CONTENTS

PREFACE

Preface xi
Communications, Services, and Additional Information xi

CHAPTER 1

MPLS Label Distribution Protocol Commands 1

backoff 3
clear mpls ldp msg-counters neighbor 4
clear mpls ldp neighbor 5
default-route 6
discovery hello 7
discovery instance-tlv disable 8
discovery targeted-hello 9
discovery transport-address 11
entropy-label 13
explicit-null 14
graceful-restart (MPLS LDP) 16
session holdtime (MPLS LDP) 18
hw-module l3 feature mpls-over-udp-decap enable 19
igp auto-config disable 20
igp sync delay 21
igp sync delay on-proc-restart 22
interface (MPLS LDP) 24
l2vpn neighbor all ldp flap 26
label accept 27
label advertise 29
label allocate 32
log graceful-restart 34
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>log neighbor</td>
<td>36</td>
</tr>
<tr>
<td>log nsr</td>
<td>37</td>
</tr>
<tr>
<td>log session-protection</td>
<td>38</td>
</tr>
<tr>
<td>mpls ldp</td>
<td>39</td>
</tr>
<tr>
<td>mpls lsd app-reg-delay disable</td>
<td>40</td>
</tr>
<tr>
<td>neighbor password</td>
<td>41</td>
</tr>
<tr>
<td>neighbor password disable</td>
<td>43</td>
</tr>
<tr>
<td>neighbor targeted</td>
<td>44</td>
</tr>
<tr>
<td>nsr (MPLS-LDP)</td>
<td>45</td>
</tr>
<tr>
<td>redistribute (MPLS LDP)</td>
<td>47</td>
</tr>
<tr>
<td>router-id (MPLS LDP)</td>
<td>48</td>
</tr>
<tr>
<td>session protection</td>
<td>50</td>
</tr>
<tr>
<td>show mpls ldp backoff</td>
<td>52</td>
</tr>
<tr>
<td>show mpls ldp bindings</td>
<td>54</td>
</tr>
<tr>
<td>show mpls ldp discovery</td>
<td>60</td>
</tr>
<tr>
<td>show mpls ldp forwarding</td>
<td>64</td>
</tr>
<tr>
<td>show mpls ldp graceful-restart</td>
<td>68</td>
</tr>
<tr>
<td>show mpls ldp igp sync</td>
<td>70</td>
</tr>
<tr>
<td>show mpls ldp interface</td>
<td>73</td>
</tr>
<tr>
<td>show mpls ldp neighbor</td>
<td>76</td>
</tr>
<tr>
<td>show mpls ldp parameters</td>
<td>82</td>
</tr>
<tr>
<td>show mpls ldp statistics msg-counters</td>
<td>85</td>
</tr>
<tr>
<td>show mpls ldp summary</td>
<td>87</td>
</tr>
<tr>
<td>show lcc</td>
<td>89</td>
</tr>
<tr>
<td>signalling dscp (LDP)</td>
<td>91</td>
</tr>
<tr>
<td>snmp-server traps mpls ldp</td>
<td>92</td>
</tr>
</tbody>
</table>

**CHAPTER 2**

**MPLS Forwarding Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls ip-ttl-propagate</td>
<td>96</td>
</tr>
<tr>
<td>mpls label range</td>
<td>98</td>
</tr>
<tr>
<td>show mpls forwarding</td>
<td>100</td>
</tr>
<tr>
<td>show mpls forwarding tunnels</td>
<td>104</td>
</tr>
<tr>
<td>show mpls forwarding exact-route</td>
<td>106</td>
</tr>
<tr>
<td>show mpls interfaces</td>
<td>110</td>
</tr>
</tbody>
</table>
CHAPTER 3

MPLS Traffic Engineering Commands 127
  adjustment-threshold (MPLS-TE) 131
  admin-weight 133
  affinity 134
  affinity-map 139
  application (MPLS-TE) 141
  attribute-flags 143
  attribute-names 145
  attribute-set 146
  auto-bw (MPLS-TE) 149
  auto-bw collect frequency (MPLS-TE) 151
  autoroute announce 153
  autoroute metric 154
  auto-tunnel backup (MPLS-TE) 156
  backup-bw 158
  backup-path tunnel-te 160
  bw-limit (MPLS-TE) 162
  clear mpls traffic-eng auto-bw (MPLS-TE EXEC) 164
  clear mpls traffic-eng auto-tunnel backup unused 166
  clear mpls traffic-eng auto-tunnel mesh 167
  clear mpls traffic-eng counters auto-tunnel mesh 168
  clear mpls traffic-eng counters auto-tunnel backup 169
  clear mpls traffic-eng counters global 170
  clear mpls traffic-eng counters signaling 171
  clear mpls traffic-eng counters soft-preemption 173
  clear mpls traffic-eng fast-reroute log 174
  clear mpls traffic-eng link-management statistics 175
### Contents

- mpls traffic-eng router-id (MPLS-TE router)  226
- mpls traffic-eng repotimize mesh group  228
- named-tunnels tunnel-te  229
- nhop-only (auto-tunnel backup)  230
- overflow threshold (MPLS-TE)  232
- path-option (MPLS-TE)  234
- path-selection ignore overload (MPLS-TE)  237
- path-selection invalidation  239
- path-selection loose-expansion affinity (MPLS-TE)  240
- path-selection loose-expansion domain-match  242
- path-selection loose-expansion metric (MPLS-TE)  243
- path-selection metric (MPLS-TE)  245
- path-selection metric (interface)  247
- pce address (MPLS-TE)  248
- pce deadtimer (MPLS-TE)  250
- pce keepalive (MPLS-TE)  252
- pce peer (MPLS-TE)  254
- pce reoptimize (MPLS-TE)  256
- pce request-timeout (MPLS-TE)  258
- pce tolerance keepalive (MPLS-TE)  260
- priority (MPLS-TE)  262
- record-route  264
- reoptimize timers delay (MPLS-TE)  265
- router-id secondary (MPLS-TE)  268
- show explicit-paths  269
- show mpls traffic-eng affinity-map  271
- show mpls traffic-eng attribute-set  273
- show mpls traffic-eng autoroute  275
- show mpls traffic-eng auto-tunnel backup  277
- show mpls traffic-eng auto-tunnel mesh  280
- show mpls traffic-eng collaborator-timers  282
- show mpls traffic-eng counters signaling  284
- show mpls traffic-eng ds-te te-class  290
- show mpls traffic-eng forwarding  292
signalling prefix-filtering default-deny-action 462
signalling rate-limit 463
signalling refresh interval 465
signalling refresh missed 467
signalling refresh reduction bundle-max-size 469
signalling refresh reduction disable 470
signalling refresh reduction reliable 472
signalling refresh reduction summary 475
window-size (RSVP) 477

