show mpls traffic-eng link-management summary

To display a summary of link management information, use the **show mpls traffic-eng link-management summary** command in EXEC mode.

show mpls traffic-eng link-management summary

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You cannot configure more than 250 links for MPLS-TE/FRR.

Task ID

Task ID	Operations
mpls-te	read

Examples

The following sample output is from the **show mpls traffic-eng link-management summary** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng link-management summary

  System Information::
        Links Count        : 6 (Maximum Links Supported 100)
        Flooding System    : enabled
        IGP Areas Count    : 2

    IGP Areas
    ----------

    IGP Area[1]:: isis   level-2
        Flooding Protocol  : ISIS
        Flooding Status    : flooded
        Periodic Flooding  : enabled (every 180 seconds)
        Flooded Links      : 4
        IGP System ID      : 0000.0000.0002.00
```

```
           MPLS-TE Router ID   : 20.20.20.20
           IGP Neighbors       : 8

      IGP Area[2]:: ospf   area 0
           Flooding Protocol   : OSPF
           Flooding Status     : flooded
           Periodic Flooding   : enabled (every 180 seconds)
           Flooded Links       : 4
           IGP System ID       : 20.20.20.20
           MPLS-TE Router ID   : 20.20.20.20
           IGP Neighbors       : 8
```

This table describes the significant fields shown in the display.

Table 43: show mpls traffic-eng link-management summary Command Field Descriptions

Field	Description
Links Count	Number of links configured for MPLS-TE. Maximum number of links supported is 100.
Flooding System	Enable status of the MPLS-TE flooding system.
IGP Areas Count	Number of IGP[25] areas described.
IGP Area	IGP type and area and level used for TE flooding.
Flooding Protocol	IGP flooding information for this area.
Flooding Status	Status of flooding for this area.
Periodic Flooding	Status of periodic flooding for this area.
Flooded Links	Links that were flooded.
IGP System ID	IGP for the node associated with this area.
MPLS-TE Router ID	MPLS-TE router ID for this node.
IGP Neighbors	Number of reachable IGP neighbors associated with this area.

25 IGP = Interior Gateway Protocol.

show mpls traffic-eng maximum tunnels

To display the maximum number of MPLS-TE tunnels that you can configure, use the **show mpls traffic-eng maximum tunnels** command in EXEC mode.

show mpls traffic-eng maximum tunnels

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 4.0.0	Sample output was modified to support the maximum number of allowed automatic backup tunnels.
Release 4.1.1	Sample output was modified to support the maximum number of allowed automatic mesh tunnels.
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read

Examples

This is sample output from the **show mpls traffic-eng maximum tunnels** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng maximum tunnels

Maximum Global Tunnel Count:

Maximum              Current Count
--------------     --------------------
  4096             2
```

```
Maximum Global Destination Count:

Maximum            Current Count
--------------     --------------------
 4096              2

Maximum AutoTunnel Backup Count:

Maximum            Current Count
--------------     --------------------
   200                122
```

This is sample output of the automatic mesh tunnels from the **show mpls traffic-eng maximum tunnels** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng maximum tunnels

Maximum Global Tunnel Count:

Maximum      Current Count
-------      -------------
 4096             12

Maximum Static Tunnel Count:

Maximum      Current Count
-------      -------------
 4096             8

Maximum Auto-tunnel Mesh Count:

Maximum      Current Count
-------      -------------
   201            3

Maximum P2MP Tunnel Count:

Maximum      Current Count
-------      -------------
   500            1

Maximum Global Destination Count:

Maximum      Current Count
-------      -------------
 4096             13

Maximum GMPLS-UNI Tunnel Count:

Maximum      Current Count
-------      -------------
   500         39
```

describes the significant fields shown in the display.

Table 44: show mpls traffic-eng maximum tunnels Command Field Descriptions

Field	Description
Maximum P2MP Tunnel Count	Maximum number of P2MP tunnels that can be configured.
Maximum Global Destination Count	Maximum number of tunnel destinations that can be configured.
Maximum	Table heading for the maximum number in each category.
Current Count	Table heading for the current count in each category.
Maximum AutoTunnel Backup Count	Maximum number of automatic backup tunnels that can be configured.
Maximum GMPLS UNI Tunnel Count	Maximum number of Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI) tunnels that can be configured and the current tunnel count.
Maximum AutoTunnel Mesh Count	Maximum number of automatic mesh tunnels that can be configured.

Related Commands

Command	Description
maxabs (MPLS-TE), on page 244	Specifies the maximum number of tunnel TE interfaces that can be configured.
tunnel-id (auto-tunnel backup), on page 423	Configures the range of tunnel interface numbers used for automatic backup tunnels.

show mpls traffic-eng pce peer

To display the status of the path computation element (PCE) peer address and state, use the **show mpls traffic-eng pce peer** command in EXEC mode.

show mpls traffic-eng pce peer [*address* | **all**]{}

Syntax Description

address	(Optional) IPv4 peer address for the PCE.
all	(Optional) Displays all the peers for the PCE.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read

Examples   The following sample output shows the status of both the PCE peer and state:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng pce peer

  PCE Address 202.202.88.8
  State Up
    PCEP has been up for: 04:18:31
  Learned through:
    OSPF 1
  Sending KA every 30 s
  Time out peer if no KA received for 120 s
  Tolerance: Minimum KA 10 s
```

```
     KA messages rxed 518 txed 517
   PCEReq messages rxed 0, txed 0
   PCERep messages rxed 0, txed 0
   PCEErr messages rxed 0, txed 0
     Last error received:  None
     Last error sent:  None
   PCE OPEN messages: rxed 1, txed 2
   PCEP session ID: local 0, remote 0

   Average reply time from peer: 0 ms
   Minimum reply time from peer: 0 ms
   Maximum reply time from peer: 0 ms
   0 requests timed out with this peer
   Transmit TCP buffer: Current 0, Maximum 12
   Receive  TCP buffer: Current 0, Maximum 12
```

This table describes the significant fields shown in the display.

Table 45: show mpls traffic-eng pce peer Field Descriptions

Field	Description
KA	PCEP keepalive.
Learned through	Learned through is how the peer was learned which is either through a static configuration or an IGP.
Average reply time from peer	Average reply time for the peer to respond to PCEReq request messages with PCERep response messages.
Minimum reply time from peer	Minimum reply time for the peer to respond to PCEReq request messages with PCERep response messages.
Maximum reply time from peer	Maximum reply for the peer to respond to PCEReq request messages with PCERep response messages.
Transmit TCP buffer Receive TCP Buffer	Number of messages that are in the TCP buffer with the peer waiting to be sent or processed locally.
0 requests timed out with this peer	Number of PCEReq messages that timed out waiting for a response from this peer.

Related Commands

Command	Description
clear mpls traffic-eng pce, on page 197	Clears the PCE statistics.
pce address (MPLS-TE), on page 282	Configures the IPv4 self address for a PCE.
pce peer (MPLS-TE), on page 288	Configures an IPv4 self address for a PCE peer.

show mpls traffic-eng pce tunnels

To display the status of the path computation element (PCE) tunnels, use the **show mpls traffic-eng pce tunnels** command in EXEC mode.

show mpls traffic-eng pce tunnels [*tunnel-id*]

Syntax Description

tunnel-id	(Optional) Tunnel identifier. The range is 0 to 4294967295.

Command Default No default behavior or values

Command Modes EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read

Examples The following sample output shows the status of the PCE tunnels:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng pce tunnels

  Tunnel : tunnel-te10
      Destination : 205.205.10.10
      State : down, PCE failed to find path

  Tunnel : tunnel-te30
      Destination : 3.3.3.3
      State : up
      Current path option: 10, path obtained from dynamically learned PCE 1.2.3.4
      Admin weight : 15
      Hop Count : 3
```

This table describes the significant fields shown in the display.

Table 46: show mpls traffic-eng pce tunnels Command Field Descriptions

Field	Description
Tunnel	Tunnel number for the MPLS-TE tunnel interface.
Destination	IP address of the destination of the tunnel.
State	State of the tunnel. Values are up, down, or admin-down.
Admin weight	Administrative weight (cost) of the link.

Related Commands

Command	Description
pce address (MPLS-TE), on page 282	Configures the IPv4 self address for a PCE.

show mpls traffic-eng preemption log

To display the log of preemption events, use the **show mpls traffic-eng preemption log** command in EXEC mode.

show mpls traffic-eng preemption log

Syntax Description

log	Displays a log of preemption events.

Command Default None

Command Modes EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced.
Release 5.0.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
mpls-te	read

Examples This is sample output from the **show mpls traffic-eng preemption log** command displaying the log of preemption events:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng preemption log
  Bandwidth Change on GigabitEthernet0/0/0/0
    Old BW (BC0/BC1): 200000/100000, New BW (BC0/BC1): 1000/500 kbps
    BW Overshoot (BC0/BC1): 1000/0 kbps
    Preempted BW (BC0/BC1): 35000/0 kbps; Soft 30000/0 kbps; Hard 5000/0 kbps;
    Preempted 2 tunnels; Soft 1 tunnel; Hard 1 tunnel
-----------------------------------------------------------------------
 TunID LSP ID       Source       Destination Preempt  Pri  Bandwidth  BW Type
                                              Type     S/H  (in kbps)
------ ------ --------------- --------------- ------- ---- ---------- --------
     1 10002     192.168.0.1         1.0.0.0  Hard    7/7       5000      BC0
```

```
          1      2      192.168.0.1      192.168.0.4      Soft  7/7      30000      BC0
```

show mpls traffic-eng topology

To display the current MPLS-TE network topology for the node, use the **show mpls traffic-eng topology** command in EXEC mode.

show mpls traffic-eng topology [*IP-address*] **[affinity] [brief] [link-only]** [**bandwidth** *number*| **exclude-srlg** *exclude-srlg-interface-address*| **explicit-path**{**identifier** *explicit-path-id-number*| **name** *explicit-path-name*}| **priority** *level*] [**isis** *nsap-address*| **ospf** *ospf-address*| [**path** { **destination** *IP-address*| **tunnel** *P2P-tunnel-number* }]| {**router** | **network**}] [**model-type** {**rdm** | **mam**}]

Syntax Description		
IP-address		(Optional) Node IP address (router identifier to interface address).
destination *IP-address*		Displays the LSP destination IPv4 address.
exclude-srlg		Specifies an IP address to get SRLG values from for exclusion.
explicit-path		Displays the explicit LSP path.
tunnel		Displays the topology path that is based on the Point-to-Point (P2P) tunnel number.
P2P -tunnel-number		P2P tunnel number. Range is 0 to 65535.
affinity		(Optional) Displays the attribute values that are required for links carrying this tunnel. A 32-bit decimal number. Range is 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.
bandwidth *number*		(Optional) Displays the bandwidth value that is required by this label switched path (LSP).
priority *level*		(Optional) Displays the priority used when signaling a LSP for this tunnel, to determine which existing tunnels can be preempted.
isis *nsap-address*		(Optional) Displays the node router identification, if Intermediate System-to-Intermediate System (IS-IS) is enabled.

ospf *ospf-address*	(Optional) Displays the node router identifier, if Open Shortest Path First (OSPF) is enabled.
path	(Optional) Displays the path to a destination from this router.
router	Displays the given OSPF address type of the router node.
network	Displays the given OSPF address type of the network node.
brief	(Optional) Displays the brief form of the output that provides a less detailed version of the topology.
link-only	(Optional) Displays the MPLS-TE topology that is filtered by the given neighbor address.
model-type { **rdm** | **mam** }	(Optional) Displays the bandwidth constraints model type, RDM or MAM.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following shows a sample output from the **show mpls traffic-eng topology** command specifying the tunnel number in brief form:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng topology path tunnel 160

  Tunnel160 Path Setup to 10.10.10.10: FULL_PATH
  bw 100 (CT0), min_bw 0, metric: 10
  setup_pri 7, hold_pri 7
  affinity_bits 0x0, affinity_mask 0xffff
  Hop0:10.2.2.1
  Hop1:10.10.10.10
```

The following shows a sample output from the **show mpls traffic-eng topology** command specifying the destination IP address:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng topology path destination 10.10.10.10

  Path Setup to 10.10.10.10:
  bw 0 (CT0), min_bw 999900, metric: 10
  setup_pri 7, hold_pri 7
  affinity_bits 0x0, affinity_mask 0xffffffff
  Hop0:10.2.2.1
  Hop1:10.10.10.10
```

The following sample output shows the MPLS-TE network topology with the name of the affinity attribute of the link:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng topology

  Link[1]:Point-to-Point, Nbr IGP Id:3.3.3.3, Nbr Node Id:9, gen:23
        Frag Id:25, Intf Address:13.9.1.1, Intf Id:0
        Nbr Intf Address:13.9.1.3, Nbr Intf Id:0
        TE Metric:1, IGP Metric:1, Attribute Flags:0x0
        Attribute Names:
        Switching Capability:, Encoding:
        BC Model ID:RDM
        Physical BW:155520 (kbps), Max Reservable BW Global:116640 (kbps)
        Max Reservable BW Sub:0 (kbps)
                              Global Pool      Sub Pool
                Total Allocated  Reservable     Reservable
                BW (kbps)        BW (kbps)      BW (kbps)
                ---------------  -----------    ----------
        bw[0]:             0      116640                0
        bw[1]:             0      116640                0
        bw[2]:             0      116640                0
        bw[3]:             0      116640                0
        bw[4]:             0      116640                0
        bw[5]:             0      116640                0
        bw[6]:             0      116640                0
        bw[7]:             0      116640                0

    Link[2]:Broadcast, DR:12.9.0.2, Nbr Node Id:1, gen:23
        Frag Id:28, Intf Address:12.9.0.1, Intf Id:0
        Nbr Intf Address:0.0.0.0, Nbr Intf Id:0
        TE Metric:1, IGP Metric:1, Attribute Flags:0x4
        Attribute Names: red2
        Switching Capability:, Encoding:
        BC Model ID:RDM
        Physical BW:1000000 (kbps), Max Reservable BW Global:10000 (kbps)
        Max Reservable BW Sub:0 (kbps)
                              Global Pool      Sub Pool
                Total Allocated  Reservable     Reservable
                BW (kbps)        BW (kbps)      BW (kbps)
                ---------------  -----------    ----------
        bw[0]:             0       10000                0
        bw[1]:             0       10000                0
```

```
              bw[2]:               0            10000                 0
              bw[3]:               0            10000                 0
              bw[4]:               0            10000                 0
              bw[5]:               0            10000                 0
              bw[6]:               0            10000                 0
              bw[7]:               0            10000                 0
```

The following shows a sample output from the **show mpls traffic-eng topology** command in detail form in prestandard DS-TE mode:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng topology

  My_System_id: 0000.0000.0002.00 (isis   level-2)
  My_System_id: 20.20.20.20 (ospf   area 0)
  My_BC_Model_Type: RDM

  Signalling error holddown: 10 sec Global Link Generation 36

  IGP Id: 0000.0000.0002.00, MPLS-TE Id: 20.20.20.20 Router Node  (isis   level-2)

  Link[0]:Point-to-Point, Nbr IGP Id:0000.0000.0003.00, Nbr Node Id:3, gen:36
        Frag Id:0, Intf Address:7.3.3.1, Intf Id:0
         Nbr Intf Address:7.3.3.2, Nbr Intf Id:0
        TE Metric:10, IGP Metric:10, Attribute Flags:0x0
        ,

BC Model ID:RDM
Physical BW:155520 (kbps), Max Reservable BW Global:100000 (kbps)
      Max Reservable BW Sub:50000 (kbps)
                                   Global Pool      Sub Pool
                   Total Allocated  Reservable      Reservable
                   BW (kbps)        BW (kbps)       BW (kbps)
                   ---------------  -----------     ----------
          bw[0]:               0        100000           50000
          bw[1]:               0        100000           50000
          bw[2]:               0        100000           50000
          bw[3]:               0        100000           50000
          bw[4]:               0        100000           50000
          bw[5]:               0        100000           50000
          bw[6]:               0        100000           50000
          bw[7]:               0        100000           50000
```

The following shows a sample output from the **show mpls traffic-eng topology** command in detail form in IETF DS-TE mode.

```
RP/0/RP0/CPU0:router# show mpls traffic-eng topology

  My_System_id: 0000.0000.0001.00 (isis 1 level-2)
  My_System_id: 10.10.10.10 (ospf 100 area 0)
  My_BC_Model_Type: MAM

  Signalling error holddown: 10 sec Global Link Generation 84

  IGP Id: 0000.0000.0001.00, MPLS-TE Id: 10.10.10.10 Router Node  (isis 1 level-2)

  Link[0]:Point-to-Point, Nbr IGP Id:0000.0000.0002.00, Nbr Node Id:6, gen:84
        Frag Id:0, Intf Address:7.2.2.1, Intf Id:0
         Nbr Intf Address:7.2.2.2, Nbr Intf Id:0

        10,
        Switching Capability:, Encoding:
BC Model ID:MAM
        Physical BW:155520 (kbps), Max Reservable BW:1000 (kbps)
        BC0:600 (kbps) BC1:400 (kbps)
                       Total Allocated   Reservable
                       BW (kbps)         BW (kbps)
                       ---------------   -----------
          TE-class[0]:             10          590
          TE-class[1]:              0          400
          TE-class[2]:              0            0
```

```
            TE-class[3]:               0             0
            TE-class[4]:               0           600
            TE-class[5]:               0           400
 Link[1]:Point-to-Point, Nbr IGP Id:0000.0000.0002.00, Nbr Node Id:6, gen:84
        Frag Id:0, Intf Address:7.1.1.1, Intf Id:0
         Nbr Intf Address:7.1.1.2, Nbr Intf Id:0

        10,
        Switching Capability:, Encoding:
        BC Model ID:MAM
        Physical BW:155520 (kbps), Max Reservable BW:1000 (kbps) BC0:600 (kbps) BC1:400
(kbps)
                        Total Allocated   Reservable
                        BW (kbps)         BW (kbps)
                        ---------------   -----------
            TE-class[0]:              10           590
            TE-class[1]:               0           400
            TE-class[2]:               0             0
            TE-class[3]:               0             0
            TE-class[4]:               0           600
            TE-class[5]:               0           400
            TE-class[6]:               0             0
            TE-class[7]:               0             0
```

The following shows a sample output for the **show mpls traffic-eng topology** command in brief form:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng topology 192.168.0.145 brief

  IGP Id: 0000.0000.0010.00, MPLS TE Id: 192.168.0.145 Router Node  (ISIS test level-1)
    Link[0]:Point-to-Point, Nbr IGP Id:0000.0000.0234.00, Nbr Node Id:4, gen:5
        Frag Id:0, Intf Address:10.3.11.145, Intf Id:0
        Nbr Intf Address:10.3.11.143, Nbr Intf Id:0
        TE Metric:10, IGP Metric:10, Attribute Flags:0x0

        Attribute Names:  red2
        Switching Capability:, Encoding:
        BC Model ID:RDM
        Physical BW:155520 (kbps), Max Reservable BW Global:0 (kbps)
        Max Reservable BW Sub:0 (kbps)
```

The following sample output shows a brief topology for the affinity attributes:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng topology affinity

  affinity
  Mon Mar 23 13:25:47.236 EST EST
  My_System_id: 1.1.1.1 (OSPF 100 area 0)
  My_System_id: 0000.0000.0001.00 (IS-IS 100 level-2)
  My_BC_Model_Type: RDM

  Signalling error holddown: 10 sec Global Link Generation 233

  IGP Id: 0000.0000.0001.00, MPLS TE Id: 11.11.1.1 Router Node  (IS-IS 100 level-2)

  IGP Id: 1.1.1.1, MPLS TE Id: 1.1.1.1 Router Node  (OSPF 100 area 0)
    Link[0]:     Intf Address: 12.9.1.1, Nbr Intf Address: 12.9.1.2
        Attribute Flags: 0x0
        Attribute Names:
    Link[1]:     Intf Address: 13.9.1.1, Nbr Intf Address: 13.9.1.3
        Attribute Flags: 0x0
        Attribute Names:
    Link[2]:     Intf Address: 12.9.0.1, DR: 12.9.0.2
        Attribute Flags: 0x4
        Attribute Names: red2
    Link[3]:     Intf Address: 14.9.0.1, DR: 14.9.0.4
        Attribute Flags: 0x0
        Attribute Names:
    Link[4]:     Intf Address: 13.9.0.1, DR: 13.9.0.3
        Attribute Flags: 0x0
        Attribute Names:
```

```
      IGP Id: 4.4.4.4, MPLS TE Id: 4.4.4.4 Router Node  (OSPF 100 area 0)
        Link[0]:     Intf Address: 34.9.1.4, Nbr Intf Address: 34.9.1.3
            Attribute Flags: 0x0
            Attribute Names:
        Link[1]:     Intf Address: 14.9.0.4, DR: 14.9.0.4
            Attribute Flags: 0x1e
            Attribute Names: red1 red2 red3 red4
        Link[2]:     Intf Address: 24.9.0.4, DR: 24.9.0.4
            Attribute Flags: 0x0
            Attribute Names:
        Link[3]:     Intf Address: 34.9.0.4, DR: 34.9.0.3
            Attribute Flags: 0x0
            Attribute Names:
        Link[4]:     Intf Address: 24.9.1.4, Nbr Intf Address: 24.9.1.2
            Attribute Flags: 0x0
            Attribute Names:
```

The following sample output for the **show mpls traffic-eng topology** command that shows the output to a single link:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng topology 12.9.1.1 link-only

Wed Sep  2 13:24:48.821 EST


IGP Id: 0000.0000.0002.00, MPLS TE Id: 2.2.2.2 Router Node  (IS-IS 100 level-2)

  Link[0]:Point-to-Point, Nbr IGP Id:0000.0000.0001.00, Nbr Node Id:-1, gen:277740
        Frag Id:0, Intf Address:12.9.1.2, Intf Id:0
        Nbr Intf Address:12.9.1.1, Nbr Intf Id:0
        TE Metric:10, IGP Metric:10, Attribute Flags:0x0
        Attribute Names:
        Switching Capability:, Encoding:
        BC Model ID:RDM
        Physical BW:155520 (kbps), Max Reservable BW Global:116640 (kbps)
        Max Reservable BW Sub:0 (kbps)
                             Global Pool     Sub Pool
            Total Allocated   Reservable      Reservable
            BW (kbps)         BW (kbps)       BW (kbps)
            ---------------   -----------     ----------
        bw[0]:           0        116640              0
        bw[1]:           0        116640              0
        bw[2]:           0        116640              0
        bw[3]:           0        116640              0
        bw[4]:           0        116640              0
        bw[5]:           0        116640              0
        bw[6]:           0        116640              0
        bw[7]:           0        116640              0

IGP Id: 2.2.2.2, MPLS TE Id: 2.2.2.2 Router Node  (OSPF 100 area 0)

  Link[3]:Point-to-Point, Nbr IGP Id:1.1.1.1, Nbr Node Id:-1, gen:277737
        Frag Id:29, Intf Address:12.9.1.2, Intf Id:0
        Nbr Intf Address:12.9.1.1, Nbr Intf Id:0
        TE Metric:1, IGP Metric:1, Attribute Flags:0x0
        Attribute Names:
        Switching Capability:, Encoding:
        BC Model ID:RDM
        Physical BW:155520 (kbps), Max Reservable BW Global:116640 (kbps)
        Max Reservable BW Sub:0 (kbps)
                             Global Pool     Sub Pool
            Total Allocated   Reservable      Reservable
            BW (kbps)         BW (kbps)       BW (kbps)
            ---------------   -----------     ----------
        bw[0]:           0        116640              0
        bw[1]:           0        116640              0
        bw[2]:           0        116640              0
        bw[3]:           0        116640              0
        bw[4]:           0        116640              0
        bw[5]:           0        116640              0
        bw[6]:           0        116640              0
```

```
        bw[7]:                0        116640                    0
```

The following shows a sample output for the **show mpls traffic-eng topology model-type mam** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng topology model-type mam

  IGP Id: 0000.0000.0001.00, MPLS-TE Id: 10.10.10.10 Router Node  (isis 1 level-2)
    Link[0]:      Intf Address:7.2.2.1, Nbr Intf Address:7.2.2.2
    Link[1]:      Intf Address:7.1.1.1, Nbr Intf Address:7.1.1.2

  IGP Id: 0000.0000.0002.00, MPLS-TE Id: 20.20.20.20 Router Node  (isis 1 level-2)
    Link[0]:      Intf Address:7.2.2.2, Nbr Intf Address:7.2.2.1
    Link[1]:      Intf Address:7.1.1.2, Nbr Intf Address:7.1.1.1
    Link[2]:      Intf Address:7.3.3.1, Nbr Intf Address:7.3.3.2

  IGP Id: 0000.0000.0003.00, MPLS-TE Id: 30.30.30.30 Router Node  (isis 1 level-2)
    Link[0]:      Intf Address:7.3.3.2, Nbr Intf Address:7.3.3.1
```

The following shows a sample output from the **show mpls traffic-eng topology** command specifying the topology for the SRLG interfaces:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng topology srlg


Tue Oct  6 13:10:30.342 UTC
My_System_id: 0000.0000.0005.00 (IS-IS 1 level-2)

       SRLG      Interface Addr  TE Router ID    IGP Area  ID
_____        _____ _____
          1       51.1.2.1        100.0.0.1       IS-IS 1 level-2
          2       51.1.2.1        100.0.0.1       IS-IS 1 level-2
          3       51.1.2.1        100.0.0.1       IS-IS 1 level-2
          4       51.1.2.1        100.0.0.1       IS-IS 1 level-2
          5       51.1.2.1        100.0.0.1       IS-IS 1 level-2
          6       51.1.2.1        100.0.0.1       IS-IS 1 level-2
          7       51.1.2.1        100.0.0.1       IS-IS 1 level-2
          8       51.1.2.1        100.0.0.1       IS-IS 1 level-2
         10       50.4.5.5        100.0.0.5       IS-IS 1 level-2
         30       50.4.5.5        100.0.0.5       IS-IS 1 level-2
         77       50.4.5.5        100.0.0.5       IS-IS 1 level-2
         88       50.4.5.5        100.0.0.5       IS-IS 1 level-2
       1500       50.4.5.5        100.0.0.5       IS-IS 1 level-2
   10000000       50.4.5.5        100.0.0.5       IS-IS 1 level-2
 4294967290       50.4.5.5        100.0.0.5       IS-IS 1 level-2
 4294967295       50.4.5.5        100.0.0.5       IS-IS 1 level-2
```

The following shows a sample output from the **show mpls traffic-eng topology path destination** command specifying the topological path with SRLG exclusion:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng topology path destination 100.0.0.2 exclude-srlg
 50.4.5.5 isis 1 level 2

Tue Oct  6 13:13:44.053 UTC
Path Setup to 100.0.0.2:
bw 0 (CT0), min_bw 0, metric: 20
setup_pri 7, hold_pri 7
affinity_bits 0x0, affinity_mask 0xffff
Exclude SRLG Intf Addr : 50.4.5.5
SRLGs Excluded: 10, 30, 77, 88, 1500, 10000000
               4294967290, 4294967295
Hop0:50.5.1.5
Hop1:50.5.1.1
Hop2:51.1.2.1
Hop3:51.1.2.2
Hop4:100.0.0.2
```

The following shows a sample output from the **show mpls traffic-eng topology path destination** command specifying the topological path based on a given explicit path:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng topology path destination 100.0.0.2 explicit-path
 name exclude-srlg isis 1 level 2

