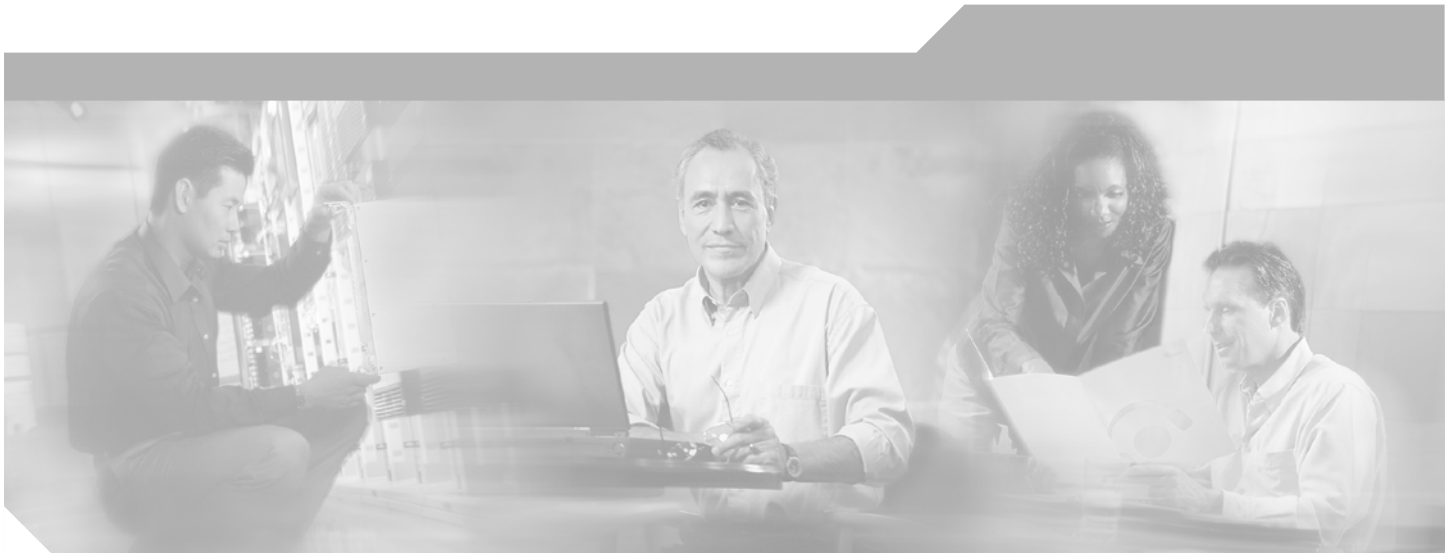

Cisco IOS-XR MPLS Command Reference

Cisco IOS-XR Software Release 2.0

Corporate 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: 408 526-4100

Text Part Number: OL-5561-01

Cisco IOS-XR MPLS Command Reference

CONTENTS

MPLS Label Distribution Protocol Commands on Cisco IOS-XR Software MPR-1

MPLS Traffic Engineering Commands on Cisco IOS-XR Software MPR-41

MPLS Forwarding Commands on Cisco IOS-XR Software MPR-119

RSVP Infrastructure Commands on Cisco IOS-XR MPR-147

MPLS Optical User Network Interface Commands on Cisco IOS-XR Software MPR-195

MPLS Label Distribution Protocol Commands on Cisco IOS-XR Software

Label Distribution Protocol (LDP) provides a standard methodology for hop-by-hop, or dynamic label, distribution in a Multiprotocol Label Switching (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 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.

The Cisco IOS-XR software implementation of LDP supports these features:

- Downstream unsolicited label distribution with liberal mode retention and independent control over frame-based interfaces.
- Support for router-id and transport-address modification.
- Support for LDP targeted sessions over MPLS Traffic-Engineering tunnels (tunnel-te).
- LDP graceful restart mechanism for Non-Stop Forwarding (NSF).
- Support for LDP MIBs.
- Use of TCP MD5 signature option for LDP session.
- L3 Load balancing across equal cost multiple IGP paths.
- Support for MPLS explicit-null label, which extends the LSP path to the ultimate router instead of the penultimate router.

backoff

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

backoff *initial maximum*

no backoff

Syntax Description

initial	Initial backoff delay in seconds. The default is 15 seconds.
maximum	Maximum backoff delay in seconds. The default is 120 seconds.

Defaults

initial:15 seconds

maximum:120 seconds

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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

This command can also be executed globally, without entering MPLS LDP configuration mode, by using the **mpls ldp backoff** command.

The default settings correspond to the lowest settings for initial and maximum backoff values defined by the LDP protocol specification.

Examples

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

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

Related Commands

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

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

Syntax Description

neighbor	Clears LDP message counters for neighbor(s).
ip-address	The neighbor IP address.
all	Clears LDP message counters for all sessions.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this 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 neighbor(s).

Examples

The following example clears the 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	Displays statistics about the type and count of the messages sent and received from neighbors.

discovery

To configure the interval between transmission of consecutive Label Distribution Protocol (LDP) discovery hello messages, the holdtime for a discovered LDP neighbor, and the neighbors from which requests for targeted hello messages may be honored, use the **discovery** command in MPLS LDP configuration mode. To reset a discovery parameter to its default value, use the **no** form of this command.

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

discovery targeted-hello accept

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

no discovery targeted-hello accept

Syntax Description

hello	Configures the intervals and holdtimes for directly connected neighbors.
targeted-hello	Configures the intervals, holdtimes, and acceptance for targeted neighbors.
accept	Accepts targeted hellos from any source.
holdtime	Selects the period of time a discovered LDP neighbor is remembered without receipt of an LDP hello message from the neighbor.
interval	Selects the period of time between the sending of consecutive hello messages.
seconds	The time value in seconds.

Defaults

The default value for the **holdtime** keyword is 15 seconds for link hello messages and 90 seconds for targeted hello messages.

The default value for the **interval** keyword is 5 seconds for link hello messages and 10 seconds for targeted hello messages.

The default behavior for the keyword **accept** is not to accept any targeted hello from any source.

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

This command can also be executed globally, without entering LDP configuration mode, by using the **mpls ldp discovery** command.

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
```

discovery transport-address

To provide an alternative address for a Transmission Control Protocol (TCP) connection, use the **discovery transport-address** command in MPLS LDP configuration mode. To disable this function, 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 advertise as the transport address in its hello discovery messages.
interface	Advertises the IP address of the interface (on which Label Distribution Protocol [LDP] is enabled) as the transport address in its hello discovery messages.

Defaults

By default, Label Distribution Protocol (LDP) advertises its LDP router ID as the transport address in LDP Discovery Hello messages sent from the interface.

Command Modes

MPLS LDP interface configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Establishing an LDP session between two routers requires a session TCP connection, and 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 the transport address for its end of a session TCP connection. The transport address advertisement itself may be explicit, in which case it appears as part of the contents of Discovery Hello messages sent to the peer, or implicit, in which case it does not, and the peer uses the source IP address of received Hello messages for the peer's transport address.

The MPLS LDP **discovery transport-address** command provides the means to modify the default behavior described above. When the interface keyword is specified, LDP advertises the IP address of the interface in LDP Discovery Hello messages sent from the interface. When the *ip-address* argument value is specified, LDP advertises the specified 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.

The command can be executed globally without entering MPLS LDP global or MPLS LDP interface mode. For example:

```
RP/0/RP0/CPU0:router(config)# mpls ldp interface POS 0/1/0/0 discovery transport-address
interface
RP/0/RP0/CPU0:router(config)# mpls ldp interface POS 0/2/0/0 discovery transport-address
10.10.4.1
```

Examples

In the following example, the **discovery transport-address** command is used to specify an exiting address (10.10.3.1) as the transport address on POS interface 0/1/0/0. Note that the neighbor is using its loopback address (router ID) by default, whereas the local LSR is using a configured address for TCP connection.

```
RP/0/RP0/CPU0:router(config)# mpls 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(config-ldp-if)# end
Uncommitted changes found, commit them? [yes]:
RP/0/RP0/CPU0:Mar 10 20:21:26.389 : %CLIENTLIBCFGMGR-6-CONFIG_CHANGE : A configuration
commit by user 'UNKNOWN' occurred at 'Mon Mar 10 20:21:26 2003 '. The  configuration
changes are saved on the router by commit Id: '1000000002'. To view configuration
change(s) use the command - 'show commit-changes'.
RP/0/RP0/CPU0:Mar 10 20:21:26.532 : %SYS-5-CONFIG_I : Configured from console by console
RP/0/RP0/CPU0:router#
RP/0/RP0/CPU0:Mar 10 20:21:38.157 : mpls_ldp[113]: %LDP-5-NBR_CHANGE : Nbr 10.44.44.44:0,
DOWN
RP/0/RP0/CPU0:Mar 10 20:21:47.671 : mpls_ldp[113]: %LDP-5-NBR_CHANGE : Nbr 10.44.44.44:0,
UP

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:
    POS0/1/0/0
  Addresses bound to this peer:
    10.10.3.2       10.44.44.44
```

Related Commands

Command	Description
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp neighbor	Displays information about LDP neighbors.

explicit-null

To configure a router to advertise an Explicit Null label in situations where it would normally advertise an Implicit Null label, use the **explicit-null** command in MPLS LDP configuration mode. To disable this function, use the **no** form of this command.

explicit-null

no explicit-null

Syntax Description

This command has no arguments or keywords.

Defaults

Implicit Null is advertised for all directly connected routes.

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Normally, LDP advertises an Implicit Null label for directly connected routes. The Implicit Null label causes the previous hop (penultimate) router to perform penultimate hop popping. Situations exist where it might be desirable to prevent the penultimate router from performing penultimate hop popping and to force it to replace the incoming label with the Explicit Null label.

When the **explicit-null** command is issued, Explicit Null is advertised in place of Implicit Null for directly connected prefixes.

This command can also be executed globally, without entering LDP configuration mode, by using the **mpls ldp explicit-null** command.

Examples

The following example shows how to configure Explicit Null to be advertised for all directly connected routes to all LDP peers:

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

Related Commands

Command	Description
show mpls forwarding	Displays global MPLS forwarding information.
show mpls ldp bindings	Displays known label bindings.
show mpls ldp forwarding	Displays MPLS LDP forwarding information.
show mpls ldp parameters	Displays LDP configuration and operational parameters settings.

graceful-restart

To configure graceful restart feature capability, use the **graceful-restart** command in MPLS LDP configuration mode. To disable this function, 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) Time (in seconds) that the local Label Distribution Protocol (LDP) instructs the LDP peer to wait for reconnection (before declaring it dead) in case of LDP communication failure. The default timeout is 120 seconds.
forwarding-state-holdtime *seconds*	(Optional) The length of time (in seconds) that local forwarding state will be preserved (without being reclaimed) after local LDP control plane restarts. The default is 180 seconds.

Defaults

Graceful restart functionality is disabled by default. The default values for **reconnect-timeout** and **forwarding-state-holdtime** are 120 seconds and 180 seconds, respectively.

Command Modes

MPLS LDP Configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

To achieve Non-Stop Forwarding (NSF) during an LDP control plane communication failure/restart, LDP Graceful Restart (GR) capability can be configured on the router by using the **graceful-restart** command. To configure an LDP session as GR between two peers, the LDP GR feature should be enabled on both LSRs.

When an LDP GR session is established and there is control plane failure (that is, a restart), then the peer LSR starts GR procedures, and initially keeps the forwarding state information pertaining to the restarting peer, and marks this state as stale. If the restarting peer does not reconnect back within the reconnect timeout, then this stale forwarding state is removed. However, if the restarting peer reconnects back within the reconnect time period, it is given recovery time to re-sync and re-instate all of its forwarding state with its peer. After the specified recovery time, any state which is not synchronized again (and that is still stale) is removed.

On restarting LSR, the value of the forwarding state hold time is used to keep the forwarding plane state associated with the LDP control plane in case of a control plane restart/failure. If the control plane fails, then the forwarding plane will keep 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 GR sessions are re-negotiated with its peers, the restarting LSR sends the remaining value of this timer as the recovery time to its peers.

Note In the presence of a peer relationship, any change to the LDP GR enable/disable configuration is not applied until next LDP process restart.

Examples

The following example shows how to specify an existing session to be graceful restartable:

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

Uncommitted changes found, commit them? [yes]:
RP/0/RP0/CPU0:Mar 10 20:54:16.118 : mpls_ldp[113]: %LDP-6-GR_CHG : Please restart LDP
process for this to take effect
RP/0/RP0/CPU0:Mar 10 20:54:16.152 : %CLIENTLIBCFGMGR-6-CONFIG_CHANGE : A configuration
commit by user 'UNKNOWN' occurred at 'Mon Mar 10 20:54:16 2003 '. The  configuration
changes are saved on the router by commit Id: '1000000009'. To view configuration
change(s) use the command - 'show commit-changes'.
RP/0/RP0/CPU0:Mar 10 20:54:16.336 : %SYS-5-CONFIG_I : Configured from console by console

RP/0/RP0/CPU0:router# process restart mpls_ldp

RP/0/RP0/CPU0:ios#RP/0/RP0/CPU0:Mar 10 20:54:41.707 : mpls_ldp[113]: %LDP-5-NBR_CHANGE :
Nbr 10.44.44.44:0, UP

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

Peer LDP Identifier: 10.44.44.44:0
  TCP connection: 10.44.44.44:65511 - 10.33.33.33:646
  Graceful Restart: Yes (Reconnect Timeout: 15 sec, Recovery: 175 sec)
  State: Oper; Msgs sent/rcvd: 11/3
  Up time: 00:00:08
  LDP Discovery Sources:
    POS0/1/0/0
  Addresses bound to this peer:
    10.10.3.2       10.44.44.44

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

  Forwarding State Hold timer : Running (156 sec remaining)
  Forwarding Entries          : 2 Checkpointed (1 GR, 1 non-GR)
                                1 Stale, 0 without PathUp
  GR Neighbors                : 1

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

Related Commands

Command	Description
show mpls ldp forwarding	Displays LDP forwarding state, written into MPLS Forwarding Infrastructure.
show mpls ldp graceful-restart	Displays graceful restart related information.
show mpls ldp neighbor	Displays information about LDP neighbors.
show mpls ldp parameters	Displays the status of the LDP parameters.
show mpls ldp summary	Displays a summary of LDP control plane (sessions, routes, interfaces, servers).

holdtime

To change the time for which a 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 disable this function, use the **no** form of this command.

holdtime *seconds*

no holdtime

Syntax Description

seconds	A number from 15 to 214748 that defines the time, in seconds, that an LDP session is maintained in the absence of LDP messages from the session peer. The default is 180 seconds.

Defaults

The default session holdtime is 180 seconds.

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

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

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

Related Commands

Command	Description
show mpls ldp parameters	Displays current LDP parameter settings.

interface (MPLS LDP)

To configure or enable the Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) on an interface, use the **interface** command and enable LDP on the desired interface in MPLS LDP configuration mode. To disable this feature, use the **no** form of this command.

interface {*type number*}

no interface {*type number*}

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function. This argument is not allowed on loopback-type virtual interfaces.
number	Either a physical interface number or a virtual interface number: • Physical interface number. Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. • Virtual interface number. Number range will vary depending on interface type. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.

Defaults

LDP is disabled on an interface.

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

When LDP is enabled on an interface, the LDP process starts discovery of a neighbor by sending link hello messages on the interface, which may result in eventual session setup with discovered neighbors. If LDP is enabled on tunnel TE interfaces, then targeted discovery procedures are used instead of link discovery procedures.

Note LDP cannot be enabled on loopback interfaces.

Examples

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

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

```
RP/0/RP0/CPU0:router(config-ldp)# interface POS0/1/0/0
RP/0/RP0/CPU0:router(config-ldp-if)# exit
```

LDP can be configured on an MPLS traffic-engineering tunnels as follows:

```
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)# exit
```

Related Commands

Command	Description
show mpls interfaces	Displays information about one or more interfaces that have been configured for label switching.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp summary	Displays summarized information regarding the LDP process.

log neighbor changes

To notify the user of any session changes, use the **log neighbor changes** command in MPLS LDP configuration mode. To disable this function, use the **no** form of this command.

log neighbor changes

no log neighbor changes

Syntax Description

This command has no arguments or keywords.

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command to get a console message when a neighbor goes up or down (for instance, in the case of an LDP session flap).

Examples

```
RP/0/RP0/CPU0:router(config-ldp)# log neighbor changes
RP/0/RP0/CPU0:router(config-ldp)# end
Uncommitted changes found, commit them? [yes]:

RP/0/RP0/CPU0:Mar 10 21:11:20.649 : %SYS-5-CONFIG_I : Configured from console by console

RP/0/RP0/CPU0:router# proc restart mpls_ldp

RP/0/RP0/CPU0:Mar 10 21:11:33.353 : mpls_ldp[113]: %LDP-5-NBR_CHANGE : Nbr 10.44.44.44:0,
UP
```

Related Commands

Command	Description
show mpls ldp neighbor	Displays information about LDP neighbors.

mpls ldp restart session

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

mpls ldp restart session {*ip-address* | **all**}

Syntax Description

ip-address	The neighbor IP address.
all	Restarts all sessions.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command to restart a single LDP session or all LDP sessions without restarting the LDP process itself.

Examples

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

```
RP/0/RP0/CPU0:router# mpls ldp restart session 10.20.20.20
```

Related Commands

Command	Description
show mpls ldp neighbor	Displays information about one or more interfaces that have been configured for label switching.

neighbor implicit-withdraw

To configure the advertisement of a new label for a Forwarding Equivalence Class (FEC) without the withdrawal of the previously advertised label, use the **neighbor implicit-withdraw** command in MPLS LDP configuration mode. To disable this function, use the **no** form of this command.

neighbor *ip-address* **implicit-withdraw**

no neighbor *ip-address* **implicit-withdraw**

Syntax Description

ip-address	IP address of the neighbor.
implicit-withdraw	Consider any earlier label mappings from a neighbor implicitly withdrawn.

Defaults

Disabled.

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

If this command is not configured, when it is necessary for Label Distribution Protocol (LDP) to change the label it has advertised to a neighbor for some prefix, it will withdraw the previously advertised label before advertising the new label to the neighbor.

Using the **implicit-withdraw** keyword avoids the overhead of label withdraw and label release message exchanges.

This command can also be executed globally, without entering MPLS LDP configuration mode, by using the **mpls ldp neighbor implicit-withdraw** command.

Examples

The following example configures LDP to not send a label-withdraw message to the neighbor whose router ID is 10.10.10.10 when a need exists to change the previously advertised label for an FEC:

```
RP/0/RP0/CPU0:router(config-ldp)# neighbor 10.10.10.10 implicit-withdraw
RP/0/RP0/CPU0:router(config-ldp)# end
```

neighbor password

To configure password authentication using the Transmission Control Protocol Message Digest 5 (TCP MD5) option for a given neighbor, use the **neighbor password** command in MPLS LDP configuration mode. To disable this function, use the **no** form of this command.

neighbor *ip-address* **password** [*encryption*] *password*

no neighbor *ip-address* **password** [*encryption*] *password*

Syntax Description

ip-address	Neighbor IP address.
encryption	(Optional) Encryption parameter for password. Use either 0 (cleartext) or 7 (already encrypted). Encryption types 1 to 6 are not supported.
password	Cleartext or already-encrypted password.

Defaults

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

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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

This command can also be executed globally, without entering MPLS LDP configuration mode, by using the **mpls ldp neighbor password** command.

Examples

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

```
RP/0/RP0/CPU0:router(config-ldp)# neighbor 10.20.20.20 password 7 cisco
```

router-id (MPLS LDP)

To specify the IP address of a preferred interface or a specific IP address as the Label Distribution Protocol (LDP) router ID, use the **router-id** command in MPLS LDP configuration mode. To disable this function, use the **no** form of this command.

router-id {*type number* | *ip-address*}

no router-id {*type number* | *ip-address*}

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function. This argument is not allowed on loopback-type virtual interfaces.
number	Either a physical interface number or a virtual interface number: • Physical interface number. Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. • Virtual interface number. Number range will vary depending on interface type. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.
ip-address	The IP address to be used as the router ID.

Defaults

LDP uses router-id as determined by global router-id agent.

Command Modes

MPLS LDP configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The **router-id** command provides the ability to specify an interface whose IP address is 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 these instances, use the **router-id** command to select the IP address of the specified loopback interface (provided that 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 (configured or computed)

This command can also be executed globally, without entering LDP configuration mode, by using the **mpls ldp router-id** command.

Note Only loopback interfaces can be configured using the **router-id** command. Any change to the router ID takes effect immediately, and causes a session reset.

Examples

The following example shows how to specify that loopback interface 1 is the preferred interface for use in determining the LDP router ID.

```
RP/0/RP0/CPU0:router(config-ldp)# router-id loopback 1
```

Related Commands

Command	Description
mpls ldp restart session	Forces a restart of MPLS LDP session(s).
show mpls ldp discovery	Displays the status of the LDP discovery process, including the local LDP router ID and the LDP router IDs of discovered LSRs.
show mpls ldp neighbor	Displays information about LDP neighbors.
show mpls ldp parameters	Displays current LDP parameters and configuration settings.

show mpls ldp backoff

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

show mpls ldp backoff

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following is 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
```

Related Commands

Command	Description
show mpls forwarding	Displays the contents of the MPLS forwarding.
show mpls ldp bindings	Displays the contents of LDP label information base (LIB).

show mpls ldp bindings

To display the contents of the label information base (LIB), use the **show mpls ldp bindings** EXEC command.

show mpls ldp bindings [*network* {*mask* | *length*}] [**local-label** *label* [**to** *label*]] [**remote-label** *label* [**to** *label*]] [**neighbor** *address*] [**local**] [**detail**] | [**summary**]

Syntax Description

network	(Optional) Defines the destination network number.
mask	Specifies the network mask, written as A.B.C.D.
length	Specifies the mask length (1 to 32 characters).
local-label *label* **to** *label*	(Optional) Displays entries matching local label values. Use the *label* **to** *label* argument to indicate the label range.
remote-label *label* **to** *label*	(Optional) Displays entries matching the label values assigned by a neighbor router. Use the *label* **to** *label* argument to indicate the label range.
neighbor *address*	(Optional) Displays the label bindings assigned by the selected neighbor.
local	(Optional) Displays the local label bindings.
detail	(Optional) Displays detailed information for given label bindings, such as local label bindings advertised to peers.
summary	(Optional) Displays a summary of the contents of the LIB.

Defaults

If no optional keyword or parameter is supplied, the command displays the entire label information base (LIB).