CHAPTER 5

MPLS OAM Commands 479

clear mpls oam counters 480
echo disable-vendor-extension 481
echo revision 482
mpls oam 483
ping mpls ipv4 484
ping pseudowire (AToM) 489
ping mpls traffic-eng tunnel-te (P2P) 493
ping mpls traffic-eng tunnel-mte (P2MP) 496
ping mpls mldp (P2MP) 502
ping mpls mldp (MP2MP) 508
show mpls oam 514
show mpls oam database 516
trace mpls ipv4 517
trace mpls multipath 520
trace mpls traffic-eng tunnel-te (P2P) 524
trace mpls traffic-eng tunnel-mte (P2MP) 527
trace mpls mldp (P2MP) 531
trace mpls mldp (MP2MP) 536
Preface

The preface contains these sections:

• Communications, Services, and Additional Information, on page xi

Communications, Services, and Additional Information

• To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
• To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
• To submit a service request, visit Cisco Support.
• To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
• To obtain general networking, training, and certification titles, visit Cisco Press.
• To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.
MPLS Label Distribution Protocol Commands

This module describes the commands used to configure Label Distribution Protocol (LDP) in a Multiprotocol Label Switching (MPLS) network on Cisco NCS 6000 Series Routers.

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

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

For detailed information about MPLS concepts, configuration tasks, and examples, see MPLS Configuration Guide for Cisco NCS 6000 Series Routers and MPLS Configuration Guide for Cisco NCS 560 Series Routers.

- backoff, on page 3
- clear mpls ldp msg-counters neighbor, on page 4
- clear mpls ldp neighbor, on page 5
- default-route, on page 6
- discovery hello, on page 7
- discovery instance-tlv disable, on page 8
- discovery targeted-hello, on page 9
- discovery transport-address, on page 11
- entropy-label, on page 13
- explicit-null, on page 14
- graceful-restart (MPLS LDP), on page 16
- session holdtime (MPLS LDP), on page 18
- hw-module l3 feature mpls-over-udp-decap enable, on page 19
- igp auto-config disable, on page 20
- igp sync delay, on page 21
- igp sync delay on-proc-restart, on page 22
- interface (MPLS LDP), on page 24
- l2vpn neighbor all ldp flap, on page 26
- label accept, on page 27
- label advertise, on page 29
- label allocate, on page 32
- log graceful-restart, on page 34
• log neighbor, on page 36
• log nsr, on page 37
• log session-protection, on page 38
• mpls ldp, on page 39
• mpls lsd app-reg-delay disable, on page 40
• neighbor password, on page 41
• neighbor password disable, on page 43
• neighbor targeted, on page 44
• nsr (MPLS-LDP), on page 45
• redistribute (MPLS LDP), on page 47
• router-id (MPLS LDP), on page 48
• session protection, on page 50
• show mpls ldp backoff, on page 52
• show mpls ldp bindings, on page 54
• show mpls ldp discovery, on page 60
• show mpls ldp forwarding, on page 64
• show mpls ldp graceful-restart, on page 68
• show mpls ldp igp sync, on page 70
• show mpls ldp interface, on page 73
• show mpls ldp neighbor, on page 76
• show mpls ldp parameters, on page 82
• show mpls ldp statistics msg-counters, on page 85
• show mpls ldp summary, on page 87
• show lcc, on page 89
• signalling dscp (LDP), on page 91
• snmp-server traps mpls ldp, on page 92
backoff

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

```
backoff initial maximum
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>initial</code></td>
<td>Initial backoff delay, in seconds. Range is 5 to 50331.</td>
</tr>
<tr>
<td><code>maximum</code></td>
<td>Maximum backoff delay, in seconds. Range is 5 to 50331.</td>
</tr>
</tbody>
</table>

**Command Default**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>initial</code></td>
<td>15</td>
</tr>
<tr>
<td><code>maximum</code></td>
<td>120</td>
</tr>
</tbody>
</table>

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls ldp backoff</td>
<td>Displays information about the configured session setup backoff parameters and LDP peers.</td>
</tr>
<tr>
<td>show mpls ldp parameters</td>
<td>Displays current LDP parameter settings.</td>
</tr>
</tbody>
</table>
### clear mpls ldp msg-counters neighbor

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

**clear mpls ldp  msg-counters neighbor  [{lsr-id  ldp-id}]**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>lsr-id</code></td>
<td>LSR ID of neighbor in A.B.C.D format.</td>
<td></td>
</tr>
<tr>
<td><code>ldp-id</code></td>
<td>LDP ID of neighbor in A.B.C.D format.</td>
<td></td>
</tr>
</tbody>
</table>

#### Command Default

No default behavior or values

#### Command Modes

XR EXEC mode

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

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

#### Examples

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

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

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mpls ldp statistics msg-counters</code></td>
<td>Displays statistics about the type and count of the messages sent and received from neighbors.</td>
</tr>
</tbody>
</table>
# clear mpls ldp neighbor

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

```
clear mpls ldp neighbor [{ip-address ldp-id}]  
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
</table>
| `ip-address`       | (Optional) Neighbor IP address.  

**Command Default**

No default behavior or values

**Command Modes**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `clear mpls ldp neighbor` 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# clear mpls ldp neighbor 10.20.20.20
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls ldp neighbor, on page 76</td>
<td>Displays information about LDP neighbors.</td>
</tr>
</tbody>
</table>
To enable Multiprotocol Label Switching (MPLS) switching for IP default route by allocating and advertising non-null label, use the `default-route` command in MPLS LDP configuration mode. To return to the default behavior, use the `no` form of this command.

**default-route**

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

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

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls ldp bindings, on page 54</td>
<td>Displays LDP label bindings.</td>
</tr>
<tr>
<td>show mpls ldp forwarding, on page 64</td>
<td>Displays LDP installed forwarding state.</td>
</tr>
</tbody>
</table>
discovery hello

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

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

**Syntax Description**

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

**Command Default**

- **holdtime**: 15
- **interval**: 5

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- **mpls-ldp**: read, write

**Examples**

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

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

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

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

**Related Commands**

- **unique_14**: Configures targeted-hello messages.
discovery instance-tlv disable

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

**discovery instance-tlv disable**

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

**Command Default**
No default behavior or values

**Command Modes**
MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_14</td>
<td>Configures targeted-hello messages.</td>
</tr>
</tbody>
</table>
discovery targeted-hello

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

\[
\text{discovery targeted-hello address-family \{} \{accept \} | [from acl] | \text{holdtime seconds} | \text{interval seconds}\}
\]

**Syntax Description**

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

**Command Default**

- **accept**: Targeted hello messages are not accepted from any source (neighbor).
- **holdtime**: 90
- **interval**: 10

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

LDP supports IPv4 standard access lists only.