Tue Oct  6 13:16:44.233 UTC
Path Setup to 100.0.0.2:
bw 0 (CT0), min_bw 0, metric: 20
setup_pri 7, hold_pri 7
affinity_bits 0x0, affinity_mask 0xffff
SRLGs Excluded: 10, 30, 77, 88, 1500, 10000000
                4294967290, 4294967295, 1, 2, 3, 4
                5, 6, 7, 8
Hop0:50.5.1.5
Hop1:50.5.1.1
Hop2:50.1.2.1
Hop3:50.1.2.2
Hop4:100.0.0.2
```

This table describes the significant fields shown in the display.

Table 47: show mpls traffic-eng topology Field Descriptions

Field	Description
My_System_id	IGP[26] system or IGP router ID.
Signalling error holddown	Link hold-down timer configured to handle path error events to exclude link from topology.
IGP Id	Identification of the advertising router.
Link	MPLS-TE link.
Frag Id	GP LSA[27] fragment identifier.
Nbr Intf Address	Neighbor Interface address of this link.
TE Metric	TE cost of link.
Switching Capability	Switching capability: packet, optical, lambda.
Physical BW	Physical line rate.
BC Model ID	Bandwidth constraint model ID (RDM or MAM).
Max Reservable BW	Maximum bandwidth (in kilobits per second) that you can reserve on a link.
Max Reservable BW Global	Maximum bandwidth (in kilobits per second) that you can reserve on a link in global-pool (prestandard and RDM).
Max Reservable BW Sub	Maximum bandwidth (in kilobits per second) that you can reserve on a link in subpool (prestandard and RDM).

Field	Description
BC0	Maximum bandwidth (in kilobits per second) that you can reserve on a link in BC0.
BC1	Maximum bandwidth (in kilobits per second) that you can reserve on a link in BC1.
TE-class[index]	Available bandwidth in TE-class (map of class-type and priority) at given index.
Total Allocated BW	Bandwidth (in Kbps) allocated at that priority.
Global Pool Reservable BW	Available bandwidth (in kbps) reservable at that priority in global pool (prestandard RDM).
Sub Pool Reservable BW	Available bandwidth (in kbps) reservable at that priority in sub-pool (prestandard RDM).
Attribute Names	Brief topology and the associated affinity attributes. The names of the affinity attribute of the link are displayed.

26 IGP = Interior Gateway Protocol.

27 LSA = link-state advertisement.

Related Commands

Command	Description
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.
interface (SRLG), on page 233	Enables SRLG on an interface and enters SRLG interface configuration mode.
srlg, on page 414	Configures an MPLS traffic enginnering SRLG values for a link on an interface.
show srlg, on page 403	Displays the SRLG interface and configuration information.

show mpls traffic-eng tunnels

To display information about MPLS-TE tunnels, use the **show mpls traffic-eng tunnels** command in XR EXEC mode.

show mpls traffic-eng tunnels [*tunnel-number*] **[affinity] [all] [auto-bw] [auto-tunnel]** [**backup** [*tunnel-number* | **auto-tunnel [mesh]** *mesh-value*| [**name** *tunnel-name*]| **promotion-timer** *promotion-timer*| **protected-interface** *type interface-path-id* | {**static**| **auto**}]] **[brief]** [**destination** *destination-address*] **[detail]** **[down]** [**interface** {**in** | **out** | **inout**} *type interface-path-id*] [**name** *tunnel-name*] **[p2p]** [**property** { **backup-tunnel** | **fast-reroute**}] [**protection [unused]**] [**reoptimized within-last** *interval*][**role** {**all** | **head** | **tail** | **middle**}] [**soft-preemption**{**desired**| **triggered**}}][**source** *source-address*] [**suboptimal constraints** {**current** | **max** | **none**}] **[summary] [tabular] [unused][up]** [**class-type** *ct*] [**igp** {**isis** | **ospf**}] [**within-last** *interval*]

Syntax Description

tunnel-number	(Optional)Number of the tunnel. Range is from 0 to 65535.
attribute-set	(Optional) Restricts the display of tunnels with an attribute set.
affinity	(Optional) Displays the affinity attributes for all outgoing links. The links, which are used by the tunnel, display color information.
all	(Optional) Displays all MPLS-TE tunnels.
auto-bw	(Optional) Restricts the display to tunnels when the automatic bandwidth is enabled.
auto-tunnel	(Optional) Restricts the display of automatically created tunnels.
mesh *mesh-value*	Displays the tunnels that belong to the specified auto-tunnel mesh group.
backup	(Optional) Displays FRR[28] backup tunnels information. The information includes the physical interface protected by the tunnel, the number of TE LSPs[29] protected, and the bandwidth protected. (Optional) Displays backup information for automatic tunnels and FRR tunnels.
name *tunnel-name*	(Optional) Displays the tunnel with given name.
promotion-timer *promotion-timer*	(Optional) Displays the configured FRR backup tunnel promotion timer value, in seconds.
protected-interface	(Optional) Displays FRR protected interfaces.

static	(Optional) Displays static backup tunnels.
auto-tunnel	(Optional) Displays protected automatic backup tunnels.
brief	(Optional) Displays the brief form of this command.
destination *destination-address*	(Optional) Restricts the display to tunnels destined for the specified IP address.
detail	(Optional) Displays detail information about headend tunnels.
down	(Optional) Displays tunnels that are down.
interface in	(Optional) Displays tunnels that use the specified input interface.
interface out	(Optional) Displays tunnels that use the specified output interface.
interface inout	(Optional) Displays tunnels that use the specified interface as an input or output interface.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
p2p	(Optional) Displays only P2P tunnels.
property backup-tunnel	(Optional) Displays tunnels with property of backup tunnel. Selects MPLS-TE tunnels used to protect physical interfaces on this router. A tunnel configured to protect a link against failure is a backup tunnel and has the backup tunnel property.
property fast-reroute	(Optional) Displays tunnels with property of fast-reroute configured. Selects FRR-protected MPLS-TE tunnels originating on (head), transmitting (router), or terminating (tail) on this router.

protection	(Optional) Displays all protected tunnels (configured as fast-reroutable). Displays information about the protection provided to each tunnel selected by other options specified with this command. The information includes whether protection is configured for the tunnel, the protection (if any) provided to the tunnel by this router, and the tunnel bandwidth protected.
reoptimized within-last *interval*	(Optional) Displays tunnels reoptimized within the last given time interval.
role all	(Optional) Displays all tunnels.
role head	(Optional) Displays tunnels with their heads at this router.
role middle	(Optional) Displays tunnels at the middle of this router.
role tail	(Optional) Displays tunnels with their tails at this router.
soft-preemption	Displays tunnels on which the soft-preemption feature is enabled.
source *source-address*	(Optional) Restricts the display to tunnels with a matching source IP address.
suboptimal constraints current	(Optional) Displays tunnels whose path metric is greater than the current shortest path constrained by the tunnel's configured options.
suboptimal constraints max	(Optional) Displays tunnels whose path metric is greater than the current shortest path, constrained by the configured options for the tunnel, and taking into consideration only the network capacity.
suboptimal constraints none	(Optional) Displays tunnels whose path metric is greater than the shortest unconstrained path.
summary	(Optional) Displays summary of configured tunnels.
tabular	(Optional) Displays a table showing TE LSPs, with one entry per line.
unused	(Optional) Displays only unused backup tunnels.
up	(Optional) Displays tunnels when the tunnel interface is up.

class-type *ct*	(Optional) Displays tunnels using the given class-type value configuration.
igp *isis*	(Optional) Displays tunnels with the path calculated as the IS-IS type for IGP.
igp *ospf*	(Optional) Displays tunnels with the path calculated as the OSPF type for IGP.
within-last *interval*	(Optional) Displays tunnels that has come up within the last given time interval.
auto-tunnel pcc	Displays stateful PCE client (PCC) auto-tunnel information.

28 FRR = Fast Reroute.
29 LSPs = Label Switched Paths.

Command Default   None

Command Modes   EXEC

Command History

Release	Modification
Release 4.0.0	These items were added to support the MPLS-TE automatic backup tunnel feature: • The **auto-tunnel** keyword was added. • The **unused** keyword was added.
Release 4.1.1	The **mesh** keyword was added.
Release 4.2.0	The **soft-preemption** and **attribute-set** keywords were added. Sample output was modified to display only tunnels on which the soft-preemption feature is enabled.
Release 5.0.0	This command was introduced.

Usage Guidelines   You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **brief** form of the **show mpls traffic-eng tunnels** command to display information specific to a tunnel interface. Use the command without the **brief** keyword to display information that includes the destination address, source ID, role, name, suboptimal constraints, and interface.

The **affinity** keyword is available for only the source router.

Selected tunnels would have a shorter path if they were reoptimized immediately.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

This sample output is not changed when no area is specified for the active path-option. If the area is specified, it is added on a line of its own after the existing path-option information.

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels 20 detail

Signalling Summary:
              LSP Tunnels Process:  running
                    RSVP Process:  running
                      Forwarding:  enabled
         Periodic reoptimization:  every 3600 seconds, next in 2400 seconds
          Periodic FRR Promotion:  every 300 seconds, next in 16 seconds
         Auto-bw enabled tunnels:  6

 Name: tunnel-te20  Destination: 130.130.130.130
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 1,  type explicit r1r2r3gig_path (Basis for Setup, path weight 200)
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 113 kbps  CT0

  Config Parameters:
    Bandwidth:       100 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
    Metric Type: TE (interface)
    AutoRoute:  enabled  LockDown: disabled    Policy class: not set
    Forwarding-Adjacency: disabled
    Loadshare:          0 equal loadshares
    Auto-bw: enabled
      Last BW Applied: 113 kbps CT0   BW Applications: 1
      Last Application Trigger: Periodic Application
      Bandwidth Min/Max: 0-4294967295 kbps
      Application Frequency: 5 min   Jitter: 0s   Time Left: 4m 19s
      Collection Frequency: 1 min
      Samples Collected: 0   Next: 14s
      Highest BW: 0 kbps   Underflow BW: 0 kbps
      Adjustment Threshold: 10%   10 kbps
      Overflow Detection disabled
      Underflow Detection disabled
    Fast Reroute: Disabled, Protection Desired: None
    Path Protection: Not Enabled
  History:
    Tunnel has been up for: 00:18:54 (since Sun Mar 14 23:48:23 UTC 2010)
    Current LSP:
      Uptime: 00:05:41 (since Mon Mar 15 00:01:36 UTC 2010)
    Prior LSP:
      ID: path option 1 [3]
      Removal Trigger: reoptimization completed
  Current LSP Info:
    Instance: 4, Signaling Area: IS-IS 1 level-2
    Uptime: 00:05:41 (since Mon Mar 15 00:01:36 UTC 2010)
    Outgoing Interface: GigabitEthernet0/5/0/21, Outgoing Label: 16009
    Router-IDs: local      110.110.110.110
                downstream 120.120.120.120
    Path Info:
      Outgoing:
      Explicit Route:
```

```
           Strict, 61.10.1.2
           Strict, 61.15.1.1
           Strict, 61.15.1.2
           Strict, 130.130.130.130
      Record Route: Disabled
      Tspec: avg rate=113 kbits, burst=1000 bytes, peak rate=113 kbits
      Session Attributes: Local Prot: Not Set, Node Prot: Not Set, BW Prot: Not Set
    Resv Info: None
      Record Route: Disabled
      Fspec: avg rate=113 kbits, burst=1000 bytes, peak rate=113 kbits
  Displayed 1 (of 6) heads, 0 (of 0) midpoints, 0 (of 0) tails
  Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```

This is a sample output from the **show mpls traffic-eng tunnels** command using the **property** keyword:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels property backup interface out pos 0/6/0/0


  Signalling Summary:
              LSP Tunnels Process:  running, not registered with RSVP
                    RSVP Process:  not running
                      Forwarding:  enabled
          Periodic reoptimization:  every 3600 seconds, next in 3595 seconds
           Periodic FRR Promotion:  every 300 seconds, next in 295 seconds
      Periodic auto-bw collection:  disabled

  Name: tunnel-te1  Destination: 1.1.1.1
    Status:
      Admin:    up Oper:   up   Path:  valid   Signalling: connected

      path option 1,  type dynamic   (Basis for Setup, path weight 1)
      G-PID: 0x0800 (derived from egress interface properties)

    Config Parameters:
      Bandwidth:       1000 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
      Metric Type: TE (default)
      AutoRoute:  disabled  LockDown: disabled
      Loadshare:       10000 bandwidth-based
      Auto-bw: disabled(0/0) 0  Bandwidth Requested:       0
      Direction: unidirectional
      Endpoint switching capability: unknown, encoding type: unassigned
      Transit switching capability: unknown, encoding type: unassigned
      Backup FRR EXP Demotion: 1 ' 7, 2 ' 1
      Class-Attributes: 1, 2, 7
      Bandwidth-Policer: off

    History:
      Tunnel has been up for: 00:00:08
      Current LSP:
        Uptime: 00:00:08

    Path info (ospf 0 area 0):
    Hop0: 10.0.0.2
    Hop1: 102.0.0.2
  Displayed 1 (of 1) heads, 0 (of 0) midpoints, 0 (of 0) tails
  Displayed 0 up, 1 down, 0 recovering, 0 recovered heads
```

This table describes the significant fields shown in the display.

Table 48: show mpls traffic-eng tunnels Command Field Descriptions

Field	Description
LSP Tunnels Process	Status of the LSP[30] tunnels process.
RSVP Process	Status of the RSVP process.

Field	Description
Forwarding	Status of forwarding (enabled or disabled).
Periodic reoptimization	Time, in seconds, until the next periodic reoptimization.
Periodic FRR Promotion	Time, in seconds, till the next periodic FRR[31] promotion.
Periodic auto-bw collection	Time, in seconds, till the next periodic auto-bw collection.
Name	Interface configured at the tunnel head.
Destination	Tail-end router identifier.
Admin/STATUS	Configured up or down.
Oper/STATE	Operationally up or down.
Signalling	Signaling connected or down or proceeding.
Config Parameters	Configuration parameters provided by tunnel mode MPLS traffic-eng, including those specific to unequal load-balancing functionality (bandwidth, load-share, backup FRR EXP demotion, class-attributes, and bandwidth-policer).
History: Current LSP: Uptime	Time LSP has been up.
Path Info	Hop list of current LSP.

[30] LSP = Link-State Packet.

[31] FRR = Fast Reroute.

This sample output shows the link attributes of links that are traversed by the tunnel (color information):

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels 11 affinity

  Signalling Summary:
              LSP Tunnels Process:  running
                     RSVP Process:  running
                       Forwarding:  enabled
           Periodic reoptimization:  every 3600 seconds, next in 2710 seconds
            Periodic FRR Promotion:  every 300 seconds, next in 27 seconds


           Auto-bw enabled tunnels:  0 (disabled)

  Name: tunnel-te11  Destination: 3.3.3.3
    Status:
      Admin:    up Oper:   up   Path:  valid   Signalling: connected

      path option 1,  type explicit gige_1_2_3 (Basis for Setup, path weight 2)
```

```
        G-PID: 0x0800 (derived from egress interface properties)
        Bandwidth Requested: 200 kbps  CT0

      Config Parameters:
        Bandwidth:      200 kbps (CT0) Priority:  2  2
        Number of affinity constraints: 1
            Include bit map      : 0x4
            Include name         : red2

        Metric Type: TE (default)
        AutoRoute: disabled  LockDown: disabled   Policy class: not set
        Forwarding-Adjacency: disabled
        Loadshare:         0 equal loadshares
        Auto-bw: disabled
        Fast Reroute: Enabled, Protection Desired: Any
        Path Protection: Not Enabled
      History:
        Tunnel has been up for: 02:55:27
        Current LSP:
          Uptime: 02:02:19
        Prior LSP:
          ID: path option 1 [8]
          Removal Trigger: reoptimization completed

      Path info (OSPF 100 area 0):
        Link0: 12.9.0.1
          Attribute flags: 0x4
          Attribute names: red2
        Link1: 23.9.0.2
          Attribute flags: 0x4
          Attribute names: red2

    Displayed 1 (of 8) heads, 0 (of 0) midpoints, 0 (of 0) tails
    Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```

This sample output shows the brief summary of the tunnel status and configuration:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels brief

  Signalling Summary:
              LSP Tunnels Process:  running
                     RSVP Process:  running
                       Forwarding:  enabled
            Periodic reoptimization:  every 3600 seconds, next in 2538 seconds
             Periodic FRR Promotion:  every 300 seconds, next in 38 seconds
            Auto-bw enabled tunnels:  0 (disabled)
                TUNNEL NAME          DESTINATION      STATUS  STATE

                 tunnel-te1060         10.6.6.6         up    up
              PE6_C12406_t607          10.7.7.7         up    up
              PE6_C12406_t608          10.8.8.8         up    up
              PE6_C12406_t609          10.9.9.9         up    up
              PE6_C12406_t610        10.10.10.10        up    up
              PE6_C12406_t621        10.21.21.21        up    up
              PE7_C12406_t706          10.6.6.6         up    up
              PE7_C12406_t721        10.21.21.21        up    up
               Tunnel_PE8-PE6          10.6.6.6         up    up
              Tunnel_PE8-PE21        10.21.21.21        up    up
               Tunnel_PE9-PE6          10.6.6.6         up    up
              Tunnel_PE9-PE21        10.21.21.21        up    up
              Tunnel_PE10-PE6          10.6.6.6         up    up
             Tunnel_PE10-PE21        10.21.21.21        up    up
            PE21_C12406_t2106          10.6.6.6         up    up
            PE21_C12406_t2107          10.7.7.7         up    up
            PE21_C12406_t2108          10.8.8.8         up    up
            PE21_C12406_t2109          10.9.9.9         up    up
            PE21_C12406_t2110        10.10.10.10        up    up
              PE6_C12406_t6070         10.7.7.7         up    up
              PE7_C12406_t7060         10.6.6.6         up    up
            tunnel-te1              200.0.0.3           up    up
            OUNI POS0/1/0/1         100.0.0.1           up    up
            OUNI POS0/1/0/2         200.0.0.1           up    up
```

```
       Displayed 1 (of 1) heads, 20 (of 20) midpoints, 0 (of 0) tails
       Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```

This section shows a sample output that results when automatic backup tunnels are created:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels brief

.
.
.
TUNNEL NAME          DESTINATION       STATUS  STATE
            tunnel-te0        200.0.0.3            up  up
            tunnel-te1        200.0.0.3            up  up
            tunnel-te2        200.0.0.3            up  up
          *tunnel-te50        200.0.0.3            up  up
          *tunnel-te60        200.0.0.3            up  up
          *tunnel-te70        200.0.0.3            up  up
          *tunnel-te80        200.0.0.3            up  up
.
.
.

* = automatically created backup tunnel
```

This is sample output that shows a summary of configured tunnels by using the **summary** keyword:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels summary

  LSP Tunnels Process:  not running, disabled
                    RSVP Process:  running
                      Forwarding:  enabled
          Periodic reoptimization:  every 3600 seconds, next in 2706 seconds
           Periodic FRR Promotion:  every 300 seconds, next in 81 seconds
      Periodic auto-bw collection:  disabled

  Signalling Summary:
      Head: 1 interfaces, 1 active signalling attempts, 1 established
            0 explicit, 1 dynamic
            1 activations, 0 deactivations
            0 recovering, 0 recovered
      Mids: 0
      Tails: 0

  Fast ReRoute Summary:
      Head:     0 FRR tunnels, 0 protected, 0 rerouted
      Mid:      0 FRR tunnels, 0 protected, 0 rerouted
      Summary:  0 protected, 0 link protected, 0 node protected, 0 bw protected




AutoTunnel Backup Summary:
    AutoTunnel Backups:
            50 created, 50 up, 0 down, 8 unused
            25 NHOP, 25 NNHOP, 10 SRLG strict, 10 SRLG pref
    Protected LSPs:
            10 NHOP, 20 NHOP+SRLG
            15 NNHOP, 5 NNHOP+SRLG
    Protected S2L Sharing Families:
            10 NHOP, 20 NHOP+SRLG
            15 NNHOP, 5 NNHOP+SRLG
    Protected S2Ls:             10 NHOP, 20 NHOP+SRLG
            15 NNHOP, 5 NNHOP+SRLG
```
This table describes the significant fields shown in the display.

Table 49: show mpls traffic-eng tunnels protection Command Field Descriptions

Field	Description
Tunnel#	Number of the MPLS-TE backup tunnel.
LSP Head/router	Node is either head or router for this LSP[32].
Instance	LSP ID.
Backup tunnel	Backup tunnel protection for NHOP/NNHOP.
out if	Backup tunnel's outgoing interface
Original	Outgoing interface, label, and next-hop of the LSP when not using backup.
With FRR	Outgoing interface and label when using backup tunnel.
LSP BW	Signaled bandwidth of the LSP.
Backup level	Type of bandwidth protection provided—pool type and limited/unlimited bandwidth.
LSP Tunnels Process	Status of the TE process [33].

[32] LSP = Link-State Packet.

[33] LSP = Label Switched Path

This is sample output from the **show mpls traffic-eng tunnels** command using the **backup** keyword. This command selects every MPLS-TE tunnel known to the router, and displays information about the FRR protection that each selected tunnel provides for interfaces on this route. The command does not generate output for tunnels that do not provide FRR protection of interfaces on this router:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels backup

  tunnel160
   Admin: up, Oper: up
   Src: 10.20.20.20, Dest: 10.10.10.10, Instance: 28
   Fast Reroute Backup Provided:
    Protected I/fs: POS0/7/0/0
    Protected lsps: 0
    Backup BW: any-class unlimited, Inuse: 0 kbps
```

This table describes the significant fields shown in the display.

Table 50: show mpls traffic-eng tunnels backup Command Field Descriptions

Field	Description
Tunnel#	MPLS-TE backup tunnel number.

Field	Description
Dest	IP address of backup tunnel destination.
State	State of the backup tunnel. Values are up, down, or admin-down.
Instance	LSP ID of the tunnel.
Protected I/fs	List of interfaces protected by the backup tunnel.
Protected lsps	Number of LSPs currently protected by the backup tunnel.
Backup BW	Configured backup bandwidth type and amount. Pool from which bandwidth is acquired. Values are any-class, CT0, and CT1. Amount is either unlimited or a configured limit in kbps.
Inuse	Backup bandwidth currently in use on the backup tunnel.

This shows a sample output from the **show mpls traffic-eng tunnels** command using the **backup** and **protected-interface** keywords:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels backup protected-interface

  Interface: POS0/5/0/1
     Tunnel100   UNUSED : out I/f:              Admin: down  Oper: down

  Interface: POS0/7/0/0
     Tunnel160    NHOP : out I/f: POS0/6/0/0  Admin:  up  Oper:  up
```

This table describes the significant fields shown in the display.

Table 51: show mpls traffic-eng tunnels backup protected-interface Command Field Descriptions

Field	Description
Interface	MPLS-TE-enabled FRR protected interface.
Tunnel#	FRR protected tunnel on the interface.
NHOP/NNHOP/UNUSED	State of Protected tunnel. Values are unused, next hop, next-next hop.
out I/f	Outgoing interface of the backup tunnel providing the protection.

This shows a sample output from the **show mpls traffic-eng tunnels up** command using the **igp ospf** keywords:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels up igp ospf

  Signalling Summary:
              LSP Tunnels Process:  running
                    RSVP Process:  running
                      Forwarding:  enabled
          Periodic reoptimization:  every 3600 seconds, next in 3381 seconds
           Periodic FRR Promotion:  every 300 seconds, next in 81 seconds
       Periodic auto-bw collection:  disabled

  Name: tunnel-te11  Destination: 30.30.30.30
    Status:
      Admin:     up Oper:   up   Path:  valid   Signalling: connected

      path option 1, type explicit back (Basis for Setup, path weight 1)
    G-PID: 0x0800 (derived from egress interface properties)

    Config Parameters:
      Bandwidth:        0 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
      Number of configured name based affinities: 2
      Name based affinity constraints in use:
         Include bit map           : 0x4 (refers to undefined affinity name)
         Include-strict bit map: 0x4

      Metric Type: TE (default)
      AutoRoute:  disabled  LockDown: disabled   Loadshare:       0 bw-based
      Auto-bw: disabled(0/0) 0  Bandwidth Requested:       0
      Direction: unidirectional
   Endpoint switching capability: unknown, encoding type: unassigned
      Transit switching capability: unknown, encoding type: unassigned

    History:
      Tunnel has been up for: 00:00:21
      Current LSP:
        Uptime: 00:00:21
      Prior LSP:
        ID: path option 1 [4]
        Removal Trigger: tunnel shutdown

    Path info (ospf   area 0):
    Hop0: 7.4.4.2
    Hop1: 30.30.30.30

  Displayed 1 (of 3) heads, 0 (of 0) midpoints, 0 (of 0) tails
  Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```

This shows a sample output from the **show mpls traffic-eng tunnels** command using the **up within-last** keywords:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels up within-last 200

  Signalling Summary:
              LSP Tunnels Process:  running
                    RSVP Process:  running
                      Forwarding:  enabled
          Periodic reoptimization:  every 3600 seconds, next in 3381 seconds
           Periodic FRR Promotion:  every 300 seconds, next in 81 seconds
       Periodic auto-bw collection:  disabled

  Name: tunnel-te11  Destination: 30.30.30.30
    Status:
      Admin:     up Oper:   up   Path:  valid   Signalling: connected

      path option 1, type explicit back (Basis for Setup, path weight 1)
    G-PID: 0x0800 (derived from egress interface properties)

    Config Parameters:
```

```
              Bandwidth:        0 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
              Number of configured name based affinities: 2
              Name based affinity constraints in use:
                  Include bit map         : 0x4 (refers to undefined affinity name)
                  Include-strict bit map: 0x4
       Metric Type: TE (default)
              AutoRoute:  disabled  LockDown: disabled   Loadshare:        0 bw-based
              Auto-bw: disabled(0/0) 0  Bandwidth Requested:        0
              Direction: unidirectional
        Endpoint switching capability: unknown, encoding type: unassigned
              Transit switching capability: unknown, encoding type: unassigned

         History:
           Tunnel has been up for: 00:00:21
           Current LSP:
             Uptime: 00:00:21
           Prior LSP:
             ID: path option 1 [4]
             Removal Trigger: tunnel shutdown

         Path info (ospf   area 0):
         Hop0: 7.4.4.2
         Hop1: 30.30.30.30

       Displayed 1 (of 3) heads, 0 (of 0) midpoints, 0 (of 0) tails
       Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```

This shows a sample output from the **show mpls traffic-eng tunnels** command using the **reoptimized within-last** keywords:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels reoptimized within-last 600

  Signalling Summary:
                LSP Tunnels Process:  running
                       RSVP Process:  running
                         Forwarding:  enabled
             Periodic reoptimization:  every 60000 seconds, next in 41137 seconds
               Periodic FRR Promotion:  every 300 seconds, next in 37 seconds
         Periodic auto-bw collection:  disabled

 Name: tunnel-te1  Destination: 30.30.30.30
   Status:
     Admin:    up Oper:   up   Path:   valid   Signalling: connected

     path option 1, type explicit prot1 (Basis for Setup, path weight 1)
  G-PID: 0x0800 (derived from egress interface properties)

   Config Parameters:
     Bandwidth:       66 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
     Metric Type: IGP (global)
     AutoRoute:   enabled  LockDown: disabled   Loadshare:       66 bw-based
     Auto-bw: disabled(0/0) 0  Bandwidth Requested:       66
     Direction: unidirectional
  Endpoint switching capability: unknown, encoding type: unassigned
     Transit switching capability: unknown, encoding type: unassigned

   History:
     Tunnel has been up for: 00:14:04
     Current LSP:
       Uptime: 00:03:52
       Selection: reoptimization
     Prior LSP:
       ID: path option 1 [2013]
       Removal Trigger: reoptimization completed

   Path info (ospf   area 0):
   Hop0: .2.2.2
   Hop1: 7.3.3.2
   Hop2: 30.30.30.30
 Displayed 1 (of 1) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

```
                 Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```

This is a sample output from the **show mpls traffic-eng tunnels** command using the **detail** keyword:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels 100 detail

  Name: tunnel-te1  Destination: 24.24.24.24
    Status:
      Admin:    up Oper:    up

          Working Path:  valid  Signalling: connected
          Protecting Path:  valid  Protect Signalling: connected
          Working LSP is carrying traffic

      path option 1,  type explicit po4 (Basis for Setup, path weight 1)
        (Basis for Standby, path weight 2)
      G-PID: 0x001d (derived from egress interface properties)
      Path protect LSP is present.

      path option 1,  type explicit po6 (Basis for Setup, path weight 1)

    Config Parameters:
      Bandwidth:        10 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
      Metric Type: TE (default)
      AutoRoute:   enabled  LockDown: disabled    Loadshare:        10 bw-based
      Auto-bw: disabled(0/0) 0  Bandwidth Requested:       10
      Direction: unidirectional
      Endpoint switching capability: unknown, encoding type: unassigned
      Transit switching capability: unknown, encoding type: unassigned

    History:
      Tunnel has been up for: 00:04:06
      Current LSP:
        Uptime: 00:04:06
      Prior LSP:
        ID: path option 1 [5452]
        Removal Trigger: path verification failed
  Current LSP Info:
      Instance: 71, Signaling Area: ospf optical area 0
      Uptime: 00:10:41
      Incoming Label: explicit-null
      Outgoing Interface: POS0/4/0/0, Outgoing Label: implicit-null
      Path Info:
        Explicit Route:
          Strict, 100.0.0.3
          Strict, 24.24.24.24
        Record Route: None
        Tspec: avg rate=2488320 kbits, burst=1000 bytes, peak rate=2488320 kbits
  Resv Info:
        Record Route:
          IPv4 100.0.0.3, flags 0x0
        Fspec: avg rate=2488320 kbits, burst=1000 bytes, peak rate=2488320 kbits
    Protecting LSP Info:
      Instance: 72, Signaling Area: ospf optical area 0
      Incoming Label: explicit-null
      Outgoing Interface: POS0/6/0/0, Outgoing Label: implicit-null
      Path Info:
        Explicit Route:
          Strict, 101.0.0.3
          Strict, 24.24.24.24
        Record Route: None
        Tspec: avg rate=2488320 kbits, burst=1000 bytes, peak rate=2488320 kbits
      Resv Info:
        Record Route:
          IPv4 101.0.0.3, flags 0x0
        Fspec: avg rate=2488320 kbits, burst=1000 bytes, peak rate=2488320 kbits
```

This is a sample output from the **show mpls traffic-eng tunnels** command using the **role mid** keyword:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels role mid
```

```
Signalling Summary:
          LSP Tunnels Process:  running
               RSVP Process:  running
                 Forwarding:  enabled
        Periodic reoptimization:  every 3600 seconds, next in 1166 seconds
          Periodic FRR Promotion:  every 300 seconds, next in 90 seconds
     Periodic auto-bw collection:  disabled
LSP Tunnel 10.10.10.10 1 [5508] is signalled, connection is up
  Tunnel Name: FRR1_t1  Tunnel Role: Mid
  InLabel: POS0/2/0/1, 33
  OutLabel: POS0/3/0/0, implicit-null
  Signalling Info:
    Src 10.10.10.10 Dst 30.30.30.30, Tunnel ID 1, Tunnel Instance 5508
    Path Info:1
    Incoming Address: 7.3.3.1
Incoming     Explicit Route:
        Strict, 7.3.3.1
        Loose, 30.30.30.30
    ERO Expansion Info:
     ospf 100 area 0, Metric 1 (TE), Affinity 0x0, Mask 0xffff, Queries 0
     Outgoing     Explicit Route:
        Strict, 7.2.2.1
        Strict, 30.30.30.30
Record Route: None
     Tspec: avg rate=10 kbits, burst=1000 bytes, peak rate=10 kbits
    Resv Info:
     Record Route:
        IPv4 30.30.30.30, flags 0x20
        Label 3, flags 0x1
        IPv4 7.3.3.2, flags 0x0
        Label 3, flags 0x1
     Fspec: avg rate=10 kbits, burst=1000 bytes, peak rate=10 kbits
Displayed 0 (of 1) heads, 1 (of 1) midpoints, 0 (of 1) tails
Displayed 0 up, 0 down, 0 recovering, 0 recovered heads
```

This sample output shows a tabular table for TE LSPs by using the **tabular** keyword:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels tabular
```

Tunnel Name	LSP ID	Destination Address	Source Address	Tun State	FRR State	LSP Role	
tunnel-te1060	2	10.6.6.6	10.1.1.1	up	Inact	Head	
PE6_C12406_t607	2	10.7.7.7	10.6.6.6	up	Inact	Mid	
PE6_C12406_t608	2	10.8.8.8	10.6.6.6	up	Inact	Mid	
PE6_C12406_t609	2	10.9.9.9	10.6.6.6	up	Inact	Mid	
PE6_C12406_t610	2	10.10.10.10	10.6.6.6	up	Inact	Mid	
PE6_C12406_t621	2	10.21.21.21	10.6.6.6	up	Inact	Mid	
PE7_C12406_t706	835	10.6.6.6	10.7.7.7	up	Inact	Mid	
PE7_C12406_t721	603	10.21.21.21	10.7.7.7	up	Inact	Mid	
Tunnel_PE8-PE6	4062	10.6.6.6	10.8.8.8	up	Inact	Mid	
Tunnel_PE8-PE21	6798	10.21.21.21	10.8.8.8	up	Inact	Mid	
Tunnel_PE9-PE6	4062	10.6.6.6	10.9.9.9	up	Inact	Mid	
Tunnel_PE9-PE21	6795	10.21.21.21	10.9.9.9	up	Inact	Mid	
Tunnel_PE10-PE6	4091	10.6.6.6	10.10.10.10	up	Inact	Mid	
Tunnel_PE10-PE21	6821	10.21.21.21	10.10.10.10	up	Inact	Mid	
PE21_C12406_t2106	2	10.6.6.6	10.21.21.21	up	Ready	Mid	
PE21_C12406_t2107	2	10.7.7.7	10.21.21.21	up	Inact	Mid	
PE21_C12406_t2108	2	10.8.8.8	10.21.21.21	up	Inact	Mid	
PE21_C12406_t2109	2	10.9.9.9	10.21.21.21	up	Inact	Mid	
PE21_C12406_t2110	2	10.10.10.10	10.21.21.21	up	Inact	Mid	
PE6_C12406_t6070	2	10.7.7.7	10.6.6.6	up	Inact	Mid	
PE7_C12406_t7060	626	10.6.6.6	10.7.7.7	up	Inact	Mid	
tunnel-te1	1	200.0.0.3	200.0.0.1	up	Inact	Head	InAct
tunnel-te100	1	200.0.0.3	200.0.0.1	up	Ready	Head	InAct
OUNI POS0/1/0/1	2	100.0.0.1	200.0.0.1	up	Inact	Head	InAct
OUNI POS0/1/0/2	6	200.0.0.1	100.0.0.1	up	Inact	Tail	InAct

This sample output shows a tabular table indicating automatic backup tunnels when using the **tabular** keyword:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels tabular

          Tunnel    LSP   Destination        Source                 FRR    LSP   Path
            Name     ID       Address        Address   State      State   Role   Prot
------------------  ------  ---------------  ---------------  -------  -------  ------  -----
     tunnel-te0     549      200.0.0.3        200.0.0.1      up    Inact   Head  InAct
     tunnel-te1     546      200.0.0.3        200.0.0.1      up    Inact   Head  InAct
     tunnel-te2       6      200.0.0.3        200.0.0.1      up    Inact   Head  InAct
    *tunnel-te50      6      200.0.0.3        200.0.0.1      up   Active   Head  InAct
    *tunnel-te60      4      200.0.0.3        200.0.0.1      up   Active   Head  InAct
    *tunnel-te70      4      200.0.0.3        200.0.0.1      up   Active   Head  InAct
    *tunnel-te80      3      200.0.0.3        200.0.0.1      up   Active   Head  InAct

* = automatically created backup tunnel
```

This table describes the significant fields shown in the display.

Table 52: show mpls traffic-eng tunnels tabular Command Field Descriptions

Field	Description
Tunnel Name	MPLS-TE tunnel name.
LSP ID	LSP ID of the tunnel.
Destination Address	Destination address of the TE tunnel (identified in Tunnel Name).
Source Address	Source address for the filtered tunnels.
Tunnel State	State of the tunnel. Values are up, down, or admin-down.
FRR State	FRR state identifier.
LSP Role	Role identifier. Values are All, Head, or Tail.

This sample output shows the MPLS-TE tunnel information only for tunnels in which the automatic bandwidth is enabled using the **auto-bw** keyword:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels auto-bw

  Signalling Summary:
            LSP Tunnels Process:  running
                  RSVP Process:  running
                    Forwarding:  enabled
         Periodic reoptimization:  every 3600 seconds, next in 636 seconds
          Periodic FRR Promotion:  every 300 seconds, next in 276 seconds
          Auto-bw enabled tunnels:  1

  Name: tunnel-te1  Destination: 0.0.0.0
    Status:
      Admin:    up Oper: down   Path: not valid   Signalling: Down
      G-PID: 0x0800 (internally specified)
      Bandwidth Requested: 0 kbps  CT0

    Config Parameters:
      Bandwidth:        0 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
```

```
          Metric Type: TE (default)
          AutoRoute: disabled  LockDown: disabled   Policy class: not set
          Loadshare:          0 equal loadshares
     Auto-bw: (collect bw only)
          Last BW Applied: 500 kbps (CT0)   BW Applications: 25
          Last Application Trigger: Periodic Application
          Bandwidth Min/Max: 10-10900 kbps
          Application Frequency: 10 min (Cfg: 10 min)  Time Left: 5m 34s
          Collection Frequency: 2 min
          Samples Collected: 2   Highest BW: 450 kbps   Next: 1m 34s
          Adjustment Threshold: 5%
          Overflow Threshold: 15%   Limit: 1/4   Early BW Applications: 0
     Direction: unidirectional
          Endpoint switching capability: unknown, encoding type: unassigned
          Transit switching capability: unknown, encoding type: unassigned
          Fast Reroute: Disabled, Protection Desired: None

     Reason for the tunnel being down: No destination is configured
     History:
Displayed 1 (of 1) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 0 up, 1 down, 0 recovering, 0 recovered heads
```

This table describes the significant fields shown in the display.