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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

A request can specify that either the entire database be displayed or the display be limited to a subset of entries according to the following:

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

The **show mpls ldp bindings summary** command displays summarized information from the LIB and can be used when testing scalability, or when employed in a large scale network.

Examples

The following is sample output from the **show mpls ldp bindings** command. This form of this command 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:10.44.44.44:0, label:16
            lsr:10.22.22.22:0, label:IMP-NULL
10.10.3.0/24 , rev 10
        local binding: label:IMP-NULL
        remote bindings :
            lsr:10.44.44.44:0, label:IMP-NULL
            lsr:10.22.22.22:0, label:22
22.22.22.22/32 , rev 14
        local binding: label:16
        remote bindings :
            lsr:10.44.44.44:0, label:17
            lsr:10.22.22.22:0, label:IMP-NULL (rewrite)
33.33.33.33/32 , rev 2
        local binding: label:IMP-NULL
        remote bindings :
            lsr:10.44.44.44:0, label:18
            lsr:10.22.22.22:0, label:23
44.44.44.44/32 , rev 16
        local binding: label:17
        remote bindings :
            lsr:10.44.44.44:0, label:IMP-NULL (rewrite)
            lsr:10.22.22.22:0, label:24
223.255.254.254/32 , rev 8
        local binding: label:IMP-NULL
        No remote bindings
```

The following is sample output from the **show mpls ldp bindings neighbor** command specifying a particular network number. The command displays labels learned from LSR 44.44.44.44 for all networks. The use of the **neighbor** option suppresses the output of remote labels learned from other neighbors.

```
RP/0/RP0/CPU0:router# show mpls ldp bindings neighbor 44.44.44.44

10.10.2.0/24 , rev 12
        local binding: label:IMP-NULL
        remote bindings :
```

```
            lsr:10.44.44.44:0, label:16
10.10.3.0/24 , rev 10
        local binding: label:IMP-NULL
        remote bindings :
            lsr:10.44.44.44:0, label:IMP-NULL
22.22.22.22/32 , rev 14
        local binding: label:16
        remote bindings :
            lsr:10.44.44.44:0, label:17
33.33.33.33/32 , rev 2
        local binding: label:IMP-NULL
        remote bindings :
            lsr:10.44.44.44:0, label:18
44.44.44.44/32 , rev 16
        local binding: label:17
        remote bindings :
            lsr:10.44.44.44:0, label:IMP-NULL (rewrite)
```

The following is sample output from the **show mpls ldp bindings summary** command.

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

LIB Summary:
  Total Prefix   : 8
  Revision No    : Current:13, Advertised:13
  Local Bindings : 8
      NULL    : 5 (implicit:5, explicit:0)
      Non-NULL: 3 (lowest:16, highest:18)
  Remote Bindings: 8
```

Related Commands

Command	Description
show mpls forwarding	Displays the contents of the MPLS forwarding.
show mpls ldp forwarding	Display the contents of LDP forwarding database.

show mpls ldp discovery

To display the status of the Label Distribution Protocol (LDP) discovery process, use the **show mpls ldp discovery** command in EXEC mode. This command shows both link discovery and targeted discovery. When no interface filter is specified, this command generates a list of interfaces over which the LDP discovery process is running.

show mpls ldp discovery [*type number*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
number	(Optional) Either a physical interface number or a virtual interface number: • Physical interface number. Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. • Virtual interface number. Number range will vary depending on interface type. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

This command displays neighbor discovery information for the default routing domain.

Examples

The following is sample output 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:
    POS0/1/0/0 : 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)
```

Related Commands

Command	Description
discovery	Configures LDP targeted-hello acceptance from targeted discovery sources.
interface (MPLS LDP)	Configures LDP on an interface.
show mpls interfaces	Displays information about one or more interfaces that have been configured for label switching.
show mpls ldp neighbor	Displays information about LDP neighbors.

show mpls ldp forwarding

To display the Label Distribution Protocol (LDP) forwarding state installed in Multiprotocol Label Switching (MPLS) forwarding, use the **show mpls ldp forwarding command** in EXEC mode. This command generates a list of forwarding entries from the LDP's perspective.

show mpls ldp forwarding [*network* {*mask* | *length*}]

Syntax Description

network	(Optional) Defines the destination network number.
mask	Specifies the network mask, written as A.B.C.D.
length	Specifies the mask length (1 to 32 characters).

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

This command displays the LDP forwarding entries.

Examples

The following is 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  Chkpt
                       In        Out  Interface
------------------  -----  ---------  ---------  -----------  --  -----  -----
10.22.22.22/32         16    ImpNull  PO0/2/0/0    10.10.2.1   N      N      Y
10.44.44.44/32         17    ImpNull  PO0/1/0/0    10.10.3.2   N      N      Y
```

Related Commands

Command	Description
show mpls forwarding	Displays the MPLS forwarding entries from the MPLS forwarding plane perspective.
show mpls ldp bindings	Displays all the label bindings with the designated entries for forwarding.

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

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

This command displays LDP graceful-restart (GR) related information if LDP GR is enabled on the router.

Examples

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

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

  Forwarding State Hold timer : Running (124 sec remaining)
  Forwarding Entries          : 3 Checkpointed (3 GR, 0 non-GR)
                                0 Stale, 0 without PathUp
  GR Neighbors                : 1

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

Related Commands

Command	Description
graceful-restart	Configures the LDP graceful restart feature.
show mpls ldp neighbor	Displays information about LDP neighbors.

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 number* | **gr** | **non-gr**] [**brief**]

Syntax Description

ip-address	(Optional) Identifies the neighbor with this IP address.
type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
number	(Optional) Either a physical interface number or a virtual interface number: • Physical interface number. Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. • Virtual interface number. Number range will vary depending on interface type. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.
gr	(Optional) Displays graceful restartable neighbors.
non-gr	(Optional) Displays non-graceful restartable neighbors.
brief	(Optional) Displays the existing LDP sessions in brief format.

Defaults

Displays information about all LDP neighbors.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The **show mpls ldp neighbor** command can provide information about all LDP neighbors for the entire routing domain, or the information can be limited to the following:

- LDP neighbors with specific IP address
- LDP neighbors on a specific interface
- LDP neighbors that are graceful restartable
- LDP neighbors that are non-graceful restartable

Examples

The following is sample output from the **show mpls ldp neighbor** command specifying a particular 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:
    POS0/2/0/0
  Addresses bound to this peer:
    10.22.22.22     10.10.2.1
```

The following is sample output from the **show mpls ldp neighbor** command specifying the non-graceful restart filter:

```
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:
    POS0/1/0/0
  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:
    POS0/2/0/0
  Addresses bound to this peer:
    10.22.22.22     10.10.2.1
```

The following is sample output from the **show mpls ldp neighbor brief** command, specifying the brief format:

```
RP/0/RP1/CPU0:router# show mpls ldp neighbor brief

  Peer              GR Up Time          TCP Connection
  ----------------- -- ---------------- -----------------------------------------
  101.101.101.101:0 N  03:56:27         101.101.101.101:646 - 102.102.102.102:65531
  104.104.104.104:0 N  00:34:15         104.104.104.104:65530 - 102.102.102.102:646
  103.103.103.103:0 N  00:34:11         103.103.103.103:65521 - 102.102.102.102:646
```

Related Commands

Command	Description
show mpls ldp discovery	Displays the status of the LDP discovery process.

show mpls ldp parameters

To display current Label Distribution Protocol (LDP) parameters, use the **show mpls ldp parameters** command in EXEC mode.

show mpls ldp parameters

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

This command displays all LDP operational and configuration parameters.

Examples

The following is 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: 10.33.33.33
  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
  Graceful Restart:
    Enabled (Configured),
    Reconnect Timeout: 120 sec, Forwarding State Hold: 180 sec
  Timeouts:
    Binding with unresolved route: 300 sec
    LSD Recovery: 60 sec
    LDP Recovery: 360 sec
```

Related Commands

Command	Description
backoff	Configures the parameters for the LDP backoff mechanism.
discovery	Configures the interval between transmission of LDP discovery messages.
explicit-null	Configures a router to advertise an Explicit Lull label.
graceful-restart	Configures LDP graceful restart capability and its parameters.
holdtime	Configures keepalive message holdtime for LDP sessions.
router-id (MPLS LDP)	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*]

Syntax Description

ip-address	(Optional) Identifies the neighbor with this IP address.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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

Examples

The following is 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
```

Related Commands

Command	Description
clear mpls ldp msg-counters neighbor	Clears MPLS LDP message counter values.
show mpls ldp bindings	Displays the contents of the LIB.
show mpls ldp forwarding	Displays the LDP forwarding state installed in MPLS forwarding.
show mpls ldp parameters	Displays current LDP parameters.

show mpls ldp summary

To display a summary of the Label Distribution Protocol (LDP) related information, use the **show mpls ldp summary** command in EXEC mode.

show mpls ldp summary

Syntax Description

This command has no keywords or arguments.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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

Examples

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

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

 Neighbors: 2 (0 Targeted, 2 Graceful Restartable)
 Known Routes: 11
 Installed forwarding rewrites: 3
 Local addresses: 4
 Known interfaces: 4 (2 LDP enabled)
 Clients: 0
 Servers:
                 Connected  Registered
                 ---------  ----------
     SysDB           Y          Y
     IM              Y          Y
     IP ARM          Y          -
     LSD             Y          Y
     FIBv4           Y          Y
```

Related Commands

Command	Description
show mpls ldp bindings	Displays the contents of the LIB.
show mpls ldp discovery	Displays the status of the LDP discovery process.
show mpls ldp forwarding	Displays the LDP forwarding state installed in MPLS forwarding.
show mpls ldp graceful-restart	Displays the status of the LDP graceful restart.
show mpls ldp parameters	Displays current LDP parameters.

snmp-server enable traps mpls ldp

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

snmp-server enable traps mpls ldp [*notification-type*]

Syntax Description

notification-type	(Optional) Type of notification (Session down, Session up, and Threshold crossed).

Command Modes

Router configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The **snmp-server enable traps mpls ldp** command enables LDP to send notifications to the Simple Network Management Protocol (SNMP) server.

There are three types of traps sent by LDP:

1. Session up trap: Generated when sessions go up.
2. Session down trap: Generated when sessions go down.
3. Threshold trap: Generated when a pre-specified number of attempts to establish a session fails. This predefined value is set to 8.

Examples

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

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

MPLS Traffic Engineering Commands on Cisco IOS-XR Software

This chapter describes the commands used to configure Multiprotocol Label Switching (MPLS) for Cisco IOS-XR software.

Your network must support the following Cisco features before you can enable MPLS traffic engineering:

- MPLS
- IP Cisco Express Forwarding (CEF)
- Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF) routing protocol

MPLS Label Description Protocol (LDP) command descriptions and Universal Control Plane (UCP) command descriptions are documented separately.

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 disable the override, use the **no** form of this command.

admin-weight *weight*

no admin-weight *weight*

Syntax Description

weight	The cost of the link. The range is 0 to 4294967295.

DefaultsDefaults

IGP is the default cost of the link.

Command Modes

MPLS TE interface configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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 interface
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
```

affinity

To configure an affinity (the properties the tunnel requires in its links) for a Multiprotocol Label Switching (MPLS) traffic engineering tunnel, use the **affinity** command in tunnel configuration mode. To disable the affinity, use the **no** form of this command.

affinity [*affinity-value*] **mask** *mask-value*

no affinity [*affinity-value*] **mask** *mask-value*

Syntax Description

affinity-value	(Optional) Attribute values required for links carrying this tunnel. A 32-bit decimal number. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.
mask *mask-value*	Link attribute to be checked. A 32-bit decimal number. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute mask is 0 or 1.

Defaults

affinity-value: 0X00000000

mask-value: 0X0000FFFF

Command Modes

Tunnel configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The affinity determines the attributes of the links that this tunnel will use (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 also be 1 in the mask. In other words, affinity and mask should be set such that:

tunnel_affinity = (tunnel_affinity and tunnel_affinity_mask).

Examples

The following example shows how to set the tunnel affinity:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# affinity 0x0101 mask 0x303
```

Related Commands

Command	Description
attribute-flags	Sets the attributes for the interface.

attribute-flags

To set the user-specified attribute flags for the interface, use the **attribute-flags** command in MPLS TE interface configuration mode. To disable attribute flags for the interface, use the **no** form of this command.

attribute-flags *attributes*

no attribute-flags *attributes*

Syntax Description

attributes	Links attributes that will be compared to the affinity bits of a tunnel during selection of a path. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits) where the value of an attribute is 0 or 1.

DefaultsDefaults

Link attributes are set to 0x0.

Command Modes

MPLS TE interface configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

This 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 is flooded globally so that it can be used as a tunnel head-end path selection criterion.

Examples

The following example shows how to set the 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	Overrides the IGP administrative weight of the link.
affinity	Configures affinity (the properties that the tunnel requires in its links) for an MPLS traffic engineering tunnel.

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 tunnel configuration mode. To specify that the IGP does not use the tunnel in its enhanced SPF calculations, use the **no** form of this command.

autoroute announce

no autoroute announce

Syntax Description

This command has no arguments or keywords.

Defaults

The IGP does not use the tunnel in its enhanced SPF calculation.

Command Modes

Tunnel configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Currently, the only way to forward traffic onto a tunnel is by enabling this feature or by explicitly configuring forwarding (for example, with an interface static route).

Examples

The following example shows how to specify that the IGP should use the tunnel in its enhanced SPF calculation if the tunnel is up:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# autoroute announce
```

Related Commands

Command	Description
route	Establishes static routes.
interface tunnel-te	Sets the mode of a tunnel to MPLS for traffic engineering, and moves the configuration mode into tunnel mode.

autoroute metric

To specify the Multiprotocol Label Switching (MPLS) traffic engineering tunnel metric that the Interior Gateway Protocol (IGP) enhanced Shortest Path First (SPF) calculation uses, use the **autoroute metric** command in tunnel configuration mode. To restore the default value, use the **no** form of this command.

autoroute metric {**absolute** | **relative**} *value*

no autoroute metric {**absolute** | **relative**} *value*

Syntax Description

absolute	Absolute metric mode; you can enter a positive metric value.
relative	Relative metric mode; you can enter a positive, negative, or zero value.
value	The metric that the IGP enhanced SPF calculation uses. The relative value can be from -10 to 10. The absolute value can be from 1 to 4294967295.

Defaults

The default is metric relative 0.

Command Modes

Tunnel configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following example shows how to designate that the IGP enhanced SPF calculation will use MPLS traffic engineering tunnel metric negative 1:

```
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	Instructs the IGP to use the tunnel (if it is up) in its enhanced SPF calculation.
show mpls traffic-eng autoroute	Displays the tunnels announced to the IGP, including interface, destination, and bandwidth.

backup-bw

To configure the backup bandwidth for a Multiprotocol Label Switching (MPLS) traffic engineering backup tunnel (that is used to protect a physical interface), use the **backup-bw** command in tunnel configuration mode. To restore the default value, use the **no** form of this command.

backup-bw {*bandwidth* | **sub-pool** {*bandwidth* | **unlimited**} | **global-pool** {*bandwidth* | **unlimited**}}

no backup-bw {*bandwidth* | **sub-pool** {*bandwidth* | **unlimited**} | **global-pool** {*bandwidth* | **unlimited**}}

Syntax Description

bandwidth	The backup bandwidth in any-pool provided by an MPLS traffic engineering backup tunnel. Bandwidth is specified in kilobits per second (kbps). The range for bandwidth is 1 to 4294967295.
sub-pool *bandwidth*	The backup bandwidth in sub-pool provided by an MPLS traffic engineering backup tunnel. Bandwidth is specified in kilobits per second. The range for bandwidth is 1 to 4294967295. Only label switched paths (LSPs) using bandwidth from the sub-pool can use the backup tunnel.
global-pool *bandwidth*	The backup bandwidth in global pool provided by an MPLS traffic engineering backup tunnel. Bandwidth is specified in kilobits per second. The range for bandwidth is from 1 to 4294967295.
unlimited	Sets unlimited bandwidth.

Defaults

Bandwidth is set to any pool unlimited.

Command Modes

Tunnel configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Backup bandwidth can be limited or unlimited. It can be specific to a global pool, sub-pool, or non-specific any-pool. Note that backup with backup-bw in global-pool can only protect global-pool LSPs and backup-bw in sub-pool can only protect sub-pool LSPs.

Backup tunnels configured with limited backup bandwidth (from any/global/sub pool) will not be assigned to protect LSPs configured with zero signaled bandwidth.

Backup-bw is configured to provide bandwidth protection feature for Fast Reroute (FRR). Bandwidth protection for FRR supports Cisco's proprietary Diff Serv traffic-engineering (two bandwidth pools).

Examples

In the following example, backup tunnel 1 is to be used only by LSPs that take their bandwidth from the global pool. The backup tunnel does not provide bandwidth protection.

Backup tunnel 2 is to be used only by LSPs that take their bandwidth from the sub-pool. Backup tunnel 2 provides bandwidth protection for up to 1000 units.

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# backup-bw global-pool unlimited

RP/0/RP0/CPU0:router(config)# interface tunnel-te 2
RP/0/RP0/CPU0:router(config-if)# backup-bw sub-pool 1000
```

Related Commands

Commands	Description
backup-path tunnel-te	Assigns one or more backup tunnels to a protected interface.
fast-reroute	Configures an LSP to request a protection via backup tunnel.

backup-path tunnel-te

To set a Multiprotocol Label Switching traffic engineering (MPLS TE) tunnel to protect a physical interface against failure, use the **backup-path tunnel-te** command in MPLS TE interface configuration mode. To disable interface protection, use the **no** form of this command.

backup-path tunnel-te *tunnel-number*

no backup-path tunnel-te *tunnel-number*

Syntax Description

tunnel-number	The number of the tunnel that will be protecting the interface. The range is from 0 to 65535.

Command Modes

MPLS TE interface configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

When the protected interface is down (shutdown or removed), the traffic it was carrying (for the other label switched paths [LSPs], referred to as the protected LSPs) is re-routed, using fast reroute (FRR) onto the backup tunnels (those entered in the command).

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 a backup tunnels.
- The backup tunnel must have a terminating-end node in the path of a protected LSP for the backup tunnel to provide protection to the given protected LSP.
- When a second loopback interface is configured, it will be used for the purpose of address substitution. However it must be reachable from the merge-point for the reservation message to be received.
- 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.

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 100
RP/0/RP0/CPU0:router(config-mpls-te-if)# backup-path tunnel 150
```

Related Commands

Command	Description
backup-bw	Configures backup bandwidth for bandwidth protection.
fast-reroute	Makes a tunnel a protected LSP.
show mpls traffic-eng tunnels	Displays tunnel information.

bandwidth (MPLS TE)

To configure the bandwidth required for a Multiprotocol Label Switching (MPLS) traffic engineering tunnel, use the **bandwidth** command in tunnel configuration mode. To restore the default setting, use the **no** form of this command.

bandwidth {*bandwidth* | **sub-pool** *bandwidth*}

no bandwidth {*bandwidth* | **sub-pool** *bandwidth*}

Syntax Description

bandwidth	The bandwidth required for an MPLS traffic engineering tunnel. Bandwidth is specified in kilobits per second. By default bandwidth is reserved in the global pool. The range is from 0 to 4294967295 kbps.
sub-pool *bandwidth*	Reserves the bandwidth in the sub-pool instead of the global pool. The range is from 1 to 4294967295 kbps. Note that sub-pool of 0 is not allowed.

Defaults

Default bandwidth is 0 in the global pool.

Command Modes

Tunnel configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The **bandwidth** command supports two bandwidth pools at present for Cisco's proprietary **Diff Serv Aware Traffic Engineering** feature.

Examples

The following example shows how to set the bandwidth required for an MPLS traffic engineering tunnel to1000 in the global pool:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# bandwidth 1000
```

The following example shows how to set the bandwidth required for an MPLS traffic engineering tunnel to1000 in the sub-pool:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# bandwidth sub-pool 1000
```

Related Commands

Command	Description
show mpls traffic-eng tunnels	Displays tunnel information.

clear mpls traffic-eng counters tunnels

To clear (set to zero) the Multiprotocol Label Switching (MPLS) tunnel signaling counters, use the **clear mpls traffic-eng counters tunnels** command in EXEC mode.

clear mpls traffic-eng counters tunnels {**all** | **name** *name* | **summary**}

Syntax Description

all	Clears counters for all MPLS traffic engineering (MPLS TE) tunnels.
name *name*	Clears counters for MPLS TE tunnel with the specified name.
summary	Clears the counter's summary.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use the **clear mpls traffic-eng counters tunnels** command to set all MPLS counters to zero so that changes can be seen easily.