**Examples**

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

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

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

```
RP/0/RP0/CPU0:router(config-ldp)# discovery targeted-hello interval 5
```
The following example shows how to configure acceptance of targeted hellos from all peers:

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

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

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

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls ldp discovery, on page 60</td>
<td>Displays LDP discovery information.</td>
<td></td>
</tr>
<tr>
<td>show mpls ldp parameters, on page 82</td>
<td>Displays LDP parameters information.</td>
<td></td>
</tr>
</tbody>
</table>
discovery transport-address

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address to be advertised as the transport address in discovery hello messages.</td>
</tr>
<tr>
<td>interface</td>
<td>Advertises the IP address of the interface as the transport address in discovery hello messages.</td>
</tr>
</tbody>
</table>

**Command Default**

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

**Command Modes**

MPLS LDP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

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

**Note**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>
The following example shows how to specify an exiting address (10.10.3.1) as the transport address on an interface POS 0/1/0/0:

```
RP/0/RP0/CPU0:router(config-ldp)# interface POS 0/1/0/0
RP/0/RP0/CPU0:router(config-ldp-if)# address-family ipv4
RP/0/RP0/CPU0:router(config-ldp-if-af)# discovery transport-address 10.10.3.1
```

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

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls ldp discovery, on page 60</td>
<td>Displays the status of the LDP discovery process.</td>
</tr>
<tr>
<td>show mpls ldp neighbor, on page 76</td>
<td>Displays information about LDP neighbors.</td>
</tr>
</tbody>
</table>
entropy-label

To enable entropy label LDP signaling on the ingress LSR in an MPLS network, use the `entropy-label` command in MPLS LDP configuration mode.

To remove this configuration, use the `no` prefix for the command.

**Command Default**

- **None**

**Command Modes**

- **MPLS LDP configuration mode.**

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Entropy labels are used by the ingress LSR for efficient load balancing of traffic through the MPLS network. An entropy label is inserted on top of the MPLS label stack at the ingress LSR. Entropy labels help the smooth operation of the transit LSRs by relieving them of the task of deep packet inspection.

The `entropy-label` command supports an orderly method for routers to signal entropy label capability (ELC) in the network. When enabled, the Cisco routers wait for the ELC signal from all downstream routers before passing their ELC to the next upstream routers in the chain. This eliminates the confusion that can occur when routers report their status randomly. If just one router in the chain does not support entropy label (EL), then the network will not use EL for load balancing. Random reporting could result in a lot of back and forth signaling before ELC is firmly established in the network.

**Example**

The following example shows how you can configure entropy label LDP signaling on transit LSR for load balancing.

```
RP/0/RP0/CPU0:router(config)# cef load-balancing fields mpls entropy-label
RP/0/RP0/CPU0:router(config)# mpls ldp
RP/0/RP0/CPU0:router(config-ldp)# entropy-label
RP/0/RP0/CPU0:router(config-ldp)# commit
RP/0/RP0/CPU0:router(config-ldp)# end
```
explicit-null

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

`explicit-null [ { to peer-acl | for prefix-acl [ to peer-acl ] } ]`

### Syntax Description

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

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

### Command Default

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

### Command Modes

MPLS LDP configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

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

LDP supports IPv4 standard access lists only.

### Examples

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

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

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

```
RP/0/RP0/CPU0:router(config-ldp)# explicit-null
RP/0/RP0/CPU0:router(config-ldp)# explicit-null for 192.168.0.0
```
The following command sequence shows how to send explicit-null for all directly connected routes to peers 10.1.1.1 and 10.2.2.2 and implicit-null to all other peers:

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

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

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

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

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

```
graceful-restart  [{reconnect-timeout  seconds | forwarding-state-holdtime  seconds}]
```

**Syntax Description**

- **reconnect-timeout** *seconds*  
  (Optional) Configures the time that the local LDP sends to its graceful restartable peer, indicating how long its neighbor should wait for reconnection in the event of a LDP session failure, in seconds. Range is 60 to 1800.

- **forwarding-state-holdtime** *seconds*  
  (Optional) Configures the time the local forwarding state is preserved (without being reclaimed) after the local LDP control plane restarts, in seconds. Range is 60 to 1800.

**Command Default**

By default, graceful restart is disabled.

- **reconnect-timeout**: 120  
  - **forwarding-state-holdtime**: 180

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

The value of the forwarding state hold time keeps the forwarding plane state associated with the LDP control-plane in case of a control-plane restart or failure. If the control plane fails, the forwarding plane retains the LDP forwarding state for twice the forwarding state hold time. The value of the forwarding state hold time is also used to start the local LDP forwarding state holder after the LDP control plane restarts. When the LDP graceful restart sessions are renegotiated with its peers, the restarting LSR sends the remaining value of this timer as the recovery time to its peers. Upon local LDP restart with graceful restart enabled, LDP does not replay forwarding updates to MPLS forwarding until the forwarding state hold timer expires.
In the presence of a peer relationship, any change to the LDP graceful restart configuration will restart LDP sessions. If LDP configuration changes from nongraceful restart to graceful restart, all the sessions are restarted. Only graceful restart sessions are restarted upon graceful restart to nongraceful restart configuration changes.

### Examples

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

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

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

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

<table>
<thead>
<tr>
<th>Peer</th>
<th>GR</th>
<th>Up Time</th>
<th>Discovery Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.3.3:0</td>
<td>Y</td>
<td>00:01:04</td>
<td>3</td>
</tr>
<tr>
<td>2.2.2.2:0</td>
<td>N</td>
<td>00:01:02</td>
<td>2</td>
</tr>
</tbody>
</table>
```

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

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls ldp forwarding, on page 64</td>
<td>Displays the contents of the LDP forwarding database.</td>
</tr>
<tr>
<td>show mpls ldp graceful-restart, on page 68</td>
<td>Displays information related to graceful restart.</td>
</tr>
<tr>
<td>show mpls ldp neighbor, on page 76</td>
<td>Displays information about LDP neighbors.</td>
</tr>
<tr>
<td>show mpls ldp parameters, on page 82</td>
<td>Displays current LDP parameter settings.</td>
</tr>
<tr>
<td>show mpls ldp summary, on page 87</td>
<td>Displays summarized information regarding the LDP process.</td>
</tr>
</tbody>
</table>
session holdtime (MPLS LDP)

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

```
session holdtime seconds
```

**Syntax Description**

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

**Command Default**

- `seconds`: 180

**Command Modes**

- MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

- `mpls-ldp` read, write

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mpls ldp parameters</code>, on page 82</td>
<td>Displays current LDP parameter settings.</td>
</tr>
</tbody>
</table>
**hw-module l3 feature mpls-over-udp-decap enable**

To enable UDP decapsulation of UDP-encapsulated MPLS traffic on the ASR 9000 Series router, configure the `hw-module l3 feature mpls-over-udp-decap enable` command in XR Config mode. To return to the default behavior, use the `no` form of this command.

**hw-module l3 feature mpls-over-udp-decap enable**

This command has no keywords or arguments.

<table>
<thead>
<tr>
<th>Command Default</th>
<th>UDP decapsulation function is disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>XR Config mode</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you enable this command on a WAN edge ASR 9000 Series router, the UDP header is removed from UDP-encapsulated MPLS traffic. Based on the MPLS label, the traffic is forwarded towards the destination. If you don’t enable this function, the WAN edge router drops the UDP-encapsulated MPLS traffic it receives.

**Examples**

The following example shows how to configure UDP decapsulation function:

```
Router# configure
Router(config)# hw-module l3 feature mpls-over-udp-decap enable
Router(config)# commit
```
igp auto-config disable

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

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

MPLS LDP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls ldp interface, on page 73</td>
<td>Displays information about LDP-enabled interfaces.</td>
</tr>
</tbody>
</table>
igp sync delay

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

```
igp sync delay  seconds
```

**Syntax Description**

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

**Command Default**

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

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- By default, LDP declares LDP sync up as soon as all the requisite conditions are met, namely:
  - LDP session is up.
  - LDP has sent all its label bindings to at least one peer.
  - LDP has received at least one label binding from a peer.

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

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mpls ldp igp sync</code></td>
<td>Displays LDP IGP sync information for link(s).</td>
</tr>
</tbody>
</table>
**igp sync delay on-proc-restart**

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

```
igp sync delay on-proc restart  seconds
```

**Syntax Description**

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

**Command Default**

This command is disabled by default.

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

```
RP/0/RP0/CPU0:router# show mpls ldp igp sync
  Process Restart Sync Delay: 60 sec, Gloal timer running (15 sec remaining)
  GigabitEthernet0/3/0/2:
    Sync status: Deferred
...
```

When the timer is not running, the output displays the following:
Process Restart Sync Delay: 60 sec, Global timer not running

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show mpls ldp igp sync, on page 70</td>
<td>Displays LDP IGP sync information for link(s).</td>
</tr>
</tbody>
</table>
interface (MPLS LDP)

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

```
interface type interface-path-id
```

**Syntax Description**

- `type`  
  Interface type. For more information, use the question mark (?) online help function.

- `interface-path-id`  
  Physical interface or a virtual interface.

**Note**  
Use the `show interfaces` command to see a list of all possible interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No default behavior or values

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

**Note**

You cannot enable LDP on loopback interfaces.

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

### Task ID Operations

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

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

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

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

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls ldp parameters, on page 82</td>
<td>Displays current LDP parameter settings.</td>
</tr>
<tr>
<td>show mpls ldp neighbor, on page 76</td>
<td>Displays LDP neighbor session parameters.</td>
</tr>
</tbody>
</table>
**l2vpn neighbor all ldp flap**

To flap the LDP sessions in order to enable interoperability with the peer router which does not support label request, use the **l2vpn neighbor all ldp flap** command in XR Config mode.

To return to the default behavior, use the **no** form of this command.

### Syntax Description

This command has no arguments or keywords.

### Command Default

None

### Command Modes

XR Config mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.4</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Configuring the **l2vpn neighbor all ldp flap** command flaps all the LDP sessions when a route processor fail over (RPFO) occurs.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

The following example shows how to flap the LDP sessions:

```
RP/0/RP0/CPU0:router#config
RP/0/RP0/CPU0:router#l2vpn neighbor all ldp flap
RP/0/RP0/CPU0:router#commit
```
label accept

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>prefix-acl</code></td>
<td>Accepts and retains remote bindings for prefixes that are permitted by the prefix access list <code>prefix-acl</code> argument.</td>
</tr>
<tr>
<td><code>ip-address</code></td>
<td>Displays the peer IP address.</td>
</tr>
</tbody>
</table>

**Command Default**

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

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

LDP supports IPv4 standard access lists only.

**Note**

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

**Task ID**

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

**Examples**

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

```
RP/0/RP0/CPU0:router(config-ldp)# label accept
RP/0/RP0/CPU0:router(config-ldp-lbl-acpt)# for pfx_acl_1 from 1.1.1.1
RP/0/RP0/CPU0:router(config-ldp-lbl-acpt)# for pfx_acl_2 from 2.2.2.2
RP/0/RP0/CPU0:router(config-ldp-lbl-acpt)# for pfx_acl_3 from 3.3.3.3
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>label advertise, on page 29</td>
<td>Controls advertisement of LDP local label bindings (outbound label filtering).</td>
</tr>
<tr>
<td></td>
<td>#unique_36</td>
<td>Resets LDP neighbor sessions.</td>
</tr>
<tr>
<td></td>
<td>show mpls ldp bindings, on page 54</td>
<td>Displays LDP binding information.</td>
</tr>
</tbody>
</table>
label advertise

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>(Optional) Disables label advertisement to all peers for all prefixes.</td>
</tr>
<tr>
<td>for prefix-acl</td>
<td>(Optional) Specifies prefix destinations for which labels will be advertised.</td>
</tr>
<tr>
<td>to peer-acl</td>
<td>(Optional) Specifies which LDP neighbors will receive label advertisements.</td>
</tr>
<tr>
<td>interface</td>
<td>(Optional) Specifies an interface for label allocation and advertisement of its interface IP address.</td>
</tr>
<tr>
<td>type</td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or a virtual interface.</td>
</tr>
</tbody>
</table>

**Note**  Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

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

**Command Modes**  MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

- Every command has a prefix-acl or peer-acl pair associated with it, as follows:
  - In the absence of the **for** or **to** keywords, the access list pair is (none, none).
  - When using the **for** keyword without the **to** keyword, the access list is (prefix-acl, none).

- A prefix can have a maximum of one (prefix-acl, peer-acl) pair, as follows:
  - A (prefix-acl, peer-acl) pair applies to a prefix only if the prefix-acl matches the prefix. A match occurs if the prefix-acl permits the prefix.
  - If more than one (prefix-acl, peer-acl) pair from multiple **label advertise** commands matches a prefix, the (prefix-acl, peer-acl) pair in the first command applies to the prefix. The order in which
the `label advertise` commands are processed is sorted based on the ACL names in a MIB-lexicographical way (shorter ACL name length will be processed first, if two ACLs are of equal length, then dictionary ordering is used).

- When an LSR is ready to advertise a label for a prefix, the LSR determines whether a (prefix-acl, peer-acl) pair applies to the prefix.
  - If none applies, and if the `disable` keyword has been configured for the command, the label for the prefix is not advertised to any peer; otherwise, the label is advertised to all peers.
  - If a (prefix-acl, peer-acl) pair applies to the prefix, and if the prefix-acl denies the prefix, the label is not advertised to the peers defined in the peer-acl. Nevertheless, the prefix may be matched in subsequent (prefix-acl, peer-acl) entries and advertised to other peers.
  - If (prefix-acl, peer-acl) pair applies to the prefix and if the prefix-acl denies the prefix, the label is not advertised to peers defined in the peer-acl. Nevertheless, the prefix may be matched in subsequent (prefix-acl, peer-acl) entries and advertised to other peers.
  - If the prefix-acl permits the prefix and there is a peer-acl, the label is advertised to all peers permitted by the peer-acl.