Table 53: show mpls traffic-eng tunnels auto-bw Command Field Descriptions

Field	Description
collect bw only	Field is displayed only if the bandwidth collection is configured in the tunnel automatic bandwidth configuration.
Last BW Applied	Last bandwidth change that is requested by the automatic bandwidth for the tunnel. In addition, this field indicates which pool is used for the bandwidth.
BW Applications	Total number of bandwidth applications that is requested by the automatic bandwidth, which includes the applications triggered by an overflow condition.
Last Application Trigger	These last application options are displayed: • Periodic Application • Overflow Detected • Manual Application
Bandwidth Min/Max	Bandwidth configured is either minimum or maximum.
Application Frequency	Configured application frequency. The Time Left field indicates the time left before the next application executes.
Collection Frequency	Globally configured collection frequency, which is the same value for all the tunnels.

Field	Description
Samples Collected	Number of samples that are collected during the current application period. This field is replaced by the Collection Disabled field if Collection Frequency is not currently configured.
Highest BW	Highest bandwidth that is collected for the application period.
Next	Time left before the next collection event.
Overflow Threshold	Overflow threshold that is configured. The Overflow field appears only if the overflow detection is configured in the tunnel automatic bandwidth configuration.
Limit	Consecutive overflow detected or configured limit.
Early BW Applications	Number of early bandwidth applications that are triggered by an overflow condition.

This is sample output from the **show mpls traffic-eng tunnels** command after the NNHOP SRLG preferred automatic backup tunnel is configured:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels 1

Signalling Summary:
            LSP Tunnels Process:  running
                  RSVP Process:  running
                    Forwarding:  enabled
        Periodic reoptimization:  every 3600 seconds, next in 2524 seconds
         Periodic FRR Promotion:  every 300 seconds, next in 49 seconds
        Auto-bw enabled tunnels:  1

Name: tunnel-te1  Destination: 200.0.0.3 (auto backup)
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 10,  type explicit (autob_nnhop_srlg_tunnel1) (Basis for Setup, path weight
 11)
    path option 20,  type explicit (autob_nnhop_tunnel1)
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 0 kbps  CT0
    Creation Time: Fri Jul 10 01:53:25.581 PST  (1h 25m 17s ago)

  Config Parameters:
    Bandwidth:        0 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
    Metric Type: TE (default)
    AutoRoute: disabled  LockDown: disabled   Policy class: not set
    Forwarding-Adjacency: disabled

Loadshare:        0 equal loadshares
    Auto-bw: disabled
    Fast Reroute: Disabled, Protection Desired: None
    Path Protection: Not Enabled
  Auto Backup:
    Protected LSPs: 4
    Protected S2L Sharing Families: 0
    Protected S2Ls: 0
```

```
      Protected i/f: Gi0/1/0/0     Protected node: 20.0.0.2
      Protection: NNHOP+SRLG
      Unused removal timeout: not running
  History:
    Tunnel has been up for: 00:00:08
    Current LSP:
      Uptime: 00:00:08
    Prior LSP:
      ID: path option 1 [545]
      Removal Trigger: configuration changed

  Path info (OSPF 0 area 0):
  Hop0: 10.0.0.2
  Hop1: 100.0.0.2
  Hop2: 100.0.0.3
  Hop3: 200.0.0.3
```

This table describes the significant fields shown in the display.

Table 54: show mpls traffic-eng tunnels Command Field Descriptions

Field	Description
Auto Backup	Auto backup section header.
Creation Time	Time when the tunnel was created and for what period was the tunnel created.
Protected LSPs	Number of ready and active LSPs protected by this backup.
Protected S2L Sharing Familes	Number of ready and active sharing families protected by this backup.
Protected S2Ls	Number of ready and active primary tunnels protected by this backup.
Protected i/f Protected node	Interface and NNHOP node protected by this backup.
Protection: NNHOP+SRLG	Type of protection provided by this backup. **Note** Protection can be different when a preferred SRLG is configured and an SRLG path is not found.
Example when backup is in use: Unused removal timeout: not running Example when backup is unused: Unused removal timeout: 1h26m	Amount of time left before the unused removal timout expires. This timer only runs when the backup is in the unused state. After the timer expires, the automatic backup tunnel is removed.

This is sample output from the **show mpls traffic-eng tunnels** command using the **detail** keyword:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels 999 detail

Name: tunnel-te999  Destination: 1.1.1.1
  Status:
```

```
      Admin:    up Oper:    up   Path:  valid   Signalling: connected

     path option 1,  type dynamic  (Basis for Setup, path weight 2)
        Path-option attribute: po
          Number of affinity constraints: 2
              Include bit map       : 0x4
              Include name          : blue
              Exclude bit map       : 0x2
              Exclude name          : red


        Bandwidth: 300 (CT0)
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 300 kbps  CT0
    Creation Time: Tue Aug 14 23:35:58 2012 (00:00:42 ago)
  Config Parameters:
    Bandwidth:      100 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
    Metric Type: TE (default)
    Hop-limit: disabled
    AutoRoute: disabled  LockDown: disabled    Policy class: not set
    Forwarding-Adjacency: disabled
    Loadshare:         0 equal loadshares
    Auto-bw: disabled
    Fast Reroute: Enabled, Protection Desired: Any
    Path Protection: Not Enabled
    Soft Preemption: Disabled
  SNMP Index: 42
  History:
    Tunnel has been up for: 00:00:30 (since Tue Aug 14 23:36:10 EST 2012)
    Current LSP:
      Uptime: 00:00:30 (since Tue Aug 14 23:36:10 EST 2012)
  Current LSP Info:
    Instance: 2, Signaling Area: OSPF 100 area 16909060
    Uptime: 00:00:30 (since Tue Aug 14 23:36:10 EST 2012)
    Outgoing Interface: GigabitEthernet0/2/0/2, Outgoing Label: 16005
    Router-IDs: local      3.3.3.3
                downstream 2.2.2.2
    Soft Preemption: None
    Path Info:
      Outgoing:
        Explicit Route:
          Strict, 23.9.0.2
          Strict, 12.9.0.2
          Strict, 12.9.0.1
          Strict, 1.1.1.1

      Record Route: Disabled
      Tspec: avg rate=300 kbits, burst=1000 bytes, peak rate=300 kbits
      Session Attributes: Local Prot: Set, Node Prot: Not Set, BW Prot: Not Set
                          Soft Preemption Desired: Not Set
    Resv Info:
      Record Route:
        IPv4 2.2.2.2, flags 0x20
        Label 16005, flags 0x1
        IPv4 23.9.0.2, flags 0x0
        Label 16005, flags 0x1
        IPv4 1.1.1.1, flags 0x20
        Label 3, flags 0x1
        IPv4 12.9.0.1, flags 0x0
        Label 3, flags 0x1
      Fspec: avg rate=300 kbits, burst=1000 bytes, peak rate=300 kbits Displayed 1 (of 8)
heads, 0 (of 3) midpoints, 0 (of 0) tails Displayed 1 up, 0 down, 0 recovering, 0 recovered
 heads
```

This is sample output from the **show mpls traffic-eng tunnels** command using the **auto-tunnel backup** keywords:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels auto-tunnel backup

AutoTunnel Backup Configuration:
  Interfaces count: 30
  Unused removal timeout: 2h
  Configured tunnel number range: 0-100
```

```
AutoTunnel Backup Summary:
        50 created, 50 up, 0 down, 8 unused
        25 NHOP, 25 NNHOP, 10 SRLG strict, 10 SRLG pref
Protected LSPs:
        10 NHOP, 20 NHOP+SRLG
        15 NNHOP, 5 NNHOP+SRLG
Protected S2L Sharing Families:
        10 NHOP, 20 NHOP+SRLG
        15 NNHOP, 5 NNHOP+SRLG
Protected S2Ls:
        10 NHOP, 20 NHOP+SRLG
        15 NNHOP, 5 NNHOP+SRLG

Cumulative Counters (last cleared 1h ago):
                   Total    NHOP   NNHOP
 Created:            550     300     250
 Connected:          500     250     250
 Removed (down):       0       0       0
 Removed (unused):   200     100     100
 Removed (in use):     0       0       0
 Range exceeded:       0       0       0
```

This table describes the significant fields shown in the display.

Table 55: show mpls traffic-eng tunnels auto-tunnel backup Command Field Descriptions

Field	Description
AutoTunnel Backup Configuration	Header for the automatic tunnel backup configuration.
Interfaces count	Number of interfaces that have automatic tunnel backup enabled.
Unused removal timeout	Configured value and time left before expiration of the unused removal timeout attribute.
Configured tunnel number range	Configured tunnel number range.
AutoTunnel Backup Summary	Header for the automatic tunnel backup summary information.
50 created	Number of automatic backup tunnels created.
50 up	Number of automatic backup tunnels in the up state.
0 down	Number of automatic backup tunnels in the down state.
8 unused	Number of automatic backup tunnels in the unused state.
25 NHOP	Number of automatic backup tunnels created for NHOP protection.
25 NNHOP	Number of automatic backup tunnels created for NNHOP protection.
10 SRLG strict	Number of automatic backup tunnels created with the SRLG preferred attribute.

Field	Description
10 SRLG pref	Number of automatic backup tunnels created with the SRLG preferred attribute.
Protected LSPs Protected S2L Sharing Families Protected S2Ls	Headings for summary information showing current status of LSPs, S2L Sharing Families, and S2Ls that are protected by the automatic tunnel backups. Numbers include primary tunnels in FRR ready and active state.
10 NHOP	Number of automatic backup tunnels that are link protected.
20 NHOP+SRLG	Number of automatic backup tunnels that are link protected and using an SRLG diverse backup path.
15 NNHOP	Number of automatic backup tunnels that are node protected.
20 NNHOP+SRLG	Number of automatic backup tunnels that are node protected and use an SRLG diverse backup path.
Cumulative Counters (last cleared 1h ago):	Cumulative counters for automatic backup tunnels.
Headers: Total, NHOP, NNHOP	Total number of counters and breakdown of NHOP and NNHOP counters.
Created:	Cumulative number of created automatic backup tunnels since the last counter was cleared.
Connected:	Cumulative number of the connected automatic backup tunnels since the last counter was cleared. **Note** Counter increments only the first time that a tunnel connects.
Removed (down/unused/in use)	Number of automatic backup tunnels that are removed based on state.
Range exceeded	Number of automatic backup tunnels attempted and later rejected when the total number exceeds the configured range.

This is sample output from the **show mpls traffic-eng tunnels name tunnel-te1 detail** command, which displays the soft preemption information for the tunnel-te1 tunnel:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels name tunnel-te1 detail
Name: tunnel-te1  Destination: 192.168.0.4
  Status:
    Admin:    up Oper:   up  Path: valid  Signalling: connected
```

```
        path option 1,  type explicit ABC1 (Basis for Setup, path weight 2)
        Last PCALC Error [Reopt]: Thu Oct 13 16:40:24 2011
          Info: Can't reach 10.10.10.2 on 192.168.0.2, from node 192.168.0.1 (bw)
        Last Signalled Error: Thu Oct 13 16:38:53 2011
          Info: [2] PathErr(34,1)-(reroute, flow soft-preempted) at 10.10.10.1
        G-PID: 0x0800 (derived from egress interface properties)
        Bandwidth Requested: 30000 kbps  CT0
        Creation Time: Thu Oct 13 15:46:45 2011 (00:53:44 ago)
      Config Parameters:
        Bandwidth:    30000 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
        Metric Type: TE (default)
        Hop-limit: disabled
        AutoRoute:  enabled  LockDown: disabled   Policy class: not set
        Forwarding-Adjacency: disabled
        Loadshare:         0 equal loadshares
        Auto-bw: disabled
        Fast Reroute: Enabled, Protection Desired: Any
        Path Protection: Not Enabled
        Soft Preemption: Enabled
      Soft Preemption:
        Current Status: Preemption pending
        Last Soft Preemption: Thu Oct 13 16:38:53 2011 (00:01:36 ago)
          Addresses of preempting links:
            10.10.10.1: Thu Oct 13 16:38:53 2011 (00:01:36 ago)
          Duration in preemption pending: 96 seconds
          Preemption Resolution: Pending
        Stats:
          Number of preemption pending events: 1
          Min duration in preemption pending: 0 seconds
          Max duration in preemption pending: 0 seconds
          Average duration in preemption pending: 0 seconds
          Resolution Counters: 0 reopt complete, 0 torn down
                               0 path protection switchover
  SNMP Index: 9
   History:
      Tunnel has been up for: 00:52:46 (since Thu Oct 13 15:47:43 EDT 2011)
      Current LSP:
        Uptime: 00:52:46 (since Thu Oct 13 15:47:43 EDT 2011)
      Reopt. LSP:
        Last Failure:
          LSP not signalled, has no S2Ls
          Date/Time: Thu Oct 13 16:40:24 EDT 2011 [00:00:05 ago]
      Prior LSP:
        ID: path option 1 [2]
        Removal Trigger: path error
   Current LSP Info:
      Instance: 2, Signaling Area: OSPF ring area 0
      Uptime: 00:52:46 (since Thu Oct 13 15:47:43 EDT 2011)
      Outgoing Interface: GigabitEthernet0/0/0/0, Outgoing Label: 16002
      Router-IDs: local      192.168.0.1
                  downstream 192.168.0.2
      Soft Preemption: Pending
        Preemption Link: GigabitEthernet0/0/0/0; Address: 10.10.10.1
        Preempted at: Thu Oct 13 16:38:53 2011 (00:01:36 ago)
        Time left before hard preemption: 204 seconds
      Path Info:
        Outgoing:
        Explicit Route:
          Strict, 10.10.10.2
          Strict, 14.14.14.2
          Strict, 14.14.14.4
          Strict, 192.168.0.4
        Record Route: Empty
        Tspec: avg rate=30000 kbits, burst=1000 bytes, peak rate=30000 kbits
        Session Attributes: Local Prot: Set, Node Prot: Not Set, BW Prot: Not Set
                            Soft Preemption Desired: Set
      Resv Info:
        Record Route:
          IPv4 192.168.0.2, flags 0x20
          Label 16002, flags 0x1
          IPv4 10.10.10.2, flags 0x0
          Label 16002, flags 0x1
          IPv4 192.168.0.4, flags 0x20
```

```
              Label 3, flags 0x1
              IPv4 14.14.14.4, flags 0x0
              Label 3, flags 0x1
        Fspec: avg rate=30000 kbits, burst=1000 bytes, peak rate=30000 kbits
Displayed 1 (of 4) heads, 0 (of 0) midpoints, 0 (of 2) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```

This is sample output from the **show mpls traffic-eng tunnels** command with the **mesh** keyword:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels auto-tunnel
Signalling Summary:
            LSP Tunnels Process:  running
                   RSVP Process:  running
                     Forwarding:  enabled
         Periodic reoptimization:  every 3600 seconds, next in 3098 seconds
          Periodic FRR Promotion:  every 300 seconds, next in 238 seconds
          Auto-bw enabled tunnels:  1000

Name: tunnel-te9000  Destination: 20.20.20.20 (auto-tunnel mesh)
  Status:
    Admin:    up Oper:   up  Path:  valid   Signalling: connected
    path option 10,  type dynamic (Basis for Setup, path weight 11)
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 0 kbps  CT0
    Creation Time: Thu Jan 14 09:09:31 2010 (01:41:20 ago)
  Config Parameters:
    Bandwidth:        0 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
    Metric Type: TE (default)
    AutoRoute: disabled  LockDown: disabled   Policy class: not set
    Forwarding-Adjacency: disabled
    Loadshare:           0 equal loadshares
    Auto-bw: disabled
    Fast Reroute: Disabled, Protection Desired: None
    Path Protection: Not Enabled
    Attribute-set: TA-NAME (type auto-mesh)
Auto-tunnel Mesh:
  Group 40: Destination-list dl-40
    Unused removal timeout: not running
  History:
    Tunnel has been up for: 01:40:53 (since Thu Jan 14 09:09:58 EST 2010)
    Current LSP:
      Uptime: 01:41:00 (since Thu Jan 14 09:09:51 EST 2010)
    Reopt. LSP:
      Last Failure:
        LSP not signalled, identical to the [CURRENT] LSP
        Date/Time: Thu Jan 14 09:42:30 EST 2010 [01:08:21 ago]

  Path info (OSPF 100 area 0):
  Hop0: 7.0.15.1
  Hop1: 20.20.20.20
```

This shows an auto-tunnel mesh summary sample output from the **show mpls traffic-eng tunnels** command using the **summary** keyword:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels summary
Thu Jan 14 10:46:34.677 EST

            LSP Tunnels Process:  running
                   RSVP Process:  running
                     Forwarding:  enabled
         Periodic reoptimization:  every 3600 seconds, next in 3354 seconds
          Periodic FRR Promotion:  every 300 seconds, next in 193 seconds
       Periodic auto-bw collection:  1000

Signalling Summary:
    Head: 2000 interfaces, 2000 active signalling attempts, 2000 established
          2000 explicit, 0 dynamic
          9250 activations, 7250 deactivations
          0 recovering, 2000 recovered
    Mids: 0
    Tails: 0

Fast ReRoute Summary:
    Head:     1000 FRR tunnels, 1000 protected, 0 rerouted
    Mid:       0 FRR tunnels, 0 protected, 0 rerouted
```

```
      Summary:  1000 protected, 500 link protected, 500 node protected, 0 bw protected

 P2MP Summary:
     Tunnel Head:          250 total, 250 connected
     Destination Head:     500 total, 500 connected
     S2L Head: 500 established, 0 proceeding
     S2L Mid:  0 established, 0 proceeding
     S2L Tail: 0 established

 P2MP Fast ReRoute Summary:
     Tunnel Head: 250 FRR enabled
     S2L Head: 500 FRR, 500 protected, 0 rerouted
     S2L Mid:  0 FRR, 0 protected, 0 rerouted
     Summary:  500 protected, 500 link protected, 0 node protected, 0 bw protected

 <snip>

 Auto-tunnel Mesh Summary:
   Auto-mesh Tunnels:
       50 created, 50 up, 0 down, 25 FRR, 20 FRR enabled
 Mesh Groups:
     4 groups, 50 destinations
```

This shows an auto-tunnel mesh summary sample output from the **show mpls traffic-eng tunnels** command using the **auto-mesh** keyword:

```
RP/0/RP0/CPU0:router show mpls traffic-eng tunnels auto-tunnel
Signalling Summary:
               LSP Tunnels Process:  running
                      RSVP Process:  running
                        Forwarding:  enabled
          Periodic reoptimization:  every 3600 seconds, next in 3098 seconds
           Periodic FRR Promotion:  every 300 seconds, next in 238 seconds
          Auto-bw enabled tunnels:  1000

Name: tunnel-te9000  Destination: 20.20.20.20  (auto-tunnel mesh)
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected
    path option 10,  type dynamic (Basis for Setup, path weight 11)
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 0 kbps  CT0
    Creation Time: Thu Jan 14 09:09:31 2010 (01:41:20 ago)
  Config Parameters:
    Bandwidth:       0 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
    Metric Type: TE (default)
    AutoRoute: disabled  LockDown: disabled   Policy class: not set
    Forwarding-Adjacency: disabled
    Loadshare:         0 equal loadshares
    Auto-bw: disabled
    Fast Reroute: Disabled, Protection Desired: None
    Path Protection: Not Enabled
    Attribute-set: TA-NAME  (type auto-mesh)
Auto-tunnel Mesh:
  Group 40: Destination-list dl-40
    Unused removal timeout: not running
  History:
    Tunnel has been up for: 01:40:53 (since Thu Jan 14 09:09:58 EST 2010)
    Current LSP:
      Uptime: 01:41:00 (since Thu Jan 14 09:09:51 EST 2010)
    Reopt. LSP:
      Last Failure:
        LSP not signalled, identical to the [CURRENT] LSP
        Date/Time: Thu Jan 14 09:42:30 EST 2010 [01:08:21 ago]

  Path info (OSPF 100 area 0):
  Hop0: 7.0.15.1
  Hop1: 20.20.20.20
```

This example includes output for Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI) configuration for the **show mpls traffic-eng tunnels** command using the **summary** keyword:

```
RP/0/RP0/CPU0:routershow mpls traffic-eng tunnels auto-tunnel
Thu Jan 14 10:46:34.677 EST

                 LSP Tunnels Process:  running
                        RSVP Process:  running
                          Forwarding:  enabled
             Periodic reoptimization:  every 3600 seconds, next in 3354 seconds
              Periodic FRR Promotion:  every 300 seconds, next in 193 seconds
         Periodic auto-bw collection:  1000

Signalling Summary:
    Head: 2000 interfaces, 2000 active signalling attempts, 2000 established
          2000 explicit, 0 dynamic
          9250 activations, 7250 deactivations
          0 recovering, 2000 recovered
    Mids: 0
    Tails: 0

Fast ReRoute Summary:
    Head:     1000 FRR tunnels, 1000 protected, 0 rerouted
    Mid:        0 FRR tunnels, 0 protected, 0 rerouted
    Summary:  1000 protected, 500 link protected, 500 node protected, 0 bw protected

P2MP Summary:
    Tunnel Head:         250 total, 250 connected
    Destination Head:    500 total, 500 connected
    S2L Head: 500 established, 0 proceeding
    S2L Mid:  0 established, 0 proceeding
    S2L Tail: 0 established

P2MP Fast ReRoute Summary:
    Tunnel Head: 250 FRR enabled
    S2L Head: 500 FRR, 500 protected, 0 rerouted
    S2L Mid:  0 FRR, 0 protected, 0 rerouted
    Summary:  500 protected, 500 link protected, 0 node protected, 0 bw protected

<snip>
GMPLS UNI Summary:
    Heads: 23 up, 4 down
    Tails: 13 up, 2 down
```

Related Commands

Command	Description
auto-tunnel backup (MPLS-TE)	Builds automatic NHOP and NNHOP backup tunnels.
backup-bw	Specifies the bandwidth type that LSPs can use for a backup tunnel, whether the backup tunnel should provide bandwidth protection, and if yes, how much and in which bandwidth pool.
srlg	Configures an SRLG membership for a link on a given interface.
soft-preemption	Enables soft-preemption on a head-end for the MPLS TE tunnel.

show mpls traffic-eng tunnels auto-bw brief

To display the list of automatic bandwidth enabled tunnels, and to indicate if the current signaled bandwidth of the tunnel is identical to the bandwidth that is applied by the automatic bandwidth, use the **show mpls traffic-eng tunnels auto-bw brief** command in System Admin EXEC mode.

show mpls traffic-eng tunnels auto-bw brief

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **show mpls traffic-eng tunnels auto-bw brief** command to determine if the automatic bandwidth application has been applied on a specified tunnel. If a single tunnel is specified, only the information for that tunnel is displayed.

Task ID

Task ID	Operations
mpls-te	read

Examples   The following sample output shows the list of automatic bandwidth enabled tunnels:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels auto-bw brief

  Tunnel     LSP  Last appl  Requested  Signalled   Highest    Application
  Name        ID  BW(kbps)    BW(kbps)   BW(kbps)   BW(kbps)    Time Left
-------------- ------ ---------- ---------- ---------- ---------- --------------
  tunnel-te0   1         10         10         50      2h 5m
  tunnel-te1   5        500        300        420      1h 10m
```

This table describes the significant fields shown in the display.

Table 56: show mpls traffic-eng tunnels auto-bw brief Field Descriptions

Field	Description
Tunnel Name	Name for the tunnel.
LSP ID	ID of the Label Switched Path that is used by the tunnel.
Last appl BW (kbps)	Last bandwidth applied (for example, requested) by the automatic-bandwidth feature for the tunnel.
Requested BW (kbps)	Bandwidth that is requested for the tunnel.
Signalled BW (kbps)	Bandwidth that is actually signalled for the tunnel.
Highest BW (kbps)	Highest bandwidth measured since the last start of the application interval.
Application Time Left	Time left until the application period ends for this tunnel.

Related Commands

Command	Description
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.

show mpls traffic-eng link-management soft-preemption

To display information about soft-preemption activity on a MPLS TE link, use the **show mpls traffic-eng link-management soft-preemption** command in EXEC mode.

show mpls traffic-eng link-management soft-preemption [**interface***type interface-path-id*]

Syntax Description

interface	Displays information on the specified interface.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default   None

Command Modes   EXEC

Command History

Release	Modification
Release 4.2.0	This command was introduced .

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read

Examples

This is sample output from the **show mpls traffic-eng link-management soft-preemption** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng link-management soft-preemption interface
POS0/1/0/1

Name: POS0/1/0/1; IPv4 Address: 1.2.3.10
Total Soft Preempted Bandwidth (BC0/BC1) kbps: 1500/1000
Currently Soft Preempted Bandwidth (BC0/BC1) kbps: 1200/800
Released Soft Preempted Bandwidth (BC0/BC1) kbps: 300/200
Currently Over-subscribed Bandwidth (BC0/BC1) kbps: 1000/600
Currently Soft Preempted Tunnels: 5 tunnels
 TunID  LSPID       Source          Destination    Pri        BW   Class  Time
                                                   S/H       Kbps   Type   out
 ------ ------ --------------- --------------- ----- ---------- -------- ----
     50     10      4.4.4.40        1.1.1.10   2/2        400      BC0  100
     51     11      4.4.4.40        1.1.1.10   2/2        600      BC0  100
     52     12      4.4.4.40        1.1.1.10   3/3        200      BC0   80
     53     11      4.4.4.40        1.1.1.10   3/3        500      BC1   90
     54     12      4.4.4.40        1.1.1.10   4/4        300      BC1   90
```

show srlg

To show the SRLG interface and configuration information, use the **show srlg** command in EXEC mode.

show srlg [**interface** *type interface-path-id*] [**location** {*node-id*| **all**| **mgmt-nodes**}] [**value** *value-number*] [**trace**{**file** *filename* **original**| **hexdump** | **last** *entries*| **reverse** | **stats**| **tailf** | **unique** | **verbose** | **wrapping**}]

Syntax Description

interface *type*	(Optional) Displays information on the specific interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note**　Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
location	(Optional) Specifies a node.
node-id	Node ID. The *node-id* argument is entered in the *rack/slot/module* notation.
all	Specifies all locations.
mgmt-nodes	Specifies all management nodes.
value *value-number*	(Optional) Displays SRLG value numbers.
trace	(Optional) Displays trace information for SRLG.
file *filename*	(Optional) Displays trace information for a specific file name.
original	Displays the original location of the file.
hexdump	(Optional) Displays traces in hexadecimal format.
last	(Optional) Displays trace information for a specific number of entries.
entries	Number of entries. Replace entries with the number of entries you want to display. For example, if you enter 5, the display shows the last 5 entries in the trace data. Range is 1 to 4294967295.
reverse	(Optional) Displays the latest traces first.

stats	(Optional) Displays the statistics in the command output.
tailf	(Optional) Displays the new traces as they are added in the command output.
unique	(Optional) Displays the unique entries with counts in the command output.
verbose	(Optional) Displays the information for internal debugging in the command output.
wrapping	(Optional) Displays the wrapping entries in the command output.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
ip-services	read

Examples   The following sample output is from the **show srlg value** command.