Examples

The following example shows how to clear all counters:

```
RP/0/RP0/CPU0:router# clear mpls traffic-eng counters tunnels all
```

The following example shows how to clear counters for tunnel 1:

```
RP/0/RP0/CPU0:router# clear mpls traffic-eng counters tunnels name tunnel-te1
```

The following example shows how to clear the counter's summary:

```
RP/0/RP0/CPU0:router# clear mpls traffic-eng counters tunnels summary
```

clear mpls traffic-eng link-management statistics

To clear all the Multiprotocol Label Switching traffic engineering (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 Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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
```

disable (explicit-path)

To prevent the path from being used by Multiprotocol Label Switching traffic engineering (MPLS TE) tunnels while it is configured, use the **disable** command in explicit path configuration mode. To re-enable a previously disabled path, use the **no** form of this command.

disable

no disable

Syntax Description

This command has no arguments or keywords.

Defaults

The explicit path is enabled.

Command Modes

Explicit path configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following example shows how to disable explicit path 200:

```
RP/0/RP0/CPU0:router(config)# explicit-path identifier 200
RP/0/RP0/CPU0:router(config-expl-path)# disable
```

Related Commands

Command	Description
exclude-address	Specifies the next IP address to exclude from the explicit path.
explicit-path	Enters the submode for IP explicit paths and creates or modifies the specified path.
next-address	Specifies the next IP address to include in the explicit path.
show explicit-paths	Displays configured IP explicit paths.

exclude-address

To exclude an address from an IP explicit path, use the **exclude-address** command in explicit path configuration mode. To remove an address exclusion from an IP explicit path, use the **no** form of the **index** command.

exclude-address *ip-address*

no index *index-id*

Syntax Description

ip-address	IP version 4 address.
index-id	Removes the specified address exclusion from an IP explicit path.

Command Modes

Explicit path configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Addresses are not excluded from an IP explicit path unless explicitly excluded by the **exclude-address** command.

You can only use the **exclude-address** command after entering the explicit path configuration mode via the **explicit-path** command.

If you enter the **exclude-address** command and specify the IP address of a link, the constraint-based SPF routine does not consider that link when it sets up MPLS traffic engineering paths. If the excluded address is a flooded MPLS traffic engineering router ID, the constraint-based SPF routine does not consider that entire node. The person performing the configuration must know the router IDs of the routers, because it will not be apparent whether the specified number is for a link or for a node.

MPLS traffic engineering will accept an IP explicit path composed of either all excluded addresses configured by the **exclude-address** command, or all included addresses configured by the **next-address** command, but not a combination of both.

Examples

The following example shows how to exclude IP addresses 192.168.3.2 and 192.168.4.2 from IP explicit path 200:

```
RP/0/RP0/CPU0:router(config)# explicit-path identifier 200
RP/0/RP0/CPU0:router(config-expl-path)# exclude-address 192.168.3.2
RP/0/RP0/CPU0:router(config-expl-path)# exclude-address 192.168.4.2
```

The following example shows how to remove IP address 192.168.3.2 from the excluded addresses for explicit path 200:

```
RP/0/RP0/CPU0:router(config)# explicit-path identifier 200
RP/0/RP0/CPU0:router(config-expl-path)# no index 1
```

Related Commands

Command	Description
explicit-path	Enters the subcommand mode for IP explicit paths and creates or modifies the specified path.
index (explicit path)	Inserts or modifies a path entry at a specified index.
show explicit-paths	Displays configured IP explicit paths.

explicit-path

To enter the command mode for Internet Protocol (IP) explicit paths and create or modify the specified path, use the **explicit-path** configuration command in global configuration mode. To delete the specified explicit path, use the **no** form of this command.

explicit-path {**identifier** *path-number* | **name** *path-name*}

no explicit-path {**identifier** *path-number* | **name** *path-name*}

Syntax Description

identifier *path-number*	Number of the explicit path. The valid values are from 1 to 65535.
name *path-name*	Name of the explicit path.

Command Modes

Global configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path.

Examples

The following example shows how to enter the explicit path subcommand mode for IP explicit paths and create path with the identifier 200:

```
RP/0/RP0/CPU0:router(config)# explicit-path identifier 200
```

The following example shows how to enter the explicit path subcommand mode for IP explicit paths and create a path with the name ToR3:

```
RP/0/RP0/CPU0:router(config)# explicit-path name ToR3
```

fast-reroute

To enable fast-reroute (FRR) protection for a Multiprotocol Label Switching traffic engineering (MPLS TE) tunnel, use the **fast-reroute** command in tunnel configuration mode. To disable FRR protection, use the **no** form of this command.

fast-reroute

no fast-reroute

Syntax Description

This command has no arguments or keywords.

Defaults

Fast-reroute is disabled.

Command Modes

Tunnel configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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 the LSP is traversing that this LSP desires link/node/bandwidth protection.

Examples

The following example shows how to enable FRR on an MPLS traffic engineering tunnel:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# fast-reroute
```

Related Commands

Command	Description
show mpls traffic-eng tunnels	Displays tunnel information.

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 settings, use the **no** form of this command.

flooding thresholds {**down** | **up**} *percent* [*percent* | *percent* | *percent*]

no flooding thresholds {**down** | **up**}

Syntax Description

down	Sets the thresholds for decreased resource availability.
up	Sets the thresholds for increased resource availability.
percent [*percent*]	Bandwidth threshold level. For both down and up, valid values are from 0 to 100.

Defaults

The **down** keyword is set to: 100, 99, 98, 97, 96, 95, 90, 85, 80, 75, 60, 45, 30, 15.

The **up** keyword is set to: 15, 30, 45, 60, 75, 80, 85, 90, 95, 97, 98, 99, 100.

Command Modes

MPLS TE interface configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

When a threshold is crossed, Multiprotocol Label Switching traffic engineering (MPLS TE) link management advertises updated link information. If no thresholds are crossed, changes can be flooded periodically unless periodic flooding was disabled.

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
mpls traffic-eng link-management timers periodic-flooding	Sets the length of the interval used for periodic flooding.
show mpls traffic-eng link-management advertisements	Displays local link information currently being flooded by MPLS traffic engineering link management into the global traffic engineering topology.
show mpls traffic-eng link-management bandwidth-allocation	Displays current local link information.

index (explicit path)

To insert or modify a path entry at a specific index, use the **index** command in explicit path configuration mode. To delete a path entry with a specified index, use the **no** form of this command.

index *index command*

no index *index command*

Syntax Description

index	Index number at which the path entry will be inserted or modified. Valid values are from 1 to 65535.
command	IP explicit path configuration commands (**next-address** and **exclude-address**) that creates or modifies a path entry.

Command Modes

Explicit path configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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(config)# explicit-path identifier 200
RP/0/RP0/CPU0:router(config-expl-path)# index 3 next-address 192.168.3.2
```

The following example shows how to remove the **next-address** 192.168.3.2 inserted in the previous step from explicit path 200:

```
RP/0/RP0/CPU0:router(config)# explicit-path identifier 200
RP/0/RP0/CPU0:router(config-expl-path)# no index 3
```

Related Commands

Command	Description
exclude-address	Specifies the next IP address to exclude from the explicit path.
explicit-path	Enters the subcommand mode for IP explicit paths and creates or modifies the specified path.
next-address	Specifies the next IP address to include in the explicit path.
show explicit-paths	Displays the configured IP explicit paths.

interface tunnel-te

To configure a Multiprotocol Label Switching traffic engineering (MPLS TE) tunnel interface, use the **interface tunnel-te** command in global configuration mode. To disable an MPLS TE tunnel interface, use the **no** form of this command.

interface tunnel-te *tunnel-id*

no interface tunnel-te *tunnel-id*

Syntax Description

tunnel-id	Specifies a tunnel instance. The valid range is from 0 to 65535.

Defaults

Tunnel interfaces are disabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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 use the loopback interface address as the source address of the tunnel.

This command specifies that the tunnel interface is for an MPLS traffic engineering tunnel and enables the various tunnel MPLS configuration options. You must enter this command to configure any of the following command options:

- **affinity**
- **autoroute announce**
- **autoroute metric**
- **backup-bw**
- **bandwidth**
- **fast-reroute**
- **path-option**
- **path-selection**

- **priority**
- **record-route**

Examples

The following example shows how to configure tunnel interface 1:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# ipv4 unnumber loopback0
```

Related Commands

Command	Description
affinity	Configures an affinity for an MPLS traffic engineering tunnel.
autoroute metric	Instructs the IGP to use the tunnel in its enhanced SPF calculation, if the tunnel is in an up state.
backup-bw	Configures backup bandwidth for FRR.
bandwidth (MPLS TE)	Configures the bandwidth required for an MPLS traffic engineering tunnel.
fast-reroute	Configures an FRR on an MPLS traffic engineering tunnel.
path-option	Configures a path option.
path-selection metric	Configures a path selection metric—TE or IGP.
priority (MPLS TE)	Configures setup and reservation priority for an MPLS traffic engineering tunnel.
record route	Configures record-route on an MPLS traffic engineering tunnel.

ipv4 unnumbered (interface)

To specify the Multiprotocol Label Switching traffic engineering (MPLS TE) tunnel Internet Protocol Version 4 (IPv4) address, use the **ipv4 unnumbered** command in tunnel configuration mode. To remove the address, use the **no** form of this command.

ipv4 unnumbered *interface-name*

no ipv4 unnumbered *interface-name*

Syntax Description

interface-name	Name of the interface; loopback is commonly used.

Defaults

No IP address is set.

Command Modes

Tunnel configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The tunnel-te is not signaled until an IP address is configured on the tunnel interface. Hence, the tunnel state will stay down without IP address configuration.

Examples

The following example shows how to designate that MPLS traffic engineering tunnel use the IPv4 address as that of loopback interface 0:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# ipv4 unnumbered loopback0
```

Related Commands

Command	Description
show ipv4 interface	Displays the IPv4 interfaces including the tunnel-te interface.

mpls traffic-eng area

To configure a router running Open Shortest Path First (OSPF) Multiprotocol Label Switching (MPLS) so that it floods traffic engineering for the indicated OSPF area, use the **mpls traffic-eng area** command in router configuration mode. To disable traffic engineering area configuration, use the **no** form of this command.

mpls traffic-eng area {*ospf-area*}

no mpls traffic-eng area {*ospf-area*}

Syntax Description

ospf-area	OSPF area on which MPLS traffic engineering is enabled.

Defaults

Traffic engineering area configuration is disabled.

Command Modes

Router configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

This command is in the routing protocol configuration tree and is supported for OSPF. The command affects the operation of MPLS traffic engineering only if MPLS traffic engineering is enabled for that routing protocol instance. Currently, only a single area can be enabled for traffic engineering.

Examples

The following example shows how to configure a router running OSPF MPLS to flood traffic engineering for OSPF area 0:

```
RP/0/RP0/CPU0:router(config)# router ospf 1
RP/0/RP0/CPU0:router(config-router)# mpls traffic-eng area 0
```

Related Commands

Command	Description
mpls traffic-eng router-id	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.
router ospf	Configures an OSPF routing process on a router.

mpls traffic-eng fast-reroute timers promotion

To specify how often the router considers switching a protected Multiprotocol Label Switching traffic engineering (MPLS TE) tunnel to a new backup tunnel if additional backup-bandwidth or a better backup tunnel becomes available, use the **mpls traffic-eng fast-reroute timers promotion** command in global configuration mode. To set the timer to the default value, use the **no** form of this command.

mpls traffic-eng fast-reroute timers promotion {*interval*}

no mpls traffic-eng 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. Valid values are from 0 to 604800. A value of 0 disables backup tunnel promotions. The default is 300.

Defaults

The timer is running and is set to a frequency of every 300 seconds (5 minutes).

Command Modes

Global configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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/assignment. Also, 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 this timer, set the timer value to zero.

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(config)# mpls traffic-eng fast-reroute timers promotion 600
```

mpls traffic-eng interface

To enter the Multiprotocol Label Switching traffic engineering (MPLS TE) interface mode, use the **mpls traffic-eng interface** command in EXEC mode.

mpls traffic-eng interface

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Configuring MPLS TE properties of physical interfaces is done in the MPLS TE interface mode. By entering this mode for a specific interface, this interface is made as MPLS TE link. See the example below on how to enter this mode.

Entering this mode will enable MPLS TE tunnel signaling on an interface (assuming that it is enabled on the device). Remove the interface to remove it from the MPLS TE domain.

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
```

mpls traffic-eng level

To configure a router running Intermediate System-to-Intermediate System (IS-IS) Multiprotocol Label Switching (MPLS) so that it floods traffic engineering for the indicated IS-IS level, use the **mpls traffic-eng level** command in router configuration mode. To disable traffic engineering area configuration, 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 on which MPLS traffic engineering is enabled.

Defaults

Traffic engineering level configuration is disabled.

Command Modes

Router configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

This command is in the routing protocol configuration tree and is supported for IS-IS. The command affects the operation of MPLS traffic engineering only if MPLS traffic engineering is enabled for that routing protocol instance. Currently, only a single level can be enabled for traffic engineering.

Examples

The following example shows how to configure a router running IS-IS MPLS to flood traffic engineering for IS-IS level 1:

```
RP/0/RP0/CPU0:router(config)# router isis 1
RP/0/RP0/CPU0:router(config-router)# mpls traffic-eng level 1
```

Related Commands

Command	Description
mpls traffic-eng router-id	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.
router isis	Configures an ISIS routing process on a router.

mpls traffic-eng link-management flood

To initiate an immediate flooding of all the local Multiprotocol Label Switching traffic engineering (MPLS TE) links, use the **mpls traffic-eng link-management flood** command in EXEC mode.

mpls traffic-eng link-management flood

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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
```

mpls traffic-eng 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 **mpls traffic-eng link-management timers bandwidth-hold** command in global configuration mode. To delete this setting, use the **no** form of this command.

mpls traffic-eng link-management timers bandwidth-hold *holdtime*

no mpls traffic-eng link-management timers bandwidth-hold *holdtime*

Syntax Description

holdtime	Length of time (in seconds) that bandwidth can be held. Valid values are from 1 to 300. The default is 15.

Defaults

Holdtime is set to 15 seconds.

Command Modes

Global configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

This command determines the amount of time allowed for an RSVP message to return from a neighbor RSVP node.

Examples

The following example shows how to set the bandwidth to be held for 10 seconds:

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng link-management timers bandwidth-hold 10
```

Related Commands

Command	Description
show mpls traffic-eng link-management bandwidth-allocation	Displays current local link information and bandwidth holdtime.

mpls traffic-eng link-management timers periodic-flooding

To set the length of the interval for periodic flooding, use the **mpls traffic-eng link-management timers periodic-flooding** command in global configuration mode. To disable periodic flooding, use the **no** form of this command.

mpls traffic-eng link-management timers periodic-flooding *interval*

no mpls traffic-eng link-management timers periodic-flooding

Syntax Description

interval	Length of the interval (in seconds) for periodic flooding. Valid values are from 0 to 3600. A value of 0 turns off periodic flooding. If you set this value from 1 to 29, it is treated as 30.

Defaults

Interval: 180 seconds (3 minutes).

Command Modes

Global configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command to advertise link state information changes that do not trigger immediate action, such as a change to the amount of allocated bandwidth that does not cross a threshold.

Examples

The following example shows how to set the interval length for periodic flooding to 120 seconds:

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng link-management timers periodic-flooding
120
```

Related Commands

Command	Description
flooding thresholds	Sets the reserved bandwidth flooding thresholds for a link.
show mpls traffic-eng link-management summary	Displays the current periodic flooding interval.

mpls traffic-eng maximum tunnels

To specify the maximum value for the number of Multiprotocol Label Switching traffic engineering (MPLS TE) tunnels that can be configured, use the **mpls traffic-eng maximum tunnels** command in global configuration mode. To return the router to its default behavior, use the **no** form of the command.

mpls traffic-eng maximum tunnels {*tunnel-limit*}

no mpls traffic-eng maximum tunnels {*tunnel-limit*}

Syntax Description

tunnel-limit	Maximum number of tunnel TE interfaces that be configured. Valid values are from 0 to 4096.

Defaults

2500

Command Modes

Global configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following example shows how to set the maximum number of tunnel-te configuration limit to 3000 overwriting default:

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng maximum tunnels 3000
```

Related Commands

Command	Description
show mpls traffic-eng maximum tunnels	Displays the configuration of the maximum tunnel-te interfaces allowed.

mpls traffic-eng path-selection metric

To specify the Multiprotocol Label Switching traffic engineering (MPLS TE) tunnel path-selection metric, use the **mpls traffic-eng path-selection metric** command in global configuration mode. To return the router to its default behavior, use the **no** form of the command.

mpls traffic-eng path-selection metric {**igp** | **te**}

no mpls traffic-eng path-selection metric {**igp** | **te**}

Syntax Description

igp	Uses an Interior Gateway Protocol (IGP) metric.
te	Uses a traffic engineering (TE) metric. This is the default.

Defaults

The TE path selection metric is used.

Command Modes

Global configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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.
- If the **mpls traffic-eng path-selection metric** command was entered to specify a metric type, use that metric type.
- Otherwise, use the default (TE) metric.

Examples

The following example shows how to set the path-selection metric to use the IGP metric overwriting default:

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng path-selection metric igp
```

mpls traffic-eng reoptimize (configuration)

To control the frequency with which tunnels with established label switched paths (LSPs) are checked for better paths, use the **mpls traffic-eng reoptimize** command in global configuration mode. To restore the default value, use the **no** form of this command.

mpls traffic-eng reoptimize *reoptimization-time*

no mpls traffic-eng reoptimize *reoptimization-time*

Syntax Description

reoptimization-time	Sets the reoptimization time in seconds. A value of 0 disables reoptimization. Valid values are from 0 to 604800. The default is 3600.

Defaults

3600 seconds (1 hour)

Command Modes

Global configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

A device with traffic engineering tunnels periodically examines tunnels with established LSPs to learn if better LSPs are available. If a better LSP appears available, the device attempts to signal the better LSP. If the signaling is successful, the device replaces the old, inferior LSP with the new, better LSP.

Examples

The following example shows how to set the reoptimization time to 1 day:

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng reoptimize 86400
```

Related Commands

Command	Description
mpls traffic-eng reoptimize (EXEC)	Reoptimizes all traffic engineering tunnels immediately.

mpls traffic-eng reoptimize (EXEC)

To force immediate reoptimization of all traffic engineering tunnels, use the **mpls traffic-eng reoptimize** command in EXEC mode.

mpls traffic-eng reoptimize [*tunnel-name*]

Syntax Description

tunnel-name	(Optional) Name of the tunnel to be reoptimized. If no tunnel name is specified, all tunnels will be reoptimized.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following example shows how to immediately reoptimize all traffic engineering tunnels reoptimized:

```
RP/0/RP0/CPU0:router# mpls traffic-eng reoptimize
```

The following example shows how to immediately reoptimize traffic engineering tunnel-te90:

```
RP/0/RP0/CPU0:router# mpls traffic-eng reoptimize tunnel-te90
```

Related Commands

Command	Description
mpls traffic-eng reoptimize (configuration)	Controls the frequency of traffic engineering tunnel reoptimization.

mpls traffic-eng reoptimize timers delay

To delay removal or relabeling of the old label switched paths (LSPs) (reoptimized LSP from the forwarding plane) after tunnel reoptimization, use the **mpls traffic-eng reoptimize timers delay** command in global configuration mode. To restore the default value, use the **no** form of this command.

mpls traffic-eng reoptimize timers delay {**cleanup** | **installation**} *delay-time*

no mpls traffic-eng reoptimize timers delay cleanup *delay-time*

Syntax Description

cleanup	Delays removal of the old LSPs after tunnel reoptimization.
installation	Delays installation of a new label after tunnel reoptimization.
delay-time	Sets the reoptimization delay time in seconds. A value of 0 disables delay. The valid range is from 0 to 300 seconds for cleanup time, and 0 to 3600 seconds for installation time.

Defaults

Cleanup delay time is set for 20 seconds, and installation delay time is set for 10 seconds.

Command Modes

Global configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

A device with Multiprotocol Label Switching traffic engineering (MPLS TE) tunnels periodically examines tunnels with established LSPs to discover if 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 head-end node replaces the labels quickly, it can result in brief packet loss. By delaying the cleanup of the old LSP using the **mpls traffic-eng reoptimize timers delay cleanup** command, packet loss is avoided.

Examples

The following example shows how to set the reoptimization cleanup delay time to 1 minute:

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng reoptimize timer delay cleanup 60
```

The following example shows how to set the reoptimization installation delay time to 1 hour:

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng reoptimize delay installation 3600
```

Related Commands

Command	Description
mpls traffic-eng reoptimize (configuration)	Controls the frequency of traffic engineering tunnel reoptimization.
mpls traffic-eng reoptimize (EXEC)	Reoptimizes all traffic engineering tunnels immediately.

mpls traffic-eng router-id

To specify that the traffic engineering router identifier for the node is the IP address associated with a given interface, use the **mpls traffic-eng router-id** command in router configuration mode. To disable this feature, use the **no** form of this command.

mpls traffic-eng router-id *interface-name*

mpls traffic-eng no router-id *interface-name*

Syntax Description

interface-name	Interface whose primary IP address is the router's identifier.

Command Modes

Router configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

This router's identifier acts as a stable IP address for the traffic engineering configuration. This IP address is flooded to all nodes. For all traffic engineering tunnels originating at other nodes and ending at this node, you must set the tunnel destination to the destination node's traffic engineering router identifier. This router ID is the address that the traffic engineering topology database at the tunnel head uses for its path calculation.

Examples

The following example shows how to specify the traffic engineering router identifier as the IP address associated with loopback interface:

```
RP/0/RP0/CPU0:Router(config)# router ospf 1
RP/0/RP0/CPU0:Router(config-router)# mpls traffic-eng router-id Loopback0
```

Related Commands

Command	Description
mpls traffic-eng area	Configures a router running OSPF MPLS so that it floods traffic engineering for the indicated OSPF area.
mpls traffic-eng level	Configures a router running OSPF MPLS so that it floods traffic engineering for the indicated IS-IS level.

mpls traffic-eng signalling advertise explicit-null

To specify that tunnels originating from a router use explicit-null labels, use the **mpls traffic-eng signalling advertise explicit-null** command in global configuration mode. To revert to the default behavior of using implicit-null labels, use the **no** form of this command.

mpls traffic-eng signalling advertise explicit-null

no mpls traffic-eng signalling advertise explicit-null

Syntax Description

This command has no arguments or keywords.

Defaults

Implicit-null labels are used.

Command Modes

Global configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command to specify that tunnels originating from a router use explicit-null labels. This command applies to tunnels when this router is a 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).

Examples

The following example shows how to configure the router to use explicit null on the tunnels:

```
RP/0/RP0/CPU0:Router(config)# mpls traffic-eng signalling advertise explicit-null
```

mpls traffic-eng topology holddown sigerr

To specify the amount of time that a router should ignore a link in its traffic engineering topology database in tunnel path Constrained Shortest Path First (CSPF) computations following a traffic engineering tunnel error on the link, use the **mpls traffic-eng topology holddown sigerr** command in global configuration mode. To disable this setting, use the **no** form of this command.

mpls traffic-eng topology holddown sigerr *seconds*

no mpls traffic-eng topology holddown sigerr *seconds*

Syntax Description

seconds	Specifies how long (in seconds) a router should ignore a link during tunnel path calculations, following a traffic engineering tunnel error on the link. The value can be from 0 to 300. The default is 10.

Defaults

Tunnel path calculations ignore a link on which there is a traffic engineering error until either 10 seconds have elapsed or a topology update is received from the Interior Gateway Protocol (IGP).

Command Modes

Global configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

A router that is at the headend for traffic engineering tunnels might receive a Resource Reservation Protocol (RSVP) No Route error message for an existing tunnel or for one being signaled due to the failure of a link the tunnel traverses before the router receives a topology update from the IGP routing protocol announcing that the link is down. In such a case, 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. You can use the **mpls traffic-eng topology holddown sigerr** command to change the link holddown time from its 10-second default value.

Examples

The following example shows how to set the link holddown time for signaling errors at 15 seconds:

```
RP/0/RP0/CPU0:Router(config)# mpls traffic-eng topology holddown sigerr 15
```

Related Commands

Command	Description
show mpls traffic-eng topology	Displays the MPLS TE global topology as currently known at this node, and displays the current signaling error holddown time.

next-address

To include the next address in an IP explicit path, use the **next-address** command in explicit path configuration mode. To remove an included address from an IP explicit path, use the **no** form of the **index** command.

next-address *ip-address*

no index *index-id*

Syntax Description

ip-address	Internet Protocol Version 4 (IPv4) address.
index-id	Removes the specified address exclusion from an IP explicit path.

Command Modes

Explicit path configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

You can only use the **next-address** command after entering explicit path configuration mode via the **explicit-path** command.

Addresses are not included in an IP explicit path unless they are included in the **next-address** command.

Examples

The following example shows how to include IP addresses 192.168.1.2 and 192.168.2.2 from IP explicit path 200:

```
RP/0/RP0/CPU0/router(config)# explicit-path identifier 200
RP/0/RP0/CPU0/router(config-expl-path)# next-address 192.168.1.2
RP/0/RP0/CPU0/router(config-expl-path)# next-address 192.168.2.2
```

The following example shows how to remove IP address 192.168.2.2 from the included addresses for explicit path 200:

```
RP/0/RP0/CPU0:router(config)# explicit-path identifier 200
RP/0/RP0/CPU0:router(config-expl-path)# no index 2
```

Related Commands

Command	Description
explicit-path	Enters the subcommand mode for IP explicit paths and creates or modifies the specified path.
index (explicit path)	Inserts or modifies a path entry at a specified index.
show explicit-paths	Displays configured IP explicit paths.

path-option

To configure a path option for a Multiprotocol Label Switching traffic engineering (MPLS TE) tunnel, use the **path-option** command in tunnel configuration mode. To disable this configuration, use the **no** form of this command.

path-option *number* {**dynamic** | **explicit** {*name-pathname* | *path-number*}} [**lockdown**]

no path-option *number* {**dynamic** | **explicit** {*name-pathname* | *path-number*}} [**lockdown**]

Syntax Description

number	Path option number. When multiple path options are configured, lower numbered options are preferred. The range is from 1 to 1000.
dynamic	Label switched path (LSP) is dynamically calculated.
explicit	LSP path is an IP explicit path.
name-pathname	Path name of the IP explicit path that the tunnel uses with this option.
path-number	Path number of the IP explicit path that the tunnel uses with this option.
lockdown	(Optional) The LSP cannot be reoptimized.

Command Modes

Tunnel configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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 setup a tunnel automatically (unless the lockdown option is used).

Examples

The following example shows how to configure the tunnel to use a named IP explicit path:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# path-option 1 explicit name test
```

Related Commands

Command	Description
explicit-path	Enters the subcommand mode for IP explicit paths, and creates or modifies the specified path.
show explicit-paths	Displays the configured IP explicit paths.

path-selection metric

To specify the Multiprotocol Label Switching traffic engineering (MPLS TE) tunnel path-selection metric type, use the **path-selection metric** command in tunnel configuration mode. To disable this configuration, use the **no** form of this command.

path-selection metric {**igp** | **te**}

no path-selection metric {**igp** | **te**}

Syntax Description

igp	Uses Interior Gateway Protocol (IGP) metrics.
te	Uses traffic engineering (TE) metrics. This is the default.