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

LDP supports IPv4 standard access lists only.

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

### Examples

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

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

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

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

RP/0/RP0/CPU0:router(config-ldp)# label advertise
RP/0/RP0/CPU0:router(config-ldp-lbl-advt)# disable
RP/0/RP0/CPU0:router(config-ldp-lbl-advt)# for pfx_acl_1
```
The following example shows how to send labels for prefix 10.0.0.0 to peers 10.1.1.1 and 10.2.2.2, labels for prefix 20.0.0.0 to peer 20.1.1.1, and labels for all other prefixes to all other peers:

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

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

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

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

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

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

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

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

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mpls ldp neighbor</code>, on page 76</td>
<td>Displays information about LDP neighbors.</td>
</tr>
<tr>
<td><code>show mpls ldp bindings</code>, on page 54</td>
<td>Displays information about LDP label bindings.</td>
</tr>
</tbody>
</table>
label allocate

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

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

**Syntax Description**

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

**Command Default**

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

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

LDP supports IPv4 standard access lists only.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list pfx_acl_1
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 192.168.1.1
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 192.168.2.2
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 192.168.3.3
RP/0/RP0/CPU0:router(config-ldp)# label allocate for pfx_acl_1
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show mpls ldp bindings, on page 54</td>
<td>Displays information about LDP label bindings.</td>
</tr>
<tr>
<td></td>
<td>show mpls ldp forwarding, on page 64</td>
<td>Displays the contents of the LDP forwarding database.</td>
</tr>
</tbody>
</table>
log graceful-restart

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

**log graceful-restart**

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

**Command Default**
No default behavior or values

**Command Modes**
MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

```
RP/0/RP0/CPU0:router: mpls_ldp[340]: %ROUTING-LDP-5-GR : GR session 4.4.4.4:0 (instance 1) disconnected
RP/0/RP0/CPU0:router: mpls_ldp[340]: %ROUTING-LDP-5-GR : GR session 4.4.4.4:0 (instance 2) reconnected
RP/0/RP0/CPU0:router: mpls_ldp[340]: %ROUTING-LDP-5-GR : GR session 5.5.5.5:0 (instance 3) timed out
RP/0/RP0/CPU0:router: mpls_ldp[336]: %ROUTING-LDP-5-GR_RESTART_COMPLETE : GR forwarding state hold timer has expired
```
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mpls ldp neighbor, on page 76</code></td>
<td>Displays information about LDP neighbors.</td>
</tr>
<tr>
<td><code>show mpls ldp graceful-restart, on page 68</code></td>
<td>Displays information about LDP GR sessions.</td>
</tr>
</tbody>
</table>
To enable logging of notices describing session changes, use the `log neighbor` command in MPLS LDP configuration mode. To return to the default behavior, use the `no` form of this command.

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

**Command Default**
No default behavior or values

**Command Modes**
MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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

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

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

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mpls ldp neighbor</code>, on page 76</td>
<td>Displays information about LDP neighbors.</td>
</tr>
</tbody>
</table>
To enable logging of nonstop routing (NSR) synchronization events, use the `log nsr` command in MPLS LDP configuration mode. To return to the default behavior, use the `no` form of this command.

**log nsr**

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

**Command Default**
No default behavior or values

**Command Modes**
MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

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

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

**Note**

Logging messages are issued when session protection events occur.

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

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mpls ldp neighbor</code>, on page 76</td>
<td>Displays information about LDP neighbors.</td>
</tr>
</tbody>
</table>
mpls ldp

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

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

XR Config mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to MPLS LDP configuration mode:

```plaintext
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls ldp
RP/0/RP0/CPU0:router(config-ldp)
```
mpls lsd app-reg-delay disable

Allows LDP to allocate labels with out any delay if segment routing will not be configured. By default, MPLS Label Switching Database (LSD) waits for segment routing enabled IGP to allocate labels first because of their global significance. LSD allows LDP to allocate labels only after segment routing enabled IGP completes label allocation. If segment routing will not be configured, this leads to additional delay and may cause traffic drops after router reload. This command avoids the delay in label allocation.

mpls lsd app-reg-delay disable

This command has no arguments or keywords.

Command Default:

No default behavior or values

Command Modes:

XR Config mode

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.3.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

No specific guidelines impact the use of this command.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

The following example shows how to configure **mpls lsd app-reg-delay disable** command:

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# mpls lsd app-reg-delay disable
neighbor password

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

```
[vrf vrf-name] neighbor ldp-id password {clear | disable | encrypted} password
no [vrf vrf-name] neighbor ldp-id password
```

**Syntax Description**

- **ldp-id**
  - LDP ID of neighbor in A.B.C.D:0 format.

- **clear**
  - Clears the password for the encryption parameter to specify that an unencrypted password will follow.

- **encrypted**
  - Specifies that an encrypted password will follow.

- **password**
  - (Clear text) Encrypted or unencrypted password string.

**Command Default**

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

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

To override the default password for a specific neighbor, use the `neighbor ldp-id password` command, where the `ldp-id` argument is the LDP ID of the neighbor.

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>
Examples

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

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor targeted, on page 44</td>
<td>Configures transmission of targeted hellos towards a neighbor.</td>
</tr>
</tbody>
</table>
neighbor password disable

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

neighbor IP-address password disable

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-address</td>
<td>Neighbor IP address.</td>
</tr>
</tbody>
</table>

Command Default

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

Command Modes

MPLS LDP configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

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

Note

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

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

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

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

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

```
address-family {} neighbor IP address targeted
no address-family {} neighbor IP address targeted
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>IP address</code></td>
<td>Neighbor IP address.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>neighbor password</code>, on page 41</td>
<td>Configures password authentication using MD5.</td>
</tr>
<tr>
<td><code>show mpls ldp neighbor</code>, on page 76</td>
<td>Displays information about LDP neighbors.</td>
</tr>
<tr>
<td><code>show mpls ldp discovery</code>, on page 60</td>
<td>Displays information about LDP discovery sources.</td>
</tr>
</tbody>
</table>
**nsr (MPLS-LDP)**

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

```
nsr
no nsr
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

By default, MPLS LDP NSR is disabled.

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

- LDP process restart
- In-service system upgrade (ISSU)
- Minimum disruption restart (MDR)

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

**Note**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable MPLS LDP NSR:

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>nsr process-failures switchover</code></td>
<td>Configures switchover as a recovery action for active instances to switch over to a standby RP or a DRP, to maintain NSR. For more information, see <em>IP Addresses and Services Command Reference</em>.</td>
</tr>
<tr>
<td><code>show mpls ldp neighbor, on page 76</code></td>
<td>Displays standby node specific information.</td>
</tr>
</tbody>
</table>
**redistribute (MPLS LDP)**

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp</td>
<td>Redistributions information from BGP protocols.</td>
</tr>
<tr>
<td>as as-number</td>
<td>Specifies the BGP autonomous system number.</td>
</tr>
<tr>
<td>advertise-to access-list</td>
<td>Advertise the redistributed route information.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS</td>
<td>read, write</td>
</tr>
<tr>
<td>LDP</td>
<td>write</td>
</tr>
</tbody>
</table>

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

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

RP/0/RP0/CPU0:router# show run mpls ldp | b bgp
bgp
   as 10000
!```
router-id (MPLS LDP)

To specify an IPv4 address to act as the router ID, use the `router-id` command in MPLS LDP configuration mode. To return to the default behavior, use the `no` form of this command.