```
 System Information::
 Interface Count   : 2 (Maximum Interfaces Supported 250)

Interface   : POS0/1/0/0, Value Count : 2
SRLG Values : 10,20

Interface   : POS0/1/0/1, Value Count : 2
SRLG Values : 10,30

Interface   : POS0/1/0/2, Value Count : 2
```

```
        SRLG Values : 10,40

        Interface  : POS0/2/0/0, Value Count : 1
        SRLG Values : 100
```

Related Commands

Command	Description
interface (MPLS-TE), on page 231	Enables MPLS-TE on an interface and enters MPLS-TE interface configuration mode.
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.

signalled-bandwidth

To configure the bandwidth required for an MPLS-TE tunnel, use the **signalled-bandwidth** command in interface configuration mode. To disable the behavior, use the **no** form of this command.

signalled-bandwidth {*bandwidth* [**class-type** *ct*]| **sub-pool** *bandwidth*}

no signalled-bandwidth {*bandwidth* [**class-type** *ct*]| **sub-pool** *bandwidth*}

Syntax Description

bandwidth	Bandwidth required for an MPLS-TE tunnel. Bandwidth is specified in kilobits per second. By default, bandwidth is reserved in the global pool. Range is from 0 to 4294967295.
class-type *ct*	(Optional) Configures the class type of the tunnel bandwidth request. Range is from 0 to 1. Class-type 0 is strictly equivalent to global-pool. Class-type 1 is strictly equivalent to subpool.
sub-pool *bandwidth*	Reserves the bandwidth in the subpool instead of the global pool. Range is 1 to 4294967295. A subpool bandwidth value of 0 is not allowed.

Command Default

The default is 0 in class-type 0.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **signalled-bandwidth** command supports two bandwidth pools (class-types) for the Diff-Serv Aware TE (DS-TE) feature.

Note   The Cisco Diff-Serve Aware TE feature is compliant to IETF standard and will interoperate with third party vendor DS-TE. Both Russian Doll Model and Maximum Allocation Model for bandwidth allocation are supported. We recommended that IETF terminology be used in DS-TE bandwidth configurations, namely, Class-type (CT) and Bandwidth Constraints (BC).

Task ID

Task ID	Operations
mpls-te	read, write

Examples

This example shows how to set the bandwidth required for an MPLS-TE tunnel to 1000 in the global pool (class-type 0):

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# signalled-bandwidth 1000

RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# signalled-bandwidth 1000 class-type 0
```

This example shows how to set the bandwidth required for an MPLS-TE tunnel to 1000 in the sub-pool (class-type 1):

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# signalled-bandwidth sub-pool 1000

RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# signalled-bandwidth 1000 class-type 1
```

Related Commands

Command	Description
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.

signalled-name

To configure the name of the tunnel required for an MPLS-TE tunnel, use the **signalled-name** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

signalled-name *name*

no signalled-bandwidth *name*

Syntax Description

name	Name used to signal the tunnel.

Command Default

Default name is the hostname_tID, where ID is the tunnel interface number.

Command Modes

Interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to set the tunnel name:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# signalled-name tunnel-from-NY-to-NJ
```

Related Commands

Command	Description
show mpls traffic-eng tunnels, on page 373	Displays information about MPLS-TE tunnels.

signalling advertise explicit-null (MPLS-TE)

To specify that tunnels terminating on a router use explicit-null labels, use the **signalling advertise explicit-null** command in MPLS-TE configuration mode. To return to the default behavior, use the **no** form of this command.

signalling advertise explicit-null

no signalling advertise explicit-null

Syntax Description   This command has no arguments or keywords.

Command Default   Implicit-null labels are advertised.

Command Modes   MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **signalling advertise explicit-null** command to specify that tunnels terminating on this router use explicit-null labels. This command applies to tunnel labels advertised to next to last (penultimate) hop.

The explicit label is used to carry quality-of-service (QoS) information up to the terminating-end router of the label switched path (LSP).

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to configure explicit null tunnel labels:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# signalling advertise explicit-null
```

Related Commands

Command	Description
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.
path-selection loose-expansion metric (MPLS-TE), on page 276	Configures a metric type to be used to expand a path to the next loose hop for a tunnel on an area border router.

snmp traps mpls traffic-eng

To enable the router to send Multiprotocol Label Switching traffic engineering (MPLS-TE) Simple Network Management Protocol (SNMP) notifications or informs, use the **snmp traps mpls traffic-eng** command in global configuration mode. To disable this behavior, use the **no** form of this command.

snmp traps mpls traffic-eng [*notification-option*] **preempt**

no snmp traps mpls traffic-eng [*notification-option*]

Syntax Description	*notification-option*	(Optional) Notification option to enable the sending of notifications to indicate changes in the status of MPLS-TE tunnels. Use one of these values:
		• up
		• down
		• reoptimize
		• reroute
		• cisco-ext
	preempt	Enables MPLS-TE tunnel preempt trap.

Command Default   None

Command Modes   Global configuration

Command History

Release	Modification
Release 4.2.0	The **preempt** keyword was added.
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If the command is entered without the *notification-option* argument, all MPLS-TE notification types are enabled.

SNMP notifications can be sent as either traps or inform requests.

The **snmp-server enable traps mpls traffic-eng** command enables both traps and inform requests for the specified notification types. To specify whether the notifications should be sent as traps or informs, use the **snmp-server host** command and specify the keyword **trap** or **informs**.

If you do not enter the **snmp traps mpls traffic-eng** command, no MPLS-TE notifications controlled by this command are sent. To configure the router to send these MPLS-TE SNMP notifications, you must enter at least one **snmp enable traps mpls traffic-eng** command. If you enter the command with no keywords, all MPLS-TE notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. To enable multiple types of MPLS-TE notifications, you must issue a separate **snmp traps mpls traffic-eng** command for each notification type and notification option.

The **snmp traps mpls traffic-eng** command is used in conjunction with the **snmp host** command. Use the **snmp host** command to specify which host or hosts receive MPLS-TE SNMP notifications. To send notifications, you must configure at least one **snmp host** command.

For a host to receive an MPLS-TE notification controlled by this command, both the **snmp traps mpls traffic-eng** command and the **snmp host** command for that host must be enabled.

Task ID

Task ID	Operations
mpls-te	read/write

Examples

This example shows how to configure a router to send MPLS-TE tunnel up SNMP notifications when a configured MPLS-TE tunnel leaves the down state and enters the up state:

```
RP/0/RP0/CPU0:router(config)# snmp traps mpls traffic-eng up
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of a SNMP notification operation.
soft-preemption	Enables soft-preemption on a head-end for the MPLS TE tunnel.

soft-preemption

To enable soft-preemption with default timeout on a head-end for the MPLS TE tunnel, use the **soft-preemption** command in MPLS TE mode. To disable this feature, use the **no** form of this command.

soft-preemption timeout *seconds*

no soft-preemption

timeout *seconds*	Defines the timeout for soft-preempted LSP, in seconds. The default timeout is 60. Range is from 30 to 300.

Command Default

The default *timeout seconds* is 60 seconds.

Command Modes

MPLS TE configuration

Tunnel Interface configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
MPLS-TE	write

Examples

This example shows how to enable soft-preemption on a specific tunnel:

```
RP/0/RP0/CPU0:router(config)#interface tunnel-te 50
RP/0/RP0/CPU0:router(config-if)#soft-preemption
```

This example shows how to enable soft-preemption on a node :

```
RP/0/RP0/CPU0:router(config)#mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)#soft-preemption
RP/0/RP0/CPU0:router(config-soft-preemption)#
```

srlg

To configure an MPLS traffic engineering shared-risk link group (SRLG) value for a link on a given interface, use the **srlg** command in global configuration mode. To disable this configuration, use the **no** form of this command.

srlg *value*

no srlg *value*

Syntax Description

value	Value number that identifies the SRLG. Range is 0 to 4294967295.

Command Default

Shared Risk Link Group memberships are not configured.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.0.0	The **value** argument was added. Command mode was changed to the global configuration mode.
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You can enter up to 30 SRLG entries on the ingress and egress ports of the interface. SRLG entries configured over 30 are silently dropped.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to configure an SRLG with 10 member links:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router#(config)# srlg
RP/0/RP0/CPU0:router#(config-srlg)# interface POS 0/3/0/2
RP/0/RP0/CPU0:router#(config-srlg-if)# value 10
```

Related Commands

Command	Description
interface (MPLS-TE), on page 231	Enables MPLS-TE on an interface and enters MPLS-TE interface configuration mode.
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.

timers loose-path (MPLS-TE)

To configure the period between the headend retries after path errors, use the **timers loose-path** command in MPLS-TE configuration mode. To return to the default behavior, use the **no** form of this command.

timers loose-path retry-period *value*

no timers loose-path retry-period *value*

Syntax Description

retry-period *value*	Configures the time, in seconds, between retries upon a path error. Range is 30 to 600.

Command Default

value: 120

Command Modes

MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to the period between retries after path errors to 300 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# timers loose-path retry-period 300
```

Related Commands

Command	Description
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.

Command	Description
path-selection loose-expansion affinity (MPLS-TE), on page 274	Specifies the affinity value to be used to expand a path to the next loose hop for a tunnel on an area border router.

timers removal unused (auto-tunnel backup)

To configure the frequency at which a timer scans backup autotunnels and removes tunnels that are not in use, use the **timers removal unused (auto-tunnel backup)**command in auto-tunnel backup configuration mode. To return to the default behavior, use the **no** form of this command.

timers removal unused *frequency*

no timers removal unused *frequency*

Syntax Description

frequency	Frequency, in minutes, between backup autotunnel scans to remove tunnels that are not used. Range is 0; 5 to 10080 minutes (7 days). A value of 0 disables the scanning and removal of tunnels.

Command Default

frequency: 60

Command Modes

auto-tunnel backup configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **unused** auto-tunnel backup tunnel is the tunnel that is not assigned to protect any FRR tunnel.

Task ID

Task ID	Operation
mpls-te	read, write

Examples

The following example shows that unused automatic backup tunnels are removed after the 10 minute timer scan is reached.

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# auto-tunnel backup
RP/0/RP0/CPU0:router(config-te-auto-bk)# timers removal unused 10
```

Related Commands

Command	Description
show mpls traffic-eng auto-tunnel backup unused	Displays the unused backup tunnels only.
auto-tunnel backup (MPLS-TE), on page 174	Builds automatic next-hop and next-next-hop tunnels, and enters auto-tunnel configuration mode.

timeout (soft-preemption)

To override the soft-preemption default timeout, use the **timeout** command in MPLS TE mode. To remove this configuration, use the **no** form of this command.

soft-preemption timeout *seconds*

no soft-preemption

Syntax Description

timeout *seconds*	Defines the timeout for soft-preempted LSP, in seconds. The default timeout is 60. Range is from 30 to 300.

Command Default

The default *timeout seconds* is 60 seconds.

Command Modes

MPLS TE configuration

Command History

Release	Modification
Release 4.2.0	This command was introduced.

Usage Guidelines

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
MPLS-TE	write

Examples

This example shows how to override the soft-preemption default timeout:

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# soft-preemption
RP/0/RP0/CPU0:router(config-soft-preemption)# timeout 60
```

topology holddown sigerr (MPLS-TE)

To specify the time that a router should ignore a link in its TE topology database in tunnel path constrained shortest path first (CSPF) computations following a TE tunnel signaling error on the link, use the **topology holddown sigerr** command in MPLS-TE configuration mode. To return to the default behavior, use the **no** form of this command.

topology holddown sigerr *seconds*

no topology holddown sigerr *seconds*

Syntax Description

seconds	Time that the router ignores a link during tunnel path calculations, following a TE tunnel error on the link, specified in seconds. Range is 0 to 300. Default is 10.

Command Default

seconds: 10

Command Modes

MPLS-TE configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

A router at the headend for TE tunnels can receive a Resource Reservation Protocol (RSVP) No Route error message before the router receives a topology update from the IGP routing protocol announcing that the link is down. When this happens, the headend router ignores the link in subsequent tunnel path calculations to avoid generating paths that include the link and are likely to fail when signaled. The link is ignored until the router receives a topology update from its IGP or a link holddown timeout occurs. Use the **topology holddown sigerr** command to change the link holddown time from its 10-second default value.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to set the link holddown time for signaling errors at 15 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# topology holddown sigerr 15
```

Related Commands

Command	Description
mpls traffic-eng, on page 246	Enters MPLS-TE configuration mode.
show mpls traffic-eng topology, on page 364	Displays the current MPLS-TE global topology of this node as well as the signaling error holddown time.

tunnel-id (auto-tunnel backup)

To configure the range of tunnel interface numbers to be used for automatic backup tunnels, use the **tunnel-id** command in auto-tunnel backup configuration mode. To delete the automatic backup tunnels, use the **no** form of this command.

tunnel-id min *number* **max** *number*

no tunnel-id

Syntax Description

min	(Optional) Minimum number for automatic backup tunnels.
number	Valid values are from 0 to 65535.
max	(Optional) Maximum number for automatic backup tunnels.

Command Default   No default behavior or values

Command Modes   Auto-tunnel backup configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If you increase the tunnel ID range, the automatic backup tunnels that failed earlier will get created the next time automatic backup assignments are processed.

Restrictions:

- Command is rejected if the **max** value minus **min** value is >= 1K.

- Command is rejected if **min** value > **max** value.

- Command is rejected if **min** value is greater than the tunnel ID of an existing automatic backup tunnel.

- Command is rejected if **max** value is smaller than the tunnel ID of an existing automatic backup tunnel.

- Command is rejected if a statically configured tunnel ID matches with the configured **min** and **max** range of values.

- Command is rejected if a static backup assignment is already configured to a tunnel with an ID within the **min** value /**max** value range.

Task ID

Task ID	Operation
mple-te	read, write

Examples

The following example allows 800 automatic backup tunnels to be created:

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# auto-tunnel backup
RP/0/RP0/CPU0:router(config-te-auto-bk)# tunnel-id min 1200 max 2000
```

Related Commands

Command	Description
auto-tunnel backup (MPLS-TE), on page 174	Builds automatic next-hop and next-next-hop tunnels, and enters auto-tunnel configuration mode.

RSVP Infrastructure Commands

This module describes the commands to configure and use Resource Reservation Protocol (RSVP) . RSVP is a signaling protocol used to set up, maintain, and control end-to-end quality-of-service (QoS) reservations over IP. RSVP is specified in Internet Engineering Task Force (IETF) RFC 2205 (ftp://ftp.isi.edu/in-notes/rfc2205.txt).

The protocol has been extended to signal Multiprotocol Label Switching traffic engineering (MPLS-TE) tunnels, as specified in the IETF RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels* . The RSVP implementation supports fault handling as specified in IETF RFC 3473, *Generalized Multiprotocol Label Switching* (GMPLS) Signaling RSVP-TE extensions. The RSVP implementation also supports cryptographic authentication and refresh overhead reduction as specified in the RFC2747, *RSVP Cryptographic Authentication* and RFC2961, *RSVP Refresh Overhead Reduction Extensions* respectively.

For detailed information about MPLS concepts, configuration tasks, and examples, see *MPLS Configuration Guide for Cisco NCS 6000 Series Routers*.

Disable or Enable RSVP Message Checksum

Starting from Cisco IOS XR Release 4.0 RSVP computes and sets the checksum field on all outgoing RSVP messages, by default. RSVP also verifies the received checksum on all RSVP received messsges to ensure its integrity.

A CLI is provided to override this default behavior and revert to the behavior exhibited in prior releases, whereby RSVP neither computes or sets the RSVP checksum field on outgoing RSVP messages, nor does it verify the checksum on received RSVP messages. This CLI is :

```
RP/0/RP0/CPU0:router(config)#rsvp signalling checksum disable
```

Note When the **rsvp signalling checksum disable** command is configured, RSVP sets a zero checksum on all outgoing RSVP messages and ignores the checksum on all received RSVP incoming messages.

authentication (RSVP)

To enter RSVP authentication mode, use the **authentication** command in global configuration mode, RSVP interface configuration mode, or RSVP neighbor configuration mode. To remove authentication parameters in the applicable mode, use the **no** form of this command.

authentication

no authentication

Syntax Description

This command has no arguments or keywords.

Command Default

The default value is no authentication, which means that the feature is disabled.

Command Modes

Global configuration

RSVP interface configuration

RSVP neighbor configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to enter RSVP authentication configuration mode from global configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp authentication
RP/0/RP0/CPU0:router(config-rsvp-auth)#
```

The following example shows how to activate the RSVP on an interface and enter RSVP authentication configuration mode:

```
RP/0/RP0/CPU0:router# configure
```

```
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/2/1/0
RP/0/RP0/CPU0:router(config-rsvp-if)# authentication
RP/0/RP0/CPU0:router(config-rsvp-if-auth)#
```

The following example shows how to configure the RSVP neighbor with IP address 1.1.1.1 and enter neighbor authentication configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp neighbor 1.1.1.1 authentication
RP/0/RP0/CPU0:router(config-rsvp-nbor-auth)#
```

Related Commands

Command	Description
key-source key-chain (RSVP), on page 452	Specifies the source of the key information to authenticate RSVP signaling messages.
life-time (RSVP), on page 454	Controls how long RSVP maintains idle security associations with trusted neighbors.
window-size (RSVP), on page 534	Specifies the tolerance to accept out-of-sequence messages.

bandwidth (RSVP)

To configure RSVP bandwidth on an interface using prestandard DS-TE mode, use the **bandwidth** command in RSVP interface configuration mode. To reset the RSVP bandwidth on that interface to its default value, use the **no** form of this command.

bandwidth [*total-reservable-bandwidth* [*largest-reservable-flow*] [**sub-pool** *reservable-bw*]] [**global-pool** *bandwidth* [**sub-pool** *reservable-bw*]] [**bc0** *bandwidth* [**bc1** *reservable-bw*]]

no bandwidth

Syntax Description

total-reservable-bandwidth	(Optional) Total reservable bandwidth (in Kbps, Mbps or Gbps) that RSVP accepts for reservations on this interface. Range is 0 to 4294967295.
largest-reservable-flow	(Optional) Largest reservable flow (in Kbps, Mbps or Gbps) that RSVP accepts for reservations on this interface. Range is 0 to 4294967295.
sub-pool *reservable-bw*	(Optional) Configures the total reservable bandwidth in the sub-pool (in Kbps, Mbps, or Gbps). Range is 0 to 4294967295.
bc0 *bandwidth*	(Optional) Configures the total reservable bandwidth in the bc0 pool (in Kbps, Mbps or Gbps). The default is Kbps. Range is 0 to 4294967295.
bc1 *reservable-bw*	(Optional) Configures the total reservable bandwidth in the bc1 pool (in Kbps, Mbps or Gbps).
global-pool *bandwidth*	(Optional) Configures the total reservable bandwidth in the global-pool. Range is 0 to 4294967295 Kbps.

Command Default

sub-pool-bw: 0

Note If the command is entered without the optional arguments, the total bandwidth is set to 75 percent of the intrinsic bandwidth of the interface. (If the interface has zero intrinsic bandwidth, none are reserved.)

Command Modes

RSVP interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

RSVP is enabled either using the **rsvp interface** command or when MPLS is configured on the interface. In addition, there are other instances in which RSVP is enabled automatically; for example, when an RSVP message is received on an interface that is not configured under RSVP or MPLS (such as out-of-band signaling for an Optical User Network Interface application).

If RSVP reservation messages are received on an interface different from the one through which the corresponding Path message was sent out, the interfaces are adjusted such that all resource reservations, such as bandwidth, are done on the outgoing interface of the Path message.

Prestandard DS-TE uses the Cisco proprietary mechanisms for RSVP signaling and IGP advertisements. This DS-TE mode does not interoperate with third-party vendor equipment. Note that prestandard DS-TE is enabled only after configuring the sub-pool bandwidth values on MPLS-enabled interfaces.

Note   You can also configure RSVP bandwidth on an interface using IETF DS-TE mode. This mode supports multiple bandwidth constraint models, including the Russian Doll Model (RDM) and the Maximum Allocation Model (MAM) both with two bandwidth pools.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to limit the total of all RSVP reservations on POS interface 0/3/0/0 to 5000 Kbps:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/3/0/0
RP/0/RP0/CPU0:router(config-rsvp-if)# bandwidth 5000
```

Related Commands

Command	Description
bandwidth mam (RSVP), on page 432	Configures RSVP bandwidth on an interface using the MAM bandwidth constraints model.
bandwidth rdm (RSVP), on page 434	Configures RSVP bandwidth on an interface using the RDM bandwidth constraints model.

bandwidth mam (RSVP)

To configure RSVP bandwidth on an interface using the Maximum Allocation Model (MAM) bandwidth constraints model, use the **bandwidth mam** command in RSVP interface configuration mode. To return to the default behavior, use the **no** form of this command.

bandwidth mam {*total-reservable-bandwidth*| **max-reservable-bw** *maximum-reservable-bw*} [*largest-reservable-flow* [**bc0** *reservable-bandwidth*] [**bc1** *reservable-bw*]]

no bandwidth mam

Syntax Description

total-reservable- bandwidth	Total reservable bandwidth (in Kbps, Mbps or Gbps) that RSVP accepts for reservations on this interface. Range is 0 to 4294967295.
max-reservable-bw *maximum-reservable-bw*	Configures the maximum reservable bandwidth (in Kbps, Mbps or Gbps) that RSVP accepts for reservations on this interface. Range is 0 to 4294967295.
largest-reservable-flow	(Optional) Largest reservable flow (in Kbps, Mbps or Gbps) that RSVP accepts for reservations on this interface. Range is 0 to 4294967295.
bc0 *reservable-bandwidth*	(Optional) Configures the total reservable bandwidth in the bc0 pool (in Kbps, Mbps or Gbps).
bc1 *reservable-bw*	(Optional) Configures the total reservable bandwidth in the bc1 pool (in Kbps, Mbps or Gbps).

Command Default No default behavior or values.

Command Modes RSVP interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Both the MAM and RDM models can be configured on a single interface to allow switching between each model.

✎

Note   Non-stop forwarding (NSF) is not guaranteed when the bandwidth constraint model is changed.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to limit the total of all RSVP reservations on POS interface 0/3/0/0 to 7500 kbps:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/3/0/0
RP/0/RP0/CPU0:router(config-rsvp-if)# bandwidth mam 7500
```

Related Commands

Command	Description
bandwidth (RSVP), on page 430	Configures RSVP bandwidth on an interface using prestandard DS-TE mode.
bandwidth rdm (RSVP), on page 434	Configures RSVP bandwidth on an interface using the RDM bandwidth constraints model.

bandwidth rdm (RSVP)

To configure RSVP bandwidth on an interface using the Russian Doll Model (RDM) bandwidth constraints model, use the **bandwidth rdm** command in RSVP interface configuration mode. To return to the default behavior, use the **no** form of this command.

bandwidth rdm {*total-reservable-bw*| **bc0** *total-reservable-bw*| **global-pool** *total-reservable-bw*} [*largest-reservable-flow*] [**bc1** *reservable-bw*] [**sub-pool** *reservable-bw*]

no bandwidth rdm

Syntax Description

total-reservable-bw	Total reservable bandwidth (in Kbps, Mbps or Gbps). The default value is expressed in Kbps.
bc0 *total-reservable-bw*	Reserves bandwidth in the bc0 pool (in Kbps, Mbps or Gbps).
global-pool	Reserves bandwidth in the global pool.
largest-reservable-flow	(Optional) Largest reservable flow (in Kbps, Mbps or Gbps). The default value is expressed in Kbps.
bc1	(Optional) Reserves bandwidth in the bc1 pool (in Kbps, Mbps or Gbps).
sub-pool	(Optional) Reserves bandwidth in the sub-pool.
reservable-bandwidth	Reservable bandwidth in the sub- and bc1 pools (in Kbps, Mbps or Gbps). The default value is expressed in Kbps.

Command Default No default behavior or values.

Command Modes RSVP interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Both the MAM and RDM bandwidth constraint models support up two bandwidth pools.

Cisco IOS XR software provides global configuration when switching between bandwidth constraint models. Both models are configured on a single interface to allow switching between models.

Note Non-stop forwarding (NSF) is not guaranteed when the bandwidth constraint model is changed.

The **global pool** and **sub-pool** keywords are included in this command for backward compatibility with prestandard DS-TE. The **global pool** keyword is equivalent to the **bc0** keyword. The **sub-pool** keyword is equivalent to the **bc1** keyword.

RDM is the default bandwidth constraint model used in both pre-standard and IETF mode.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to limit the total of all RSVP reservations on POS interface 0/3/0/0 to 7500 kbps, and allows each single flow to reserve no more than 1000 kbps:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/3/0/0
RP/0/RP0/CPU0:router(config-rsvp-if)# bandwidth rdm 7500 1000
```

Related Commands

Command	Description
bandwidth (RSVP), on page 430	Configures RSVP bandwidth on an interface using prestandard DS-TE mode.
bandwidth mam (RSVP), on page 432	Configures RSVP bandwidth on an interface using the MAM bandwidth constraints model.

clear rsvp authentication

To eliminate RSVP security association (SA) before the lifetime expires, use the **clear rsvp authentication** command in EXEC mode.

clear rsvp authentication [*type interface-path-id*] [**destination** *IP address*] [**source** *IP address*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
destination *IP address*	(Optional) Eliminates the RSVP security associations (SA) before their lifetimes expire. All SAs with this destination IP address are cleared.
source *IP address*	(Optional) Eliminates the RSVP security associations (SA) before their lifetimes expire. All SAs with this source IP address are cleared.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **clear rsvp authentication** command for the following reasons:

- To eliminate security associations before their lifetimes expire

- To free up memory

- To resolve a problem with a security association being in an indeterminate state

You can delete all RSVP security associations if you do not enter an optional filter (interface, source, or destination IP address).

If you delete a security association, it is recreated as needed.

Task ID

Task ID	Operations
mpls-te	execute

Examples

The following example shows how to clear each SA:

```
RP/0/RP0/CPU0:router# clear rsvp authentication
```

The following example shows how to clear each SA with the destination address1.1.1.1:

```
RP/0/RP0/CPU0:router# clear rsvp authentication destination 1.1.1.1
```

The following example shows how to clear each SA with the source address 2.2.2.2:

```
RP/0/RP0/CPU0:router# clear rsvp authentication source 2.2.2.2
```

The following example shows how to clear each SA with the POS interface 0/2/1/0:

```
RP/0/RP0/CPU0:router# clear rsvp authentication POS 0/2/1/0
```

The following example shows how to clear each SA on the POS interface 0/2/1/0, destination address 1.1.1.1, and source address 2.2.2.2:

```
RP/0/RP0/CPU0:router# clear rsvp authentication POS 0/2/1/0 destination 1.1.1.1 source
2.2.2.2
```

Related Commands

Command	Description
life-time (RSVP), on page 454	Controls how long RSVP maintains idle security associations with other trusted RSVP neighbors.

clear rsvp counters authentication

To eliminate RSVP counters for each security association (SA), use the **clear rsvp counters authentication** command in EXEC mode.

clear rsvp counters authentication [*type interface-path-id*] [**destination** *IP address*][**source** *IP address*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
destination *IP address*	(Optional) Eliminates authentication-related statistics for each security association (SA) with this destination IP address.
source *IP address*	(Optional) Eliminates authentication-related statistics for each security association (SA) with this source IP address.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	execute

Examples   The following example shows how to clear authentication counters for each SA:

```
RP/0/RP0/CPU0:router# clear rsvp counters authentication
```

The following example shows how to clear authentication counters for each SA with the destination address 1.1.1.1:

```
RP/0/RP0/CPU0:router# clear rsvp counters authentication destination 1.1.1.1
```

The following example shows how to clear authentication counters for each SA with the source address 2.2.2.2:

```
RP/0/RP0/CPU0:router# clear rsvp counters authentication source 2.2.2.2
```

The following example shows how to clear authentication counters for each SA with the POS interface 0/2/1/0:

```
RP/0/RP0/CPU0:router# clear rsvp counters authentication POS 0/2/1/0
```

The following example shows how to clear authentication counters for each SA on the POS interface 0/2/1/0, destination address 1.1.1.1, and source address 2.2.2.2:

```
RP/0/RP0/CPU0:router# clear rsvp counters authentication POS 0/2/1/0 destination 1.1.1.1
source 2.2.2.2
```

clear rsvp counters all

To clear (set to zero) all RSVP message and event counters that are being maintained by the router, use the **clear rsvp counters all** command in EXEC mode.

clear rsvp counters all [*type interface-path-id*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface.
	Note Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router.
	For more information about the syntax for the router, use the question mark (?) online help function.

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to clear all message and event counters:

```
RP/0/RP0/CPU0:router# clear rsvp counters all
```

Related Commands

Command	Description
clear rsvp counters events, on page 444	Clears all RSVP event counters that are being maintained by the router.
clear rsvp counters messages, on page 446	Clears all RSVP message counters that are being maintained by the router.
show rsvp counters, on page 473	Shows all RSVP message/event counters that are being maintained by the router.

clear rsvp counters chkpt

To clear RSVP checkpoint counters, use the **clear rsvp counters chkpt** command in EXEC mode.

clear rsvp counters chkpt

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to clear all message and event counters:

```
RP/0/RP0/CPU0:router# clear rsvp counters chkpt
```

Related Commands

Command	Description
clear rsvp counters events, on page 444	Clears all RSVP event counters that are being maintained by the router.
clear rsvp counters messages, on page 446	Clears all RSVP message counters that are being maintained by the router.
show rsvp counters, on page 473	Shows all RSVP message/event counters that are being maintained by the router.

clear rsvp counters events

To clear (set to zero) all RSVP event counters that are being maintained by the router, use the **clear rsvp counters events** command in EXEC mode.

clear rsvp counters events [*type interface-path-id*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface.
	Note Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router.
	For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **clear rsvp counters events** command to set all RSVP event counters to zero.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to clear all event counters:

```
RP/0/RP0/CPU0:router# clear rsvp counters events
```

Related Commands

Command	Description
clear rsvp counters messages, on page 446	Clears all RSVP message counters that are being maintained by the router.
show rsvp counters, on page 473	Shows RSVP event counters that are being maintained by the router when the *events* option is specified.

clear rsvp counters messages

To clear (set to zero) all RSVP message counters that are being maintained by the router, use the **clear rsvp counters messages** command in EXEC mode.

clear rsvp counters messages [*type interface-path-id*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **clear rsvp counters messages** command to set all RSVP message counters to zero.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to set all RSVP message counters for POS interface 0/3/0/2 to zero:

```
RP/0/RP0/CPU0:router# clear rsvp counters messages pos0/3/0/2
```

Related Commands

Command	Description
show rsvp counters, on page 473	Displays the number of RSVP messages sent and received.

clear rsvp counters oor

To clear internal RSVP counters on out of resources (OOR) events, use the **clear rsvp counters oor** command in EXEC mode.

clear rsvp counters oor [*type interface-path-id*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **clear rsvp counters oor** command to set RSVP OOR counters to zero.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example show how to clear all RSVP message counters for POS interface 0/3/0/2 to zero:

```
RP/0/RP0/CPU0:router# clear rsvp counters oor pos0/3/0/2
```

Related Commands

Command	Description
show rsvp counters oor, on page 477	Displays the internal RSVP counters on OOR events.

clear rsvp counters prefix-filtering

To clear internal prefix-filtering related RSVP counters, use the **clear rsvp counters prefix-filtering** command in EXEC mode.

clear rsvp counters prefix-filtering {**interface** [*type interface-path-id*]| **access-list** [*aclname*]}

Syntax Description

interface	Clears RSVP prefix-filtering counters for all interfaces.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
access-list	Clears RSVP prefix-filtering counters for access control list.
aclname	(Optional) Name of the access list.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **clear rsvp counters prefix-filtering** command to set RSVP prefix-filtering related RSVP counters to zero.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to set all RSVP message counters for POS interface 0/3/0/2 to zero:

```
RP/0/RP0/CPU0:router# clear rsvp counters prefix-filtering interface pos0/3/0/2
```

The following example shows how to set all RSVP prefix-filtering counters for access-list banks to zero:

```
RP/0/RP0/CPU0:router# clear rsvp counters prefix-filtering access-list banks
```

Related Commands

Command	Description
show rsvp counters prefix-filtering, on page 479	Displays the internal prefix-filtering related RSVP counters.

key-source key-chain (RSVP)

To specify the source of the key information to authenticate RSVP messages, use the **key-source key-chain** command in the appropriate RSVP authentication configuration mode. To remove the key source from the appropriate RSVP authentication configuration mode, use the **no** form of this command.

key-source key-chain *key-chain-name*

no key-source key-chain *key-chain-name*

Syntax Description

key-chain-name	Name of the keychain. The maximum number of characters is 32.

Command Default

The default value is none, which means that the key source is not specified.

Command Modes

RSVP authentication configuration

RSVP interface authentication configuration

RSVP neighbor authentication configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note

- RSVP authentication is enabled regardless of whether or not the specified keychain exists or has no available keys to use. If the specified keychain does not exist or there are no available keys in the keychain, RSVP authentication processing fails.

- The **key-source key-chain** command does not create a keychain but just specifies which keychain to use. You must configure a keychain first. For an example of how a key chain is configured, see .

- The **no key-source key-chain** command does not necessarily disable the authentication.

- RSVP authentication supports only keyed-hash message authentication code (HMAC)-type algorithms.

For inheritance procedures, see .

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows that the source of the key information is specified for the keychain mpls-keys in RSVP authentication configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp authentication
RP/0/RP0/CPU0:router(config-rsvp-auth)# key-source key-chain mpls-keys
```

The following example shows that the source of the key information is specified for the keychain mpls-keys for a POS interface in RSVP authentication configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface POS 0/2/1/0
RP/0/RP0/CPU0:router(config-rsvp-if)# authentication
RP/0/RP0/CPU0:router(config-rsvp-if-auth)# key-source key-chain mpls-keys
```

The following example shows that the source of the key information is specified for the keychain mpls-keys in RSVP neighbor authentication configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp neighbor 1.1.1.1 authentication
RP/0/RP0/CPU0:router(config-rsvp-nbor-auth)# key-source key-chain mpls-keys
```

Related Commands

Command	Description
life-time (RSVP), on page 454	Controls how long RSVP maintains idle security associations with other trusted RSVP neighbors.
window-size (RSVP), on page 534	Specifies the tolerance to accept out-of-sequence messages.

life-time (RSVP)

To control how long RSVP maintains idle security associations with other trusted RSVP neighbors, use the **life-time** command in the appropriate RSVP authentication configuration mode. To disable the lifetime setting, use the **no** form of this command.

life-time *seconds*

no life-time *seconds*

Syntax Description

seconds	Length of time, in seconds, that RSVP maintains security associations with other trusted RSVP neighbors. Range is 30 to 86400.