Defaults

The default is use TE metric.

Command Modes

Tunnel configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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.
- If the **mpls traffic-eng path-selection metric** command was entered to specify a metric type, use that metric type.
- Otherwise, use the default (TE) metric.

Examples

The following example shows how to designate that the MPLS traffic engineering tunnel use the IGP metric for path selection:

```
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	Displays the tunnel path used.

priority (MPLS TE)

To configure the setup and reservation priority for a Multiprotocol Label Switching traffic engineering (MPLS TE) tunnel, use the **priority** command in tunnel configuration mode. To disable this configuration, use the **no** form of this command.

priority *setup-priority hold-priority*

no priority *setup-priority hold-priority*

Syntax Description

setup-priority	The priority used when signaling a label switched path (LSP) for this tunnel to determine which existing tunnels can be preempted. Valid values are from 0 to 7, where 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	The priority associated with an LSP for this tunnel to determine if it should be preempted by other LSPs that are being signaled. Valid values are from 0 to 7, where a lower number indicates a higher priority.

Defaults

Setup-priority: 7

Hold-priority: The same value as the setup-priority

Command Modes

Tunnel configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

When an LSP is signaled and an interface does not currently have enough bandwidth available for that LSP, the call admission software preempts lower-priority LSPs (if necessary) so that the new LSP can be admitted.

In the determination described, the new LSP priority is its setup priority and the existing LSP priority is its 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 better (numerically smaller) than the hold priority.

Examples

The following example shows how to configure a tunnel with a setup and hold priority of 1.

```
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	Sets the mode of a tunnel to MPLS for traffic engineering, and enters tunnel configuration mode.

record route

To record the route used by a tunnel, use the **record route** command in tunnel configuration mode. To not record the route, use the **no** form of this command.

record route

no record route

Syntax Description

This command has no arguments or keywords.

Defaults

Record route is disabled by default.

Command Modes

Tunnel configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following example shows how to enable record-route on the traffic engineering (TE) tunnel.

```
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	Displays the hops traversed by the tunnel.

show explicit-paths

To display the configured IP explicit paths, use the **show explicit-paths** command in EXEC mode. An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path.

show explicit-paths [*path-name* | *identifier-number*]

Syntax Description

path-name	(Optional) Name of the explicit path.
identifier-number	(Optional) Number of the explicit path. Valid values are from 1 to 65535.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following is sample output from the **show explicit-paths** command:

```
RP/0/RP0/CPU0:router# show explicit-paths
Path ToR2    status enabled
        1:  next-address 192.168.1.2
        2:  next-address 10.20.20.20
Path ToR3    status enabled
        1:  next-address 192.168.1.2
        2:  next-address 192.168.2.2
        3:  next-address 10.30.30.30
Path 100    status enabled
        1:  next-address 192.168.1.2
        2:  next-address 10.20.20.20
Path 200    status enabled
        1:  next-address 192.168.1.2
        2:  next-address 192.168.2.2
        3:  next-address 10.30.30.30
```

The following is sample output from the **show explicit-paths** command with a path name specified:

```
RP/0/RP0/CPU0:router# show explicit-paths name ToR3
Path ToR3    status enabled
        1:  next-address 192.168.1.2
        2:  next-address 192.168.2.2
        3:  next-address 10.30.30.30
```

The following is sample output from the **show explicit-paths** command with a path number specified:

```
RP/0/RP0/CPU0:router# show explicit-paths identifier 200
Path 200    status enabled
        1:  next-address 192.168.1.2
        2:  next-address 192.168.2.2
        3:  next-address 10.30.30.30
```

Related Commands

Command	Description
explicit-path	Enters the command mode for IP explicit paths so that you can create or modify the named path.
index (explicit path)	Inserts or modifies a path entry at a specific index.
next-address	Specifies the next IP address in the explicit path.

show mpls traffic-eng autoroute

To display tunnels that are announced to the Interior Gateway Protocol (IGP), including information about nexthop and destinations, use the **show mpls traffic-eng autoroute** command in EXEC mode.

show mpls traffic-eng autoroute

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The enhanced shortest path first (SPF) calculation of the IGP has been modified so that it uses traffic engineering tunnels. This command displays which tunnels IGP is currently using in its enhanced SPF calculation (that is, which tunnels are up and have autoroute configured).

Examples

The following is sample output from the **show mpls traffic-eng autoroute** command. Tunnels are organized by destination. All tunnels to a destination carry a share of the traffic tunneled to that destination:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng autoroute

  Destination 10.10.10.10 has 1 tunnels
    tunnel160 (traffic share 10000, nexthop 10.10.10.10 , relative metric 2)
```

Related Commands

Command	Description
autoroute metric	Specifies the MPLS traffic engineering tunnel metric that the IGP-enhanced SPF calculation will use.
mpls traffic-eng topology holddown sigerr	Causes the IGP to use the tunnel (if it is up) in its enhanced SPF calculation.
show mpls traffic-eng tunnels	Displays information about tunnels.

show mpls traffic-eng counters tunnel

To display tunnel signaling statistics, use the **show mpls traffic-eng counters tunnel** command in EXEC mode.

show mpls traffic-eng counters tunnel {**all** | **name** | **summary**}

Syntax Description

all	Displays all tunnels.
name	Displays a specific tunnel.
summary	Displays a summary of signaling statistics.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following is sample output from the **show mpls traffic-eng counters tunnel** command, which displays tunnel signaling statistics for all tunnels:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng counters tunnel all

Tunnel Head: tunnel160
Match Resv Create:       5  Sender Create:       4  Path Error:        0
Match Resv Change:       0  Sender Modify:       1  Path Change:       0
Match Resv Delete:       3  Sender Delete:       3  Path Delete:       1
Total:                  21  Unknown:             4

Tunnel Head: tunnel170
Match Resv Create:       0  Sender Create:       0  Path Error:        0
Match Resv Change:       0  Sender Modify:       0  Path Change:       0
Match Resv Delete:       0  Sender Delete:       0  Path Delete:       0
Total:                   0  Unknown:             0
```

Related Commands

Command	Description
clear mpls traffic-eng counters tunnels	Clears the counters for MPLS TE tunnels.

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 [**interface** *type number*]

Syntax Description

interface	(Optional) Displays information on the specified interface.
type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
number	(Optional) Either a physical interface number or a virtual interface number: • Physical interface number. Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. • Virtual interface number. Number range will vary depending on interface type. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following is sample output from the **show mpls traffic-eng forwarding** command for a specific interface:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng forwarding interface pos 0/7/0/1

  System Information::
      Tunnels Count     : 3
      Tunnels Selected  : 3

TUNNEL ID              UP IF      DOWN IF      LOC_LBL  OUT_LBL  Backup
---------------------- ---------- ------------ -------- -------- ----------
10.20.20.20 1_1407     -          POS0/7/0/1   0        3        -
10.20.20.20 333_1385   -          POS0/7/0/1   0        3        -
10.20.20.20 777_1378   -          POS0/7/0/1   0        3        -
```

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 number*]

Syntax Description

interface	(Optional) Displays information on the specified interface.
type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
number	(Optional) Either a physical interface number or a virtual interface number: • Physical interface number. Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. • Virtual interface number. Number range will vary depending on interface type. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following is 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

  System Information::
      Tunnels Count     : 3
      Tunnels Selected  : 3
  Bandwidth descriptor legend:
    G = global pool, S = subpool, R = bw locked, H = bw held

TUNNEL ID                UP IF      DOWN IF    PRI STATE          BW (kbps)
------------------------ ---------- ---------- --- -------------- ----------
10.20.20.20 1_1407       -          PO0/7/0/1  7/7 Resv Admitted  2000      RG
10.20.20.20 333_1385     -          PO0/7/0/1  4/4 Resv Admitted  1000      RG
10.20.20.20 777_1378     -          PO0/7/0/1  7/7 Resv Admitted  0          G
```

show mpls traffic-eng link-management advertisements

To display local link information that Multiprotocol Label Switching traffic engineering (MPLS TE) link management is currently flooding into the global traffic engineering 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 Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following is sample output from the **show mpls traffic-eng link-management advertisements** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng link-management advertisements

Flooding Status : ready
Last Flooding : 63 seconds ago
Last Flooding Trigger : TE Link came Up
Next Periodic Flooding In : 111 seconds
Configured Areas : 1
IGP Area[1]:: ospf area 0
Flooding Protocol : OSPF
IGP System ID : 10.20.20.20
MPLS TE Router ID : 10.20.20.20
Flooded Links : 1
Link ID:: 0 (POS0/7/0/1)
Link IP Address : 10.15.12.1
Neighbor : ID 10.90.90.90, IP 10.15.12.2
SRLGs :
TE Metric : 1
IGP Metric : 1
Physical BW : 155520 kbits/sec
Res Global BW : 100000 kbits/sec
Res Sub BW : 0 kbits/sec
Downstream::
Global Pool Sub Pool
----------- -----------
Reservable BW[0]: 1000000 0 kbits/sec
Reservable BW[1]: 1000000 0 kbits/sec
Reservable BW[2]: 1000000 0 kbits/sec
Reservable BW[3]: 1000000 0 kbits/sec
```

```
Reservable BW[4]: 1000000 0 kbits/sec
Reservable BW[5]: 1000000 0 kbits/sec
Reservable BW[6]: 1000000 0 kbits/sec
Reservable BW[7]: 998000 0 kbits/sec
Attribute Flags: 0x00000000
```

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 number*]

Syntax Description

interface	(Optional) Displays information on the specified interface.
type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
number	(Optional) Either a physical interface number or a virtual interface number: • Physical interface number. Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. • Virtual interface number. Number range will vary depending on interface type. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Advertised and current information might differ depending on how flooding is configured.

Examples

The following is 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
0/7/0/1

  System Information::
      Links Count         : 2
      Bandwidth Hold time : 15 seconds

  Link ID:: POS0/7/0/1 (15.15.12.1)
    Link Status:
      Link Label Type     : PSC
      Physical BW         : 155520 kbits/sec
      Max Res Global BW   : 1000000 kbits/sec (reserved: 0% in, 0% out)
      Max Res Sub BW      : 0 kbits/sec (reserved: 100% in, 100% 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  : 1
BW Descriptors      : 2 (including 0 Sub Pool descriptors)
Admin Weight        : 1 (IGP)
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 Global Pool (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       1000            1000
              4          0             0          0            1000
              5          0             0          0            1000
              6          0             0          0            1000
              7          0             0       2000            3000

  Downstream Sub Pool (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          0               0
```

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* | *ip-address*]

Syntax Description

igp-id	(Optional) Displays the IGP neighbors that are using a specified IGP identification.
isis *isis-address*	(Optional) Displays the specified Intermediate System-to-Intermediate System (IS-IS) neighbor when neighbors are displayed by IGP ID.
ospf *ospf-id*	(Optional) Displays the specified Open Shortest Path first (OSPF) neighbor when neighbors are displayed by IGP ID.
ip-address	(Optional) Displays the IGP neighbors that are using a specified IGP IP address.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following is 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)
```

show mpls traffic-eng link-management interface

To display interface resource or a summary of link management information, use the **show mpls traffic-eng link-management interface** command in EXEC mode.

show mpls traffic-eng link-management interface [*type number*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
number	(Optional) Either a physical interface number or a virtual interface number: • Physical interface number. Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. • Virtual interface number. Number range will vary depending on interface type. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.

Defaults

Displays resource and configuration information for all MPLS TE configured interfaces.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following is 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 0/7/0/1

  System Information::
      Links Count         : 2

  Link ID:: POS0/7/0/1 (15.15.12.1)
    Link Status:
      Link Label Type     : PSC
      Physical BW         : 155520 kbits/sec
      Max Res Global BW   : 1000000 kbits/sec (reserved: 0% in, 0% out)
      Max Res Sub BW      : 0 kbits/sec (reserved: 100% in, 100% 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  : 1
Admin Weight        : 1 (IGP)
Neighbors           :
                      ID 10.90.90.90, IP 10.15.12.2 (Up)
Flooding Status: (1 area)
  IGP Area[1]: ospf   area 0, flooded
```

show mpls traffic-eng link-management statistics

To display interface resource 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 number*]

Syntax Description

statistics	(Optional) Displays statistics on link management.
summary	(Optional) Shows the summary of the statistics.
interface	(Optional) Name of interface for which information is requested.
type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
number	(Optional) Either a physical interface number or a virtual interface number: • Physical interface number. Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. • Virtual interface number. Number range will vary depending on interface type. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.

Defaults

Displays resource and configuration information for all configured interfaces.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following is 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
```

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 [**interface** *type number*]

Syntax Description

interface	(Optional) Name of interface for which information is requested.
type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
number	(Optional) Either a physical interface number or a virtual interface number: • Physical interface number. Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. • Virtual interface number. Number range will vary depending on interface type. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following is sample output from the **show mpls traffic-eng link-management summary** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng link-management summary interface pos 0/7/0/1

  System Information::
      Links Count         : 2
      Flooding System     : enabled
      IGP Areas Count     : 1

  IGP Areas
  ----------

  IGP Area[1]:: ospf   area 0
      Flooding Protocol   : OSPF
      Flooding Status     : flooded
      Periodic Flooding   : enabled (every 3000 seconds)
      Flooded Links       : 1
      IGP System ID       : 10.20.20.20
```

```
    MPLS TE Router ID   : 10.20.20.20
    IGP Neighbors       : 1


Link ID:: POS0/7/0/1 (10.15.12.1)
  Link Status:
    Link Label Type     : PSC
    Physical BW         : 155520 kbits/sec
    Max Res Global BW   : 1000000 kbits/sec (reserved: 0% in, 0% out)
    Max Res Sub BW      : 0 kbits/sec (reserved: 100% in, 100% 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  : 1
```

show mpls traffic-eng maximum tunnels

To display the maximum number of Multiprotocol Label Switching traffic engineering (MPLS TE) tunnels that can be configured, use the **show mpls traffic-eng maximum tunnels** command in EXEC mode.

show mpls traffic-eng maximum tunnels

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following is sample output from the **show mpls traffic-eng maximum tunnels** command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng maximum tunnels

Current Max    Absolute Max     Current Count
-----------    ------------     -------------
       2500            4096                20
```

Related Commands

Command	Description
mpls traffic-eng maximum tunnels	Specifies the maximum number of tunnel TE interfaces that can be configured.

show mpls traffic-eng topology

To display the Multiprotocol Label Switching (MPLS) traffic engineering network topology currently known at this node, use the **show mpls traffic-eng topology** command in EXEC mode.

show mpls traffic-eng topology [**path destination** *ip-address*] | **isis** *nsap-address* | **ospf** *ospf-address*] [**brief**]

Syntax Description

path destination	(Optional) Displays path of a tunnel or a destination from this router.
ip-address	(Optional) Node IP address (router identifier to interface address).
isis *nsap-address*	(Optional) Node router identification, if Intermediate System-to-Intermediate System (IS-IS) is enabled.
ospf *ospf-address*	(Optional) Node router identifier, if Open Shortest Path First (OSPF) is enabled.
brief	(Optional) Brief form of the output; gives a less detailed version of the topology.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following is sample output from the **show mpls traffic-eng topology** command specifying the IP address in brief form:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng topology path tunnel 160 brief

Tunnel160 Path Setup to 10.10.10.10: FULL_PATH
bw 100 (Global), 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 is sample output from the **show mpls traffic-eng topology** command specifying the 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 (Global), 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
```

Related Commands

Command	Description
show mpls traffic-eng tunnels	Displays information about tunnels.

show mpls traffic-eng tunnels

To display information about tunnels, use the **show mpls traffic-eng tunnels** command in EXEC mode.

show mpls traffic-eng tunnels [**backup** [**name** *tunnel-name* | **promotion-timer** *promotion-timer* | **protected-interface** | **topology**]] [**brief**] [**destination** *destination-address*] [**down**] [**interface** [**in** | **out** | **inout**] *interface-id*]] [**name** *tunnel-name*] [**property** [**backup-tunnel** | **fast-reroute**]] [**protection**] [**roll** [**all** | **head** | **tail**]] [**source** *source-address*] [**suboptimal constraints** [**current** | **max** | **none**]] [**summary** | **up**]

Syntax Description

backup	(Optional) Displays fast-reroute backup tunnels information. The information includes the physical interface protected by the tunnel, the number of traffic engineering label switched paths (TE LSPs) protected, and the bandwidth protected.
name *tunnel-name*	(Optional) Displays the name of the tunnel to be shown.
promotion-timer	(Optional) Displays the configured fast-reroute (FRR) backup tunnel promotion timer value in seconds.
protected-interface	(Optional) Displays FRR protected interfaces.
topology	(Optional) Displays FRR topology.
brief	(Optional) Brief form of command.
destination *destination-address*	(Optional) Restricts the display to tunnels destined to the specified IP address.
down	(Optional) Displays tunnels that are down.
interface in *interface-id*	(Optional) Displays tunnels that use the specified input interface.
interface out *interface-id*	(Optional) Displays tunnels that use the specified output interface.
interface inout *interface-id*	(Optional) Displays tunnels that use the specified interface as an input or output interface.
name *tunnel-name*	(Optional) Displays tunnels of the specified name.
property backup-tunnel	(Optional) Displays tunnels with property of backup tunnel. Selects Multiprotocol Label Switching traffic engineering (MPLS TE) tunnels being 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.
role all	(Optional) Displays all tunnels.
role head	(Optional) Displays tunnels with their heads at this router.
role tail	(Optional) Displays tunnels with their tails at this router.

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. Selected tunnels would have a shorter path if they were reoptimized immediately.
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 considering only the network capacity. Selected tunnels would have a shorter path if no other tunnels were consuming network resources.
suboptimal constraints none	(Optional) Displays tunnels whose path metric is greater than the shortest unconstrained path. Selected tunnels have a longer path than the Interior Gateway Protocol (IGPs) shortest path.
summary	(Optional) Displays summary of configured tunnels.
up	(Optional) Displays tunnels if the tunnel interface is up. Tunnel router points and tails are typically up or not present.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use the **brief** form of this command to display information specific to a tunnel interface. Use the command form without the **brief** keyword to display information including the destination address, source ID, role, name, suboptimal constraints, and interface.

Examples

The following is 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
                     RSVP Process:  running
                       Forwarding:  enabled
           Periodic reoptimization:  every 10000 seconds, next in 4679 seconds
            Periodic FRR Promotion:  every 10 seconds, next in 2 seconds
       Periodic auto-bw collection:  every 300 seconds, next in 278 seconds

Name: tunnel160  Destination: 10.10.10.10
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 1, type explicit 60 (Basis for Setup, path weight 10)
```

```
  Config Parameters:
    Bandwidth:      100 kpbs (Global) Priority:  7  7 Affinity: 0x0/0xffff
    Metric Type: IGP (interface)
    AutoRoute:   enabled  LockDown: disabled   Loadshare:      100
    Auto-bw: disabled(0/0) 0  Bandwidth Requested:      100
    Direction: unidirectional

  History:
    Current LSP:
      Uptime: 02:12:21
    Prior LSP:
      ID: path option 1 [27]
      Removal Trigger: tunnel shutdown

  Path info:
  Hop0: 10.2.2.1
  Hop1: 10.10.10.10
Displayed 1 (of 2) heads, 0 (of 0) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```

The following is sample output from the **show mpls traffic-eng tunnels** command with the **summary** keyword:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels summary

Signalling Summary:
LSP Tunnels Process: running
RSVP Process: running
Forwarding: enabled
Head: 62 interfaces, 1 6 active signalling attempts, 1 6 established
4 6 activations, 3 deactivations
0 recovering, 1 recovered
Tails: 0
Periodic reoptimization: every 10000 seconds, next in 4873 seconds
Periodic FRR Promotion: every 10 seconds, next in 6 seconds
Periodic auto-bw collection: every 300 seconds, next in 172 seconds
Fast ReRoute Summary:
Head: 4 frr tunnels, 4 protected, 0 rerouted
router: 0 frr tunnels, 0 protected, 0 rerouted
Summary: 4 protected, 4 link protected, 0 node protected, 0 bw protected
Backup: 1 tunnels, 1 assigned
Interface: 2 protected, 0 rerouted
```

The following is sample output from the **show mpls traffic-eng tunnels** command with the **protection** keyword specified. This command selects every MPLS TE tunnel known to the router that was signaled as an FRR-protected LSP (property fast-reroute) and displays information about the protection this router provides to each selected tunnel:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels protection

tunnel160
  LSP Head, Admin: up, Oper: up
  Src: 10.20.20.20, Dest: 10.10.10.10, Instance: 28
  Fast Reroute Protection: None

tunnel170
  LSP Head, Admin: up, Oper: up
  Src: 10.20.20.20, Dest: 10.10.10.10, Instance: 945
  Fast Reroute Protection: Requested
    Outbound: FRR Ready
     Backup tunnel160 to LSP nhop
      tunnel160: out i/f: POS0/6/0/0
     LSP signalling info:
```

```
      Original: out i/f: POS0/7/0/0, label:  3, nhop: 10.10.10.10
      With FRR: out i/f: tunnel160, label:  3
    LSP bw: 10 kbps, Backup level: any unlimited, type: global-pool
```

The following 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 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-pool unlimited, Inuse: 0 kbps
```

The following is sample output from the **show mpls traffic-eng tunnels** command with the **backup** and **protected-interface** keywords specified:

```
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
```

Related Commands

Command	Description
backup-bw	Specifies the bandwidth type LSPs can use for a backup tunnel, whether the backup tunnel should provide bandwidth protection, and if so, how much and in which bandwidth pool.
mpls traffic-eng interface	Enables MPLS traffic engineering tunnel signaling on an interface.

snmp-server enable 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-server enable traps mpls traffic-eng** command in global configuration mode. To disable MPLS traffic engineering SNMP notifications, use the **no** form of this command.

snmp-server enable traps mpls traffic-eng [*notification-option*]

no snmp-server enable traps mpls traffic-eng [*notification-option*]

Syntax Description

notification-option	(Optional) Specifies the notification option to enable the sending of notifications to indicate changes in the status of MPLS traffic engineering tunnels. Use one of the following values: • **up** • **down** • **reoptimize** • **reroute** If you do not specify a specific notification type in conjunction with the **snmp-server enable traps mpls traffic-eng** command, all four types of MPLS traffic engineering tunnel notifications will be sent.