```
router-id  lsr-id
no   router-id
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>lsr-id</th>
<th>LSR ID in A.B.C.D format.</th>
</tr>
</thead>
</table>

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

**Command Modes**
MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

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

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

**Examples**
The following example shows how to specify an LSR ID as the router ID:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls ldp discovery, on page 60</td>
<td>Displays the status of the LDP discovery process.</td>
</tr>
<tr>
<td>show mpls ldp neighbor, on page 76</td>
<td>Displays information about LDP neighbors.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td><code>show mpls ldp parameters, on page 82</code></td>
<td>Displays current LDP parameter settings.</td>
</tr>
</tbody>
</table>
session protection

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

```
session protection [{duration seconds | infinite}] [for peer-acl]
```

**Syntax Description**

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

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

**Command Modes**
MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

LDP supports only IPv4 standard access lists.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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

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

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

```
RP/0/RP0/CPU0:router(config-ldp)# session protection for peer_acl duration 30
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show mpls ldp neighbor, on page 76</td>
<td>Displays information about LDP neighbors.</td>
</tr>
</tbody>
</table>
**show mpls ldp backoff**

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

```
show mpls ldp backoff [{location node-id | standby}]
```

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

**Command Default**
No default behavior or values

**Command Modes**
XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

**Examples**

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

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

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

Backoff Table: (2 entries)

<table>
<thead>
<tr>
<th>LDP Id</th>
<th>Backoff (sec)</th>
<th>Waiting (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>33.33.33.33:0</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>11.11.11.11:0</td>
<td>30</td>
<td>30</td>
</tr>
</tbody>
</table>
```

This table describes the significant fields shown in the display.

**Table 1: show mpls ldp backoff Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backoff Time</td>
<td>Initial and maximum backoff time parameters, in seconds.</td>
</tr>
</tbody>
</table>
List of discovered LDP neighbors for which session setup is being delayed because of previous failures to establish a session due to incompatible configuration. The backoff table incorporates the following information:

**LDP Id**
- Identifies the LDP neighbors.

**Backoff (sec)**
- Specifies the time that the session setup is delayed.

**Waiting (sec)**
- Specifies an approximate time the session setup has been delayed.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_52</td>
<td>Configures LDP backoff parameters.</td>
</tr>
<tr>
<td>show mpls ldp forwarding, on page 64</td>
<td>Displays the contents of MPLS forwarding table.</td>
</tr>
<tr>
<td>show mpls ldp bindings, on page 54</td>
<td>Displays the contents of LDP LIB.</td>
</tr>
</tbody>
</table>
show mpls ldp bindings

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix</td>
<td>(Optional) Destination prefix, written in A.B.C.D format.</td>
</tr>
<tr>
<td>length</td>
<td>(Optional) Network mask length, in bits. Range is 0 to 32.</td>
</tr>
<tr>
<td>advertisement-acls</td>
<td>(Optional) Displays the label bindings as applied for (advertisement) outbound label filtering ACLs.</td>
</tr>
<tr>
<td>brief</td>
<td>(Optional) Displays all the prefixes in the LDP database.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays the total counts of advertised-to and remote-binding peers in IP address sort order, with remote bindings in tabular format.</td>
</tr>
<tr>
<td>local</td>
<td>(Optional) Displays the local label bindings.</td>
</tr>
<tr>
<td>local-label label [to label]</td>
<td>(Optional) Displays entries matching local label values. Add the <code>label to label</code> argument to indicate the label range.</td>
</tr>
<tr>
<td>local-only</td>
<td>(Optional) Displays binding matches with a local label only.</td>
</tr>
<tr>
<td>neighbor address</td>
<td>(Optional) Displays the label bindings assigned by the selected neighbor.</td>
</tr>
<tr>
<td>remote-only</td>
<td>(Optional) Displays bindings matches with a remote label only.</td>
</tr>
</tbody>
</table>
### show mpls ldp bindings

| remote-label label [to label] | (Optional) Displays entries matching the label values assigned by a neighbor router. Add the `label to label` argument to indicate the label range. Range is from 0 to 2147483647. |
| summary | (Optional) Displays a summary of the contents of the Label Information Base (LIB). |
| location node-id | (Optional) Displays location information for the specified node ID. |
| standby | (Optional) Displays standby-node-specific information. |

#### Command Default
No default behavior or values

#### Command Modes
EXEC

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

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

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

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

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

#### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read</td>
</tr>
</tbody>
</table>

#### Examples

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

```
RP/0/RP0/CPU0:router# show mpls ldp bindings
5.41.0.0/16 , rev 4
```
The following sample output shows detailed information for the total counts of advertised-to and remote-binding peers in IP address sort order, with remote bindings for 150.150.150.32:

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

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

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

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

The following sample output shows detailed information for the total counts of advertised-to and remote-binding peers in IP address sort order, with remote bindings for 10.10.2.0/24:

```
local binding: label:IMP-NULL
No remote bindings

5.43.98/32 , rev 6
local binding: label:IMP-NULL
No remote bindings

10.10.2.0/24 , rev 12
local binding: label:IMP-NULL
remote bindings:
  lsr:10.255.255.255:0, label:16
  lsr:10.256.256.256:0, label:IMP-NULL

10.10.3.0/24 , rev 10
local binding: label:IMP-NULL
remote bindings:
  lsr:10.255.255.255:0, label:IMP-NULL
  lsr:10.256.256.256:0, label:22

22.22.22.22/32 , rev 14
local binding: label:16
remote bindings:
  lsr:10.255.255.255:0, label:17
  lsr:10.256.256.256:0, label:22

33.33.33.33/32 , rev 2
local binding: label:IMP-NULL
remote bindings:
  lsr:10.255.255.255:0, label:18
  lsr:10.256.256.256:0, label:23
```
This table describes the significant fields shown in the display.