Command Default

seconds: 1800 (30 minutes)

Command Modes

RSVP authentication configuration

RSVP interface authentication configuration

RSVP neighbor authentication configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

For inheritance procedures, see .

Use the **life-time (RSVP)** command to indicate when to end idle security associations with RSVP trusted neighbors.

By setting a larger lifetime, the router remembers the state for a long period time which provides better protection against a replay attack.

Use the **clear rsvp authentication** command to free security associations before their lifetimes expire.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to configure a lifetime of 2000 seconds for each SA in RSVP authentication configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp authentication
RP/0/RP0/CPU0:router(config-rsvp-auth)# life-time 2000
```

The following example shows how to configure a lifetime of 2000 seconds for each SA in RSVP neighbor authentication configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp neighbor 1.1.1.1 authentication
RP/0/RP0/CPU0:router(config-rsvp-nbor-auth)# life-time 2000
```

The following example shows how to configure a lifetime of 2000 seconds for each SA in RSVP interface authentication configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface POS 0/2/1/0
RP/0/RP0/CPU0:router(config-rsvp-if)# authentication
RP/0/RP0/CPU0:router(config-rsvp-if-auth)# life-time 2000
```

Related Commands

Command	Description
clear rsvp authentication, on page 436	Clears out RSVP security associations.
key-source key-chain (RSVP), on page 452	Specifies the source of the key information to authenticate RSVP signaling messages.
window-size (RSVP), on page 534	Specifies the tolerance to accept out-of-sequence messages.

rsvp

To enable functionality for Resource Reservation Protocol (RSVP) and enter RSVP configuration commands, use the **rsvp** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

rsvp

no rsvp

Syntax Description   This command has no keywords or arguments.

Command Default   No default behavior or values

Command Modes   Global configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to enable RSVP functionality and enter the sub-mode for RSVP configuration commands:

```
RP/0/RP0/CPU0:router(config)# rsvp
RP/0/RP0/CPU0:router(config-rsvp)#
```

rsvp bandwidth mam

To configure the RSVP default interface bandwidth for the maximum reservable bandwidth parameters using the Maximum Allocation Model (MAM) bandwidth constraints model, use the **rsvp bandwidth mam** command in global configuration mode. To return to the default of 75% for the global (BC0) and BC1 pools, use the **no** form of this command.

rsvp bandwidth mam percentage max-reservable *percent* [**bc0** *bc0-percent*] [**bc1** *bc1-percent*]

no rsvp bandwidth mam percentage max-reservable *percent* [**bc0** *bc0-percent*] [**bc1** *bc1-percent*]

Syntax Description

percentage	Configures bandwidths as percentages of physical link bandwidth.
max-reservable	Configures the maximum reservable bandwidth.
percent	Configures the maximum reservable bandwidth interface percentage.
bc0	(Optional) Configures the BC0 global pool bandwidth percentage.
bc0-percent	Percentage for the BC0 pool bandwidth interface. Range is from 0 to 10000. Use this range to under-book or over-book RSVP bandwidth on the interface. **Note** Before you configure the percentage for the BC0 pool, configure the maximum reservable bandwidth pool.
bc1	(Optional) Configures the BC1 subpool bandwidth percentage.

bc1-percent	Percentage for the BC1 pool bandwidth interface. Range is from 0 to 10000. Use this range to under-book or over-book RSVP bandwidth on the interface .
	Note Before you configure the percentage for the BC1 pool, configure the maximum reservable bandwidth for the BC0 pool.

Command Default

If the command is entered without the optional arguments, the RSVP total bandwidth is set to 75 percent of the intrinsic bandwidth of the interface. If the interface has no (0) intrinsic bandwidth, then no bandwidth is reserved for RSVP.

Command Modes

Global configuration

Command History

Release	Modification
Release 4.3.1	The **percentage** keyword was positioned as a global option for the command in the syntax.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note

The percentage keyword was positioned as a global option in the command syntax, thus changing the command syntax from **rsvp bandwidth mam max-reservable percentage** *percent* [**bc0 percentage** *bc0-percent*] [**bc1 percentage** *bc1-percent*] to **rsvp bandwidth mam percentage max-reservable** *percent* [**bc0** *bc0-percent*] [**bc1** *bc1-percent*].

The **percentage** keyword allows for over-booking. The configured value overwrites the current default value of 75%.

RSVP and MPLS-TE uses these defaults to automatically set the BC0 (global pool) and BC1 (subpool) for any RSVP configured interface without specifying an absolute bandwidth.

The bandwidth is configured as a percentage instead of an absolute number. Automatic adjustment is based on the total interface bandwidth changes. The maximum reservable bandwidth automatically is readjusted when the interface bandwidth changes, for example, when adding or removing a bundle member.

You can specify the default percentage for the maximum reservable bandwidth, BC0 (global pool), BC1 (subpool), or either pool.

To configure a default for the BC0 pool, first configure one for the global pool. To configure a default for the BC1 pool, first configure one for the BC0 pool.

Each pool uses the following values:

- Explicit value configured on the interface for this pool.

- Default percentage value configured for this pool.

- Pool parent value (global is parent of both BC0 and BC1). This does not apply to the global pool since it does not have a parent.

Task ID

Task ID	Operation
mpls-te	read, write
ouni	read, write

Examples

This example shows how to configure RSVP default interface bandwidth percentage for the maximum reservable bandwidth using MAM.

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#rsvp bandwidth mam percentage max-reservable 1000 bc0 1000 bc1
 1000
```

Related Commands

Command	Description
bandwidth mam (RSVP), on page 432	Configures RSVP bandwidth on an interface using the Maximum Allocation Model (MAM) bandwidth constraints model.
bandwidth rdm (RSVP), on page 434	Configures RSVP bandwidth on an interface using the Russian Doll Model (RDM) bandwidth constraints model.
rsvp bandwidth rdm, on page 460	Configures the RSVP default interface bandwidth for the maximum reservable bandwidth parameters using the Russian Doll Model (RDM) bandwidth constraints model.
show rsvp interface, on page 494	Displays information about all interfaces with RSVP enabled.

rsvp bandwidth rdm

To configure the RSVP default interface bandwidth for the maximum reservable bandwidth parameters using the Russian Doll Model (RDM) bandwidth constraints model, use the **rsvp bandwidth rdm** command in global configuration mode. To return to the default of 75% for the maximum reservable BC0 pool and 0% for the BC1 pools, use the **no** form of this command.

rsvp bandwidth rdm percentage max-reservable-bc0 *percent* [**bc1** *bc1-percent*]

no rsvp bandwidth rdm percentage max-reservable-bc0 *percent* [**bc1** *bc1-percent*]

Syntax Description

percentage	Configures bandwidths as percentages of physical link bandwidth.
max-reservable-bc0	Configures the maximum reservable bandwidth for the BC0 global pool.
percent	Percentage for the BC0 pool bandwidth interface. Range is from 0 to 10000. Use this range to under-book or over-book RSVP bandwidth on the interface
bc1	Optional) Configures the BC1 subpool percentage for the bandwidth.
bc1-percent	Percentage for the BC1 pool bandwidth interface. Range is from 0 to 10000. **Note** Before you configure the percentage for the BC1 pool, configure the maximum reservable bandwidth for the BC0 pool.

Command Default

If the command is entered without the optional arguments, the RSVP total bandwidth is set to 75 percent of the intrinsic bandwidth of the interface. If the interface has no (0) intrinsic bandwidth, then no bandwidth is reserved for RSVP.

Command Modes

Global configuration

Command History	Release	Modification
	Release 4.3.1	The **percentage** keyword was positioned as a global option for the command in the syntax.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

> **Note**
>
> The **percentage** keyword was positioned as a global option in the command syntax, thus changing the command syntax from **rsvp bandwidth rdm max-reservable-bc0 percentage** *percent* [**bc1 percentage** *bc1-percent* to **rsvp bandwidth rdm percentage max-reservable-bc0** *percent* [**bc1** *bc1-percent*].

The **percentage** keyword allows for over-booking. The configured value overwrites the current default value of 75%.

RSVP and MPLS-TE use these defaults to automatically set the BC0 (global pool) and BC1 (subpool) for any RSVP configured interface without specifying an absolute bandwidth.

The bandwidth is configured as a percentage instead of an absolute number. Automatic adjustment is based on the total interface bandwidth changes. The maximum reservable bandwidth is automatically readjusted when the interface bandwidth changes, for example, when adding or removing a bundle member.

You can specify the default percentage for the maximum reservable bandwidth for the BC0 (global pool), BC1 (subpool), or either pool.

Each pool uses the following values:

- Explicit value configured on the interface for this pool.

- Default percentage value configured for this pool.

Task ID

Task ID	Operation
mpls-te	read, write
ouni	read, write

Examples

This example shows how to configure RSVP default interface bandwidth percentage for the maximum reservable bandwidth using RDM:

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#rsvp bandwidth rdm percentage max-reservable-bc0 1000 bc1 1000
```

Related Commands

Command	Description
bandwidth mam (RSVP), on page 432	Configures RSVP bandwidth on an interface using the Maximum Allocation Model (MAM) bandwidth constraints model.
bandwidth rdm (RSVP), on page 434	Configures RSVP bandwidth on an interface using the Russian Doll Model (RDM) bandwidth constraints model.
rsvp bandwidth mam, on page 457	Configures the RSVP default interface bandwidth for the maximum reservable bandwidth parameters using the Maximum Allocation Model (MAM) bandwidth constraints model.
show rsvp interface, on page 494	Displays information about all interfaces with RSVP enabled.

rsvp interface

To configure RSVP on an interface, use the **rsvp interface** command in global configuration mode. To disable RSVP on that interface, use the **no** form of this command.

rsvp interface *type interface-path-id*

no rsvp interface *type interface-path-id*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface.
	Note Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router.
	For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

RSVP is enabled by default on an interface under the following conditions. (Enabling RSVP on an interface means that interface can be used by RSVP to send and receive RSVP messages).

- RSVP is configured on that interface using the **rsvp interface** command.

- MPLS is configured on that interface.

- Automatically enabled as in the case of out-of-band signaling for the Optical User Network Interface (O-UNI) application, where an RSVP message could be received on an interface which is not configured under RSVP or MPLS.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When RSVP is enabled on an interface by any of the three methods mentioned in the above section, the default bandwidth is 0. Use the bandwidth command in RSVP interface configuration mode to configure the bandwidth on an interface.

If the interface bandwidth is 0, RSVP can be used only to signal flows that do not require bandwidth on this interface.

The **rsvp interface** command enables the RSVP interface configuration mode.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to enable the RSVP interface configuration mode and to enable RSVP on this interface with 0 bandwidth:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/3/0/0
```

Related Commands

Command	Description
bandwidth (RSVP), on page 430	Configures RSVP bandwidth on an interface using prestandard DS-TE mode.
signalling dscp (RSVP), on page 508	Gives all RSVP packets sent out on a specific interface higher priority in the network by marking them with a particular DSCP.

rsvp neighbor

To specify an RSVP neighbor, use the **rsvp neighbor** command in global configuration mode. To deactivate authentication for a neighbor, use the **no** form of this command.

rsvp neighbor *IP-address* **authentication**

no rsvp neighbor *IP-address* **authentication**

Syntax Description

IP-address	IP address of the neighbor. A single IP address of a specific neighbor; usually one of the neighbor's physical or logical (loopback) interfaces.
authentication	Configures RSVP authentication parameters.

Command Default   No default values or behaviors

Command Modes   Global configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note   RSVP neighbor configuration mode can be used only if you want to configure authentication for a particular neighbor.

Task ID

Task ID	Operations
mpls-te	read, write

Examples The following example shows how to enter RSVP neighbor authentication configuration mode for IP address 1.1.1.1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp neighbor 1.1.1.1 authentication
RP/0/RP0/CPU0:router(config-rsvp-nbor-auth)#
```

Related Commands

Command	Description
key-source key-chain (RSVP), on page 452	Specifies the source of the key information to authenticate RSVP signaling messages.
life-time (RSVP), on page 454	Controls how long RSVP maintains idle security associations with other trusted RSVP neighbors.
window-size (RSVP), on page 534	Specifies the tolerance to accept out-of-sequence messages.

show rsvp authentication

To display the database for the security association that RSVP has established with other RSVP neighbors, use the **show rsvp authentication** command in EXEC mode.

show rsvp authentication [*type interface-path-id*] [**destination** *IP-address*] [**detail**] [**mode** {**receive** | **send**}] [**neighbor** *IP-address*] [**source** *IP-address*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
destination *IP-address*	(Optional) Displays the database for the security association (SA) for the destination IP address. The *IP address* argument is the IP address of the destination address.
detail	(Optional) Displays additional information about RSVP security SAs.
mode	(Optional) Specifies the SA type. An SA is used to authenticate either incoming (receive) or outgoing (send) messages.
receive	Displays SAs for incoming messages.
send	Displays SAs for outgoing messages.
neighbor *IP-address*	(Optional) Displays the RSVP authentication information for the neighbor IP address. The *IP-address* argument is the IP address of the neighbor. For the send SA, the neighbor address is the destination address. For receive, the neighbor address is the source address.
source *IP-address*	(Optional) Displays the database for the SA for the source IP address. The *IP-address* argument is the IP address of the source address.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read

Examples

The following sample output displays information for RSVP authentication:

```
RP/0/RP0/CPU0:router# show rsvp authentication

  Codes: S - static, G - global, N - neighbor, I -interface, C - chain

  Source Address  Dest Address   Interface    Mode Key-Source Key-ID Code
  3.0.0.1         3.0.0.2        PO0/7/0/2    Send mpls-keys   1     SGC
  3.0.0.2         3.0.0.1        PO0/7/0/2    Recv mpls-keys   1     SGC
```

This table describes the significant fields shown in the display.

Table 57: show rsvp authentication Command Field Descriptions

Field	Description
Source Address	IP address of the sender. For Send mode, this is the local address (either the address of the Interface field or the local router ID). For Recv mode, this is the address of the RSVP neighbor.
Dest Address	IP address of the receiver. For Send mode, this is the address of the RSVP neighbor. For Recv mode, this is the local address (either the address of the Interface field or the local router ID).
Interface	Name of the interface over which the security association is being maintained.

Field	Description
Mode	Direction of the association for the following mode types: **Send** Authenticates messages that you forward. **Recv** Authenticates messages that you receive.
Key-Source	Key source identification string that is currently set to the configured keychain name.
Key-ID	The last successful key ID that is used for authentication and maps to the keychain ID configuration. If the value is too large to fit into the column, it is truncated and a (..) suffix is appended. Use the detail mode to see the non-truncated key ID.
Code	Code field has the following terms: **Static** Key is static and configured. **Global** Key is global-based. **Neighbor** Key is neighbor-based. **Interface** Key is interface-based. **Chain** Key is part of a keychain.

The following sample output shows detailed information about a Send mode SA that is followed by a Receive mode SA:

```
RP/0/RP0/CPU0:router# show rsvp authentication detail

  RSVP Authentication Information:
    Source Address:       3.0.0.1
    Destination Address:  3.0.0.2
    Neighbour Address:    3.0.0.2
    Interface:            POS0/7/0/2
    Direction:            Send
```

```
        LifeTime:               1800 (sec)
        LifeTime left:          1305 (sec)
        KeyType:                Static Global KeyChain
        Key Source:             name1
        Key Status:             No error
        KeyID:                  1
        Digest:                 HMAC MD5 (16)
        Challenge:              Not supported
        TX Sequence:            5023969459702858020 (0x45b8b99b00000124)
        Messages successfully authenticated:    245
        Messages failed authentication:         0

  Receive Errors:
        Incomplete security association:    0
        Missing INTEGRITY object:           0
        Incorrect digest:                   0
        Digest type mismatch:               0
        Duplicate sequence number:          0
        Out-of-range sequence number:       0
        Invalid message format:             0
```

This table describes the significant fields shown in the display.

Table 58: show rsvp authentication detail Command Field Descriptions

Field	Description
Source Address	IP address of the sender. For Send mode, this is the local address (either the address of the Interface field or the local router ID). For Recv mode, this is the address of the RSVP neighbor.
Destination Address	IP address of the receiver. For Send mode, this is the address of the RSVP neighbor. For Recv mode, this is the local address (either the address of the Interface field or the local router ID).
Neighbor Address	IP address of the RSVP neighbor with which the security association is being maintained.
Interface	Name of the interface over which the security association is being maintained.
Direction	Direction of the association for the following mode types: **Send** Authenticates messages that you forward. **Recv** Authenticates messages that you receive.
LifeTime	Configured expiration timer value.
LifeTime left	Number of seconds until the expiration timer expires.

Field	Description
KeyType	Keys that are used: **Static** Key is static and configured. **Global** Key is global-based. **Neighbor** Key is neighbor-based. **Interface** Key is interface-based. **Chain** Key is part of a keychain.
Key-Source	Key source identification string that is currently set to the configured keychain name.
Key Status	Last status reported from the key source.
Key-ID	Last successful key ID that is used for authentication and that maps to the keychain ID configuration. If the value is too large to fit into the column, it is truncated and a (..) suffix is appended. (Use the detail mode to see the non-truncated key ID.)
Digest	Digest algorithm that is used. The algorithms are either HMAC-MD5 or HMAC-SHA1.
Challenge	Current challenge status (always not supported) reported.
Tx Sequence	Last sequence number that was sent.
Messages successfully authenticated	Number of messages authenticated by using this SA.
Messages failed authentication	Number of messages that failed authentication using this SA.
Sequence Window Size	Maximum configured RX sequence number window.
Sequence Window Count	Currently used size of the RX sequence number window.

Field	Description
Incomplete security association	Number of messages that are dropped due to a key failure.
Incorrect digest	Number of messages that are dropped due to an incorrect digest.
Digest type mismatch	Number of messages that are dropped due to an incorrect digest length, which implies an algorithm mismatch.
Duplicate sequence number	Number of messages that are dropped due to a duplicate sequence number.
Out-of-range sequence number	Number of messages that are dropped due to a sequence number range (window-size) checking.
Invalid message format	Number of messages that are dropped due to formatting errors, such as incorrect objects.

show rsvp counters

To display internal RSVP counters, use the **show rsvp counters** command in EXEC mode.

show rsvp counters {**messages** [*type interface-path-id*| **summary**]| **events** | **database**}

Syntax Description

messages	Displays a historical count of the number of messages RSVP has received and sent on each interface along with a summation.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
summary	(Optional) Displays the aggregate counts of all interfaces.
events	Displays the number of states expired for lack of refresh and a count of received No Acknowledgements (NACKs).
database	Displays counters on RSVP database, including number of paths, session, and so on.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 3.9.0	The **summary** keyword was added.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

In message counters, bundle messages are counted as single bundle messages. The component messages are not counted separately.

The **messages** keyword shows the counters for all the interfaces. In addition, the aggregate summary is shown by using both the **messages** and **summary** keywords.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following is sample output from the **show rsvp counters messages** command for POS0/3/0/0:

```
RP/0/RP0/CPU0:router# show rsvp counters messages POS 0/3/0/0

  POS0/3/0/0          Recv    Xmit                        Recv    Xmit
    Path                24       1    Resv                   0       0
    PathError            0       0    ResvError              0       0
    PathTear             5       1    ResvTear               0       0
    ResvConfirm          0       0    Ack                   34       0
    Bundle               0            Hello                  0       0
    SRefresh         10118       0    OutOfOrder             0
    Retransmit                   0    Rate Limited                   0
```

This table describes the significant fields shown in the display.

Table 59: show rsvp counters messages Command Field Descriptions

Field	Description
Path	Number of Path messages sent downstream or received from an upstream node.
PathError	Number of PathError messages received from a downstream neighbor or sent to an upstream neighbor.
PathTear	Number of PathTear messages sent downstream, or messages received, from upstream neighbors.
ResvConfirm	Number of ResvConfirm messages received from an upstream neighbor or sent to a downstream neighbor.
Bundle	Number of Bundle messages containing RSVP messages sent and received by the neighbor.
SRefresh	Number of Summary Refresh messages sent to and received by a neighbor to refresh the path and reservation states.
Retransmit	Number of messages retransmitted to ensure reliable messaging (related to refresh reduction).
Resv	Number of Reservation messages received from a downstream neighbor or sent to an upstream neighbor to reserve resources.

Field	Description
ResvError	Number of Reservation Error messages received from a upstream neighbor or sent to a downstream neighbor.
ResvTear	Number of Reservation Tear messages received from a downstream neighbor or sent to an upstream neighbor to tear down RSVP flows.
Ack	Number of Acknowledgement messages sent and received by a neighbor acknowledging receipt of a message.
Hello	Number of Hello messages sent to and received by a neighbor.
OutOfOrder	Number of messages received that are out of order.
Rate Limited	Number of RSVP packets affected by rate limiting.

The following is sample output from the **show rsvp counters events** command:

```
RP/0/RP0/CPU0:router# show rsvp counters events

 Ethernet0/0/0/0                       tunnel1
  Expired Path states        0          Expired Path states        0
  Expired Resv states        0          Expired Resv states        0
  NACKs received             0          NACKs received             0
 POS0/3/0/1                            POS0/3/0/2
  Expired Path states        0          Expired Path states        0
  Expired Resv states        0          Expired Resv states        0
  NACKs received             0          NACKs received             0
 POS0/3/0/3                            All RSVP Interfaces
  Expired Path states        0          Expired Path states        0
  Expired Resv states        0          Expired Resv states        0
  NACKs received             0          NACKs received             0
```

This table describes the significant fields shown in the display.

Table 60: show rsvp counters events Command Field Descriptions

Field	Description
Expired Path states	Number of Path states expired for lack of refresh.
Expired Reserve states	Number of Resv states expired for lack of refresh.
NACKS received	Number of NACKS received.

The following is sample output from the **show rsvp counters database** command:

```
RP/0/RP0/CPU0:router# show rsvp counters database

  Sessions: 0
  Locally created and incoming paths: 0
  Outgoing paths: 0
  Locally created and incoming Reservations: 0
  Outgoing Reservations: 0
  Interfaces: 4
```

This table describes the significant fields shown in the display.

Table 61: show rsvp counters database Command Field Descriptions

Field	Description
Sessions	RSVP sessions.
Locally created and incoming paths	Path states created by a: • Local application on the node. • Path message received from the network.
Outgoing paths	Outgoing path states.
Locally created and incoming Reservations	Reservations created by a: • Local application on the node. • Path message received from the network.
Outgoing Reservations	Outgoing reservation (request) states.
Interfaces	Known RSVP interfaces.

show rsvp counters oor

To display internal RSVP counters on out of resources (OOR) events, use the **show rsvp counters oor** command in EXEC mode.

show rsvp counters oor [*type interface-path-id*| **summary**]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface.
	Note Use the **show interfaces**command to see a list of all possible interfaces currently configured on the router.
	For more information about the syntax for the router, use the question mark (?) online help function.
summary	(Optional) Displays a summary of OOR events.

Command Default No default behavior or values

Command Modes EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Examples The following is sample output from the **show rsvp counters oor** command:

```
RP/0/RP0/CPU0:router# show rsvp counters oor
```

```
POS 0/3/0/0           Rejected
    Path                  24
POS 0/3/0/2           Rejected
    Path                  31
All RSVP Interfaces   Rejected
    Path                  55
```

This table describes the significant fields shown in the display.

Table 62: show rsvp counters oor Command Field Descriptions

Field	Description
Path	Number of Path messages received on the interface that were rejected due to oor conditions.

show rsvp counters prefix-filtering

To display internal prefix-filtering related RSVP counters, use the **show rsvp counters prefix-filtering** command in EXEC mode.

show rsvp counters prefix-filtering interface [*type interface-path-id*| **summary**] **access-list** [*aclname*]

Syntax Description

interface	Displays RSVP prefix-filtering counters for all interfaces.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface.
	Note Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router.
	For more information about the syntax for the router, use the question mark (?) online help function.
summary	(Optional) Displays a summary of RSVP prefix-filtering counters on all interfaces.
access-list	Displays RSVP prefix-filtering counters for the access control list.
aclname	(Optional) Name of the access control list.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

✎

Note   Counters do not increment if you have not configured an access control list for prefix-filtering.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following is sample output from the **show rsvp counters prefix-filtering** command:

```
RP/0/RP0/CPU0:router# show rsvp counters prefix-filtering interface

  Routed        Fwd      Local       Drop      Def-Drop     Def-Proc      Total
  Path          4                                                             4
  PathTear      0                                                             0
  ResvConfirm   0                                                             0
  Total         4                                                             4

  POS0/5/0/1    Fwd      Local       Drop      Def-Drop     Def-Proc      Total
  Path                    1           0          219           2           222
  PathTear                0           0           31           0            31
  ResvConfirm             0           0            0           0             0
  Total                   1           0          219           2           253

  POS0/5/0/2    Fwd      Local       Drop      Def-Drop     Def-Proc      Total
  Path                    0           0            0           1             1
  PathTear                0           0            0           0             0
  ResvConfirm             0           0            0           0             0
  Total                   0           0            0           1             1

  ALL RSVP
  Interfaces    Fwd      Local       Drop      Def-Drop     Def-Proc      Total
  Path          4         1           0          219           3           227
  PathTear      0         0           0           31           0            31
  ResvConfirm   0         0           0            0           0             0
  Total         4         1           0          250           3           258
```

The following is sample output from the **show rsvp counters prefix-filtering interface** *type interface-path-id*command:

```
RP/0/RP0/CPU0:router# show rsvp counters prefix-filtering interface POS 0/5/0/1

  POS0/5/0/1    Fwd      Local       Drop      Def-Drop     Def-Proc      Total
  Path                    1           0          219           2           222
  PathTear                0           0           31           0            31
  ResvConfirm             0           0            0           0             0
  Total                   1           0          250           2           253
```

The following is sample output from the **show rsvp counters prefix-filtering interface summary** command:

```
RP/0/RP0/CPU0:router# show rsvp counters prefix-filtering interface summary

  ALL RSVP
  Interfaces    Fwd      Local       Drop      Def-Drop     Def-Proc      Total
  Path          4         1           0          219           3           227
  PathTear      0         0           0           31           0            31
  ResvConfirm   0         0           0            0           0             0
  Total         4         1           0          250           3           258
```

The following is sample output from the **show rsvp counters prefix-filtering access-list banks**command:

```
RP/0/RP0/CPU0:router# show rsvp counters prefix-filtering access-list banks

  ACL: banks        Forward        Local        Drop         Total
```

```
Path                        0            0            0            0
PathTear                    0            0            0            0
ResvConfirm                 0            0            0            0
Total                       0            0            0            0
```

This table describes the significant fields shown in the display.

Table 63: show rsvp counters prefix-filtering interface and summary CommandField Descriptions

Field	Description
Fwd	Number of messages forwarded to the next router. **Note** The messages are counted against the *routed* interface only because RSVP has no record of what interface the messages will be forwarded to.
Local	Number of messages not forwarded (because they are locally destined).
Drop	Number of messages dropped.
Def-Drop	Number of messages dropped when an access control list match returns an implicit deny. (Results when RSVP is configured to drop implicit deny messages.)
Def-Proc	Number of messages processed by RSVP when an access control list match returns an implicit deny.
Path	Number of Path messages.
PathTear	Number of Path Tear messages.
ResvConfirm	Number of ResvConfirm messages.

show rsvp fast-reroute

To display RSVP Fast-Reroute (FRR) information, use the **show rsvp fast-reroute** command in EXEC mode.

show rsvp fast-reroute [**destination** *IP -address*] [**dst-port** *port*] [**source** *IP-address*] [**src-port** *source-port*] [**summary**]

Syntax Description

destination *IP-address*	(Optional) Displays the entries that match the specified address.
dst-port *port*	(Optional) Displays the port address of the destination router.
source *IP-address*	(Optional) Displays the IP address of the source network.
src-port *source-port*	(Optional) Displays the port number of the source router.
summary	(Optional) Displays summarized information about the FRR database.

Command Default None

Command Modes EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Examples This is sample output from the **show rsvp fast-reroute** command:

```
RP/0/RP0/CPU0:router# show rsvp fast-reroute

 Type          Destination      TunID        Source        PSBs        RSBs
 --------      ---------------  -----------  ------------  ---------  -------
```

```
        LSP4          70.70.70.70          1          50.50.50.50      Ready          Ready
```

This table describes the significant fields shown in the display.

Table 64: show rsvp fast-reroute Command Field Descriptions

Field	Description
Type	Type of session.
Destination	Destination address of session.
TunID	Tunnel ID number.
Source	Source address of session.
PSBs	PSB FRR[34] state.
RSBs	RSB FRR state.

[34] Fast reroute.

This is sample output from the **show rsvp fast-reroute summary** command:

```
RP/0/RP0/CPU0:router# show rsvp fast-reroute summary

  States         Total          Ready          Act-Wait          Active
  PSBs             1              1               0                 0
  RSBs             1              1               0                 0
```

This table describes the significant fields shown in the display.

Table 65: show rsvp fast-reroute summary Command Field Descriptions

Field	Description
States	FRR[35] state.
Total	Total number of path and reservation states.
Ready	Number of states in FRR ready state. No FRR processing has been done on these states.
Act-Wait	Number of states in "Active Wait" FRR state. • For PSBs, this indicates that after FRR the path message has not yet been sent. • For RSBs, this indicates that after FRR, the reservation message has not yet been received.

Field	Description
Active	Number of states in "Active" FRR state. • For PSBs, this indicates that after FRR the path message has been sent. • For RSBs, this indicates that after FRR, the reservation message has been received.

35 Fast reroute.

Related Commands

Command	Description
show mrib mpls traffic-eng fast-reroute	Configures the multicast routing information base MPLS traffic engineering fast reroute information.

show rsvp graceful-restart

To display the local graceful-restart information for RSVP, use the **show rsvp graceful-restart** command in EXEC mode.

show rsvp graceful-restart [neighbors] [*IP-address*] **[detail]**

Syntax Description

neighbors	(Optional) Displays single-line status for each neighbor. If this keyword is not specified, only a multiline table entry is displayed showing local graceful-restart information.
IP-address	(Optional) Address of the neighbor you are displaying. Displays a specific neighbor with that destination address only. If this keyword is not specified, all neighbors are displayed.
detail	(Optional) Displays multiline status for each neighbor. If this keyword is not specified, only a single-line table entry is displayed.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Graceful-restart neighbors are displayed in ascending order of neighbor IP address.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following is sample output from the **show rsvp graceful-restart** command:

```
RP/0/RP0/CPU0:router# show rsvp graceful-restart
```

```
Graceful restart: enabled  Number of global neighbors: 1
Local MPLS router id: 192.168.55.55
Restart time: 60 seconds  Recovery time: 120 seconds
Recovery timer: Not running
Hello interval: 5000 milliseconds Maximum Hello miss-count: 4
```

This table describes the significant fields shown in the display.

Table 66: show rsvp graceful-restart Command Field Descriptions

Field	Description
Graceful restart	Indicates whether graceful restart is configured locally.
Number of global neighbors	Number of neighbors identified by a unique router ID.
Local MPLS router id	Local router ID used for the MPLS applications.
Restart time	Amount of time after a loss in hello messages within which RSVP hello session is reestablished. This setting is manually configurable.
Recovery time	Local recovery time advertised to neighbors. This is dynamically computed based on the number of LSPs established and is the time used by neighbors to refresh states in the event of a failure.
Recovery timer	Countdown timer which, upon expiry, causes un-refreshed data forwarding states to be deleted (usually beginning with a value that is equivalent to the sum of the restart and recovery times).
Hello interval	Interval at which hello messages are sent to neighbors.
Maximum hello miss-count	Number of hellos from a neighbor that can be missed before declaring hellos down.

The following is sample output from the **show rsvp graceful-restart neighbors** command, which displays information about graceful restart neighbors in the router:

```
RP/0/RP0/CPU0:router# show rsvp graceful-restart neighbors

 Neighbor        App  State Recovery      Reason               Since  LostCnt
 --------------- ----- ------ -------- ------------ -------------------- --------
 192.168.77.77 MPLS    UP    DONE      N/A  19/12/2002 17:02:25        0
```

This table describes the significant fields shown in the display.

Table 67: show rsvp graceful-restart neighbors Command Field Descriptions

Field	Description
Neighbor	Router ID of a global neighbor.
App	Application type of a global neighbor ( ).
State	State of the hello session to a global neighbor (up, down, INIT).
Recovery	State at which the local node is recovering a global neighbor.
Reason	Last reason for which communication has been lost for a global neighbor. If none has occurred, this field is marked as N/A.
Since	Time at which the current hello state for a global neighbor has been established.
LostCnt	Number of times hello communication has been lost with a global neighbor.

The following is sample output from the **show rsvp graceful-restart neighbors detail** command, which displays detailed information about all graceful restart neighbors:

```
RP/0/RP0/CPU0:router# show rsvp graceful-restart neighbors detail

  Neighbor: 192.168.77.77 Source: 192.168.55.55 (MPLS)
    Hello instance for application MPLS
      Hello State: UP        (for 00:20:52)
      Number of times communications with neighbor lost: 0
      Reason: N/A
    Recovery State: DONE
    Number of Interface neighbors: 1
      address: 192.168.55.0
    Restart time: 120 seconds  Recovery time: 120 seconds
    Restart timer: Not running
    Recovery timer: Not running
    Hello interval: 5000 milliseconds  Maximum allowed missed Hello messages: 4
```

This table describes the significant fields shown in the display.

Table 68: show rsvp graceful-restart neighbors detail Command Field Descriptions

Field	Description
Neighbor	Router ID of a global neighbor.
Source	Local router ID and application type.
Hello State	State of the hello instance for the global neighbor (up, down, or init) and duration of the current state.

Field	Description
Number of times communications with neighbor lost	Number of times hello communication has been lost with a global neighbor.
Reason	Last reason indicating why communication was lost for a global neighbor. If none has occurred, this field is marked as N/A.
Recovery State	State at which the local node is recovering a global neighbor.
Number of Interface neighbors	Number of interfaces belonging to a global neighbor.
Address	IP address of the interface neighbor.
Recovery timer	Remote recovery time for a global neighbor.
Hello interval	Interval at which hello messages are sent by the remote global neighbor.
Maximum allowed missed Hello messages	Number of hellos that can be missed by the remote global neighbor before declaring hellos down.

show rsvp hello instance

To display the RSVP hello instances, use the **show rsvp hello instance** command in EXEC mode.

show rsvp hello instance [*Hostname* or *IP-address*] **[detail]**

Syntax Description		
Hostname or *IP-address*	(Optional) Address of the neighbor you are displaying. If this argument is not specified, all neighbors are displayed.	
detail	(Optional) Displays multiline status for each hello instance. If this keyword is not specified, only a single-line table entry is displayed.	

Command Default No default behavior or values

Command Modes EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Hello instances are displayed in ascending order of neighbor IP address.

Task ID

Task ID	Operations
mpls-te	read, write

Examples The following is sample output from the **show rsvp hello instance** command, which displays brief information about all hello instances in the router:

```
RP/0/RP0/CPU0:router# show rsvp hello instance

  Neighbor        Type    State    Interface    LostCnt
  --------------- ------  -------- ------------ --------
  192.168.77.77   ACTIVE  UP       None         0
```

This table describes the significant fields shown in the display.

Table 69: show rsvp hello instance Command Field Descriptions

Field	Description
Neighbor	Router ID of a global neighbor hosting the hello instance.
Type	Hello instance type (active or passive). Active type indicates that a node is sending hello requests and passive indicates that a node is sending hello acknowledgements.
State	State of the hello session to a global neighbor (up, down, or init).
Interface	Interface for interface bound hello's used for FRR[36]. Hello instances bound to a global neighbor show Interface as None. Hellos used for FRR are currently not supported.
LostCnt	Number of times hello communication has been lost with a global neighbor.

[36] Fast reroute.

The following is sample output from the **show rsvp hello instance** command, which displays detailed information about all hello instances in the router:

```
RP/0/RP0/CPU0:router# show rsvp hello instance detail

 Neighbor: 192.168.77.77 Source: 192.168.55.55 (MPLS)
   State: UP        (for 00:07:14)
   Type: ACTIVE    (sending requests)
   I/F: None
   Hello interval (msec) (used when ACTIVE)
   Configured: 5000
   Src_instance 0x484b01, Dst_instance 0x4d4247
   Counters:
   Communication with neighbor lost:
     Num of times: 0     Reasons:
       Missed acks:            0
       New Src_Inst received:   0
       New Dst_Inst received:   0
       I/f went down:          0
       Neighbor disabled Hello: 0
   Msgs Received:   93
     Sent:        92
     Suppressed: 87
```

This table describes the significant fields shown in the display.

Table 70: show rsvp hello instance detail Command Field Descriptions

Field	Description
Neighbor	Router ID of a global neighbor.
Source	Local router ID and application type.
State	State of the hello instance for the global neighbor (up, down or init) and duration of the current state.
Type	Hello instance type (active or passive). Active type indicates that a node is sending hello requests and passive indicates that a node is sending hello acks.
I/F	Interface for interface bound hellos. Hello instances for Graceful restart show interface as None.

show rsvp hello instance interface-based

To display the RSVP hello instances on a specific interface, use the **show rsvp hello instance interface-based** command in EXEC mode.

show rsvp hello instance interface-based [*IP-address*] **[detail]**

Syntax Description

IP-address	(Optional) Address of the neighboring interface. you are displaying. If this argument is not specified, all neighbors are displayed.
detail	(Optional) Displays detailed information for the specified interface.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Hello instances are displayed in ascending order of neighbor IP address.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following is sample output from the **show rsvp hello instance interface-based** command, which displays detailed information about hello instances on a specific interface:

```
RP/0/RP0/CPU0:router# show rsvp hello instance interface-based 10.10.10.10

  Neighbor        Type    State    Interface    LostCnt
  --------------- ------  -------- -----------  --------
  10.10.10.10     ACTIVE  UP       None         0
```

This table describes the significant fields shown in the display.

Table 71: show rsvp hello instance interface-based Command Field Descriptions

Field	Description
Neighbor	Router ID of a global neighbor hosting the hello instance.
Type	Hello instance type (active or passive). Active type indicates that a node is sending hello requests and passive indicates that a node is sending hello acknowledgements.
State	State of the hello session to a global neighbor (up, down, or init).
Interface	Interface for interface bound hello's used for FRR[37]. Hello instances bound to a global neighbor show interface as none. Hellos used for FRR are currently not supported.
LostCnt	Number of times hello communication has been lost with a global neighbor.

[37] Fast reroute.

show rsvp interface

To display information about all interfaces with RSVP enabled, use the **show rsvp interface** command in EXEC mode.

show rsvp interface [*type interface-path-id*] **[detail]**

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or a virtual interface. **Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
detail	(Optional) Displays multiline status for each interface. If this keyword is not specified, only a single-line table entry is displayed.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	Sample output was modified.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **show rsvp interface** command to display various configuration settings such as the list of neighbors and their refresh reduction capabilities.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following is sample output from the **show rsvp interface** command, which displays brief information about the RSVP-configured interfaces running in prestandard DS-TE mode:

```
RP/0/RP0/CPU0:router# show rsvp interface gigabitEthernet 0/3/0/0

Thu Oct 22 20:35:07.737 UTC
INTERFACE: GigabitEthernet0/3/0/0 (ifh=0x4000300).
 BW (bits/sec): Max=750M. MaxFlow=750M.
               Allocated=0 (0%).
               BC0=750M. BC1=0.
```

The following is sample output from the **show rsvp interface** command, which displays brief information about the RSVP-configured interfaces for the GigabitEthernet interface type:

```
RP/0/RP0/CPU0:router# show rsvp interface gigabitEthernet 0/3/0/0

Thu Oct 22 20:35:42.323 UTC
Interface   MaxBW (bps) MaxFlow (bps) Allocated (bps)     MaxSub (bps)
----------- ----------- ------------- -------------------- ------------
Gi0/3/0/0        750M          750M            0 (  0%)             0
```

This following is sample output from the **show rsvp interfaces detail** command running in standard DS-TE mode:

```
RP/0/RP0/CPU0:router# show rsvp interface gigabitEthernet 0/3/0/0 detail

Thu Oct 22 20:35:11.638 UTC
INTERFACE: GigabitEthernet0/3/0/0 (ifh=0x4000300).
 VRF ID: 0x60000000 (Default).
 BW (bits/sec): Max=750M. MaxFlow=750M.
               Allocated=0 (0%).
               BC0=750M. BC1=0.
 Signalling: No DSCP marking. No rate limiting.
 States in: 0. Max missed msgs: 4.
 Expiry timer: Not running. Refresh interval: 45s.
 Normal Refresh timer: Not running. Summary refresh timer: Running.
 Refresh reduction local: Enabled. Summary Refresh: Enabled (1472 bytes max).
 Reliable summary refresh: Disabled. Bundling: Enabled. (1500 bytes max).
 Ack hold: 400 ms, Ack max size: 1500 bytes. Retransmit: 900ms.
 Neighbor information:
   Neighbor-IP    Nbor-MsgIds States-out  Refresh-Reduction Expiry(min::sec)
 -------------- -------------- ---------- ------------------ ----------------
        9.0.0.1              0          6            Enabled 14::56
     10.10.10.10             0          0            Enabled 14::33
```

This table describes the significant fields shown in the display.

Table 72: show rsvp interface detail Command Field Descriptions

Field	Description
Bandwidth	Configured values on the interface and currently allocated bandwidth.
Ack hold	Time, in milliseconds, before RSVP responds with an acknowledgment.
Neighbor-IP	Address of peer that RSVP is exchanging messages on that interface.

Field	Description
Nbor-msglds	Message IDs received from the neighbor (corresponding to the number of LSPs with reliable messaging).
States-out	States (including paths or reservations) sent on this interface to the neighbor.
Refresh Reduction	Neighbor Refresh Reduction capability.
Expiry	Time a neighbor entry in the interface database expires if there is no activity on this interface with the corresponding neighbor.

Related Commands

Commands	Description
show rsvp counters, on page 473	Displays internal RSVP counters.

show rsvp request

To list all the requests that RSVP knows about on a router, use the **show rsvp request** command in EXEC mode.

show rsvp request [**destination** *IP-address*] **[detail]** [**dst-port** *port-num*] [**source** *IP-address*] [**src-port** *port-num*]

Syntax Description

detail	(Optional) Displays multiline status for each path. If this keyword is not specified, only a single-line table entry is displayed.
destination *IP-address*	(Optional) Displays the entries that match the specified address.
dst-port *port-num*	(Optional) Displays destination port and tunnel information.
source *IP-address*	(Optional) Displays source address information.
src-port *port-num*	(Optional) Displays port and LSP ID information.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command displays information about upstream reservations only; that is, reservations being sent to upstream hops. Information about downstream reservations (that is, incoming or locally created reservations) is available using the **show rsvp reservation** command.

Reservations are displayed in ascending order of destination IP address, destination port, source IP address, and source port.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following is sample output from the **show rsvp request** command:

```
RP/0/RP0/CPU0:router# show rsvp request

       Dest Addr DPort      Source Addr SPort Pro   OutputIF Sty Serv Rate Burst
  ---------------- ----- ---------------- ----- --- ---------- --- ---- ---- -----
    192.168.40.40 2001    192.168.67.68    2   0   PO0/7/0/1  SE LOAD    0    1K
```

The following is sample output from the **show rsvp request detail** command, which displays detailed information about all requests in the router. Requests are reservation states for the reservation messages sent upstream:

```
RP/0/RP0/CPU0:router# show rsvp request detail

  REQ:  IPv4-LSP Session addr: 192.168.40.40. TunID: 2001. LSPId: 2.
    Source addr: 192.168.67.68. ExtID: 192.168.67.68.
    Output interface: POS0/7/0/1. Next hop: 192.168.67.68 (lih: 0x19700001).
    Flags: Local Receiver.
    Style: Shared-Explicit. Service: Controlled-Load.
    Rate: 0 bits/sec. Burst: 1K bytes. Peak: 0 bits/sec.
    MTU min: 0, max: 500 bytes.
    Policy:  Forwarding. Policy source(s): MPLS/TE.
    Number of supporting PSBs: 1
    Destination Add DPort      Source Add SPort Pro     Input IF Rate Burst Prot
     192.168.40.40  2001       192.168.67.68 2   0     PO0/7/0/1   0   1K     Off
    Number of supporting RSBs: 1
    Destination Add DPort      Source Add SPort Pro    Input IF Sty Serv Rate Burst
     192.168.40.40  2001       65.66.67.68 2   0       None SE LOAD    0    1K
```

This table describes the significant fields shown in the display.

Table 73: show rsvp request detail Command Field Descriptions

Field	Description
Number of supporting PSBs	Number of senders for this session (typically, 1).
Number of supporting RSBs	Number of reservations per session (typically, 1).
Policy	Admission control status.
Policy source	Entity performing the admission control (MPLS-TE or COPS).

Related Commands

Commands	Description
show rsvp reservation, on page 499	Displays internal RSVP reservation counters.

show rsvp reservation

To display all reservations that RSVP knows about on a router, use the **show rsvp reservation** command in EXEC mode.

show rsvp reservation [**destination** *IP address*] [**detail**] [**dst-port** *port-num*] [**source** *IP-address*] [**src-port** *port-num*]

Syntax Description

detail	(Optional) Displays multiline status for each reservation. If the **detail** keyword is not specified, only a single-line table entry is displayed.
destination *IP-address*	(Optional) Displays the entries that match the specified address.
dst-port *port-num*	(Optional) Displays destination port and tunnel ID information.
source *IP-address*	(Optional) Displays source address information.
src-port *port-num*	(Optional) Displays source port and LSP ID information.

Command Default　　No default behavior or values

Command Modes　　EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines　　To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show rsvp reservation** command displays information about downstream reservations only (that is, reservations received on this device or created by application program interface (API) calls). Upstream reservations or requests are displayed using the **show rsvp request** command.

Task ID

Task ID	Operations
mpls-te	read, write

The following is sample output from the **show rsvp reservation** command:

```
RP/0/RP0/CPU0:router# show rsvp reservation

        Dest Addr DPort     Source Addr SPort Pro   Input IF Sty Serv Rate Burst
---------------- ----- --------------- ----- --- ---------- --- ---- ---- -----
   192.168.40.40 2001   192.168.67.68     2   0       None  SE LOAD    0   1K
   192.168.67.68 2000      10.40.40.40   15   0 PO0/7/0/1  SE LOAD    0   1K
```

The following example displays detailed information about all reservations in the router:

```
RP/0/RP0/CPU0:router# show rsvp reservation detail

 RESV: IPv4-LSP Session addr: 192.168.40.40. TunID: 2001. LSPId: 2.
  Source addr: 192.168.67.68. ExtID: 192.168.67.68.
  Input adjusted interface: None. Input physical interface: None.
  Next hop: 0.0.0.0 (lih: 0x0).
  Style: Shared-Explicit. Service: Controlled-Load.
  Rate: 0 bits/sec. Burst: 1K bytes. Peak: 0 bits/sec.
  MTU min: 40, max: 500 bytes.
  Flags: Local Receiver.
  State expires in 0.000 sec.
  Policy:  Accepted. Policy source(s): MPLS/TE.
  Header info: RSVP TTL=255. IP TTL=255. Flags: 0x0. TOS=0xff.
  Resource:
   Labels: Local downstream: 3.

 RESV: IPv4-LSP Session addr: 192.168.67.68. TunID: 2000. LSPId: 15.
  Source addr: 192.168.40.40. ExtID: 10.10.40.40.
  Input adjusted interface: PO0/7/0/1. Input physical interface: PO0/7/0/1.
  Next hop: 10.66.67.68 (lih: 0x8DE00002).
  Style: Shared-Explicit. Service: Controlled-Load.
  Rate: 0 bits/sec. Burst: 1K bytes. Peak: 0 bits/sec.
  MTU min: 0, max: 500 bytes.
  Flags: None.
  State expires in 361.184 sec.
  Policy:  Accepted. Policy source(s): MPLS/TE.
  Header info: RSVP TTL=254. IP TTL=254. Flags: 0x1. TOS=0xff.
  Resource:
   Labels: Outgoing downstream: 3.
```

This table describes the significant fields shown in the display.

Table 74: show rsvp reservation detail Command Field Descriptions

Field	Description
Input adjusted interface	Interface to reflect the path's outgoing interface.
Input physical interface	Interface where the reservation was received.
Next hop	Address of the downstream node that sent the reservation to this node.
Lih	Logical interface handle sent in the hop object of path returned to us in the reservation to figure out what interface the path was sent on.
Flags	Indicates path state, including as Local Repair, Local Sender (LSP[38] ingress node), and others.

Field	Description
Policy	Admission control status.
Policy source	Entity performing the admission control on the LSP.
Header info	RSVP header information as described in RFC 2205.

38 Link-state packet

Related Commands

Command	Description
show rsvp request, on page 497	Lists all the requests that RSVP knows about on a router.

show rsvp sender

To display all path states that RSVP knows about on this router, use the **show rsvp sender** command in EXEC mode.

show rsvp sender [**destination** *IP-address*] **[detail]** [**dst-port** *port-num*] [**source** *IP-address*] [**src-port** *port-num*]

Syntax Description

detail	(Optional) Displays multiline status for each path. If the **detail** keyword is not specified, only a single-line table entry is displayed.
destination *IP-address*	(Optional) Displays the entries that match the specified address.
dst-port *port-num*	(Optional) Displays destination port and tunnel ID information.
source *IP-address*	(Optional) Displays source address information.
src-port *port-num*	(Optional) Displays source port and LSP ID information.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show rsvp sender** command displays information about path states.

Task ID

Task ID	Operations
mpls-te	read, write

Examples The following is sample output from the **show rsvp sender**command:

```
RP/0/RP0/CPU0:router# show rsvp sender

  Dest Addr        DPort    Source Addr SPort   Pro  Input IF     Rate Burst Prot
  ---------------- -----  --------------- ----- --- ------------ ---- ----- ----
  10.40.40.40      2001     10.66.67.68     2   0    PO0/7/0/1    0    1K   Off
  10.66.67.68      2000     10.40.40.40    15   0    None         0    1K   Off
```

This table describes the significant fields shown in the display.

Table 75: show rsvp sender Command Field Descriptions

Field	Description
DProt	Destination port number and tunnel-id.
Dest Address	Destination and session address of LSP[39].
SPort	Source port and LSP ID.
Source Addr	Address of the ingress node of the LSP.
Input IF	Interface on which the Path message was received.

[39] Link-state packet

The following example displays detailed information about all paths in the system:

```
RP/0/RP0/CPU0:router# show rsvp sender detail

 PATH: IPv4-LSP Session addr: 65.66.67.68. TunID: 1. LSPId: 25.
  Source addr: 40.40.40.40. ExtID: 40.40.40.40.
  Prot: Off. Backup tunnel: None.
  Setup Priority: 7, Reservation Priority: 0
  Rate: 0 bits/sec. Burst: 1K bytes. Peak: 0 bits/sec.
  Min unit: 40 bytes, Max unit: 500 bytes
  Flags: Bidirectional.
  State expires in 370.154 sec.
  Policy:  Accepted. Policy source(s): Default.
  Header info: RSVP TTL=254. IP TTL=254. Flags: 0x1. TOS=0xc0.
  Input interface: PO0/3/0/0. Previous hop: 40.40.40.40 (lih: 0x40600001).
  Resource:
   Labels: Outgoing upstream: 3.
  Class-Type: None.
  Explicit Route (Incoming):
      Strict, 65.66.67.68(interface-path-id 5)
      Strict, 65.66.67.68/32
```

This table describes the significant fields shown in the display.

Table 76: show rsvp sender detail Command Field Descriptions

Field	Description
Prot	LSP configured as a protected tunnel.

Field	Description
Backup tunnel	Name of the backup tunnel assigned to protect this LSP[40].
Flags	Path state, including as local repair, local sender (LSP ingress node), and others.
Policy	Admission control status for Path message in the incoming direction.
Policy source	Entity doing the admission control, such as COPS or MPLS-TE[41].
Header info	RSVP header information as described in RFC 2205.
Input interface	Interface on which the path was received. At ingress mode, it is None.
Previous hop	Address of the upstream peer who sent us the Path message. May be the interface address or node-id depending on LSP (packet or optical).
Lih	Logical interface handle received in the hop object of the path.
Output interface	Interface on which the path was forwarded to the downstream neighbor
Policy	Admission control status for the path in the outgoing direction.
Explicit route	Explicit route specified in the explicit-route object of the Path message.

40 Link-state packet
41 MPLS-Traffic Engineering

show rsvp session

To list all sessions that RSVP knows about on this router, use the **show rsvp session** command in EXEC mode.

show rsvp session [**destination** *IP-address*] [**detail**] [**dst-port** *port-num*] [**tunnel-name** *tunnel-name*]

Syntax Description

detail	(Optional) Displays multiline status for each path. If the **detail** keyword is not specified, only a single-line table entry is displayed.
destination *IP-address*	(Optional) Displays the entries that match the specified address.
dst-port *port-num*	(Optional) Displays destination port and tunnel ID information.
tunnel-name *tunnel-name*	(Optional) Displays status for the session matching the specified tunnel-name.

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Sessions are displayed in ascending order of destination IP address, destination port, and source IP address.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following is sample output from the **show rsvp session** command:

```
RP/0/RP0/CPU0:router# show rsvp session

  Type    Session Addr  Port  Proto/ExtTunID  PSBs  RSBs  Reqs
  ----  --------------- ----- --------------- ----- ----- -----
  LSP4    10.40.40.40   2001    10.66.67.68     1     1     1
```

```
      LSP4    10.66.67.68  2000     10.40.40.40    1    1     0
```

This table describes the significant fields shown in the display.

Table 77: show rsvp session Command Field Descriptions

Field	Description
Type	Type of data flow (Traffic-Engineering LSP (LSP4 or IPV4 session).
Session Addr	Destination address of the data packets and also tail of the LSP.
Port	Destination port or tunnel ID in case of TE tunnels.
Proto/ExtTunID	Source address of TE tunnels or protocol as in the case of IPV4 sessions.
PSBs	Number of path state blocks for this session.
RSBs	Number of reservation state blocks pertaining to incoming or local reservations for this session.
Reqs	Number of requests. State data structure representing reservations sent up-stream.

The following is sample output for the **show rsvp session detail** command:

```
RP/0/RP0/CPU0:router# show rsvp session detail

  SESSION: IPv4-LSP Addr: 65.66.67.68, TunID: 1, ExtID: 40.40.40.40
  PSBs: 1, RSBs: 1, Requests: 0
  LSPId: 1
  Tunnel Name: newhead_t1
   RSVP Path Info:
    InLabel: No intf, No label
    Incoming Address: Unknown
    Explicit Route:
      Strict, 65.66.67.68(interface-path-id 5)
      Strict, 65.66.67.68/32
    Record Route: None
    Tspec: avg rate=0, burst=1K, peak rate=0
   RSVP Resv Info:
    OutLabel: POS0/7/0/1, 5
    FRR OutLabel: No intf, No label
    Record Route:
      Node-id 65.66.67.68, interface index 5
    Fspec: avg rate=0, burst=1K, peak rate=0
```

This table describes the significant fields shown in the display.

Table 78: show rsvp session detail Command Field Descriptions

Field	Description
TunID	Tunnel identifier and the destination port of the LSP[42].
ExtID	Ingress node address of LSP.
Tunnel Instance	Source port of the LSP (with the ExtId forming the source parameters).
Tunnel Name	Name of the tunnel and LSP.
InLabel	Incoming interface and label info for the LSP in the upstream direction. At the egress node, using penultimate hop popping at the egress node, (implicit-null) appears as *No Label*.
Incoming Address	Address of the ingress interface.
Explicit Route	Explicit route specified in the explicit-route object of the Path message.
Record Route	Record route object in either the path or reservation message.
Tspec	Traffic parameters.
OutLabel	Outgoing interface and label sent downstream.
FRR OutLabel	For FRR[43], displays the backup tunnel and Merge-point label.
Fspec	Flow spec parameters for specified QoS.

[42] Link-state packet.
[43] Fast reroute.

signalling dscp (RSVP)

To give all RSVP signaling packets sent out on a specific interface higher priority in the network by marking them with a particular Differentiated Service Code Point (DSCP), use the **signalling dscp** command in RSVP interface configuration submode. To return to the default behavior, use the **no** form of this command.

signalling dscp *dscp*

no signalling *dscp*

Syntax Description

dscp	DSCP priority number. Range is 0 to 63.

Command Default   No default behavior or values

Command Modes   RSVP interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

DSCP marking improves signaling setup and teardown times.

Ordinarily, when a router receives Path messages for a particular state marked with a DSCP value, it sends out Path messages for that state marked with the same DSCP value. This command overrides that DSCP persistence and ensures that all messages sent out a particular interface are marked with a specified DSCP.

Though this command controls RSVP signaling packets, it has no effect on ordinary IP or MPLS data packets traveling along the path created or reserved by this RSVP session.

DSCP persistence operates on a per-state basis, but this command operates on a per-interface basis. So, if some incoming message (for example, multicast Path) with DSCP 10 causes two outgoing messages on interfaces A and B, ordinarily both are sent with DSCP 10. If **signalling dscp 5** is configured for RSVP on interface A, the Path messages being sent out interface A is marked with DSCP 5, but the Path messages being sent out interface B are marked with DSCP 10.

There is a difference between the **signalling dscp 0** and **no signalling dscp** commands. The first command instructs RSVP to explicitly set to 0 the DSCP on all packets sent out this interface. The second command removes any override on the packets being sent out this interface, and allows the DSCP of received packets that created this state to persist on packets forwarded out this interface.

The RFC specifies a standard mapping from the eight IP precedence values to eight values in the 64-value DSCP space. You can use those special DSCP values to specify IP precedence bits only.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to mark all RSVP packets going out on POS interface 0/1/0/1 as DSCP 20:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/1/0/1
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling dscp 20
```

The following example shows how to disable DSCP marking of signaling packets going out POS interface 0/1/0/1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/1/0/1
RP/0/RP0/CPU0:router(config-rsvp-if)# interface pos 0/1/0/1
RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling dscp
```

signalling graceful-restart

To enable or disable RSVP signaling graceful restart, use the **signalling graceful-restart** command in RSVP configuration mode. To return to the default behavior, use the **no** form of this command.

signalling graceful-restart [**recovery-time** *time*| **restart-time** *time*]

no signalling graceful-restart

Syntax Description

recovery-time	(Optional) Configures the recovery time that is advertised in the Restart Cap object in the Hello messages.
time	Time, in seconds, for the neighbor to wait for the node to recover (replay) existing states after the Hello session is reestablished before initiating TEARs. Range is 0 to 3600.
restart-time	(Optional) Configures the restart time that is advertised in the Restart Cap object in hello messages.
time	Time, in seconds, after a control-plane restart that RSVP can start exchanging hello messages. Range is 60 to 3600. Default is 120.

Command Default

RSVP signaling graceful restart is disabled.

Command Modes

RSVP configuration

Command History

Release	Modification
Release 3.9.0	The **recovery-time** keyword was added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **signalling graceful-restart** command provides a mechanism that helps minimize the negative effects on MPLS traffic for the following types of faults. This is an implementation of the fault handling section of the IETF standard RFC 3473:

Control-channel-failure

Disruption of communication channels between 2 nodes when the communication channels are separated from the data channels.

Node-failure

Control plane of a node fails, but the node preserves its data forwarding states.

The **signalling graceful-restart** command instigates the exchange of RSVP hello messages between the router and its neighbor nodes. After the hello messages are established with a given neighbor, RSVP can detect these types of faults when they occur.

If no hello messages are received from a neighbor within a certain number of hello intervals, a node assumes that communication with the neighbor has been lost. The node waits the amount of time advertised by the last restart time communicated by the neighbor, before invoking procedures for recovery from communication loss.

The configured restart time is important in case of recovery from failure. The configured value should accurately reflect the amount of time within which, after a control-plane restart, RSVP can start exchanging hello messages.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to enable RSVP signalling graceful restart:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp
RP/0/RP0/CPU0:router(config-rsvp)# signalling graceful-restart
```

The following example shows how to set the restart time:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp
RP/0/RP0/CPU0:router(config-rsvp)# signalling graceful-restart restart-time 200
```

The following example shows how to reset the restart time to the default of 120 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp
RP/0/RP0/CPU0:router(config-rsvp)# no signalling graceful-restart restart-time
```

signalling hello graceful-restart refresh interval

To configure the interval at which RSVP graceful-restart hello messages are sent to each neighbor, use the **signalling hello graceful-restart refresh interval** command in RSVP configuration mode. To return to the default behavior, use the **no** form of this command.

signalling hello graceful-restart refresh interval *refresh-interval*

no signalling hello graceful-restart refresh interval

Syntax Description

refresh-interval	Interval, in milliseconds, at which RSVP graceful-restart hello messages are sent to each neighbor. Range is 3000 to 30000.