Defaults

This command is disabled. If the command is entered without the *notification-option* argument, the default is to enable all MPLS TE notification types.

Command Modes

Global configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

SNMP notifications can be sent as either traps or inform requests.

This 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-server enable traps mpls traffic-eng** command, no MPLS TE notifications controlled by this command will be sent. In order to configure the router to send these MPLS TE SNMP notifications, you must enter at least one **snmp-server enable traps mpls traffic-eng** command. If you enter the command with no keywords, all MPLS traffic engineering notification types

are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. In order to enable multiple types of MPLS traffic engineering notifications, you must issue a separate **snmp-server enable traps mpls traffic-eng** command for each notification type and notification option.

The **snmp-server enable traps mpls traffic-eng** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts will receive MPLS TE SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

For a host to receive an MPLS TE notification controlled by this command, both the **snmp-server enable traps mpls traffic-eng** command and the **snmp-server host** command for that host must be enabled.

Examples

The following example shows how to configure a router to send MPLS TE tunnel up SNMP notifications when a configured MPLS TE tunnel is about to leave the down state and enter the up state:

```
RP/0/RP0/CPU0:router(config)# snmp enable traps mpls traffic-eng up
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification.

MPLS Forwarding Commands on Cisco IOS-XR Software

This chapter describes the commands related to configuration and operations of Multiprotocol Label Switching (MPLS) forwarding for Cisco IOS-XR software.

clear mpls forwarding counters

To clear (set to zero) the Multiprotocol Label Switching (MPLS) forwarding counters, use the **clear mpls forwarding counters** command in EXEC mode.

clear mpls forwarding counters

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use the **clear mpls forwarding counters** command to set all MPLS forwarding counters to zero so that you can easily see future changes.

Examples

The following example shows sample output before and after clearing all counters:

```
RP/0/RP0/CPU0:router# show mpls forwarding
Local  Outgoing    Prefix            Outgoing     Next Hop        Bytes       T
Label  Label       or ID             Interface                    Switched    O
-----  --------  -------------  ----------  ------------  ---------  -
18     Exp-Null-v4 33.33.33.33/32    PO0/2/0/0    10.1.2.3        1572

RP/0/RP0/CPU0:router# clear mpls forwarding counters

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

Local  Outgoing    Prefix            Outgoing     Next Hop        Bytes       T
Label  Label       or ID             Interface                    Switched    O
-----  --------  -------------  ----------  ------------  ---------  -
18     Exp-Null-v4 33.33.33.33/32    PO0/2/0/0    10.1.2.3        0
```

Related Commands

Command	Description
show mpls forwarding	Displays the contents of MPLS forwarding table.

clear mpls packet counters

To clear (set to zero) the Multiprotocol Label Switching (MPLS) forwarded packet counters, use the **clear mpls packet counters** command in EXEC mode.

clear mpls packet counters [*interface-type interface-number*] [**location** *node-id*]

Syntax Description

interface-type	(Optional) Specifies the interface type for which the packet counter information will be cleared on a given node. • If no interface type is specified, all packet counter information will be cleared on all interfaces.
interface-number	(Optional) Specifies a physical interface number or a virtual interface number. • Physical interface number: Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. • Virtual interface number. Number range will vary depending on interface type. • If no interface number is specified, all packet counter information will be cleared on the specified node. For more information about the numbering syntax of the router, use the question mark (**?**) online help function.
location *node-id*	(Optional) Clears the information on a given node. If not specified, assumes current location where the CLI is being executed.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use the **clear mpls packet counters** command to set all MPLS forwarded counters to zero so that you can see future changes easily.

The forwarded packet counters currently include counts for:

- drop packets
- failed lookup packets
- fragmented packets

Examples

The following example shows sample output before and after clearing all packet counters:

```
RP/0/RP0/CPU0:router# show mpls packet counters summary location 0/1/CPU0

Pkts dropped:    0
Pkts fragmented: 10
Failed lookups:  0

RP/0/RP0/CPU0:router# clear mpls packet counters location 0/1/CPU0

RP/0/RP0/CPU0:router# show mpls packet counters summary location 0/1/CPU0

Pkts dropped:    0
Pkts fragmented: 0
Failed lookups:  0
```

Related Commands

Command	Description
show mpls packet counters	Displays the contents of MPLS forwarding counters for a given interface or aggregated counters for a given location (node).

clear mpls traffic-eng fast-reroute log

To clear the log of Multiprotocol Label Switching (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 Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following example shows sample output before and after 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

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

Related Commands

Command	Description
show mpls traffic-eng fast-reroute database	Displays the contents of the FRR database.
show mpls traffic-eng fast-reroute log	Shows the history of recorded FRR events.

mpls ip-ttl-propagate

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

mpls ip-ttl-propagate disable

no mpls ip-ttl-propagate

Syntax Description

disable	Since the default for the behavior is enabled, the only option available is disable. If disabled, the IP TTL will not be propagated to and from the MPLS header.

Defaults

IP TTL propagation is enabled by default. You can disable it using the **mpls ip-ttl-propagate disable** command.

Command Modes

Global configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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.

Examples

The following example shows how to disable IP TTL propagation:

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

mpls label range

To configure the range of local labels available for use on packet interfaces, use the **mpls label range** command in global configuration mode. To revert to the platform defaults, 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, then the global table is assumed. Currently, you can only specify table 0.
minimum	The smallest label allowed in the label space. The default is 16.
maximum	The largest label allowed in the label space. The default is 1048575.

Defaults

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

table-id: 0, the global label table

minimum: 16

maximum: 1048575

Command Modes

Global configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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).

Examples

The following example shows how to configure the size of the local label space. In this example, the *minimum* argument is set with a value of 200, and the *maximum* argument is set with a value of 120000. The new range takes effect immediately, although labels lying outside the range that are currently allocated by MPLS applications are left in circulation until they are released.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls label range 200 120000
```

Related Commands

Command	Description
show mpls label range	Displays the range of the MPLS local label space.

show mpls forwarding

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

show mpls forwarding [**prefix** {*network/mask* | *length*} | **labels** *label* [*label*] [**both-eos** | **eos0**] | **interface** *type number* | **tunnels** [*tunnel-id*] | **summary**] | [**detail**] | [**debug**] | [**location** *node-id*]

Syntax Description

prefix *network/mask* | *length*	(Optional) Specifies the destination address and mask/prefix length.
labels *label* [*label*] [**both-eos** | **eos0**]	(Optional) Displays only entries with a specified local labels range. The first label specifies the start label, and the second (optional label) specifies the end label. On the line card, MPLS forwarding creates entries for packets forwarding with End-of-Stack (EOS) =1 and packets with EOS=0. By default, the output from the **show mpls forwarding** command on a line card displays entries related to EOS=1. In order to debug hardware issues, it is possible to display either to match MPLS forwarding entries related to EOS1 (default), or EOS0, or both. The options **both-eos** and **eos0** only work on a line card.
interface *type number*	(Optional) Displays MPLS forwarding information related to the specified interface.
tunnels [*tunnel-id*]	(Optional) Displays entries either for a specified LSP tunnel or all LSP tunnel entries.
summary	(Optional) Displays summarized forwarding information.
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).
debug	(Optional) Displays the failure reason if "?" is displayed in the "Byte Switched" field of output. The typical reasons for failure to obtain statistics include Communication Error b/w global and per-node forwarding process, No such entry in per-node forwarding, and H/W stats error.
location *node-id*	(Optional) Displays information on a given node. If not specified, this option will bring information from the global database.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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

Examples

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

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

Local  Outgoing    Prefix             Outgoing  Next Hop        Bytes        T
Label  Label       or ID              Interface                 Switched     O
------ ----------- ------------------ --------- --------------- ------------ -
22     Pop Label   10.1.2.0/24        PO0/1/0/0 10.1.1.2        0
23     Pop Label   10.1.3.0/24        PO0/1/0/0 10.1.1.2        0
24     Pop Label   22.22.22.22/32     PO0/1/0/0 10.1.1.2        0
25     Unlabeled  33.33.33.33/32     tt13      point2point     0
```

The following is sample output from the **show mpls forwarding** command with the **detail** keyword specified:

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

Local  Outgoing    Prefix             Outgoing  Next Hop        Bytes        T
Label  Label       or ID              Interface                 Switched     O
------ ----------- ------------------ --------- --------------- ------------ -
22     Pop Label   10.1.2.0/24        PO0/1/0/0 10.1.1.2        0
     MAC/Encaps: 4/8, MTU: 4470
     Label Stack (Top -> Bottom): { Imp-Null }
     Packets Switched: 0

23     Pop Label   10.1.3.0/24        PO0/1/0/0 10.1.1.2        0
     MAC/Encaps: 4/8, MTU: 4470
     Label Stack (Top -> Bottom): { Imp-Null }
     Packets Switched: 0

24     Pop Label   22.22.22.22/32     PO0/1/0/0 10.1.1.2        0
     MAC/Encaps: 4/8, MTU: 4470
     Label Stack (Top -> Bottom): { Imp-Null }
     Packets Switched: 0

25     Unlabeled  33.33.33.33/32     tt13      point2point     0
     MAC/Encaps: 4/8, MTU: 4470
     Label Stack (Top -> Bottom): { 18 }
     Packets Switched: 0
```

The following is sample output from the s**how mpls forwarding** command with the **location** keyword and node ID specified.

```
RP/0/RP0/CPU0:router# show mpls forwarding location 0/1/CPU0

Local  Outgoing    Outgoing     Next Hop        Bytes
Label  Label       Interface                    Switched
------ ----------- ------------ --------------- ------------
22     Pop Label   PO0/1/0/0    10.1.1.2        0
23     Pop Label   PO0/1/0/0    10.1.1.2        0
24     Pop Label   PO0/1/0/0    10.1.1.2        0
25     Unlabeled  tt13         point2point     0
```

The following is sample output from the **show mpls forwarding** command with the **tunnels** keyword specified:

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

Tunnel   Outgoing    Outgoing     Next Hop        Bytes
Name     Label       Interface                    Switched
-------- ----------- ------------ --------------- ------------
tt13     18          PO0/1/0/0    10.1.1.2        13200
```

The following is sample output from the **show mpls forwarding** command with the **summary** keyword specified:

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

Forwarding entries:
   Label switching: 4
   IPv4 label imposition: 4
   MPLS TE tunnel head: 1
   MPLS TE fast-reroute: 0
Forwarding updates:
   42 updates, 28 messages
Labels in use:
   Reserved: 4
   Lowest: 22
   Highest: 25
```

show mpls forwarding hw

To display the contents of the Multiprotocol Label Switching (MPLS) Label Forwarding Information Base (LFIB) in the Packet Switching Engine of the line card, use the **show mpls forwarding hw** command in EXEC mode.

show mpls forwarding hw [**ingress** | **egress**] **label** {*label* | *min max* | **all**} [**location** *node-id*]

Syntax Description

ingress | **egress**	(Optional) Direction of packet flow with respect to the input/output interface as seen by the Packet Switching Engine.
label | *label min max* | **all**	Local label specified as either a single label value, a range of label values for which the information is displayed, or all labels for which there is information in the switching engine. When range is desired the minimum and maximum label values defining the range should be specified.
location *node-id*	(Optional) Displays information on a given node. If not specified, this option will bring information from RP. This option is not currently available with the prefix option.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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

Examples

The following is sample output from the **show mpls forwarding hw** command:

```
RP/0/RP0/CPU0:router# show mpls forwarding hw ingress label 20 location 0/1/CPU1

label 20 eos 0: PLU: type 0, entry type FORWARD, QoS group 0
PLU: 0x4000000 00000000 00000000 0x420000
L3 LoadInfo
Next Ptr: 10200 Num paths: 1
    00000000 0x010200 00000000 0x010000

L3 Entry
Next Ptr: 800a
    00000000 00000000 00000000 0x800a00

L2 LoadInfo
Num Paths: 1, Next Ptr: 20a
    0x400000 00000000 00000000 0x020a00
```

```
L2 Entry
Dest Addr : 4 Sponge Queue: 84 Egress Port: 118006
RP Destined: No Num Sponges: 0, Hash Type: 0
    00000000 0x4084000 0x1180060 00000000

label 20 eos 1: PLU: type 0, entry type FORWARD, QoS group 0
PLU: 0x4000000 00000000 00000000 0x420100
L3 LoadInfo
Next Ptr: 10201 Num paths: 1
    00000000 0x010201 00000000 0x010000

L3 Entry
Next Ptr: 800a
    00000000 00000000 00000000 0x800a00

L2 LoadInfo
Num Paths: 1, Next Ptr: 20a
    0x400000 00000000 00000000 0x020a00

L2 Entry
Dest Addr : 4 Sponge Queue: 84 Egress Port: 118006
RP Destined: No Num Sponges: 0, Hash Type: 0
    00000000 0x4084000 0x1180060 00000000
```

The following is sample output from the **show mpls forwarding hw** command with the **label** keyword specified:

```
RP/0/RP0/CPU0:router# show mpls forwarding hw egress label 20 location 0/1/CPU1

label 20 eos 0: PLU: type 0, entry type FORWARD, prefix_counter 0
PLU: 0x4000000 00000000 00000000 0x440000
L3 LoadInfo
Drop: No Next Ptr: 1010400 Num Paths: 1
    00000000 0x1010400 00000000 0x010000

L3 Entry
Label: 30 Total Labels: 1 Adj Counter: d110 uidb index: 1 Next ptr: 8005
    0x01e300 0xd1100000 0x000001 0x800500

L2 LoadInfo
Num Paths: 1 Encap: f008847 Next Ptr: 205
    0x400000 00000000 0xf008847 0x020500

L2 Entry
MTU: 4474 Default Sharq Queue: 9 Member Link: 0
    00000000 0x117a0000 00000000 0x480000

label 20 eos 1: PLU: type 0, entry type FORWARD, prefix_counter 0
PLU: 0x4000000 00000000 00000000 0x440100
L3 LoadInfo
Drop: No Next Ptr: 1010401 Num Paths: 1
    00000000 0x1010401 00000000 0x010000

L3 Entry
Label: 30 Total Labels: 1 Adj Counter: d110 uidb index: 1 Next ptr: 8005
    0x01e300 0xd1100000 0x000001 0x800500

L2 LoadInfo
Num Paths: 1 Encap: f008847 Next Ptr: 205
    0x400000 00000000 0xf008847 0x020500

L2 Entry
MTU: 4474 Default Sharq Queue: 9 Member Link: 0
    00000000 0x117a0000 00000000 0x480000
```

show mpls interfaces

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

show mpls interfaces [*type number*] [**location** *node-id*] | [**detail**]

Syntax Description

type number	(Optional) Displays information about the selected interface.
location *node-id*	(Optional) Displays interface information from specified location. If not specified, this option will bring information from global forwarding.
detail	(Optional) Displays detailed MPLS information. This keyword cannot be specified when the **location** keyword is also specified.

Defaults

If no optional keyword or argument is specified, summary information is displayed for each interface that has been configured for MPLS.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*..

This command displays MPLS information about the specified interface or about all of the interfaces for which MPLS has been configured.

Examples

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

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

Interface              LDP      Tunnel   Enabled
---------------------- -------- -------- --------
POS0/3/0/0             No       Yes      Yes
```

The following is sample output from the **show mpls interfaces** command with the **detail** keyword specified:

```
RP/0/RP0/CPU0:router# show mpls interfaces POS 0/3/0/0 detail

Interface POS0/3/0/0:
        LDP labelling not enabled
        LSP Tunnel labelling enabled (TE-Link)
        MPLS Frame Relay Transport labelling not enabled
        MPLS ATM Transport labelling not enabled
```

```
        MPLS enabled
        MTU = 4474
```

The following is sample output from the **show mpls interfaces** command with the location keyword specified:

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

Interface Caps  MTU
--------- ---- -----
PO0/2/0/0 M     4470
PO0/2/0/1 M     4470
```

Related Commands

Command	Description
interface (MPLS LDP)	Enables MPLS LDP on an interface.
mpls traffic-eng interface	Enables MPLS traffic engineering tunnel signaling on an interface.

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 Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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

Examples

The following is sample output from the **show mpls label range** command:

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

Range for dynamic labels: Min/Max: 16/1048575
```

Related Commands

Command	Description
mpls label range	Configures a range of values for use as local labels.

show mpls label table

To display the local labels contained in the Multiprotocol Label Switching (MPLS) label table, use the **show mpls label table** command in EXEC mode.

show mpls label table *table-id* [**application** *application* | *label*]

Syntax Description

table-id	The index of the label table to display. The global label table is 0. Currently, you can only specify table 0.
application *application*	(Optional) Displays all labels owned by the selected application. Options are: **internal**, **ldp**, **none**, **rsvp**, **static**, **te-control**, **te-link**, **test**, **snmp**.
label	Displays only the selected label.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following is 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
```

The following is sample output from the **show mpls label table** command with the **application** keyword specified:

```
RP/0/RP0/CPU0:router# show mpls label table 0 application te-link

Table Label   Owner      State  Rewrite
----- ------- ---------- ------ -------
0     16      TE-Link    InUse  Yes
```

The entries displayed by this command include a State field which is interpreted in Table 1:

Table 1 State Values

Value	Description
InUse	The label has been allocated and is being used by an application.
Alloc	The label has been allocated but is not yet being used by any application.
Pend	The label was being used by an application that has terminated unexpectedly, and the application has not yet reclaimed the label.
Pend-S	The label was being used by an application, but the MPLS Label Switching Database (LSD) server has recently restarted, and the application has not yet reclaimed the label.

Related Commands

Command	Description
show mpls forwarding	Displays entries in the MPLS forwarding table. Label switching entries are indexed by their local label.
show mpls lsd applications	Displays all the MPLS applications which are registered with the MPLS LSD server.

show mpls lsd applications

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

show mpls lsd applications

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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** command), but not all clients are applications.

Examples

The following is 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
```

The possible values for the State field are defined in Table 2:

Table 2 State values

Value	Description
Active	The application is registered with MPLS LSD and is functioning correctly.
Recover	The application is 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 transitions to the Active state.
Zombie	The application was previously registered with MPLS LSD but has not reregistered yet after unexpected termination. In this case, the RecoveryTime value indicates how many seconds are left before MPLS LSD gives up on the application.

Related Commands

Command	Description
show mpls lsd clients	Displays the MPLS clients which are connected to the MPLS LSD server.

show mpls lsd clients

To display the Multiprotocol Label Switching (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 Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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.

Examples

The following is 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
```

This display is intended as a form of debug output and is intentionally terse. The interpretation of the Services field is as follows: 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. There can occasionally be multiple BCDL Agent clients depending on system conditions; this is normal.

Note that all LSD applications are LSD clients but not all clients are applications.