**Table 2: show mpls ldp bindings and show mpls ldp bindings neighbor Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.b.c.d/n</td>
<td>IP prefix and mask for a particular destination (network/mask).</td>
</tr>
<tr>
<td>rev</td>
<td>Revision number (rev) that is used internally to manage label distribution for this destination.</td>
</tr>
<tr>
<td>local binding</td>
<td>Locally assigned label for a prefix.</td>
</tr>
<tr>
<td>remote bindings</td>
<td>Outgoing labels for this destination learned from other LSRs. Each item in this list identifies the LSR from which the outgoing label was learned and reflects the label associated with that LSR. Each LSR in the transmission path is identified by its LDP identifier.</td>
</tr>
</tbody>
</table>

1 Label switched routers.

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

```
RP/0/RP0/CPU0:router# show mpls ldp bindings summary
LIB Summary:
  Total Prefix : 20
  Revision No  : Current:34, Advertised:34
  Local Bindings : 14
    NULL : 10 (implicit:10, explicit:0)
    Non-NULL: 4 (lowest:48, highest:51)
  Remote Bindings: 24
```

This table describes the significant fields shown in the display.

**Table 3: show mpls ldp bindings summary Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Prefix</td>
<td>Number of prefixes (routes) known to LDP LIB. All invalid and timed-out routes display as no-routes.</td>
</tr>
</tbody>
</table>

[^1]: Label switched routers.
**Field** | **Description**
--- | ---
Revision No | Current revision number of LIB entries as well as the minimum revision number that has been advertised to all peers.
Local Bindings | Total number of local bindings, with information on how many of them are Null, non-null, and lowest/highest label assigned or allocated by LDP.
Remote Bindings | Number of remote bindings.

The following sample output shows the access-list advertisement:

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

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

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

This table describes the significant fields shown in the display.

**Table 4: show mpls ldp bindings advertisement-acls Command Field Descriptions**

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

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

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

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Local</th>
<th>Advertised</th>
<th>Remote</th>
<th>Bindings</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.2.2/32</td>
<td>-</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1.2.3.4/32</td>
<td>16010</td>
<td>396</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>4.4.4.4/32</td>
<td>16004</td>
<td>396</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>10.0.0.0/24</td>
<td>19226</td>
<td>396</td>
<td>395</td>
<td></td>
</tr>
</tbody>
</table>

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

**RP/0/RP0/CPU0:router# show mpls ldp bindings local-only**
The following sample output shows that the binding matches with a remote label:

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

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

10.43.4.0/24, rev 0
No local binding
Remote bindings: (1 peers)
Peer Label
----------------- --------
10.4.4.4:0 IMP-NULL

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>label accept, on page 27</td>
<td>Configures the LDP remote label acceptance.</td>
</tr>
<tr>
<td>label advertise, on page 29</td>
<td>Configures the LDP local label advertisement control.</td>
</tr>
<tr>
<td>show mpls ldp neighbor, on page 76</td>
<td>Displays information on the LDP neighbors.</td>
</tr>
<tr>
<td>show mpls ldp forwarding, on page 64</td>
<td>Displays the contents of the LDP forwarding database.</td>
</tr>
</tbody>
</table>
show mpls ldp discovery

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

```
show mpls ldp     [{} ]  discovery   [{}  type  interface-path-id  |  brief  |  link  |  targeted  |  summary  [all]]]  [detail]  [{}  location  node-id  |  standby]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>type</strong></td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><strong>interface-path-id</strong></td>
<td>Physical interface or a virtual interface.</td>
</tr>
<tr>
<td><strong>brief</strong></td>
<td>(Optional) Displays concise information about a specified LDP-enabled interface.</td>
</tr>
<tr>
<td><strong>link</strong></td>
<td>(Optional) Displays link information for LDP discovery.</td>
</tr>
<tr>
<td><strong>targeted</strong></td>
<td>(Optional) Displays targeted information for LDP discovery.</td>
</tr>
<tr>
<td><strong>summary</strong></td>
<td>(Optional) Displays summarized information for LDP discovery.</td>
</tr>
<tr>
<td><strong>detail</strong></td>
<td>(Optional) Displays detailed information (including, inbound label filtering, session KAs, and session protection state) for an LDP session.</td>
</tr>
<tr>
<td><strong>location node-id</strong></td>
<td>(Optional) Displays location information for the specified node ID.</td>
</tr>
<tr>
<td><strong>standby</strong></td>
<td>(Optional) Displays standby node-specific information.</td>
</tr>
</tbody>
</table>
**Command Default**
No default behavior or values

**Command Modes**
XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read</td>
</tr>
</tbody>
</table>

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

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

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

This table describes the significant fields shown in the display.

**Table 5: show mpls ldp discovery Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local LDP Identifier</td>
<td>LDP identifier for the local router. An LDP identifier is a 6-byte construct displayed in the form IP address:number. By convention, the first 4 bytes of the LDP identifier constitute the router ID; integers, starting with 0, constitute the final two bytes of the IP address:number construct.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Interfaces engaged in LDP discovery activity, as follows:</td>
</tr>
<tr>
<td></td>
<td><strong>xmit field</strong></td>
</tr>
<tr>
<td></td>
<td>Indicates that the interface is transmitting LDP discovery hello packets.</td>
</tr>
<tr>
<td></td>
<td><strong>recv field</strong></td>
</tr>
<tr>
<td></td>
<td>indicates that the interface is receiving LDP discovery hello packets.</td>
</tr>
<tr>
<td></td>
<td>The LDP identifiers indicate the LDP neighbors discovered on the interface.</td>
</tr>
<tr>
<td>Transport Address</td>
<td>Address associated with this LDP peer (advertised in hello messages).</td>
</tr>
<tr>
<td>LDP Id</td>
<td>LDP identifier of the LDP peer.</td>
</tr>
</tbody>
</table>
The following sample output summarizes information for LDP discovery by using the `summary` keyword:

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

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

This table describes the significant fields shown in the display.

**Table 6: show mpls ldp discovery summary Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDP Identifier</td>
<td>The LDP identifier for the local router.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Summary of interfaces engaged in LDP activity.</td>
</tr>
<tr>
<td>Configured</td>
<td>Number of interfaces configured for LDP.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Number of interfaces on which LDP is actively enabled and is thus sending LDP hellos. An interface configured for LDP is enabled only if running IP and not in the down state.</td>
</tr>
<tr>
<td>Discovery</td>
<td>Summary of LDP discovery process.</td>
</tr>
<tr>
<td>Hello xmit</td>
<td>Number of local LDP discovery sources (including link and targeted hellos) emitting LDP hellos.</td>
</tr>
<tr>
<td>Hello recv</td>
<td>Number of discovered hello sources via link or targeted hello mechanics.</td>
</tr>
</tbody>
</table>

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

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

Local LDP Identifier: 192.168.0.3:0

<table>
<thead>
<tr>
<th>Discovery Source</th>
<th>VRF Name</th>
<th>Peer LDP Id</th>
<th>Holdtime</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO0/3/0/2</td>
<td>default</td>
<td>192.168.0.1:0</td>
<td>15</td>
<td>Y</td>
</tr>
</tbody>
</table>
The following sample shows the MPLS LDP afi-all discovery brief command output:

RP/0/0/CPU0:router# show mpls ldp afi-all discovery brief

Local LDP Identifier: 192.168.0.1:0

<table>
<thead>
<tr>
<th>Discovery Source</th>
<th>AFI</th>
<th>VRF Name</th>
<th>Peer LDP Id</th>
<th>Holdtime</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO0/3/0/0</td>
<td>IPv6</td>
<td>default</td>
<td>192.168.0.2:0</td>
<td>15</td>
<td>Y</td>
</tr>
<tr>
<td>PO0/3/0/1</td>
<td>IPv4</td>
<td>default</td>
<td>192.168.0.3:0</td>
<td>15</td>
<td>Y</td>
</tr>
<tr>
<td>PO0/3/0/2</td>
<td>IPv4</td>
<td>default</td>
<td>192.168.0.4:0</td>
<td>15</td>
<td>Y</td>
</tr>
<tr>
<td>PO0/3/0/3</td>
<td>IPv6</td>
<td>default</td>
<td>192.168.0.3:0</td>
<td>15</td>
<td>Y</td>
</tr>
<tr>
<td>PO0/3/0/4</td>
<td>IPv6</td>
<td>default</td>
<td>192.168.0.5:0</td>
<td>15</td>
<td>Y</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_53</td>
<td>Configures LDP link hello parameters.</td>
</tr>
<tr>
<td>#unique_14</td>
<td>Configures LDP targeted-hello parameters.</td>
</tr>
<tr>
<td>neighbor targeted, on page 44</td>
<td>Configures LDP targeted neighbor.</td>
</tr>
<tr>
<td>session protection, on page 50</td>
<td>Configures LDP session protection.</td>
</tr>
<tr>
<td>interface (MPLS LDP), on page 24</td>
<td>Configures LDP on an interface.</td>
</tr>
<tr>
<td>show mpls ldp neighbor, on page 76</td>
<td>Displays information about LDP neighbors.</td>
</tr>
</tbody>
</table>
### show mpls ldp forwarding

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