Command Default

refresh interval: 5000

Command Modes

RSVP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **signalling hello graceful-restart refresh interval** command determines how often hello messages are sent to each neighbor. If the interval is made short, the hello messages are sent more frequently. Although a short interval may help detect failures quickly, it also results in increased network traffic. Optimizations in the RSVP hello mechanism exist to reduce the number of hello messages traveling over the network.

When an RSVP hello message is received, the receiving node acknowledges the hello and restarts its hello timer to the neighbor. By doing this, a hello is transmitted to the neighbor only if a hello is not received before the hello refresh interval has expired.

If two neighboring nodes do not have the same hello interval, the node with the larger hello interval has to acknowledge its neighbor's (more frequent) hellos. For instance, if node A has a hello interval of 5 seconds, and node B has a hello interval of 10 seconds, node B still has to send hello messages every 5 seconds.

The hello backoff mechanism is an optimization that is tailored to minimize the number of hello messages from a neighbor that either does not have graceful restart enabled, or that fails to come back up during the restart interval. The restart interval is provided by the neighbor in the restart cap object.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example sets the hello graceful-restart refresh interval to 4000 msecs:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp
RP/0/RP0/CPU0:router(config-rsvp)# signalling hello graceful-restart refresh interval 4000
```

Related Commands

Command	Description
signalling hello graceful-restart refresh misses, on page 514	Configures the number of consecutive missed RSVP hello messages before a neighbor is declared down or unreachable.

signalling hello graceful-restart refresh misses

To configure the number of consecutive missed RSVP hello messages before a neighbor is declared down or unreachable, use the **signalling hello graceful-restart refresh misses** command in RSVP configuration mode. To return to the default behavior, use the **no** form of this command.

signalling hello graceful-restart refresh misses *refresh-misses*

no signalling hello graceful-restart refresh misses

Syntax Description

refresh-misses	Number of misses for hello messages before a neighbor is declared down or unreachable. Range is 1 to 10. Default is 3.

Command Default

refresh-misses: 3

Command Modes

RSVP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If no hello messages (request or ACK) are received from a neighbor within the configured number of refresh misses, the node assumes that communication with the neighbor has been lost.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to set hello graceful-restart refresh misses to 4:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp
RP/0/RP0/CPU0:router(config-rsvp)# signalling hello graceful-restart refresh misses 4
```

Related Commands

Command	Description
signalling hello graceful-restart refresh interval, on page 512	Configures the interval at which RSVP graceful restart hello messages are sent per neighbor.

signalling prefix-filtering access-list

To specify the extended access control list to use for prefix filtering of RSVP Router Alert messages, use the **signalling prefix-filtering access-list** command in RSVP configuration mode. To return to the default behavior, use the **no** form of this command.

signalling prefix-filtering access-list *access list name*

no signalling prefix-filtering access-list *access list name*

Syntax Description

access list name	Extended access-list name as a string (maximum 32 characters).

Command Default   No default behavior or values

Command Modes   RSVP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note   The extended access control list containing the source and destination prefixes used for packet filtering is configured separately.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to configure the access control list name banks for prefix-filtering of RSVP Router Alert messages:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp
```

```
RP/0/RP0/CPU0:router(config-rsvp)# signalling prefix-filtering access-list banks
```

The following example shows how to disable RSVP prefix-filtering of RSVP Router Alert messages:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp
RP/0/RP0/CPU0:router(config-rsvp)# no signalling prefix-filtering access-list banks
```

Related Commands

Command	Description
signalling prefix-filtering default-deny-action, on page 518	Configures RSVP to drop messages when an access control list match yields an implicit deny.

signalling prefix-filtering default-deny-action

To configure RSVP to drop RSVP Router Alert messages when an access control list match returns an implicit deny, use the **signalling prefix-filtering default-deny-action** command in RSVP configuration mode. To return to the default behavior, use the **no** form of this command.

signalling prefix-filtering default-deny-action drop

no signalling prefix-filtering default-deny-action drop

Syntax Description

drop	Specifies when RSVP router alert messages are dropped.

Command Default

Performs normal RSVP processing of Path, Path Tear, and ResvConfirm message packets.

Command Modes

RSVP configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to configure RSVP Router Alert messages when an access control list match returns an implicit deny:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp
RP/0/RP0/CPU0:router(config-rsvp)# signalling prefix-filtering default-deny-action drop
```

Related Commands

Command	Description
signalling prefix-filtering access-list, on page 516	Configures extended access control lists for prefix-filtering of an RSVP Router Alert messages.

signalling rate-limit

To limit the rate of RSVP signaling messages being sent out a particular interface, use the **signalling rate-limit** command in RSVP interface configuration mode. To return to the default behavior, use the **no** form of this command.

signalling rate-limit[**rate** *messages*] [**interval** *interval-length*]

no signalling rate-limit [**rate** *messages*] [**interval** *interval-length*]

Syntax Description

rate *messages*	(Optional) Configures the number of messages sent per scheduling interval. Range is 1 to 500 messages.
interval *interval-length*	(Optional) Specifies the length, in milliseconds, between scheduling intervals. Range is 250 to 2000.

Command Default

messages: 100

interval-length: 1,000 (1 second)

Command Modes

RSVP interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the rate-limiting feature with caution. Limiting the rate of RSVP signaling has the advantage of avoiding an overload of the next hop router's input queue, because such overloads would cause the next hop router to drop RSVP messages. However, reliable messaging and rapid retransmit usually enable the router to recover very rapidly from message drops; so rate limiting might not be necessary.

If the rate is set too low, it causes slower convergence times. This command limits all RSVP messages except acknowledgments (ACK) and SRefresh messages. The command does not let you make a router generate messages faster than its inherent limit. (That limit differs among router models.)

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to enable rate-limiting:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface POS0/3/0/0
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling rate-limit
```

The following example shows how to limit the rate to 50 messages per second:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/3/0/0
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling rate-limit rate 50
```

The following example shows how to set a limit at 40 messages for every 250 milliseconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/3/0/0
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling rate-limit rate 40 interval 250
```

The following example shows how to restore the rate to the default of 100 messages per second:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/3/0/0
RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling rate-limit rate
```

The following example shows how to disable rate-limiting:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/3/0/0
RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling rate-limit
```

Related Commands

Command	Description
signalling refresh reduction bundle-max-size, on page 526	Specifies the maximum bundle size of maximum size of single RSVP bundle message.

signalling refresh interval

To change the frequency with which a router updates the network about the RSVP state of a particular interface, use the **signalling refresh interval** command in RSVP interface configuration mode. To return to the default behavior, use the **no** form of this command.

signalling refresh interval *seconds*

no signalling refresh interval

Syntax Description

seconds	Number of seconds the router waits to update the network about the RSVP state of an interface, in seconds. Range is 10 to 180. Default is 45.

Command Default

seconds: 45

Command Modes

RSVP interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

RSVP relies on a soft-state mechanism to maintain state consistency in the face of network losses. That mechanism is based on continuous refresh messages to keep a state current. Each RSVP router is responsible for sending periodic refresh messages to its neighbors.

The router attempts to randomize network traffic and reduce metronomic burstiness by jittering the actual interval between refreshes by as much as 50 percent. As a result, refreshes may not be sent at exactly the interval specified. However, the average rate of refreshes are within the specified refresh interval.

Lengthening the interval reduces the refresh load of RSVP on the network but causes downstream nodes to hold state longer. This reduces the responsiveness of the network to failure scenarios. Shortening the interval improves network responsiveness but expands the messaging load on the network.

The reliable messaging extension, implemented through the **signalling refresh reduction reliable** command, may cause new or changed messages to be temporarily refreshed at a more rapid rate than specified to improve network responsiveness.

The use of reliable messaging with rapid retransmit substantially improves network responsiveness in case of transient message loss; if the refresh interval is changed when using the reliable messaging feature, it is more useful to lengthen the interval than to shorten it.

The summary refresh extension, implemented through the **signalling refresh reduction summary** command, provides a lower-cost mechanism to refresh RSVP state. The router uses the same refresh interval between successive refreshes of a single state when using summary refresh and when using ordinary message-based refresh.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to specify a refresh interval of 30 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface tunnel-te 2
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling refresh interval 30
```

The following example shows how to restore the refresh interval to the default value of 45 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface tunnel-te 2
RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling refresh interval
```

Related Commands

Command	Description
signalling refresh missed, on page 524	Specifies the number of successive missed refresh messages before RSVP deems the state expired and tears it down.
signalling refresh reduction reliable, on page 529	Customizes acknowledgment message size and hold interval, and the RSVP message retransmit interval.
signalling refresh reduction summary, on page 532	Enables and configures the maximum size of the SRefresh message.

signalling refresh missed

To specify the number of successive refresh messages that can be missed before the RSVP deems a state to be expired (resulting in the state to be torn down), use the **signalling refresh missed** command in RSVP interface configuration mode. To return to the default behavior, use the **no** form of this command.

signalling refresh missed *number*

no signalling refresh missed

Syntax Description

number	Number of successive missed refresh messages. Range is 1 to 8. Default is 4.

Command Default   *number*: 4

Command Modes   RSVP interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Decreasing the missed-message number improves RSVP responsiveness to major failures like router failure or link faults, but decreases the resilience of RSVP resulting in packet drops or temporary network congestion. The latter condition makes RSVP too sensitive.

Increasing the missed-message number increases the resilience of RSVP to such transient packet loss, but decreases the RSVP responsiveness to more intransient network failures such as router failure or link fault.

The default value of 4 provides a balance of resilience and responsiveness factors.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to specify a missed refresh limit of six (6) messages:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface tunnel-te 2
```

```
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling refresh missed 6
```

The following example shows how to return the missed refresh limit to the default value of four (4):

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface tunnel-te 2
RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling refresh missed
```

Related Commands

Command	Description
signalling refresh interval, on page 522	Changes the frequency with which a router updates the network about the RSVP state of an interface.
signalling refresh reduction reliable, on page 529	Customizes acknowledgment message size and hold interval, and the RSVP message retransmit interval.
signalling refresh reduction summary, on page 532	Enables and configures the maximum size of the SRefresh message.

signalling refresh reduction bundle-max-size

To configure the maximum size of a single RSVP bundle message, use the **signalling refresh reduction bundle-max-size** command in RSVP interface configuration mode.

signalling refresh reduction bundle-max-size *size*

Syntax Description

size	Maximum size, in bytes, of a single RSVP bundle message. Range is 512 to 65000.

Command Default

size: 4096

Command Modes

RSVP interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to set the maximum bundle size of a single RSVP bundle message to 4000:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface tunnel-te 2
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling refresh reduction bundle-max-size 4000
```

Related Commands

Command	Description
show rsvp interface, on page 494	Displays information about all interfaces with RSVP enabled.

signalling refresh reduction disable

To disable RSVP refresh reduction on an interface, use the **signalling refresh reduction disable** command in RSVP interface configuration mode. To return to the default behavior, use the **no** form of this command.

signalling refresh reduction disable

no signalling refresh reduction disable

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values

Command Modes   RSVP interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The following features of the IETF refresh reduction standard RFC 2961 are enabled with this command:

- Setting the refresh-reduction-capable bit in message headers

- Message-ID usage

- Reliable messaging with rapid retransmit, acknowledgment (ACK), and NACK messages

- Summary refresh extension

Because refresh reduction relies on cooperation of the neighbor, the neighbor must also support the standard. If the router detects that a neighbor is not supporting the refresh reduction standard (either through observing the refresh-reduction-enabled bit in messages received from the next hop, or by sending a Message-ID object to the next hop and receiving an error), refresh reduction is not used on this link. That information is obtained through use of the **show rsvp interface detail** command.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to disable RSVP refresh reduction on an interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface tunnel-te 2
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling refresh reduction disable
```

The following example shows how to enable RSVP refresh reduction on the interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface tunnel-te 2
RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling refresh reduction disable
```

Related Commands

Command	Description
show rsvp interface, on page 494	Displays information about all interfaces with RSVP enabled.
signalling refresh interval, on page 522	Changes the frequency with which a router updates the network about the RSVP state of an interface.
signalling refresh reduction reliable, on page 529	Customizes acknowledgment message size and hold interval, and the RSVP message retransmit interval.
signalling refresh reduction summary, on page 532	Enables and configures the maximum size of the signalling refresh message.

signalling refresh reduction reliable

To configure the parameters of reliable messaging, use the **signalling refresh reduction reliable** command in RSVP interface configuration mode. To return to the default behavior, use the **no** form of this command.

signalling refresh reduction reliable {**ack-max-size** *bytes*| **ack-hold-time***milliseconds*| **retransmit-time** *milliseconds*| **summary-refresh**}

no signalling refresh reduction reliable {**ack-max-size***bytes*| **ack-hold-time***milliseconds*| **retransmit-time** *milliseconds*| **summary-refresh**}

Syntax Description

ack-max-size	Specifies the maximum size of the RSVP component within a single acknowledgment message.
bytes	Number of bytes that define the maximum size of an RSVP component. Range is 20 to 65000.
ack-hold-time	Specifies the maximum amount of time a router holds an acknowledgment before sending it, in an attempt to bundle several acknowledgments into a single acknowledgment message.
milliseconds	Number of milliseconds that define the acknowledgment hold time. Range is 100 to 5000.
retransmit-time	Specifies the amount of time the router initially waits for an acknowledgment message before resending the RSVP message.
milliseconds	Number of milliseconds that define the retransmit time. Range is 100 to 10000.
summary-refresh	Enables the use of reliable transmission for RSVP summary refresh messages.

Command Default

ack-max-size *bytes*: 4096

ack-hold-time *milliseconds*: 400 (0.4 seconds)

retransmit-time *milliseconds*: 900 (0.9 seconds)

Command Modes   RSVP interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

For reliable messaging to work properly, configure the retransmit time on the send router (A) and acknowledgment hold time on the peer router (B). (Vice versa for messages in reverse direction.)

The retransmit time must be greater than the acknowledgment hold time, so that the acknowledgment message has time to get back to the sender before the message retransmits. We recommend that the retransmit-time interval be at least twice the acknowledgment hold-time interval. If the retransmit-time value is smaller than the acknowledgment hold-time value, then router A retransmits the message even though router B may have received the message and is waiting for an acknowledgment hold time to time out to send the acknowledgment. This causes unnecessary network traffic.

Reducing the value of **ack-max-size** causes more acknowledgment messages to be issued, with fewer acknowledgments contained within each acknowledgment message. However, reducing the acknowledgment-max-size does not speed up the rate at which acknowledgment messages are issued because their frequency is still controlled by the time values (acknowledgment hold time and retransmit time).

To use reliable messaging for summary refresh messages, use the**rsvp interface** *interface-name* and **signalling refresh reduction summary** commands.

Task ID

Task ID	Operations
mpls-te	read, write

Examples

The following example shows how to set the maximum acknowledgment message size to 4096 bytes on POS interface 0/4/0/1:

```
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/4/0/1
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling refresh reduction reliable ack-max-size
4096
```

The following example shows how to return the maximum acknowledgment message size to the default of 1000 bytes on POS interface 0/4/0/1:

```
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/4/0/1
RP/0/RP0/CPU0:router(config-rsvp-if)# no rsvp signalling refresh reduction reliable
```

The following example shows how to set the acknowledgment hold time to 1 second:

```
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/4/0/1
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling refresh reduction reliable ack-hold-time
1000
```

The following example shows how to return the acknowledgment hold time to the default of 0.4 second:

```
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/4/0/1
RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling refresh reduction reliable ack-hold-time
```

The following example shows how to set the retransmit timer to 2 seconds:

```
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/4/0/1
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling refresh reduction reliable retransmit-time
 2000
```

The following example shows how to return the retransmit timer to the default of 0.9 seconds:

```
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/4/0/1
RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling refresh reduction reliable
```

The following example shows how to enable the use of reliable transmission for RSVP summary refresh messages:

```
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling refresh reduction reliable summary-refresh
```

The following example shows how to disable the use of reliable transmission for RSVP summary refresh messages:

```
RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling refresh reduction reliable summary-refresh
```

Related Commands

Command	Description
signalling refresh reduction disable, on page 527	Disables RSVP refresh reduction on an interface.

signalling refresh reduction summary

To configure RSVP summary refresh message size on an interface, use the **signalling refresh reduction summary** command in RSVP interface configuration mode. To return to the default behavior, use the **no** form of this command.

signalling refresh reduction summarymax-size*bytes*

no signalling refresh reduction summary max-size*bytes*

Syntax Description

max-size *bytes*	Specifies the maximum size, in bytes, of a single RSVP summary refresh message. Range is 20 to 65000.

Command Default *bytes*: 4096

Command Modes RSVP interface configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **signalling refresh reduction summary** command to specify the maximum size of the summary refresh messages sent. Message size is verified using the **show rsvp interface detail** command.

Task ID

Task ID	Operations
mpls-te	read, write

Examples The following example shows how to change the summary message maximum size on an interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface tunnel-te 2
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling refresh reduction summary max-size 6000
```

The following example shows how to return the summary message maximum size to the default value on an interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface tunnel-te 2
RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling refresh reduction summary max-size 6000
```

Related Commands

Command	Description
show rsvp interface, on page 494	Displays information about all interfaces with RSVP enabled.
signalling refresh interval, on page 522	Changes the frequency with which a router updates the network about the RSVP state of an interface.

window-size (RSVP)

To specify the maximum number of RSVP authenticated messages that can be received out of sequence, use the **window-size** command in RSVP authentication configuration mode, RSVP interface authentication configuration mode, or RSVP neighbor authentication configuration mode. To disable the window size, use the **no** form of this command.

window-size N

no window-size

Syntax Description	N Size of the window to restrict out-of-sequence messages. Range is 1 to 64. Default is 1. All out-of-sequence messages are dropped.

Command Default N: 1

Command Modes RSVP authentication configuration

RSVP interface authentication configuration

RSVP neighbor authentication configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **window-size** command to specify the maximum number of authenticated messages that are received out of sequence. All RSVP authenticated messages include a sequence number that is used to prevent replays of RSVP messages.

With a default window size of one message, RSVP rejects any out-of-order or out-of-sequence authenticated messages because they are assumed to be replay attacks. However, sometimes bursts of RSVP messages become reordered between RSVP neighbors. If this occurs on a regular basis, and you can verify that the node sending the burst of messages is trusted, you can use the window-size option to adjust the burst size such that RSVP does not discard such reordered bursts. RSVP checks for duplicate messages within these bursts.

Task ID

Task ID	Operations
mpls-te	read, write

Examples   The following example shows how to configure the size of the window to 33 in RSVP neighbor authentication configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp neighbor 1.1.1.1 authentication
RP/0/RP0/CPU0:router(config-rsvp-nbor-auth)# window-size 33
```

The following example shows how to configure the size of the window to 33 in RSVP authentication configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp authentication
RP/0/RP0/CPU0:router(config-rsvp-auth)# window-size 33
```

The following example shows how to configure the size of the window to 33 in RSVP interface authentication configuration mode by using the **rsvp interface** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface POS 0/2/1/0
RP/0/RP0/CPU0:router(config-rsvp-if)# authentication
RP/0/RP0/CPU0:router(config-rsvp-if-auth)# window-size 33
```

Related Commands

Command	Description
key-source key-chain (RSVP), on page 452	Specifies the source of the key information to authenticate RSVP signaling messages.
life-time (RSVP), on page 454	Controls how long RSVP maintains idle security associations with other trusted RSVP neighbors.

MPLS OAM Commands

This module describes Multiprotocol Label Switching (MPLS) label switched path (LSP) verification commands. These commands provide a means to detect and diagnose data plane failures and are the first set of commands in the MPLS Operations, Administration, and Maintenance (OAM) solution.

For detailed information about MPLS concepts, configuration tasks, and examples, see .

clear mpls oam counters

To clear MPLS OAM counters, use the **clear mpls oam counters** command in EXEC mode.

clear mpls oam counters {**global**| **interface** [*type interface-path-id*]| **packet**}

Syntax Description

global	Clears global counters.
interface	Clears counters on a specified interface.
type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.
packet	Clears global packet counters.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	execute
mpls-ldp	execute
mpls-static	execute

Examples   The following example shows how to clear all global MPLS OAM counters:

RP/0/RP0/CPU0:router# **clear mpls oam counters global**

echo disable-vendor-extension

To disable sending the vendor extension type length and value (TLV) in the echo request, use the **echo disable-vendor extension** command in MPLS OAM configuration mode. To return to the default behavior, use the **no** form of this command.

echo disable-vendor-extension

no echo disable-vendor-extension

Syntax Description   This command has no arguments or keywords.

Command Default   The default value is 4.

Command Modes   MPLS OAM configuration mode

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write
mpls-ldp	read, write
mpls-static	read, write

Examples   The following example shows how to disable inclusion of the vendor extensions TLV in the echo requests:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls oam
RP/0/RP0/CPU0:router(config-oam)# echo disable-vendor-extension
```

echo revision

To set the echo packet revision, use the **echo revision** command in MPLS OAM configuration mode. To return to the default behavior, use the **no** form of this command.

echo revision {**1** | **2** | **3** | **4** }

no echo revision

Syntax Description	**1**	**2**	**3**	**4**	Draft revision number:
	• 1: draft-ietf-mpls-lsp-ping-03 (initial)
	• 2: draft-ietf-mpls-lsp-ping-03 (rev 1)
	• 3: draft-ietf-mpls-lsp-ping-03 (rev 2)
	• 4: draft-ietf-mpls-lsp-ping-09 (initial)

Command Default

The default echo revision is 4 (in draft 9).

Command Modes

MPLS OAM configuration mode

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read, write
mpls-ldp	read, write
mpls-static	read, write

Examples   The following example shows how to set the echo packet default revision:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls oam
RP/0/RP0/CPU0:router(config-oam)# echo revision 1
```

mpls oam

To enable MPLS OAM LSP verification, use the **mpls oam** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

mpls oam

no mpls oam

Syntax Description   This command has no arguments or keywords.

Command Default   By default, MPLS OAM functionality is disabled.

Command Modes   Global configuration

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **mpls oam** command and OAM functionality is described in the IETF LSP ping draft.

Task ID

Task ID	Operations
mpls-te	read, write
mpls-ldp	read, write
mpls-static	read, write

Examples   The following example shows how to enable MPLS OAM:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls oam
RP/0/RP0/CPU0:router(config-oam)#
```

ping mpls ipv4

To check MPLS host reachability and network connectivity by specifying the destination type as a Label Distribution Protocol (LDP) IPv4 address, use the **ping mpls ipv4** command in EXEC mode.

ping mpls ipv4 *address/mask* [**destination** *start-address end-address increment*] **[dsmap]** [**exp** *exp-bits*] **[force-explicit-null]** [**interval** *min-send-delay*] [**output interface** *type interface-path-id* [**nexthop** *nexthop-address*]][**pad** *pattern*][**repeat** *count*] [**reply** {**dscp** *dscp-value* | **reply mode**{**ipv4** | **no-reply** | **router-alert**}| **reply pad-tlv**}] [**revision** *version*] [**size** *packet-size*] [**source** *source-address*] [**sweep** *min value max value increment*] [**timeout** *timeout*] [**ttl** *value*] **[verbose]** [**fec-type** {**bgp** | **generic** | **ldp**}]

Syntax Description

address/mask	Address prefix of the target and number of bits in the target address network mask.
destination *start address end address address increment*	(Optional) Specifies a network 127/8 address to be used as the destination address in the echo request packet.
	start address
	Start of the network address.
	end address
	Start of the ending network address.
	address increment
	Incremental value of the network address, which is expressed as a decimal number value or IP address.
dsmap	(Optional) Indicates that a downstream mapping (DSMAP) type length and value should be included in the LSP echo request.
exp *exp-bits*	(Optional) Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.
force-explicit-null	(Optional) Forces an unsolicited explicit null label to be added to the MPLS label stack and allows LSP ping to be used to detect LSP breakages at the penultimate hop.
interval *min-send-delay*	(Optional) Specifies a send interval, in milliseconds, between requests. Range is 0 to 3600000. Default is 0.

output interface	(Optional) Specifies the output interface where echo request packets are sent.
type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information, use the question mark (**?**) online help function.
nexthop	(Optional) Specifies the nextop as an IP address.
nexthop-iaddress	(Optional) IP address for the next hop.
pad *pattern*	(Optional) Specifies the pad pattern for an echo request.
repeat *count*	(Optional) Specifies the number of times to resend a packet. Range is 1 to 2147483647. Default is 5.
reply dscp *dscp-value*	Specifies the differentiated service codepoint value for an MPLS echo reply.
reply mode [**ipv4** | **router-alert** | **no-reply**]	Specifies the reply mode for the echo request packet. **no-reply** 　Do not reply **ipv4** 　Reply with an IPv4 UDP packet (this is the default) **router-alert** 　Reply with an IPv4 UDP packet with the IP router alert set
reply pad-tlv	Indicates that a pad TLV should be included.

revision *version*	(Optional) Specifies the Cisco extension TLV versioning field: • 1 draft-ietf-mpls-lsp-ping-03 (initial) • 2 draft-ietf-mpls-lsp-ping-03 (rev 1) • 3 draft-ietf-mpls-lsp-ping-03 (rev 2) • 4 draft-ietf-mpls-lsp-ping-09 (initial)
size *packet size*	(Optional) Specifies the packet size or number of bytes in each MPLS echo request packet. Range is 100 to 17986. Default is 100.
source *source-address*	(Optional) Specifies the source address used in the echo request packet.
sweep *min value max value interval*	(Optional) Specifies a range of sizes for the echo packets sent. *min value* Minimum or start size for an echo packet (range is 100 to 17986) *max value* Maximum or end size for an echo packet(range is 100 to 17986) *interval* Number used to increment an echo packet size(range is 1 to 8993)
timeout *timeout*	(Optional) Specifies the timeout interval, in seconds. Range is 0 to 3600. Default is 2.
ttl *value*	(Optional) Specifies the TTL value to be used in the MPLS labels (range is 1 to 255).
verbose	(Optional) Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.

Command Default

exp *exp bits*: 0

interval *min-send-delay*: 0

repeat *count* : 5

reply-mode: IPv4

timeout *timeout* : 2

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **output interface** keyword specifies the output interface on which the MPLS echo request packets are sent. If the specified output interface is not part of the LSP, the packets are not transmitted.

In cases where the sweep keyword is used, values larger than the outgoing interface's MTU are not transmitted.

The **ping** command sends an echo request packet to an address, and then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

> **Note**   The **ping mpls** command is not supported on optical LSPs. If an optical LSP is encountered along the LSP's path, it is treated as a physical interface.

For detailed configuration information about the MPLS **ping** command, see *System Monitoring Configuration Guide* .

Task ID

Task ID	Operations
mpls-te	read, write
mpls-ldp	read, write

Examples   The following example shows the destination type as a label distribution protocol (LDP) prefix and specifies a range of sizes for the echo packets sent:

```
RP/0/RP0/CPU0:router# ping mpls ipv4 140.140.140/32 verbose sweep 100 200 15 repeat 1

  Sending 1, [100..200]-byte MPLS Echos to 140.140.140.140/32,
       timeout is 2 seconds, send interval is 0 msec:

  Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'I' - unknown upstream index,
    'X' - unknown return code, 'x' - return code 0
```

```
Type escape sequence to abort.
!    size 100, reply addr 196.100.1.26, return code 3
!    size 115, reply addr 196.100.1.26, return code 3
!    size 130, reply addr 196.100.1.26, return code 3
!    size 145, reply addr 196.100.1.26, return code 3
!    size 160, reply addr 196.100.1.26, return code 3
!    size 175, reply addr 196.100.1.26, return code 3
!    size 190, reply addr 196.100.1.26, return code 3

Success rate is 100 percent (7/7), round-trip min/avg/max = 5/6/8 ms
```

The following example shows the destination type as a label distribution protocol (LDP) prefix and specifies FEC type as generic and verbose option:

```
RP/0/RP0/CPU0:router# ping mpls ipv4 11.11.11.11/32 fec-type generic output interface
gigabitEthernet 0/0/0/3
nexthop 172.40.103.2 verbose

Sending 5, 100-byte MPLS Echos to 11.11.11.11/32,
      timeout is 2 seconds, send interval is 0 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

!    size 100, reply addr 11.101.11.11, return code 3
!    size 100, reply addr 11.101.11.11, return code 3
!    size 100, reply addr 11.101.11.11, return code 3
!    size 100, reply addr 11.101.11.11, return code 3
!    size 100, reply addr 11.101.11.11, return code 3

Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/6 ms
```

ping mpls traffic-eng

To specify the destination type as an MPLS-TE tunnel and tunnel interface, use the **ping mpls traffic-eng** command in EXEC mode.

ping mpls traffic-eng tunnel *tunnel-ID* [**dsmap**] [**exp** *exp-bits*] [**force-explicit-null**] [**interval** *min-send-delay*] [**pad** *pattern*] [**repeat** *count*] [**reply** {**dscp** *dscp-value* | **reply mode** {**ipv4** | **no-reply** | **router-alert**}| **reply pad-tlv**}] [**revision** *version*] [**size** *packet-size*] [**source** *source-address*] [**sweep** *min-value max-value increment*] [**timeout** *timeout*] [**ttl** *value*] [**verbose**]

Syntax Description

tunnel *tunnel-ID*	Specifies the destination type as an MPLS traffic engineering (TE) tunnel and the tunnel interface number. The range for the tunnel interface number is from 0 to 65535.
dsmap	(Optional) Indicates that a downstream mapping (DSMAP) type length and value should be included in the LSP echo request.
exp *exp-bits*	(Optional) Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.
force-explicit-null	(Optional) Forces an unsolicited explicit null label to be added to the MPLS label stack and allows LSP ping to be used to detect LSP breakages at the penultimate hop.
interval *min-send-delay*	(Optional) Specifies a send interval, in milliseconds, between requests. Range is 0 to 3600000. Default is 0.
pad *pattern*	(Optional) Specifies the pad pattern for an echo request.
repeat *count*	(Optional) Specifies the number of times to resend a packet. Range is 1 to 2147483647. Default is 5.
reply dscp *dscp-value*	(Optional) Specifies the differentiated service codepoint value for an MPLS echo reply.

reply mode [**ipv4** | **router-alert** | **no-reply**]	(Optional) Specifies the reply mode for the echo request packet.
	
	no-reply
	
	    Do not reply
	
	ipv4
	
	    Reply with an IPv4 UDP packet (this is the default)
	
	router-alert
	
	    Reply with an IPv4 UDP packet with the IP router alert set

reply pad-tlv	(Optional) Indicates that a pad TLV should be included.

revision *version*	(Optional) Specifies the Cisco extension TLV versioning field: • 1 draft-ietf-mpls-lsp-ping-03 (initial) • 2 draft-ietf-mpls-lsp-ping-03 (rev 1) • 3 draft-ietf-mpls-lsp-ping-03 (rev 2) • 4 draft-ietf-mpls-lsp-ping-09 (initial)
size *packet-size*	(Optional) Specifies the packet size or number of bytes in each MPLS echo request packet. Range is 100 to 17986. Default is 100.
source *source-address*	(Optional) Specifies the source address used in the echo request packet.

sweep *min-value max-value interval*	(Optional) Specifies a range of sizes for the echo packets sent.
	
	min-value
	
	    Minimum or start size for an echo packet (range is 100 to 17986)
	
	max-value
	
	    Maximum or end size for an echo packet(range is 100 to 17986)
	
	interval
	
	    Number used to increment an echo packet size(range is 1 to 8993)

timeout *timeout*	(Optional) Specifies the timeout interval, in seconds. Range is 0 to 3600. Default is 2.
ttl *value*	(Optional) Specifies the TTL value to be used in the MPLS labels (range is 1 to 255).
verbose	(Optional) Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.

Command Default

exp *exp-bits*: 0

interval *min-send-delay*: 0

repeat *count*: 5

reply-mode: IPv4

timeout *timeout* : 2

Command Modes

EXEC

Command History

Release	Modification
Release 4.0.0	This command was introduced. This command was replaced by the **ping mpls traffic-eng tunnel-te (P2P)** command.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **output interface** keyword specifies the output interface on which the MPLS echo request packets are sent. If the specified output interface is not part of the LSP, the packets are not transmitted.

In cases where the **sweep** keyword is used, values larger than the outgoing interface's MTU are not transmitted.

The **ping** command sends an echo request packet to an address, and then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

Note The **ping mpls traffic-eng** command is not supported on optical LSPs. If an optical LSP is encountered along the LSP's path, it is treated as a physical interface.

Task ID

Task ID	Operations
mpls-te	read, write
mpls-ldp	read, write

Examples

The following example shows how to check connectivity by using the **ping mpls traffic-eng** command when a TE tunnel 10 is present. Return code, reply address, and packet size are displayed due to the **verbose** keyword.