Related Commands

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

show mpls packet counters

To display the values of the Multiprotocol Label Switching (MPLS) forwarded packet counters, use the **show mpls packet counters** command in EXEC mode.

show mpls packet counters [**summary** | **interface** *type number*] [**location** *node-id*]

Syntax Description

summary	Displays aggregate information on a given node.
interface	Displays information for the specified interface.
type	Interface type. For more information, use the question mark (**?**) online help function.
number	Either a physical interface number or a virtual interface number: • Physical interface number. Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. • Virtual interface number. Number range will vary depending on interface type. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.
location *node-id*	(Optional) Displays detailed packet information for the designated node. The *node-id* argument is entered in the rack/slot/module notation. If not specified, the output displays the current location where the CLI is being executed.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

This command is used to display MPLS forwarded packet counters and currently displays counters for:

- dropped packets
- failed lookup packets
- fragmented packets

Examples

The following is sample output from the **show mpls packet counters** command:

```
RP/0/RP0/CPU0:router# show mpls packet counters summary location 0/2/CPU0

Pkts dropped:    0
Pkts fragmented: 0
Failed lookups:  0
```

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 [*prefix* [*mask* | *mask-length*] | **backup-interface** [*type number* | **unresolved**] | **interface** *type number* | **labels** *low-label* [*high-label*] | **role** [**head** | **midpoint**]] [**state** {**active** | **complete** | **partial** | **ready**}] [**summary**]

Syntax Description

prefix	(Optional) IP address of the destination network. This address functions as the prefix of the FRR rewrite.
mask	(Optional) Bit combination indicating the portion of the IP address that is being used for the subnet address.
mask-length	(Optional) Number of bits in the mask of the destination.
backup-interface *type number*	(Optional) Displays entries with the specified backup interface. The summary suboption is available.
unresolved	(Optional) Displays entries whose backup interface has not yet been fully resolved.
interface *type number*	(Optional) Displays entries with this primary outgoing interface. The **summary** suboption is available.
labels	(Optional) Displays only 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.
low-label	(Optional) Starting label value or lowest value in the range.
high-label	(Optional) Highest label value in the range.
role	(Optional) Displays entries associated either with the tunnel **head** or tunnel **midpoint**. The **summary** suboption is available.
state	(Optional) Filter the database according to the state of the entry: **active**—Indicates the FRR rewrite is in the forwarding database (where it can be placed onto appropriate incoming packets). **complete**—State after the FRR rewrite has been assembled: ready or active. **partial**—State before the FRR rewrite has been fully created; its backup routing information is still incomplete. **ready**—Indicates the FRR rewrite was created but is not in the forwarding database.
summary	(Optional) Displays summarized information about the FRR database.

Defaults

If no optional keywords or arguments are specified, then the entire contents of the FRR database are displayed.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

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

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

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

The following command displays filtering of the FRR database using the *prefix* option:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng fast-reroute database 175.10.200.253

Tunnel head FRR information:
Prefix             Tunnel     In-label Out intf/label   FRR intf/label   Status
------------------ ---------- -------- ---------------- ---------------- -------
175.10.200.253/32  tu4000     Tun hd   PO0/3/0/0:34     tt1000:34        Ready
```

The Prefix field indicates the IP address to which packets with this label are going.

The following command displays filtering of the FRR database using the **backup-interface** option:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng fast database backup-interface tunnel-te 1000

Tunnel head FRR information:
Tunnel     In-label Out intf/label   FRR intf/label   Status
---------- -------- ---------------- ---------------- -------
tu4000     Tun hd   PO0/3/0/0:34     tt1000:34        Ready
```

The following command 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     In-label Out intf/label   FRR intf/label   Status
---------- -------- ---------------- ---------------- -------
tt4000     Tun hd   PO0/3/0/0:34     tt1000:34        Ready
tt4001     Tun hd   PO0/3/0/0:35     tt1001:35        Ready
tt4002     Tun hd   PO0/3/0/0:36     tt1001:36        Ready
```

The following command shows 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
Other       0
```

The following command shows the FRR database filtered according to the state of the entries. Note that FRR has been triggered:

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

Tunnel head FRR information:
Tunnel     In-label Out intf/label   FRR intf/label   Status
---------- -------- ---------------- ---------------- -------
tt4000     Tun hd   tt1000:34                         Active
tt4001     Tun hd   tt1001:35                         Active
tt4002     Tun hd   tt1001:36                         Active
```

The following command shows the FRR database with protected midpoints:

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

LSP midpoint FRR information:
LSP identifier                In-label Out intf/label   FRR intf/label   Status
----------------------------- -------- ---------------- ---------------- -------
10.10.10.10 5000 [48]         18       PO0/1/0/1:18     tt2001:18        Ready
10.10.10.10 8000 [105]        19       PO0/1/0/1:19     tt2000:19        Ready
```

The following command shows the FRR database filtered according to the inbound label. This output only applies to LSP midpoint entries:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng fast-reroute database labels 18 18

LSP midpoint FRR information:
LSP identifier                In-label Out intf/label   FRR intf/label   Status
----------------------------- -------- ---------------- ---------------- -------
10.10.10.10 5000 [48]         18       PO0/1/0/1:18     tt2001:18        Ready
```

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

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

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

Related Commands

Command	Description
show mpls traffic-eng fast-reroute log	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** *type number* | **node** *node-id*]

Syntax Description

interface *type number*	Displays all FRR events for the selected protected interface.
node *node-id*	Displays all FRR events that occurred on the selected node.

Defaults

If no optional keyword and argument is specified, then the entire contents of the FRR log are displayed.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following is 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
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
```

Related Commands

Command	Description
clear mpls traffic-eng fast-reroute log	Clears the history of recorded FRR events.
show mpls traffic-eng fast-reroute database	Displays the contents of the FRR database.

RSVP Infrastructure Commands on Cisco IOS-XR

Resource Reservation Protocol (RSVP) is a signaling protocol that is 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* and Optical UNI tunnels, as specified in the Optical Interworking Forum (OIF) document OIF2000.125.7, *User Network Interface (UNI) 1.0, Signalling Specification*. The RSVP implementation also supports Fault handling as specified in IETF RFC 3473, Generalized Multiprotocol Label Switching (GMPLS) Signaling RSVP-TE extensions.

bandwidth (RSVP)

To configure Resource Reservation Protocol (RSVP) bandwidth on an interface, 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-bandwidth max-flow* **sub-pool** *sub-pool-bw*

no bandwidth

Syntax Description

total-bandwidth	(Optional) Total reservable bandwidth (in kbps) that RSVP will accept for reservations on this interface. The range is from 0 to 10000000.
max-flow	(Optional) Maximum size (in kbps) of a single reservation. The range is from 0 to 10000000.
sub-pool *sub-pool-bw*	(Optional) Subpool bandwidth (in kbps) on the interface. This is for Multiprotocol Label Switching (MPLS) DiffServ Traffic Engineering (TE). This value cannot be bigger than the total bandwidth.

Defaults

There is no RSVP bandwidth on an interface until the **bandwidth** command is entered.

sub-pool-bw: 0

Command Modes

RSVP interface configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

When RSVP is enabled on an interface, no bandwidth resources are specified for RSVP on that interface. This command is used to specify the RSVP bandwidth on an interface so that RSVP can make bandwidth reservations on behalf of applications (for instance, MPLS Traffic Engineering). If the RSVP bandwidth on an interface is 0, RSVP can only be used to signal for flows which do not require bandwidth.

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 zero intrinsic bandwidth, then none can be reserved for RSVP. In the case of the Optical User Network Interface (O-UNI), 0 bandwidth is not an issue as it does not use bandwidth as a resource.

The *max-flow* argument default equals the total RSVP bandwidth on the interface (that is, the *total-bandwidth* parameter value).

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.

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(config)# rsvp interface pos 0/3/0/0
RP/0/RP0/CPU0:router(config-rsvp-if)# bandwidth 7500 1000
```

The following example limits the total of all RSVP reservations on POS interface 0/3/0/0 to 7500 kbps, allows each single flow to reserve no more than 1000 kbps, and limits the subpool bandwidth to 2000 kbps:

```
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/3/0/0
RP/0/RP0/CPU0:router(config-rsvp-if)# bandwidth 7500 1000 sub-pool 2000
```

The following example limits the total of all RSVP reservations on POS interface 0/3/0/0 to 5000 kbps, but specifies no limit on single flow bandwidth. By default then, a single flow can use the entire RSVP bandwidth on the interface—in this example, 5000 kbps:

```
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/3/0/0
RP/0/RP0/CPU0:router(config-rsvp-if)# bandwidth 5000
```

The following example specifies for POS interface 0/3/0/0 the default maximum reservable bandwidth and maximum flow bandwidth, namely 75 percent of the interface bandwidth, and the default sub-pool bandwidth (0):

```
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/3/0/0
RP/0/RP0/CPU0:router(config-rsvp-if)# bandwidth
```

The following example clears the RSVP bandwidth on POS interface 0/3/0/0:

```
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/3/0/0
RP/0/RP0/CPU0:router(config-rsvp-if)# no bandwidth
```

Related Commands

Command	Description
rsvp interface	Configures RSVP bandwidth on an interface.

clear rsvp counters all

To clear (set to zero) all Resource Reservation Protocol (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 number*

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
number	Either a physical interface number or a virtual interface number: • Physical interface number. Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. • Virtual interface number. Number range will vary depending on interface type. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use the **clear rsvp counters all** command to set all RSVP message and event counters to zero.

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	Clears (sets to zero) all RSVP event counters that are being maintained by the router.
clear rsvp counters messages	Clears (sets to zero) all RSVP message counters that are being maintained by the router.
show rsvp counters	Shows all RSVP message/event counters that are being maintained by the router.

clear rsvp counters events

To clear (set to zero) all Resource Reservation Protocol (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 number*

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
number	Either a physical interface number or a virtual interface number: • Physical interface number. Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. • Virtual interface number. Number range will vary depending on interface type. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use the **clear rsvp counters events** command to set all RSVP event counters to zero.

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	Clears (sets to zero) all RSVP message counters that are being maintained by the router.
show rsvp counters	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 Resource Reservation Protocol (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 number*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
number	(Optional) Either a physical interface number or a virtual interface number: • Physical interface number. Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. • Virtual interface number. Number range will vary depending on interface type. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.

Defaults

Clears message counters for all interfaces.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use the **clear rsvp counters messages** command to set all RSVP message counters to zero.

Examples

The following example uses the **clear rsvp counters messages** command 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	Displays the number of RSVP messages that were sent and received.

rsvp

To enter Resource Reservation Protocol (RSVP) configuration submode, use the **rsvp** command in global configuration mode. From this submode, RSVP global and interface configuration commands can be entered.

rsvp

Syntax Description

This command has no keywords or arguments.

Command Modes

Global configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The **rsvp** command enters the rsvp configuration submode.

This submode allows configuration of global RSVP parameters such as graceful restart (signaling) and interface-specific configuration.

Examples

The following example shows how to enable rsvp configuration submode:

```
RP/0/RP0/CPU0:router(config)# rsvp
RP/0/RP0/CPU0:router(config-rsvp)#
```

Related Commands

Command	Description
rsvp interface	Configures RSVP interface related parameters.
rsvp signalling graceful-restart	Configures RSVP graceful-restart parameters.
rsvp signalling hello graceful-restart refresh interval	Configures RSVP hello refresh interval for graceful-restart feature.
rsvp signalling hello graceful-restart refresh misses	Configures number of hello's which can be missed for graceful-restart feature.
rsvp signalling graceful-restart restart-time	Configures restart time to be advertised to neighbor as part of graceful-restart feature.

rsvp interface

To configure Resource Reservation Protocol (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. This command changes the configuration mode to rsvp-interface submode within which you can enter interface-specific configuration commands.

rsvp interface *type number*

no rsvp interface *type number*

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
number	Either a physical interface number or a virtual interface number: • Physical interface number. Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. • Virtual interface number. Number range will vary depending on interface type. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.

Defaults

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 Multiprotocol Label Switching (MPLS).

Command Modes

Global configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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 only be used to signal flows that do not require bandwidth on this interface. In the case of O-UNI, 0 bandwidth is not an issue, as O-UNI does not use bandwidth as a resource.

The **rsvp interface** command enables the rsvp interface configuration submode.

Examples

The following example shows how to enable the rsvp interface configuration submode and enables RSVP on this interface with 0 bandwidth:

```
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/3/0/0
```

Related Commands

Command	Description
bandwidth (RSVP)	Configures RSVP bandwidth on an interface.

rsvp signalling graceful-restart

To enable or disable Resource Reservation Protocol (RSVP) signaling graceful restart, use the **rsvp signalling graceful-restart** command in RSVP configuration mode. To disable signaling graceful-restart, enter the **no** form of this command.

rsvp signalling graceful-restart

no rsvp signalling graceful-restart

Syntax Description

This command has no arguments or keywords.

Defaults

RSVP signalling graceful restart is disabled.

Command Modes

RSVP configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The **rsvp signalling graceful-restart** command provides a mechanism that helps minimize the negative effects on Multiprotocol Label Switching (MPLS) and Optical User Network Interface (O-UNI) 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: the control plane of a node fails, but the node preserves its data forwarding states.

The **rsvp signalling graceful-restart** command instigates the exchange of RSVP hello messages between the router and its neighbor nodes. Once the hello messages are established with a given neighbor, RSVP can then detect the above two types of faults when they occur with the neighbor in question.

Examples

The following example enables RSVP signalling graceful restart:

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

The following example disables RSVP signalling graceful restart:

```
RP/0/RP0/CPU0:router(config)# no rsvp signalling graceful-restart
```

Related Commands

Command	Description
rsvp signalling graceful-restart restart-time	Configures the restart time that is advertised in the Restart Cap object in hello messages.

rsvp signalling hello graceful-restart refresh interval

To configure the interval at which Resource Reservation Protocol (RSVP) graceful-restart hello messages are sent to each neighbor, use the **rsvp signalling hello graceful-restart refresh interval** command in global configuration mode. To reset to the default value of 5000 milliseconds, use the **no** form of the command.

rsvp signalling hello graceful-restart refresh interval *refresh-interval*

no rsvp signalling hello graceful-restart refresh interval

Syntax Description

refresh-interval	Interval at which RSVP Graceful-Restart hello messages are sent to each neighbor (3000 to 30000 milliseconds).

Defaults

The default interval is 5000 milliseconds.

Command Modes

Global configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

This command determines how often hello messages are sent to each neighbor. If the interval is made short, the hello messages are sent more frequently. While 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 back-off 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 fails to come back up during the restart interval. The restart interval is provided by the neighbor in the restart cap object.

Examples

The following example sets the hello graceful-restart refresh interval to 4000 msecs:

```
RP/0/RP0/CPU0:router(config)# rsvp signalling hello graceful-restart refresh interval 4000
```

Related Commands

Command	Description
rsvp signalling hello graceful-restart refresh misses	Configures the number of consecutive missed RSVP hello messages before a neighbor is declared down or unreachable.

rsvp signalling hello graceful-restart refresh misses

To configure the number of consecutive missed Resource Reservation Protocol (RSVP) hello messages before a neighbor is declared down or unreachable, use the **rsvp signalling hello graceful-restart refresh misses** command in global configuration mode. To reset to the default value of 3, use the **no** form of the command.

rsvp signalling hello graceful-restart refresh misses *refresh-misses*

no rsvp signalling hello graceful-restart refresh misses

Syntax Description

refresh-misses	The number of misses for hello messages (3 to 10) before a neighbor is declared down or unreachable. The default is 3.

Defaults

refresh-misses: 3

Command Modes

Global configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

If no hello messages (request or ACK) are received from a neighbor within the configured number of refresh misses, then the node assumes that communication with the neighbor has been lost.

Examples

The following example sets hello graceful-restart refresh misses to 4:

```
RP/0/RP0/CPU0:router(config)# rsvp signalling hello graceful-restart refresh misses 4
```

Related Commands

Command	Description
rsvp signalling hello graceful-restart refresh interval	Configures the interval at which RSVP graceful restart hello messages are sent per neighbor.

rsvp signalling graceful-restart restart-time

To configure the restart time that is advertised in the Restart Cap object in hello messages, use the **rsvp signalling graceful-restart restart-time** command in global configuration mode. To reset the restart-time to the default value, enter the **no** form of this command.

rsvp signalling graceful-restart restart-time *restart-time*

no rsvp signalling graceful-restart restart-time

Syntax Description

restart-time	The amount of time after a control-plane restart that RSVP can start exchanging hello messages (60 to 3600 seconds). The default value is 120 seconds.

Defaults

restart-time: 120 seconds

Command Modes

Global configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

If no hello messages are received from a neighbor within a certain number of hello intervals, then 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.

Examples

The following example shows how to set the restart-time:

```
RP/0/RP0/CPU0:router(config)# rsvp signalling graceful-restart restart-time 200
```

The following example shows how to resets the restart-time to the default of 120 seconds:

```
RP/0/RP0/CPU0:router(config)# no rsvp signalling graceful-restart restart-time
```

Related Commands

Command	Description
rsvp signalling graceful-restart	Enables or disables graceful restart.

show rsvp counters

To display internal Resource Reservation Protocol (RSVP) counters, use the **show rsvp counters** command in EXEC mode.

show rsvp counters [**messages** *type number*] [**summary** | **events**]

Syntax Description

messages	(Optional) 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.
number	(Optional) Either a physical interface number or a virtual interface number: • Physical interface number. Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. • Virtual interface number. Number range will vary depending on interface type. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.
summary	(Optional) Displays a summation number of messages RSVP has received and sent on all interfaces.
events	(Optional) Displays the number of states expired for lack of refresh and also a count of NACKs received.

Defaults

Displays summary information for all interfaces.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

In message counters, bundle messages are counted as single bundle messages. The component messages are not counted separately.

Examples

The following is sample output from the **show rsvp counters summary** command:

```
RP/0/RP0/CPU0:router# show rsvp counters messages summary

     All RSVP Interfaces    Recv     Xmit                        Recv     Xmit
        Path                  41        1    Resv                   0       40
        PathError              0        0    ResvError              0        0
        PathTear               7        1    ResvTear               0       16
        ResvConfirm            0        0    Ack                   34       16
        Bundle                 0             Hello                 25        0
        SRefresh           10119    10132    OutOfOrder             0
        Retransmit                     22    Rate Limited                    0
```

The following is sample output from the **show rsvp counters messages** command for POS interface 0/3/0/0:

```
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
```

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
```

show rsvp graceful-restart

To display the local graceful restart information for Resource Reservation Protocol (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 the neighbors keyword is not specified, only a multiline table entry is displayed showing the local graceful restart information.
ip-address	(Optional) Address of the neighbor you are displaying. Displays a specific neighbor with that destination address only. If no address is specified, all neighbors are displayed.
detail	(Optional) Displays multiline status for each neighbor. If the **detail** keyword is not specified, only a single-line table entry is displayed.

Defaults

Displays all interfaces in single-line table entry format.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Graceful restart neighbors are displayed in ascending order of neighbor IP address.

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
```

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
```

The following is sample output from the **show rsvp graceful-restart neighbors detail** command, which displays detailed information about all graceful restart neighbors for the router:

```
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: 8.8.8.9
  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
```

show rsvp hello instance

To display the Resource Reservation Protocol (RSVP) hello instances, use the **show rsvp hello instance** command in EXEC mode.

show rsvp hello instance [*ip-address* | **detail**]

Syntax Description

ip-address	(Optional) Address of the neighbor you are displaying. Displays a specific neighbor with that destination address only. If no address/name is specified, all neighbors are displayed.
detail	(Optional) Displays multiline status for each hello instance. If the **detail** keyword is not specified, only a single-line table entry is displayed.

Defaults

Displays all interfaces in single-line table entry format.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Hello instances are displayed in ascending order of neighbor IP address.

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
```

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
```

show rsvp interface

To display information about all interfaces with Resource Reservation Protocol (RSVP) enabled, use the **show rsvp interface** command in EXEC mode.

show rsvp interface *type number* [**detail**]

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
number	Either a physical interface number or a virtual interface number: • Physical interface number. Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. • Virtual interface number. Number range will vary depending on interface type. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.
detail	(Optional) Displays multiline status for each interface. If the **detail** keyword is not specified, only a single-line table entry is displayed.

Defaults

Displays all interfaces in single-line table entry format.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command to display various configuration settings such as the list of neighbors and their refresh reduction capabilities.

Examples

The following is sample output from the **show rsvp interface** command, which displays brief information about all RSVP-configured interfaces on the router:

```
RP/0/RP0/CPU0:router# show rsvp interface

    Interface   MaxBW    MaxFlow  Allocated        MaxSub
    ---------- -------- -------- --------------- -------
    tu2000         0        0        0 (  0%)        0
    PO0/3/0/0  1000M    1000M     200K(  0%)        0
```

This following is sample output from the **show rsvp interfaces detail** command, which displays detailed information about all RSVP-configured interfaces on the router:

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

INTERFACE: tunnel2000 (ifh=0x1000980).
 BW (bits/sec): Max=0. MaxFlow=0. Allocated=0 (0%). MaxSub=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: Not running.
 Refresh reduction local: Enabled. Summary Refresh: Enabled (4096 bytes max).
 Reliable summary refresh: Disabled.
 Ack hold: 400 ms, Ack max size: 4096 bytes. Retransmit: 900ms.