```
RP/0/RP0/CPU0:router# ping mpls traffic-eng tunnel 10 repeat 1 verbose

  Sending 1, 100-byte MPLS Echos to tunnel-te10,
        timeout is 2 seconds, send interval is 0 msec:

  Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'X' - unknown return code, 'x' - return code 0

  Type escape sequence to abort.
  !    size 100, reply addr 196.100.1.18, return code 3

  Success rate is 100 percent (1/1), round-trip min/avg/max = 15/15/15 ms
```

Command	Description
show mpls traffic-eng tunnels	Displays information about MPLS-TE tunnels.
ping mpls traffic-eng tunnel-te (P2P)	Verifies the connectivity of the LSP path for the MPLS-TE tunnel.

ping pseudowire (AToM)

To verify connectivity between provider edge (PE) LSRs in an Any Transport over MPLS (AToM) setup, use the **ping pseudowire** command in EXEC mode.

ping [mpls] pseudowire *remote-PE -address pw-id* [**exp** *exp-bits*] [**interval** *min-send-delay*] [**pad** *pattern*] [**repeat** *count*] [**reply** {**dscp** *dscp-value* | **reply mode** {**ipv4** | **no-reply** | **router-alert** | **control-channel**}| **reply pad-tlv**}] [**size** *packet-size*] [**source** *source-address*] [**sweep** *min-value max-value increment*] [**timeout** *timeout*] [**ttl** *value*] **[verbose]**

Syntax Description

mpls	(Optional) Verifies the Labeled Switch Path (LSP).
remote-PE address	IP address of the remote PE LSR.
pw-id	Pseudowire ID that identifies the pseudowire in which MPLS connectivity is being verified. The pseudowire is used to send the echo request packets. The range is from 1 to 4294967295.
exp *exp-bits*	(Optional) Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.
interval *min-send-delay*	(Optional) Specifies a send interval, in milliseconds, between requests. Range is 0 to 3600000. Default is 0.
pad *pattern*	(Optional) Specifies the pad pattern for an echo request.
repeat *count*	(Optional) Specifies the number of times to resend a packet. Range is 1 to 2147483647. Default is 5.
reply dscp *dscp-value*	(Optional) Specifies the differentiated service codepoint value for an MPLS echo reply.

reply mode {**ipv4** | **router-alert** | **no-reply** | **control-channel**}	(Optional) Specifies the reply mode for the echo request packet.
	no-reply
	Do not reply
	ipv4
	Reply with an IPv4 UDP packet (the default)
	router-alert
	Reply with an IPv4 UDP packet with the IP router alert set
	control-channel
	Force the use of a VCCV control channel.
	Reply using an application for a defined control channel. This applies only to pseudowires in which VCCV is used in the reply path. This is the default choice for pseudowire ping.
reply pad-tlv	(Optional) Indicates that a reply pad TLV should be included.
size *packet-size*	(Optional) Specifies the packet size or number of bytes in each MPLS echo request packet. Range is 100 to 17986. Default is 100.
source *source-address*	(Optional) Specifies the source address used in the echo request packet.
sweep *min-value max-value interval*	Specifies a range of sizes for the echo packets sent.
	min-value
	Minimum or start size for an echo packet (range is 100 to 17986)
	max-value
	Maximum or end size for an echo packet(range is 100 to 17986)
	interval
	Number used to increment an echo packet size(range is 1 to 8993)
timeout *timeout*	(Optional) Specifies the timeout interval in seconds. Range is 0 to 3600. Default is 2 seconds.
ttl *value*	(Optional) Specifies the TTL value to be used in the MPLS labels (range is 1 to 255).

verbose	(Optional) Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.

Command Default

exp *exp bits*: 0

interval *min-send-delay*: 0

repeat *count*: 5

reply-mode: IPv4

timeout *timeout* : 2

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	The following keywords and arguments were added: • **force-control-channel**, **control-word**, **ra-label** and **ttl-expiry** keywords were added.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

In cases in which the **sweep** keyword is used, values larger than the outgoing interface's MTU are not transmitted.

The **ping** command sends an echo request packet to an address, and then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

Note

The **ping mpls** command is not supported on optical LSPs. If an optical LSP is encountered along the LSP's path, it is treated as a physical interface.

AToM VCCV allows the sending of control packets inband of an AToM pseudowire (PW) from the originating provider edge (PE) router. The transmission is intercepted at the destination PE router, instead of being forwarded to the customer edge (CE) router. This lets you use MPLS LSP ping to test the pseudowire section of AToM virtual circuits (VCs).

The no interactive version of the **ping pseudowire (AToM)** command is supported.

The control word setting is either enabled along the entire path between the Terminating-Provider Edge (T-PE) or it is completely disabled. If the control word configuration is enabled on one segment and disabled on another segment, the multisegment pseudowire does not come up.

Task ID

Task ID	Operations
mpls-te	read, write
mpls-ldp	read, write

Examples

The following example shows how the **ping mpls pseudowire** command is used to verify PE to PE connectivity in which the remote PE address is 150.150.150.150. Only one echo request packet is sent and the remote PE is to answer using IPv4 instead of the control channel.

```
RP/0/RP0/CPU0:router# ping mpls pseudowire 150.150.150.150 21 repeat 1 reply mode ipv4

  Sending 1, 100-byte MPLS Echos to 150.150.150.150 VC: 21,
        timeout is 2 seconds, send interval is 0 msec:

  Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
    'L' - labeled output interface, 'B' - unlabeled output interface,
    'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
    'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
    'P' - no rx intf label prot, 'p' - premature termination of LSP,
    'R' - transit router, 'I' - unknown upstream index,
    'X' - unknown return code, 'x' - return code 0

  Type escape sequence to abort.
  !
  Success rate is 100 percent (1/1), round-trip min/avg/max = 23/23/23 ms
```

ping mpls traffic-eng tunnel-te (P2P)

To specify the destination type as an MPLS-TE tunnel and tunnel interface, use the **ping mpls traffic-eng tunnel-te** command in EXEC mode.

ping mpls traffic-eng tunnel-te *tunnel-ID* {**destination** *start-address end-address increment*}[**dsmap**] [**exp** *exp-bits*] [**force-explicit-null**] [**interval** *min-send-delay*] [**pad** *pattern*] [**repeat** *count*] [**reply** {**dscp** *dscp-value* | **mode** {**ipv4** | **no-reply** | **router-alert**}| **pad-tlv**}] [**revision** *version*] [**size** *packet-size*] [**source** *source-address*] [**sweep** *min-value max-value increment*] [**timeout** *timeout*] [**ttl** *value*] [**verbose**]

Syntax Description

tunnel-te *tunnel-ID*	Specifies the destination type as an MPLS traffic engineering (TE) tunnel and the tunnel interface number. The range for the tunnel interface number is 0 to 65535.
destination *start-address end-address increment*	Specifies a network 127/8 address to be used as the destination address in the echo request packet.
	start address
	Start of the network address.
	end address
	Start of the ending network address.
	address increment
	Incremental value of the network address, which is expressed as a decimal number value or IP address.
dsmap	(Optional) Indicates that a downstream mapping (DSMAP) type length and value should be included in the LSP echo request.
exp *exp-bits*	(Optional) Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.
force-explicit-null	(Optional) Forces an unsolicited explicit null label to be added to the MPLS label stack and allows LSP ping to be used to detect LSP breakages at the penultimate hop.
interval *min-send-delay*	(Optional) Specifies a send interval, in milliseconds, between requests. Range is 0 to 3600000. Default is 0.
pad *pattern*	(Optional) Specifies the pad pattern for an echo request.
repeat *count*	(Optional) Specifies the number of times to resend a packet. Range is 1 to 2147483647. Default is 5.

reply dscp *dscp-value*	(Optional) Specifies the differentiated service codepoint value for an MPLS echo reply.

mode [**ipv4** | **router-alert** | **no-reply**]	(Optional) Specifies the reply mode for the echo request packet.
	
	no-reply
	
	    Do not reply
	
	ipv4
	
	    Reply with an IPv4 UDP packet (this is the default)
	
	router-alert
	
	    Reply with an IPv4 UDP packet with the IP router alert set

reply pad-tlv	(Optional) Indicates that a pad TLV should be included.
revision *version*	(Optional) Specifies the Cisco extension TLV versioning field: • 1 draft-ietf-mpls-lsp-ping-03 (initial) • 2 draft-ietf-mpls-lsp-ping-03 (rev 1) • 3 draft-ietf-mpls-lsp-ping-03 (rev 2) • 4 draft-ietf-mpls-lsp-ping-09 (initial)
size *packet-size*	(Optional) Specifies the packet size or number of bytes in each MPLS echo request packet. Range is 100 to 17986. Default is 100.
source *source-address*	(Optional) Specifies the source address used in the echo request packet.

sweep *min-value max-value interval*	(Optional) Specifies a range of sizes for the echo packets sent.
	min-value
	Minimum or start size for an echo packet (range is 100 to 17986)
	max-value
	Maximum or end size for an echo packet(range is 100 to 17986)
	interval
	Number used to increment an echo packet size(range is 1 to 8993)
timeout *timeout*	(Optional) Specifies the timeout interval, in seconds. Range is 0 to 3600. Default is 2.
ttl *value*	(Optional) Specifies the TTL value to be used in the MPLS labels (range is 1 to 255).
verbose	(Optional) Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.

Command Default

exp *exp-bits*: 0

interval *min-send-delay*: 0

repeat *count*: 5

reply-mode: IPv4

timeout *timeout* : 2

Command Modes   EXEC

Command History

Release	Modification
Release 4.0.0	This command was introduced. This command replaces the **ping mpls traffic-eng** command.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **output interface** keyword specifies the output interface on which the MPLS echo request packets are sent. If the specified output interface is not part of the LSP, the packets are not transmitted.

In cases where the **sweep** keyword is used, values larger than the outgoing interface's MTU are not transmitted.

The **ping** command sends an echo request packet to an address, and then waits for a reply. Ping output helps you evaluate path-to-host reliability, delays over the path. It also helps you determine whether the host is reachable or is functioning.

Task ID

Task ID	Operation
mpls-te	read, write
mpls-ldp	read, write

Related Commands

Command	Description
show mpls traffic-eng tunnels	Displays information about MPLS-TE tunnels.

show mpls oam

To display MPLS OAM information, use the **show mpls oam** command in EXEC mode.

show mpls oam {**client**| **counters** {**global**| **packet**}| **interface** *type interface-path-id*}

Syntax Description

client	Displays clients registered with LSPV server.
counters global	Displays LSP verification global counters.
counters packet	Displays LSP verification packet counters.
counters interface	Displays LSP verification information for a specific interface.
type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Command Default   No default behavior or values

Command Modes   EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read
mpls-ldp	read

Task ID	Operations
mpls-static	read

Examples

The following example shows how to display MPLS OAM client information:

```
RP/0/RP0/CPU0:router# show mpls oam client

  Client Process: l2vpn_mgr Node: 0/0/SP Pid: 418014
  Client Process: te_control Node: 0/0/SP Pid: 639227
```

This table describes the significant fields shown in the display.

Table 79: show mpls oam client Command Field Descriptions

Field	Description
Client Process	Process of client.

show mpls oam database

To display MPLS OAM database information, use the **show mpls oam database** command in EXEC mode.

show mpls oam database { **requests** | **tt-requests**} **[detail]** [**handle** *handle-value*]

Syntax Description

requests	Displays request database
tt-requests	Displays tree trace request database
detail	(Optional) Displays displayed information.
handle	(Optional) Displays handle information.
handle-value	Generic handle value. Range is from 0 to 4294967295.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 4.0.0	The **replies** keyword was removed.
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
mpls-te	read
mpls-ldp	read
mpls-static	read

Examples   The following example shows how to display detailed MPLS OAM database information:

```
RP/0/RP0/CPU0:router# show mpls oam database request detail
```

traceroute mpls ipv4

To learn the routes that packets follow when traveling to their Label Distribution Protocol (LDP) IPv4 destination, use the **traceroute mpls** command in EXEC mode.

traceroute mpls ipv4 *address/mask* [**destination** *start-address end-address address-increment*] [**exp** *exp-bits*] **[flags fec] [force-explicit-null]** [**output interface** *type interface-path-id* [**nexthop** *nexthop-address*]] [**reply** {**dscp** *dscp-value* | **reply mode** {**ipv4** | **router-alert**}}] [**revision** *version*] [**source** *source-address*] [**timeout** *timeout*] [**ttl** *value*] **[verbose]** [**fec-type** {**bgp** | **generic** | **ldp**}]

Syntax Description

address/mask	Specifies the destination type as a label distribution protocol (LDP) prefix. Address prefix of the target and number of bits in the target address network mask.
destination *start-address end-address address-increment*	Specifies a network 127 address to be used as the destination address in the echo request packet.
	start address
	Start of the network address.
	end address
	End of the network address.
	address increment
	Incremental value of the network address.
exp *exp-bits*	(Optional) Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.
flags fec	(Optional) Specifies that forwarding equivalent class (FEC) stack checking is to be performed at transit routers.
force-explicit-null	(Optional) Forces an unsolicited explicit null label to be added to the MPLS label stack and allows LSP ping to be used to detect LSP breakages at the penultimate hop.
output interface	(Optional) Specifies the output interface in which echo request packets are sent.
type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface.
	Note Use the **show interfaces** command to see a list of all interfaces currently configured on the router.
	For more information, use the question mark (**?**) online help function.

nexthop	(Optional) Specifies the IP address for the next hop.
nexthop-address	(Optional) IP address for the next hop.
reply dscp *dscp-value*	(Optional) Specifies the differentiated service codepoint value for an MPLS echo reply.
reply mode { **ipv4** | **router-alert**}	(Optional) Specifies the reply mode for the echo request packet. **ipv4** Reply with IPv4 UDP packet (this is the default) **router-alert** Reply with IPv4 UDP packet with router alert
revision *version*	(Optional) Specifies the Cisco extension TLV versioning field: • 1 draft-ietf-mpls-lsp-ping-03 (initial) • 2 draft-ietf-mpls-lsp-ping-03 (rev 1) • 3 draft-ietf-mpls-lsp-ping-03 (rev 2) • 4 draft-ietf-mpls-lsp-ping-09 (initial)
source *source-address*	(Optional) Specifies the source address used in the echo request packet.
timeout *timeoutt*	(Optional) Specifies the timeout interval, in seconds. Range is from 0 to 3600. Default is 2.
ttl *value*	(Optional) Specifies the maximum number of hops (range is 1 to 255).
verbose	(Optional) Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.

Command Default
exp *exp-bits*: 0

reply mode: IPv4

timeout *timeout*: 2

Command Modes EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

✎

Note   The **traceroute mpls** command is not supported on optical LSPs. If an optical LSP is encountered along the LSPs path, it is treated as a physical interface.

For detailed configuration information about MPLS LSP trace operations, see .

Task ID

Task ID	Operations
mpls-te	read, write
mpls-ldp	read, write

Examples   The following example shows how to trace a destination:

```
RP/0/RP0/CPU0:router# traceroute mpls ipv4 140.140.140.140/32
destination 127.0.0.10 127.0.0.15.1


Tracing MPLS Label Switched Path to 140.140.140.140/32, timeout is 2
seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

Destination address 127.0.0.10

  0 196.100.1.41 MRU 4470 [Labels: 19 Exp: 0]
L 1 196.100.1.42 MRU 4470 [Labels: 86 Exp: 0] 360 ms
  2 196.100.1.50 MRU 4470 [Labels: implicit-null Exp: 0] 8 ms
! 3 196.100.1.18 9 ms
```

The following example shows how to trace a destination with FEC type specified as generic and verbose option:

```
RP/0/RP0/CPU0:router# traceroute mpls ipv4 11.11.11.11/32 fec-type generic output interface
 gigabitEthernet 0/0/0/3
nexthop 172.40.103.2 verbose


Tracing MPLS Label Switched Path to 11.11.11.11/32, timeout is 2 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
```

```
      'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

  0 172.40.103.1 172.40.103.2 MRU 1500 [Labels: 16038 Exp: 0]
L 1 172.40.103.2 173.101.103.1 MRU 1500 [Labels: 16037 Exp: 0] 6 ms, ret code 8
L 2 173.101.103.1 11.101.11.11 MRU 1500 [Labels: implicit-null Exp: 0] 4 ms, ret code 8
! 3 11.101.11.11 6 ms, ret code 3
```

traceroute mpls multipath

To discover all possible paths of an LSP between the ingress and egress routers, use the **traceroute mpls multipath** command in EXEC mode.

traceroute mpls multipath ipv4 *address/mask* [**destination** *start-address end-address address-increment*] [**exp** *exp-bits*] [**flags fec**] [**force-explicit-null**] [**hashkey ipv4 bitmap** *bit-size*] [**interval** *min-send-delay*] [**output interface** *type interface-path-id* [**nexthop** *nexthop-address*]] [**reply** {**dscp** *dscp-value* | **reply mode**{**ipv4** | **router-alert**}}] [**retry-count** *count*] [**revision** *version*] [**source** *source-address*] [**timeout** *timeout*] [**ttl** *value*] [**verbose**] [**fec-type** {**bgp** | **generic** | **ldp**}]

Syntax Description

ipv4	Specifies the destination type as a Label Distribution Protocol (LDP) IPv4 address.
address/mask	Address prefix of the target and number of bits in the target address network mask.

destination *start-address end-address address-increment*	(Optional) Specifies a network 127 address to be used as the destination address in the echo request packet.
	
	start-address
	    Start of the network address.
	
	end-address
	    End of the network address.
	
	address-increment
	    Incremental value of the network address.

exp *exp-bits*	(Optional) Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.
flags fec	(Optional) Specifies that forwarding equivalent class (FEC) stack checking is to be performed at transit routers.
force-explicit-null	(Optional) Forces an unsolicited explicit null label to be added to the MPLS label stack and allows LSP ping to be used to detect LSP breakages at the penultimate hop.
hashkey ipv4 bitmap *bit-size*	(Optional) Allows user control of the hash key/multipath settings. Range is 0 to 256. The default is 32.
interval *min-send-delay*	(Optional) Specifies a send interval, in milliseconds, between requests. Range is 0 to 3600000. Default is 0.
output interface	(Optional) Specifies the output interface where echo request packets are sent.

type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information, use the question mark (**?**) online help function.
nexthop	(Optional) Specifies the IP address for the next hop.
nexthop-address	(Optional) IP address for the next hop.
reply dscp *dscp-value*	(Optional) Specifies the differentiated service codepoint value for an MPLS echo reply.

reply mode [**ipv4** | **router-alert**]	(Optional) Specifies the reply mode for the echo request packet.
	
	ipv4
	
	    Reply with IPv4 UDP packet (this is the default)
	
	router-alert
	
	    Reply with IPv4 UDP packet with router alert

retry-count *count*	(Optional) Specifies the number of retry attempts during multipath LSP traceroute. A retry is attempted if an outstanding echo request • times out waiting for the corresponding echo reply. • fails to find a valid destination address set to exercise a specific outgoing path. Range is 0 to 10. Default is 3.
revision *version*	(Optional) Specifies the Cisco extension TLV versioning field: • 1 draft-ietf-mpls-lsp-ping-03 (initial) • 2 draft-ietf-mpls-lsp-ping-03 (rev 1) • 3 draft-ietf-mpls-lsp-ping-03 (rev 2) • 4 draft-ietf-mpls-lsp-ping-09 (initial)
source *source-address*	(Optional) Specifies the source address used in the echo request packet.
timeout *timeout*	(Optional) Specifies the timeout interval, in seconds. Range is from 0 to 3600. Default is 2.
ttl *value*	(Optional) Specifies the maximum number of hops (range is 1 to 255).
verbose	(Optional) Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.

Command Default

exp *exp-bits* : 0

hashkey ipv4 bitmap *bit-size*: 4

interval *min-send-delay*: 0

reply mode: IPv4

retry-count: 3

timeout *timeout* : 2

Command Modes

EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **hashkey ipv4 bitmap** keyword and *bit-size* value control how many addresses are encoded in the DSMAP multipath field. Larger values allow more coverage of equal cost multiple paths throughout the network, but with more processing at the head, mid, and tail routers.

Task ID

Task ID	Operations
mpls-te	read, write
mpls-ldp	read, write

Examples

The following example shows how to specify the destination type as an LDP IPv4 prefix:

```
RP/0/RP0/CPU0:router# traceroute mpls multi ipv4 140.140.140.140/32 verbose
force-explicit-null

  Starting LSP Path Discovery for 140.140.140.140/32

  Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

  Type escape sequence to abort.

  LL!
```

```
 Path 0 found,
 output interface POS0/2/0/3 source 196.100.1.61 destination 127.0.0.1
 0 196.100.1.61 196.100.1.62 MRU 4470 [Labels: 18/explicit-null Exp: 0/0] multipaths 0
 L 1 196.100.1.62 196.100.1.10 MRU 4470 [Labels: 17/explicit-null Exp: 0/0] ret code 8
multipaths 1
 L 2 196.100.1.10 196.100.1.18 MRU 4470 [Labels: implicit-null/explicit-null Exp: 0/0] ret
 code 8 multipaths 1
 ! 3 196.100.1.1018, ret code 3 multipaths 0
 LL!
 Path 1 found,
 output interface GigabitEthernet0/3/0/0 source 196.100.1.5 destination 127.0.0.1
 0 196.100.1.5 196.100.1.37 6 MRU 1500 [Labels: 18/explicit-null Exp: 0/0] multipaths 0
 L 1 196.100.1.6 196.100.1.10 MRU 4470 [Labels: 17/explicit-null Exp: 0/0] ret code 8
multipaths 1
 L 2 10196.0100.21.5 1010 196.0100.21.10 18 MRU 4470 [Labels: implicit-null/explicit-null
 Exp: 0/0] ret code 8 multipaths 1
 ! 3 10196.0100.21.1018, ret code 3 multipaths 0

 Paths (found/broken/unexplored) (2/0/0)
 Echo Request (sent/fail) (6/0)
 Echo Reply (received/timeout) (6/0)
 Total Time Elapsed 80 ms
```

The following example shows how to specify the FEC type as LDP with verbose option:

```
RP/0/RP0/CPU0:router#  traceroute mpls multipath ipv4 11.11.11.11/32 fec-type ldp output
interface gigabitEthernet 0/0/0/3
nexthop 172.40.103.2 verbose

Starting LSP Path Discovery for 11.11.11.11/32

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

LL!
Path 0 found,
 output interface GigabitEthernet0/0/0/3 nexthop 172.40.103.2
 source 172.40.103.1 destination 127.0.0.0
  0 172.40.103.1 172.40.103.2 MRU 1500 [Labels: 16038 Exp: 0] multipaths 0
L 1 172.40.103.2 173.101.103.1 MRU 1500 [Labels: 16037 Exp: 0] ret code 8 multipaths 1
L 2 173.101.103.1 11.101.11.11 MRU 1500 [Labels: implicit-null Exp: 0] ret code 8 multipaths
 1
! 3 11.101.11.11, ret code 3 multipaths 0

Paths (found/broken/unexplored) (1/0/0)
 Echo Request (sent/fail) (3/0)
 Echo Reply (received/timeout) (3/0)
 Total Time Elapsed 21 ms
```

traceroute mpls traffic-eng

To specify the destination type as an MPLS traffic engineering (TE) tunnel, use the **traceroute mpls traffic-eng** command in EXEC mode.

traceroute mpls traffic-eng tunnel *tunnel-ID* [**destination** *start-address end-address address-increment increment-mask*] [**exp** *exp-bits*] [**flags fec**] [**force-explicit-null**] [**reply** {**dscp** *dscp-value* | **reply mode** {**ipv4** | **router-alert**}}] [**revision** *version*] [**source** *source-address*] [**timeout** *timeout*] [**ttl** *value*] [**verbose**]

Syntax Description

tunnel	Specifies the MPLS-TE tunnel type.
tunnel-ID	Tunnel interface.
destination *start-address end-address address -increment increment-mask*	(Optional) Specifies a network 127 address to be used as the destination address in the echo request packet. *start-address* Start of the network address. *end-address* End of the network address. *address-increment* Incremental value of the network address. *increment-mask* Incremental mask of the network address.
exp *exp-bits*	(Optional) Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.
flags fec	(Optional) Specifies that forwarding equivalent class (FEC) stack checking is to be performed at transit routers.
force-explicit-null	(Optional) Forces an unsolicited explicit null label to be added to the MPLS label stack and allows LSP ping to be used to detect LSP breakages at the penultimate hop.
reply dscp *dscp-value*	(Optional) Specifies the differentiated service codepoint value for an MPLS echo reply.

reply mode [**ipv4** | **router-alert**]	(Optional) Specifies the reply mode for the echo request packet.
	ipv4
	Reply with IPv4 UDP packet (this is the default)
	router-alert
	Reply with IPv4 UDP packet with router alert
revision *version*	(Optional) Specifies the Cisco extension TLV versioning field:
	• 1 draft-ietf-mpls-lsp-ping-03 (initial)
	• 2 draft-ietf-mpls-lsp-ping-03 (rev 1)
	• 3 draft-ietf-mpls-lsp-ping-03 (rev 2)
	• 4 draft-ietf-mpls-lsp-ping-09 (initial)
source *source-address*	(Optional) Specifies the source address used in the echo request packet.
timeout *timeout*	(Optional) Specifies the timeout interval, in seconds. Range is from 0 to 3600. Default is 2.
ttl *value*	(Optional) Specifies the maximum number of hops (range is 1 to 255).
verbose	(Optional) Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.

Command Default

exp *exp-bits* : 0

reply mode: IPv4

timeout *timeout* : 2

Command Modes   EXEC

Command History

Release	Modification
Release 4.0.0	This command was replaced by the **traceroute mpls traffic-eng tunnel-te (P2P)** command.

Usage Guidelines   To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
mpls-te	read
mpls-ldp	read

Examples

The following example shows how to specify the destination as a MPLS-TE tunnel:

```
RP/0/RP0/CPU0:router#  traceroute mpls traffic-eng tunnel 13

Tracing MPLS TE Label Switched Path on tunnel-te13, timeout is 2 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

 0 0.0.0.0 11.0.0.1 MRU 1500 [Labels: 16003 Exp: 0]
 L 1 192.168.200.2 192.168.170.1 MRU 1500 [Labels: implicit-null Exp: 0] 110 ms
 ! 2 192.168.170.1 0.0.0.0 MRU 0 [No Label] 169 ms
```

Related Commands

Command	Description
ping mpls traffic-eng tunnel-te (P2P)	Displays information about MPLS-TE tunnel for a point-to-point connection.

traceroute mpls traffic-eng tunnel-te (P2P)

To specify the destination type as an MPLS traffic engineering (TE) tunnel for a point-to-point connection, use the **traceroute mpls traffic-eng tunnel-te (P2P)** command in EXEC mode.

traceroute mpls traffic-eng tunnel-te *tunnel-ID* [**destination** *start-address end-address address-increment increment-mask*] [**exp** *exp-bits*] [**flags fec**] [**force-explicit-null**] [**reply** {**dscp** *dscp-value* | **mode** {**ipv4** | **router-alert**}}] [**revision** *version*] [**source** *source-address*] [**timeout** *timeout*] [**ttl** *value*] [**verbose**]

Syntax Description

tunnel-te	Specifies the MPLS-TE tunnel type.
tunnel-ID	Tunnel interface.

destination *start-address end-address address -increment increment-mask*	(Optional) Specifies a network 127 address to be used as the destination address in the echo request packet.
	
	start-address
	
	    Start of the network address.
	
	end-address
	
	    End of the network address.
	
	address-increment
	
	    Incremental value of the network address.
	
	increment-mask
	
	    Incremental mask of the network address.

exp *exp-bits*	(Optional) Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.
flags fec	(Optional) Specifies that forwarding equivalent class (FEC) stack checking is to be performed at transit routers.
force-explicit-null	(Optional) Forces an unsolicited explicit null label to be added to the MPLS label stack and allows LSP ping to be used to detect LSP breakages at the penultimate hop.
reply dscp *dscp-value*	(Optional) Specifies the differentiated service codepoint value for an MPLS echo reply.

reply-mode [**ipv4** | **router-alert**]	(Optional) Specifies the reply mode for the echo request packet.
	
	ipv4
	
	    Reply with IPv4 UDP packet (this is the default)
	
	router-alert
	
	    Reply with IPv4 UDP packet with router alert

revision *version*	(Optional) Specifies the Cisco extension TLV versioning field:
	
	  • 1 draft-ietf-mpls-lsp-ping-03 (initial)
	
	  • 2 draft-ietf-mpls-lsp-ping-03 (rev 1)
	
	  • 3 draft-ietf-mpls-lsp-ping-03 (rev 2)
	
	  • 4 draft-ietf-mpls-lsp-ping-09 (initial)

source *source-address*	(Optional) Specifies the source address used in the echo request packet.
timeout *timeout*	(Optional) Specifies the timeout interval, in seconds. Range is from 0 to 3600. Default is 2.
ttl *value*	(Optional) Specifies the maximum number of hops (range is 1 to 255).
verbose	(Optional) Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.

Command Default

exp *exp-bits* : 0

reply-mode: IPv4

timeout *timeout* : 2

Command Modes

EXEC

Command History

Release	Modification
Release 4.0.0	This command was introduced. This command replaces the **traceroute mpls traffic-eng** command.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operation
mpls-te	read
mpls-ldp	read

Examples

The following example shows how to specify the destination as a MPLS-TE tunnel:

```
RP/0/RP0/CPU0:router#  traceroute mpls traffic-eng tunnel-te 13

Tracing MPLS TE Label Switched Path on tunnel-te13, timeout is 2 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

 0 0.0.0.0 11.0.0.1 MRU 1500 [Labels: 16003 Exp: 0]
L 1 192.168.200.2 192.168.170.1 MRU 1500 [Labels: implicit-null Exp: 0] 110 ms
! 2 192.168.170.1 0.0.0.0 MRU 0 [No Label] 169 ms
```

Related Commands

Command	Description
show mpls traffic-eng tunnels	Displays information about MPLS-TE tunnels.

I N D E X