INTERFACE: POS0/3/0/0 (ifh=0x4000100).
 Bandwidth (bits/sec): Max=1000M. MaxFlow=1000M. Allocated=200K (0%). MaxSub=0.
 Signalling: No DSCP marking. No rate limiting.
 States in: 1. Max missed msgs: 4.
 Expiry timer: Running (every 30s). Refresh interval: 45s.
 Normal Refresh timer: Not running. Summary refresh timer: Running.
 Refresh reduction local: Enabled. Summary Refresh: Enabled (4096 bytes max).
 Reliable summary refresh: Disabled.
 Ack hold: 400 ms, Ack max size: 4096 bytes. Retransmit: 900ms.
 Neighbor information:
    Neighbor-IP    Nbor-MsgIds   States-out  Refresh-Reduction Expiry(min::sec)
 -------------- --------------   ----------  ----------------- ----------------
     1.1.1.2           1             1       Enabled           14::50
```

Related Commands

Commands	Description
show rsvp counters	Displays internal RSVP counters.

show rsvp request

To list all the requests that Resource Reservation Protocol (RSVP) knows about on a router, use the **show rsvp request** command in EXEC mode.

show rsvp request [**detail**] [**destination** *ip-address* | **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) Destination address to filter on for the reservations to display.
dst-port *port-num*	(Optional) Destination port/tunnel ID to filter on for the reservations to display.
source *ip-address*	(Optional) Source address to filter on for the reservations to display.
src-port *port-num*	(Optional) Source port/lsp ID to filter on for the reservations to display.

Defaults

Displays all interfaces in single-line table entry format.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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.

Examples

The following example displays brief information about all requests in the router:

```
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
```

Related Commands

Commands	Description
show rsvp reservation	Displays internal RSVP reservation counters.

show rsvp reservation

To list all reservations that Resource Reservation Protocol (RSVP) knows about on a router, use the **show rsvp reservation** command in EXEC mode.

show rsvp reservation [**detail**] [**destination** *ip-address* | **dst-port** *port-num* | **source** *ip-address* | **src-port** *port-num*]

Syntax Description

detail	(Optional) Displays multi-line status for each reservation. If the **detail** keyword is not specified, only a single-line table entry is displayed.
destination *ip-address*	(Optional) Destination address to filter on for the reservations to display.
dst-port *port-num*	(Optional) Destination port/tunnel ID to filter on for the reservations to display.
source *ip-address*	(Optional)Source address to filter on for the reservations to display.
src-port *port-num*	(Optional) Source port/lsp ID to filter on for the reservations to display.

Defaults

Displays all interfaces in single-line table entry format.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

This 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.

Examples

The following example displays brief information about all reservations in the router:

```
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.
```

Related Commands

Command	Description
show rsvp request	Lists all the requests that RSVP knows about on a router.

show rsvp sender

To list all path states that Resource Reservation Protocol (RSVP) knows about on this router, use the **show rsvp sender** command in EXEC mode.

show rsvp sender [**detail**] [**destination** *ip-address* | **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) Destination address to filter on for the paths to display.
dst-port *port-num*	(Optional) Destination port/tunnel ID to filter on for the paths being displayed.
source *ip-address*	(Optional) Source address to filter on for the paths to display.
src-port *port-num*	(Optional) Source port/lsp ID to filter on for the paths to display.

Defaults

Displays all interfaces in single-line table entry format.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

This command displays information about path states on the router.

Examples

The following example displays brief information about all paths in the router:

```
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
```

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: 10.10.40.40. TunID: 2001. LSPId: 2.
 Source addr: 10.66.67.68. ExtID: 10.66.67.68.
 Prot: Off. Backup tunnel: None.
```

```
 Rate: 0 bits/sec. Burst: 1K bytes. Peak: 0 bits/sec.
 Flags: None.
 State expires in 341.054 sec.
 Policy:  Accepted. Policy source(s): MPLS/TE.
 Header info: RSVP TTL=254. IP TTL=254. Flags: 0x1. TOS=0xff.
 Input interface: PO0/7/0/1. Previous hop: 10.66.67.68 (lih: 0x19700001).

PATH: IPv4-LSP Session addr: 10.66.67.68. TunID: 2000. LSPId: 15.
 Source addr: 10.40.40.40. ExtID: 10.40.40.40.
 Prot: Off. Backup tunnel: None.
 Rate: 0 bits/sec. Burst: 1K bytes. Peak: 0 bits/sec.
 Flags: Local Sender.
 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.
 Input interface: None. Previous hop: 0.0.0.0 (lih: 0x0).
 Output on PO0/7/0/1. Policy: Forwarding.
```

show rsvp session

To list all sessions that Resource Reservation Protocol (RSVP) knows about on this router, use the **show rsvp session** command in EXEC mode.

show rsvp session [**detail**] [**destination** *ip-address* | **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) Destination address to filter on for the sessions to display.
dst-port *port-num*	(Optional) Destination port/tunnel ID to filter on for the sessions to display.
tunnel-name *tunnel-name*	(Optional) Displays status for the session matching the tunnel-name specified.

Defaults

Displays all interfaces in single-line table entry format.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Sessions are displayed in ascending order of destination IP address, destination port, and source IP address.

Examples

The following example displays brief information about all paths in the router:

```
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
```

The following example displays detailed information about all sessions in the system:

```
RP/0/RP0/CPU0:router# show rsvp session detail

SESSION: IPv4-LSP Addr: 10.40.40.40, TunID: 2001, ExtID: 10.66.67.68
 PSBs: 1, RSBs: 1, Requests: 1
 Tunnel Instance: 2
 Tunnel Name: RSVP5_t2001
  RSVP Path Info:
   InLabel: POS0/7/0/1, No label.
   Incoming Address: 10.31.31.31
   Explicit Route:
     10.31.31.31
     10.40.40.40
   Record Route: None
   Tspec: avg rate=0, burst=1K, peak rate=0
  RSVP Resv Info:
   OutLabel: No intf, No label
   FRR OutLabel: No intf, No label
   Record Route: None
   Fspec: avg rate=0, burst=1K, peak rate=0

SESSION: IPv4-LSP Addr: 10.66.67.68, TunID: 2000, ExtID: 10.40.40.40
 PSBs: 1, RSBs: 1, Requests: 0
 Tunnel Instance: 15
 Tunnel Name: MFR-345-ROUTER_t2000
  RSVP Path Info:
   InLabel: No intf, No label
   Incoming Address: Unknown
   Explicit Route:
     10.40.40.40
     10.31.31.32
     10.66.67.68
   Record Route: None
   Tspec: avg rate=0, burst=1K, peak rate=0
  RSVP Resv Info:
   OutLabel: POS0/7/0/1, 3
   FRR OutLabel: No intf, No label
   Record Route: None
   Fspec: avg rate=0, burst=1K, peak rate=0
```

signalling dscp

To give all Resource Reservation Protocol (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 disable the override of DSCP on the interface, use the **no** form of this command.

signalling dscp *dscp*

no signalling *dscp*

Syntax Description

dscp	A DSCP priority number from 0 to 63.

Defaults

No override of DSCP.

Command Modes

RSVP Interface configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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 Multiprotocol Label Switching (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 will be sent out with DSCP 10. If **signalling dscp 5** is configured for RSVP on interface A, the Path messages being sent out interface A would be marked with DSCP 5, but the Path messages being sent out interface B would still be 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.

Examples

The following example shows how to specify that all RSVP packets going out on POS interface 0/1/0/1 be marked with DSCP 20:

```
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(config)# interface pos 0/1/0/1
RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling dscp
```

signalling rate-limit

To limit the rate of Resource Reservation Protocol (RSVP) signaling messages being sent out a particular interface, use the **signalling rate-limit** command in RSVP interface configuration mode. To disable signalling rate-limiting, use the **no** form of the command.

signalling rate-limit rate *messages* **interval** *interval-length*

no signalling rate-limit rate *messages* **interval** *interval-length*

Syntax Description

rate *messages*	(Optional) Number of messages to be sent per scheduling interval. The range is from 1 to 500. The default is 100 messages.
interval *interval-length*	(Optional) Interval length between scheduling intervals (specified in milliseconds). The range is from 250 to 2000 milliseconds. The default is 1000 milliseconds (1 second).

Defaults

The default rate is 100 messages, and the default interval is 1 second. By default, rate-limiting is disabled.

Command Modes

RSVP interface configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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.)

Examples

The following example shows how to enable rate-limiting:

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

signalling refresh interval

To change the frequency with which a router updates the network about the Resource Reservation Protocol (RSVP) state of a particular interface, use the **signalling refresh interval** command in RSVP interface configuration mode. To return the refresh interval to its default of 45 seconds, 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 (specified in seconds). Range is from 10 to 180 seconds. The default is 45 seconds.

Defaults

The default interval is 45 seconds.

Command Modes

RSVP interface configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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, in order 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.

Examples

The following example shows how to specify a refresh interval of 30 seconds:

```
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(config-rsvp-if)# no signalling refresh interval
```

Related Commands

Command	Description
signalling refresh missed	Specifies the number of successive refresh messages that can be missed before RSVP deems the state to be expired and tears it down.
signalling refresh reduction reliable	Customizes acknowledgment message size and hold interval, and the RSVP message retransmit interval.
signalling refresh reduction summary	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 Resource Reservation Protocol (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 the missed-messages number to its default value of four messages, use the **no** form of this command.

signalling refresh missed *number*

no signalling refresh missed

Syntax Description

number	Number of successive missed refresh messages. The range is from 1 to 8. The default is 4.

Defaults

number: 4

Command Modes

RSVP interface configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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.

Examples

The following example shows how to specify a missed refresh limit of six (6) messages:

```
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(config-rsvp-if)# no signalling refresh missed
```

Related Commands

Command	Description
signalling refresh interval	Changes the frequency with which a router updates the network about the RSVP state of an interface.
signalling refresh reduction reliable	Customizes acknowledgment message size and hold interval, and the RSVP message retransmit interval.
signalling refresh reduction summary	Enables and configures the maximum size of the SRefresh message.

signalling refresh reduction disable

To disable Resource Reservation Protocol (RSVP) refresh reduction on an interface, use the **signalling refresh reduction disable** command in RSVP interface configuration mode. To enable RSVP refresh reduction on the interface, 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.

Defaults

Refresh reduction is enabled.

Command Modes

RSVP interface configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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 will not be used on this link. That information can be obtained through use of the **show rsvp interface detail** command.

Examples

The following example shows how to disable RSVP refresh reduction on an interface:

```
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(config-rsvp-if)# no signalling refresh reduction disable
```

Related Commands

Command	Description
show rsvp interface	Displays information about all interfaces with RSVP enabled.
signalling refresh interval	Changes the frequency with which a router updates the network about the RSVP state of an interface.
signalling refresh reduction reliable	Customizes acknowledgment message size and hold interval, and the RSVP message retransmit interval.
signalling refresh reduction summary	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 restore the parameters to their default values, 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	(Optional) The maximum size of the Resource Reservation Protocol (RSVP) component within a single acknowledgment message. This length includes the RSVP message header and any other RSVP object headers. It does not include the IP header or any other Layer 3 (L3) or Layer 2 (L2) overheads.
bytes	(Optional) The number of bytes that define the maximum size of an RSVP component. The range is from 32 to 8000. (Because all RSVP objects are sized in multiples of 4, when you specify a size that is not a multiple of 4, RSVP uses the largest multiple of 4 just under the specified value.)
ack-hold-time	(Optional) The maximum amount of time a router will hold onto an acknowledgment before sending it, in an attempt to bundle several acknowledgments into a single acknowledgment message.
milliseconds	(Optional) The number of milliseconds that define the acknowledgment hold time. The range is from 100 to 5000.
retransmit-time	(Optional) The amount of time the router initially waits for an acknowledgment message before resending the RSVP message. If still no acknowledgment is received, the router doubles this interval and resends again. After five such successive backoffs, the original RSVP message is sent via normal refresh mechanism (if Path or Reservation) or is discarded (if Error or Tear).
milliseconds	(Optional) The number of milliseconds that define the retransmit time. The range is from 100 to 10000.
summary-refresh	(Optional) Enables the use of reliable transmission for RSVP summary refresh messages.

Defaults

Reliable messaging is automatically enabled whenever refresh reduction is enabled (by the **signalling refresh reduction** command). Refresh reduction is enabled by default.

The acknowledgment message size is 4096 bytes.

The acknowledgment-hold time is 400 milliseconds (0.4 seconds).

The resend time is 900 milliseconds (0.9 seconds).

The reliable transmission of RSVP summary refresh messages is disabled.

Command Modes

RSVP interface configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

For reliable messaging to work properly, configure the retransmit-time on the router (A) sending the message 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 is retransmitted. 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 will retransmit 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 acknowledgment-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* **signalling refresh reduction summary** command.

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	Disables RSVP refresh reduction on an interface.

signalling refresh reduction summary

To configure Resource Reservation Protocol (RSVP) summary refresh message size on an interface, use the **signalling refresh reduction summary** command in RSVP interface configuration mode. To restore RSVP summary refresh message size to default on the interface, use the **no** form of this command.

signalling refresh reduction summary [**max-size** *bytes*]

no signalling refresh reduction summary [**max-size** *bytes*]

Syntax Description

max-size *bytes*	(Optional) Specifies the maximum size in bytes of a single RSVP summary refresh message. The valid range is from 20 to 6500 bytes, and the default value is 4096 bytes.

Defaults

The default is 4096 byte sized messages.

Command Modes

RSVP interface configuration submode.

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use the **signalling refresh reduction summary** command to specify the maximum size of the summary refresh messages sent. The configured message size can be verified by entering the **show rsvp interface detail** command.

Examples

The following example shows how to change the summary message maximum size on an interface:

```
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(config-rsvp-if)# no signalling refresh reduction summary max-size
6000
```

Related Commands

Command	Description
show rsvp interface	Displays information about all interfaces with RSVP enabled.
signalling refresh interval	Changes the frequency with which a router updates the network about the RSVP state of an interface.

MPLS Optical User Network Interface Commands on Cisco IOS-XR Software

The Unified Control Plane (UCP) (sometimes called the Optical Control Plane [OCP]) is a standards-based approach toward an open architecture for the control and provisioning of optical transport elements and capacity. It allows customers to establish standards-based Optical Internetworking Forum (OIF) connections through heterogeneous optical networks (OTNs) based on the Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH) specifications. These connections can be made across OTNs comprising Cisco equipment or third-party vendor equipment.

This chapter contains commands for configuring, monitoring, and troubleshooting the Optical User Network Interface (O-UNI). It provides a description of the static link management protocol (LMP) commands. Static Link Management Protocol (LMP) is a user-configured version of the Internet Engineering Task Force's (IETF) LMP; hence, the keyword **lmp** is used in the management commands.

destination address ipv4

To establish an Optical User Network Interface (O-UNI) connection to a specific destination Transport Network Address (TNA), use the **destination address ipv4** command in MPLS O-UNI interface configuration mode. To initiate the graceful deletion of the connection, use the **no** form of this command.

destination address ipv4 *destination-TNA*

no destination address ipv4 *destination-TNA*

Syntax Description

destination-TNA	The destination TNA to which a connection should be created.

Command Modes

MPLS O-UNI configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command whenever an O-UNI connection should be established by the router. Both O-UNI-C sides participating in an O-UNI connection may be configured with the **destination address ipv4** command. In this case, the destination TNA specified by each side must correspond to the TNA configured by the other side.

Note Based on the contention detection and backoff mechanisms defined in O-UNI 1.0, one of the routers will act as though it was configured with the **passive** command.

Examples

The following example shows how to configure the interface to initiate an O-UNI connection to TNA 10.10.10.10:

```
RP/0/RP0/CPU0:router(config)# mpls optical-uni
RP/0/RP0/CPU0:router(config-mpls-ouni)# interface POS 0/1/0/1
RP/0/RP0/CPU0:router(config-mpls-ouni-if)# destination address ipv4 10.10.10.10
```

The following example shows how to delete an interface as the initiator of an O-UNI connection to TNA 10.10.10.10:

```
RP/0/RP0/CPU0:router(config-mpls-ouni-if)# no destination address ipv4 10.10.10.10
```

Related Commands

Command	Description
passive	Configures an interface to terminate an O-UNI connection.

interface pos

To enter the O-UNI interface configuration mode, issue the **interface pos** command in MPLS O-UNI configuration mode.

interface pos [**location** *node-id*]

Syntax Description

location *node-id*	(Optional) Enters the interface configuration submode for the designated node. The *node-id* argument is entered in the rack/slot/module notation.

Command Modes

MPLS O-UNI configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command when an interface is to be configured for O-UNI. This command enters the configuration submode from which all O-UNI interface configurations are entered.

Examples

The following example shows how to enter MPLS O-UNI interface configuration mode for POS interface 0/1/0/0:

```
RP/0/RP0/CPU0:router(config)# mpls optical-uni
RP/0/RP0/CPU0:router(config-mpls-ouni)# interface POS 0/1/0/0
```

ipcc routed

To configure an Internet Protocol Control Channel (IPCC) that is routable, use the **ipcc routed** command in LMP neighbor configuration mode. When a routed IPCC is configured to a given neighbor, control traffic destined to that neighbor is IP routed to the configured remote router ID for that neighbor. A correctly configured routed IPCC to a given Link Management Protocol (LMP) neighbor is required before an Optical User Network Interface (O-UNI) label switched path (LSP) connection to that neighbor can be established. To remove the routed IPCC, use the **no** form of this command.

ipcc routed

no ipcc routed

Syntax Description

This command has no arguments or keywords.

Command Modes

LMP neighbor configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

This type of IPCC is IPv4 routed to the O-UNI neighbor to which it is connected. Ensure that the O-UNI neighbor is configured with a reachable IPv4 node ID.

Examples

The following example shows how to configure a routed IPCC for the O-UNI neighbor router1 whose destination IP address is the node ID of the neighbor router1 on an interface determined dynamically by an IP routing protocol:

```
RP/0/RP0/CPU0:router(config)# mpls optical-uni
RP/0/RP0/CPU0:router(config-mpls-ouni)# lmp neighbor router1
RP/0/RP0/CPU0:router(config-lmp-nbr)# ipcc routed
```

lmp data-link adjacency

To enter LMP data-link adjacency mode and configure the remote parameters of an O-UNI datalink, use the **lmp data-link adjacency** command in MPLS O-UNI configuration mode. To remove the remote configuration, use the **no** form of this command.

lmp data-link adjacency

no lmp data-link adjacency

Syntax Description

This command has no arguments or keywords.

Command Modes

MPLS O-UNI configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command to configure the remote parameters of an O-UNI datalink. The neighbor name of the remote end on the channel must be specified.

To remove all the remote datalink parameters at the same time, use the **no lmp data-link adjacency** command.

Examples

The following example shows how to configure the remote parameters of an O-UNI datalink:

```
RP0/2/RP0/CPU0:router(config)# mpls optical-uni
RP0/2/RP0/CPU0:router(config-mpls-ouni)# interface POS 0/1/0/0
RP0/2/RP0/CPU0:router(config-mpls-ouni-if)# lmp data-link adjacency
RP0/2/RP0/CPU0:router(config-mpls-ouni-if-adj)#
```

lmp neighbor

To configure or update a new or existing Optical User Network Interface (O-UNI) specific Link Management Protocol (LMP) neighbor and its associated parameters, use the **lmp neighbor** command in MPLS O-UNI configuration mode. To delete the record of the specified neighbor, use the **no** form of this command.

lmp neighbor *neighbor-name*

no lmp neighbor *neighbor-name*

Syntax Description

neighbor-name	A text string representing the name of the LMP neighbor.

Command Modes

MPLS O-UNI configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Neighbor names must be unique. A neighbor does not become operational until both the remote node ID and a routed Internet Protocol Control Channel (IPCC) are configured for that neighbor.

Note For Cisco IOS-XR software, you can configure up to ten LMP neighbors for each router.

Examples

The following example shows how to enter LMP neighbor configuration mode for neighbor router1, and also create the LMP neighbor if it does not already exist.

```
RP2/0/RP0/CPU0:router(config)# mpls optical-uni
RP2/0/RP0/CPU0:router(config-mpls-ouni)# mpls optical-uni lmp neighbor router1
```

The following example shows how to delete the neighbor router1:

```
RP/0/RP0/CPU0:router(config)# no mpls optical-uni lmp neighbor router1
```

mpls optical-uni

To enter Optical User Network Interface (O-UNI) and Link Management Protocol (LMP) commands, use the **mpls optical-uni** command in global configuration mode. This command will enter the MPLS O-UNI configuration mode, from where these commands are issued. To exit this submode, use the **exit** command.

mpls optical-uni

Syntax Description

This command has no arguments or keywords.

Command Modes

Global configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command when the router is to be configured for O-UNI. This command enters the configuration mode from which all O-UNI configuration is entered.

Examples

The following example shows how to enter the MPLS O-UNI configuration mode:

```
RP/0/RP0/CPU0:router(config)# mpls optical-uni
```

The following example shows how to exit the MPLS O-UNI configuration mode:

```
RP/0/RP0/CPU0:router(config-mpls-ouni)# exit
```

Related Commands

Command	Description
show mpls optical-uni	Displays general information about O-UNI connections.

neighbor

To associate an interface with a given Link Management Protocol (LMP) neighbor, use the **neighbor** command in LMP datalink adjacency configuration mode. To delete this association, use the **no** form of this command.

neighbor *neighbor-name*

no neighbor *neighbor-name*

Syntax Description

neighbor-name	A string of alphanumeric characters that defines the name of the LMP neighbor to create or modify.

Command Modes

LMP datalink adjacency configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

You can specify a forward reference to a neighbor that you have not yet configured. A neighbor does not become operational until both the remote node ID and a routed Internet Protocol Control Channel (IPCC) is configured for that neighbor. LMP neighbors are configured under the MPLS O-UNI configuration mode.

Examples

The following example shows how to associate the neighbor router1 with the datalink POS interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# mpls optical-uni
RP/0/RP0/CPU0:router(config-mpls-ouni)# interface POS0/1/0/1
RP/0/RP0/CPU0:router(config-mpls-ouni-if)# lmp data-link adjacency
RP/0/RP0/CPU0:router(config-mpls-ouni-if-adj)# neighbor router1
```

passive

To terminate an Optical User Network Interface (O-UNI) connection, use the **passive** command in the MPLS O-UNI interface configuration mode. To delete the connection, use the **no** form of this command.

passive

no passive

Syntax Description

This command has no arguments or keywords.

Command Modes

MPLS O-UNI configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command whenever the router is to terminate an O-UNI connection. The interface accepts the incoming connection request of any O-UNI-C. The router does not actively attempt to create a connection, but rather waits for an incoming connection request.

Note If a **destination address ipv4** command is configured, you must first enter the **no destination address ipv4** command before attempting to configure the **passive** command. Otherwise, you will get an error.

Examples

The following example shows how to configure POS interface 0/1/0/1 as the passive end of an O-UNI:

```
RP/0/RP0/CPU0:router(config)# mpls optical-uni
RP/0/RP0/CPU0:router(config-mpls-ouni)# interface POS 0/1/0/1
RP/0/RP0/CPU0:router(config-mpls-ouni-if)# passive
```

The following example shows how to delete the termination of the passive O-UNI interface:

```
RP/0/RP0/CPU0:router(config-mpls-ouni-if)# no passive
```

Related Commands

Command	Description
remote interface-id	Configures the remote datalink interface ID.

remote interface-id

To configure the remote datalink interface ID, use the **remote interface-id** command in LMP neighbor adjacency configuration mode. To delete the configuration, use the **no** form of this command.

remote interface-id *remote-interface-id*

no remote interface-id *remote-interface-id*

Syntax Description

remote-interface-id	This configured value is the interface ID of the neighbor's datalink. This is a number in the range of 1 to 4294967295.

Defaults

No remote datalink interface ID is configured.

Command Modes

LMP neighbor adjacency configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The remote interface ID must be set to the local interface ID at the neighbor end of the datalink.

Examples

The following example shows how to configure the interface-id for the remote neighbor of the datalink that is associated with POS interface 0/1/0/1:

```
RP/0/RP0/CPU0:router(config)# mpls optical-uni
RP/0/RP0/CPU0:router(config-mpls-ouni)# interface pos 0/2/0/0 lmp data-link adjacency
RP/0/RP0/CPU0:router(config-mpls-ouni-if)# lmp data-link adjacency
RP/0/RP0/CPU0:router(config-mpls-ouni-if-adj)# remote interface-id 2
```

Related Commands

Command	Description
snmp-server ifindex persist	Makes the interface index persistent.

remote node-id

To configure the remote node-id for an Optical User Network Interface (O-UNI) Link Management Protocol (LMP) neighbor, use the **remote node-id** command in the LMP neighbor configuration mode.

remote node-id *ip-address*

Syntax Description

ip-address	The address to which routed control messages are sent.

Command Modes

LMP neighbor configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The remote node ID must be set to the local LMP node ID of the neighbor.

Examples

The following example shows how to configure the node ID for a neighbor node:

```
RP/0/RP0/CPU0:router(config)# mpls optical-uni
RP/0/RP0/CPU0:router(config-mpls-ouni)# lmp neighbor router1
RP/0/RP0/CPU0:router(config-ouni-nbr-router1)# remote node-id 192.168.20.10
```

router-id (MPLS O-UNI)

To configure the local Optical User Network Interface (O-UNI) Link Management Protocol (LMP) node ID, also known as a router ID, on a router, use the **router-id** command in MPLS O-UNI configuration mode.

router-id {*ip-address* | *interface-name*}

Syntax Description

ip-address	IPv4 address to use as the router ID.
interface-name	Name of an interface whose address will be used as the LMP node ID.

Command Modes

MPLS O-UNI configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following example shows how to configure the node ID for a neighbor node:

```
RP/0/RP0/CPU0:router(config)# mpls optical-uni
RP/0/RP0/CPU0:router(config-mpls-ouni)# router-id loopback0
```

show mpls lmp clients

To display information about Link Management Protocol (LMP) clients, use the **show mpls lmp clients** command in EXEC mode.

show mpls lmp clients

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command to display a list of LMP client names with associated job IDs, the nodes on which the client is running, and the client uptime.

Examples

The following is sample output from the **show mpls lmp clients** command:

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

Current time: Thu Mar  6 07:26:27 2003
Total Number of Clients = 2
    Client    | Job ID |    Node     |       Uptime       |          Since
--------------+--------+-------------+--------------------+-------------------------
         rsvp      114   node0_0_0              36m13s   Tue Jul  1 11:22:39 2003
    ucp_O-UNI      116   node0_0_0              28m51s   Tue Jul  1 11:30:01 2003
```

show mpls lmp interface-id

To display the local Link Management Protocol (LMP) interface ID (also known as port ID, or component interface ID) for a given interface, use the **show mpls lmp interface-id** command in EXEC mode.

show mpls lmp interface-id *type number*

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
number	A physical interface number: • Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following is sample output from the **show mpls lmp interface-id** command:

```
RP/0/RP0/CPU0:router# show mpls lmp interface-id pos 0/7/0/0

Local LMP interface ID: Hex = 0xa, Dec = 10
```

Related Commands

Command	Description
show mpls optical-uni interface	Displays O-UNI information for an interface.

show mpls optical-uni

To display information about the state of Optical User Network Interface (O-UNI) connections, use the **show mpls optical-uni** command in EXEC mode.

show mpls optical-uni

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command to display brief information for the state of O-UNI connection states.

Examples

The following is sample output from the **show mpls optical-uni** command:

```
RP/0/RP0/CPU0:router# show mpls optical-uni

Index of abbreviations:
-----------------------
M=O-UNI configuration Mode.
P=Passive
AR =active/receiver
AS=active/sender
U=Unknown

Interface   TunID     M   Sig State     CCT Up Since          Remote Addr
--------- ---------  --- -----------   --------------------   -----------
POS2/0/0/0 000001    AS  Connected     27/02/2002 05:20:35    10.3.4.2
```

Related Commands

Command	Description
show mpls optical-uni interface	Displays detailed O-UNI information for a specific interface.

show mpls optical-uni checkpoint

To display Optical User Network Interface (O-UNI) information used during restart operations, use the **show mpls optical-uni checkpoint** command in EXEC mode.

show mpls optical-uni checkpoint

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command to display O-UNI information to be used during restart operations.

Note In general, this command is not used during normal operation. This command is used to diagnose problem conditions within the O-UNI process and should only be used when an O-UNI internal error occurs.

Examples

The following is sample output from the **show mpls optical-uni checkpoint** command:

```
RP/0/RP0/CPU0:router# show mpls optical-uni checkpoint

Interface         TunID  LspID CCT Up Since
---------------   -----  ----- --------------------
POS0_2_0_2       00004  00004 04/11/2003 15:01:07
```

show mpls optical-uni diagnostics

To display diagnostics information for an Optical User Network Interface (O-UNI) connection for a specific interface, use the **show mpls optical-uni diagnostics** command in EXEC mode.

show mpls optical-uni diagnostics [**interface** *type number* | **all**]

Syntax Description

interface	(Optional) Displays O-UNI diagnostics information related to the interface specified by *type number*.
type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
number	(Optional) A physical interface number: • Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.
all	(Optional) The diagnostics information is displayed for all O-UNI interfaces.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command to display O-UNI diagnostics information for a specific interface.

Examples

The following is sample output from the **show mpls optical-uni diagnostics** command:

```
RP/0/RP0/CPU0:router# show mpls optical-uni diagnostics interface POS 0/2/0/2
Interface [POS0/2/0/2]
Configuration: Active->User
Signaling State: [Path Retry]

Connection to OLM/LMP established? Yes
O-UNI to OLM/LMP DB sync. status: Synchronized

Connection to RSVP established? Yes
RSVP to OLM/LMP DB sync. status: Synchronized

The neighbor [router1] has been configured, and has the node id [55.56.
57.58]
```

```
Found a route to the neighbor [router1]

Remote switching capability is TDM.
TNA [10.0.0.5] configured.

All required configs have been entered.

Global Code: No Error/ Success @ unknown time
Datalink Code: PathErr Received @ 04/11/2003 17:06:48
```

Related Commands

Command	Description
show mpls optical-uni	Displays information about the state of O-UNI connections.

show mpls optical-uni interface

To display detailed Optical User Network Interface (O-UNI) information for a specific interface, use the **show mpls optical-uni interface** command in EXEC mode.

show mpls optical-uni interface *type number*

Syntax Description

type	Interface type. For more information, use the question mark (**?**) online help function.
number	A physical interface number: • Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command to display O-UNI information for a specific interface.

Examples

The following is sample output from the **show mpls optical-uni interface** command:

```
RP/0/RP0/CPU0:router# show mpls optical-uni interface POS 0/2/0/2
Interface POS0/2/0/2
Configuration: Active->User
Signaling State: Connected since 04/11/2003 15:01:07
TNA: 10.0.0.5
Sender NodeID/Tunnel ID: 11.12.13.14/4
Local Data Link ID: 2
Remote Data Link ID: 2
Local Switching Capability: PSC 1
Remote Switching Capability: TDM
Primary IPCC:  Interface: Routed
               Local IP Address:  0.0.0.0
               Remote IP Address: 55.56.57.58
```

Related Commands

Command	Description
show mpls optical-uni	Displays information about the state of all O-UNI connections.

show mpls optical-uni lmp

To display information related to the Link Management Protocol (LMP), use the **show mpls optical-uni lmp** command in EXEC mode.

show mpls optical-uni lmp [**neighbor** [*neighbor-name*] | **ipcc** | **interface** *type number*]

Syntax Description

neighbor	(Optional) Displays detailed information about all or a specific LMP neighbor identified by *neighbor-name*.
neighbor-name	(Optional) A string of alphanumeric characters that defines the name of the LMP neighbor. When not specified, information about all neighbors is displayed.
ipcc	(Optional) Displays configured IP control channels (IPCCs) and the status of each.
interface	(Optional) Displays LMP information related to the interface specified by *type number.*
type	(Optional) Interface type. For more information, use the question mark (**?**) online help function.
number	(Optional) A physical interface number: • Interface rack, slot, module, and port numbers in this notation: rack/slot/module/port. A slash mark between numbers is required as part of the notation. For more information about the numbering syntax for the router, use the question mark (**?**) online help function.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command to display information about LMP.

Examples

The following is sample output from the **show mpls optical-uni lmp neighbor** command for a neighbor named router1:

```
RP/0/RP0/CPU0:router# show mpls optical-uni lmp neighbor router1

LMP Neighbor
Name: router1, IP: 10.33.44.11, Owner: Optical UNI
 IPCC ID: 1, State Up
  Known via             : Configuration
  Type                  : Routed
  Destination IP        : 10.33.44.11
  Source IP             : None
Data Link I/F  |  Lcl Data Link ID | Link TNA Addr | Data Link LMP state
---------------+------------------+----------------+--------------------
     POS0/1/0/0    2              10.0.0.20          Up      Alloc
```

The following is sample output from the **show mpls optical-uni lmp ipcc** command:

```
RP/0/RP0/CPU0:router# show mpls optical-uni lmp ipcc

                IPCC                        |  Neighbor
  Id |    Type    |      IP       Status   |    Name
-----+------------+--------------+--------+----------------
   2      Routed     10.21.21.21   Up           router1
   1      Routed       10.42.8.4   Up           router12
```

The following is sample output from the **show mpls optical-uni lmp** command, which summarizes all LMP information about neighbors and IPCCs. In addition, it displays the local LMP router ID:

```
RP/0/RP0/CPU0:router# show mpls optical-uni lmp

Local O-UNI CLI LMP Node ID: 10.3.3.3
(Source: O-UNI LMP CLI configuration, I/F: Loopback0)

LMP Neighbor
Name: router1, IP: 10.33.44.11, Owner: Optical UNI
 IPCC ID: 1, State Up
  Known via             : Configuration
  Type                  : Routed
  Destination IP        : 30.31.32.33
  Source IP             : None

Data Link I/F  |  Lcl Data Link ID | Link TNA Addr | Data Link LMP state
---------------+------------------+----------------+--------------------
     POS0/4/0/2                   1         10.4.4.4                 UP
```

The following is sample output from the **show mpls optical-uni lmp interface** command:

```
RP/0/RP0/CPU0:router# show mpls optical-uni lmp interface POS0/2/0/0

                          Interface: POS0/2/0/0
                              Owner: Optical UNI
             Local data link ID type: Unnumbered
                  Local data link ID: Hex = 0x1, Dec = 1
                    TNA address type: IPv4
                         TNA address: 10.0.0.50
  Local TE link switching capability: Packet-Switch Capable-1 (PSC-1)
                Remote neighbor name: router1
             Remote neighbor node ID: 10.33.44.11
            Remote data link ID type: Unnumbered
                 Remote data link ID: Dec = 1, Hex = 0x1
 Remote TE link switching capability: Time-Division-Multiplex Capable (TDM)
                 Data link I/F state: Up
                 Data link LMP state: Up/Allocated
```

```
          TE link LMP state: Up
Data link allocation status: Allocated
                    IPCC ID: 2
                  IPCC type: Routed
IPCC destination IP address: 10.41.11.1
```

Related Commands

Command	Description
show mpls optical-uni	Displays general information about O-UNI connections.

show mpls optical-uni timers all

To display the state of all timers running within the Optical User Network Interface (O-UNI) process, use the **show mpls optical-uni timers all** command in EXEC mode.

show mpls optical-uni timers all

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command to display a list of all timers running within the O-UNI process. The output of the command also displays the associated interface name, the type and name of the timer, the time the timer was set, and how long the timer should run before expiring.

Note This command can be used during normal operational conditions in order to determine the time left until a timer expires.

Examples

The following is sample output from the **show mpls optical-uni timers all** command:

```
RP/0/RP0/CPU0:router# show mpls optical-uni timers all
Present Time: 04/11/2003 15:59:45

O-UNI timers presently active for nodes:

IP addr.    Type     Name         Set@                  Timeout
----------  -------- ------------ --------------------  -------
55.56.57.5  Node Id  NBRREFR      04/11/2003 15:59:35   0000120

Present Time: 04/11/2003 15:59:45

O-UNI timers presently active on interfaces:

Ifname          Type      Name         Set@                  Timeout
--------------- --------- ------------ --------------------- -------
POS0/2/0/2      Interface RETRY        04/11/2003 15:59:26   0000060


Present Time: 04/11/2003 15:59:45
```

```
O-UNI global timers presently active:

Type     Name         Set@                  Timeout
-------- ------------ --------------------  -------
```

Related Commands

Command	Description
show mpls optical-uni timers global	Displays a list of global timers running within the O-UNI process.
show mpls optical-uni timers interfaces	Displays a list of interface timers running within the O-UNI process.
show mpls optical-uni timers nodes	Displays a list of internal process node timers running within the O-UNI process.

show mpls optical-uni timers global

To display a list of global timers running within the Optical User Network Interface (O-UNI) process, use the **show mpls optical-uni timers global** command in EXEC mode.

show mpls optical-uni timers global

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command to determine the state of O-UNI internal global process timers.

Examples

The following is sample output from the **show mpls optical-uni timers global** command:

```
RP/0/RP0/CPU0:router# show mpls optical-uni timers global
Present Time: 04/11/2003 16:45:38

O-UNI global timers presently active:

Type     Name         Set@                 Timeout
-------- ------------ -------------------  -------
Global   OLM Registra 04/11/2003 16:45:38   0000005
```

Related Commands

Command	Description
show mpls optical-uni timers all	Displays a list of all timers running within the O-UNI process.
show mpls optical-uni timers interfaces	Displays a list of interface timers running within the O-UNI process.
show mpls optical-uni timers nodes	Displays a list of node timers running within the O-UNI process.

show mpls optical-uni timers interfaces

To display interface timers running within the Optical User Network Interface (O-UNI) process, use the **show mpls optical-uni timers interfaces** command in EXEC mode.

show mpls optical-uni timers interfaces

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command to determine the state of O-UNI internal interface process timers.

Examples

The following is sample output from the **show mpls optical-uni timers interfaces** command:

```
RRP/0/RP0/CPU0:router# show mpls optical-uni timers interfaces
Present Time: 04/11/2003 16:54:57

O-UNI timers presently active on interfaces:

Ifname           Type      Name         Set@                 Timeout
---------------- --------- ------------ -------------------- -------
POS0/2/0/2       Interface RETRY        04/11/2003 16:54:38  0000060
```

Related Commands

Command	Description
show mpls optical-uni timers all	Displays a list of all timers running within the O-UNI process.
show mpls optical-uni timers global	Displays a list of global timers running within the O-UNI process.
show mpls optical-uni timers nodes	Displays a list of node timers running within the O-UNI process.

show mpls optical-uni timers nodes

To display the state of Optical User Network Interface (O-UNI) internal process node timers, use the **show mpls optical-uni timers nodes** command in EXEC mode.

show mpls optical-uni timers nodes

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use this command to display O-UNI internal process node timers.

Examples

The following is sample output from the **show mpls optical-uni timers nodes** command:

```
RP/0/RP0/CPU0:router# show mpls optical-uni timers nodes
Present Time: 04/11/2003 17:02:34

O-UNI timers presently active for nodes:

IP addr.    Type     Name         Set@                  Timeout
----------  -------- ------------ --------------------  -------
55.56.57.5  Node Id  NBRREFR      04/11/2003 17:02:21   0000120
```

Related Commands

Command	Description
show mpls optical-uni timers all	Displays a list of all timers running within the O-UNI process.
show mpls optical-uni timers global	Displays a list of global timers running within the O-UNI process.
show mpls optical-uni timers interfaces	Displays a list of interface timers running within the O-UNI process.

tna ipv4

To configure the transport network address (TNA) for an Optical User Network Interface (O-UNI) datalink, use the **tna ipv4** command in LMP datalink adjacency configuration mode.

tna ipv4 *ip-address*

Syntax Description

ip-address	The O-UNI TNA. This address is assigned by the optical transport network (OTN) operator.

Command Modes

LMP datalink adjacency configuration

Command History

Release	Modification
Release 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 the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Examples

The following example shows how to configure the datalink for POS interface 0/1/0/1 to the TNA 192.168.4.5:

```
RP/0/RP0/CPU0:router(config)# mpls optical-uni
RP/0/RP0/CPU0:router(config-mpls-ouni)# interface pos 0/1/0/1
RP/0/RP0/CPU0:router(config-mpls-ouni-if)# lmp data-link adjacency
RP/0/RP0/CPU0:router(config-mpls-ouni-if-adj)# tna ipv4 192.168.4.5
```

HR	Cisco IOS-XR Interface and Hardware Component Command Reference
IR	Cisco IOS-XR IP Addresses and Services Command Reference
MCR	Cisco IOS-XR Multicast Command Reference
MPR	Cisco IOS-XR MPLS Command Reference
RR	Cisco IOS-XR Routing Command Reference
SMR	Cisco IOS-XR System Management Command Reference
SR	Cisco IOS-XR System Security Command Reference

A

admin-weight command **MPR-42**
affinity command **MPR-43**
attribute-flags command **MPR-45**
autoroute announce command **MPR-46**
autoroute metric command **MPR-47**

B

backoff command **MPR-2**
backup-bw command **MPR-48**
backup-path tunnel-te command **MPR-50**
bandwidth (MPLS TE) command **MPR-52**
bandwidth (RSVP) command **MPR-148**

C

clear mpls forwarding counters command **MPR-120**
clear mpls ldp msg-counters neighbor command **MPR-4**
clear mpls packet counters command **MPR-121**
clear mpls traffic-eng counters tunnels command **MPR-54**
clear mpls traffic-eng fast-reroute log command **MPR-123**
clear mpls traffic-eng link-management statistics command **MPR-55**
clear rsvp counters all command **MPR-150**
clear rsvp counters events command **MPR-152**
clear rsvp counters messages command **MPR-153**

D

destination address ipv4 command **MPR-196**
disable (explicit-path) command **MPR-56**
discovery command **MPR-5**
discovery transport-address command **MPR-7**

E

exclude-address command **MPR-57**
explicit-null command **MPR-9**
explicit-path command **MPR-59**

F

fast-reroute command **MPR-60**
flooding thresholds command **MPR-61**

G

graceful-restart command **MPR-11**

H

holdtime command **MPR-14**

I

index (explicit path) command **MPR-63**
interface (MPLS LDP) command **MPR-15**
interface pos command **MPR-197**
interface tunnel-te command **MPR-64**

ipcc routed command MPR-198
ipv4 unnumbered (interface) command MPR-66

L

lmp data-link adjacency command MPR-199
lmp neighbor command MPR-200
log neighbor changes command MPR-17

M

mpls ip-ttl-propagate command MPR-124
mpls label range command MPR-125
mpls ldp restart session command MPR-18
mpls optical-uni command MPR-201
mpls traffic-eng area command MPR-67
mpls traffic-eng fast-reroute timers promotion command MPR-68
mpls traffic-eng interface command MPR-69
mpls traffic-eng level command MPR-70
mpls traffic-eng link-management flood command MPR-71
mpls traffic-eng link-management timers bandwidth-hold command MPR-72
mpls traffic-eng link-management timers periodic command MPR-73
mpls traffic-eng maximum tunnels command MPR-74
mpls traffic-eng path-selection metric command MPR-75
mpls traffic-eng reoptimize (configuration) command MPR-76
mpls traffic-eng reoptimize (EXEC) command MPR-77
mpls traffic-eng reoptimize timers delay command MPR-78
mpls traffic-eng router-id command MPR-80
mpls traffic-eng signalling advertise explicit-null command MPR-81
mpls traffic-eng topology holddown sigerr command MPR-82

N

neighbor command MPR-202
neighbor implicit-withdraw command MPR-19
neighbor password command MPR-18, MPR-20
next-address command MPR-84

P

passive command MPR-203
path-option command MPR-85
path-selection metric command MPR-87
priority (MPLS TE) command MPR-89

R

record route command MPR-91
remote interface-id command MPR-204
remote node-id command MPR-205
router-id (MPLS LDP) command MPR-21
router-id (MPLS O-UNI) command MPR-206
rsvp command MPR-154
rsvp interface command MPR-155
rsvp signalling graceful-restart command MPR-157
rsvp signalling graceful-restart restart-time command MPR-162
rsvp signalling hello graceful-restart refresh interval command MPR-159
rsvp signalling hello graceful-restart refresh misses command MPR-161

S

show explicit-paths command MPR-92
show mpls forwarding command MPR-127
show mpls forwarding hw command MPR-130
show mpls interfaces command MPR-132
show mpls label range command MPR-134
show mpls label table command MPR-135

show mpls ldp backoff command MPR-23
show mpls ldp bindings command MPR-24
show mpls ldp discovery command MPR-27
show mpls ldp forwarding command MPR-29
show mpls ldp graceful-restart command MPR-30
show mpls ldp neighbor command MPR-31
show mpls ldp parameters command MPR-33
show mpls ldp statistics msg-counters command MPR-35
show mpls ldp summary command MPR-37
show mpls lmp clients command MPR-207
show mpls lmp interface-id command MPR-208
show mpls lsd applications command MPR-137
show mpls lsd clients command MPR-139
show mpls optical-uni checkpoint command MPR-210
show mpls optical-uni command MPR-209
show mpls optical-uni diagnostics command MPR-211
show mpls optical-uni interface command MPR-213
show mpls optical-uni lmp command MPR-215
show mpls optical-uni timers all command MPR-218
show mpls optical-uni timers global command MPR-220
show mpls optical-uni timers interfaces command MPR-221
show mpls optical-uni timers nodes command MPR-222
show mpls packet counters command MPR-140
show mpls traffic-eng autoroute command MPR-94
show mpls traffic-eng counters tunnel command MPR-95
show mpls traffic-eng fast-reroute database command MPR-142
show mpls traffic-eng fast-reroute log command MPR-145
show mpls traffic-eng forwarding command MPR-96
show mpls traffic-eng link-management admission-control command MPR-97
show mpls traffic-eng link-management advertisements command MPR-98
show mpls traffic-eng link-management bandwidth-allocation command MPR-100
show mpls traffic-eng link-management igp-neighbors command MPR-102
show mpls traffic-eng link-management interface command MPR-103
show mpls traffic-eng link-management statistics command MPR-105
show mpls traffic-eng link-management summary command MPR-107
show mpls traffic-eng maximum tunnels command MPR-109
show mpls traffic-eng topology command MPR-110
show mpls traffic-eng tunnels command MPR-112
show rsvp counters command MPR-164
show rsvp graceful-restart command MPR-166
show rsvp hello instance command MPR-168
show rsvp interface command MPR-170
show rsvp request command MPR-172
show rsvp reservation command MPR-174
show rsvp sender command MPR-176
show rsvp session command MPR-178
signalling dscp command MPR-180
signalling rate-limit command MPR-182
signalling refresh interval command MPR-184
signalling refresh missed command MPR-186
signalling refresh reduction disable command MPR-188
signalling refresh reduction reliable command MPR-190
signalling refresh reduction summary command MPR-193
snmp-server enable traps mpls ldp command MPR-39
snmp-server enable traps mpls traffic-eng command MPR-116

T

tna ipv4 command MPR-223