```bash
show mpls ldp forwarding [prefix/length] [fast-reroute] [detail] [next-hop {address ip-address | interface interface-path-id | label label-value | neighbor ldp-id | unlabelled}] [local-label label-value] [{location node-id | summary | standby}]
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix</td>
<td>(Optional) Destination prefix, written in A.B.C.D format.</td>
</tr>
<tr>
<td>length</td>
<td>(Optional) Network mask length, in bits. Range is 0 to 32.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays detailed information for the LDP timestamp that is used for the routing and forwarding update.</td>
</tr>
<tr>
<td>fast-reroute</td>
<td>(Optional) Displays the prefix that is LFA FRR protected in nature.</td>
</tr>
<tr>
<td>next-hop</td>
<td>Matches prefixes by next-hop IP address.</td>
</tr>
<tr>
<td>local-label</td>
<td>(Optional) Displays the prefix with the specified local label. Range is from 0 to 1048575.</td>
</tr>
<tr>
<td>neighbor</td>
<td>Matches prefixes with a path through specified LDP neighbor.</td>
</tr>
<tr>
<td>unlabelled</td>
<td>Matches prefixes containing unlabelled paths.</td>
</tr>
<tr>
<td>location</td>
<td>(Optional) Displays location information for the specified node ID.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays the summary information for the LDP forwarding information base (LFIB).</td>
</tr>
<tr>
<td>standby</td>
<td>(Optional) Displays standby-node specific information.</td>
</tr>
</tbody>
</table>

#### Command Default

No default behavior or values

#### Command Modes

EXEC
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.0.0</td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

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

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>mpls-ldp read</td>
</tr>
</tbody>
</table>

Examples

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

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

Prefix Label Label Outgoing Next Hop GR Stale
------------------ ----- ---------- ------------ --------------- -- -----  
2.2.2.2/32 22 ImpNull PO0/2/0/1 12.0.0.2 N N
3.0.0.1/32 24 20 PO0/2/0/1 12.0.0.2 N N
3.0.0.2/32 25 21 PO0/2/0/1 12.0.0.2 N N
3.0.0.3/32 26 22 PO0/2/0/1 12.0.0.2 N N
4.4.4.4/32 20 ExpNullv4 tt10 4.4.4.4 N N
4.4.4.5/32 21 ExpNullv4 tt10 4.4.4.4 N N
123.0.0.0/24 23 ImpNull PO0/2/0/1 12.0.0.2 N N
3.3.3.3/32 1600 PO0/2/0/3.1 131.1.1.4 Y N
16002 PO0/2/0/3.2 131.1.2.4 Y N
16003 PO0/2/0/3.3 131.1.3.4 N N
16002 PO0/2/0/1 192.11.1.1 (!) Y N
Unlabelled PO0/2/0/2 192.11.2.1 (!) N N
```

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

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

```
RP/0/RP0/CPU0:router# show mpls ldp forwarding 1.1.1.32 detail

Prefix Label Label Outgoing Next Hop GR Stale
------------------ ------- ---------- ------------ --------------- -- -----  
3.3.3.3/32 16000 16001 PO0/2/0/3.1 131.1.1.4 N N
16002 PO0/2/0/3.2 131.1.2.4 Y N
16003 PO0/2/0/3.3 131.1.3.4 N N
16002 PO0/2/0/1 192.11.1.1 (!) Y N
Unlabelled PO0/2/0/2 192.11.2.1 (!) N N
```

Note

The (!) symbol refers to a non-primary LFA backup path.
This sample output shows only LDP prefixes with protection (ECMP or secondary LFA backups) update from the `fast-reroute` keyword:

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

```
RP/0/RP0/CPU0:router# show mpls ldp forwarding summary
Forwarding Server (LSD):
  Connected: Yes
  Forwarding State Holdtime: 360 sec
Forwarding States:
  Interfaces: 10
  Local labels: 8
Rewrites:
  Prefix:
    Total: 8 (0 with ECMP, 8 FRR protected)
    Labelled:
      Primary pathset: 8 labelled (0 partial), 0 unlabelled
      Backup pathset: 8 labelled (0 partial), 0 unlabelled
      Complete pathset: 8 labelled (0 partial), 0 unlabelled
Paths:
  Total: 16 (0 backup, 8 FRR protected)
  Labelled: 16 (8 backup)
```

This table describes the significant fields shown in the display.

### Table 7: show mpls ldp forwarding Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix/mask</td>
<td>Prefix on the FEC² for an MPLS forwarding entry.</td>
</tr>
<tr>
<td>Label In</td>
<td>Local label assigned to the prefix/mask.</td>
</tr>
<tr>
<td>Label Out</td>
<td>Outgoing label for the prefix/mask.</td>
</tr>
<tr>
<td>Outgoing Interface</td>
<td>Outgoing physical interface.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Next Hop address.</td>
</tr>
<tr>
<td>GR</td>
<td>Graceful restart status (Y or N).</td>
</tr>
<tr>
<td>Stale</td>
<td>Status of the entry, stale or not stale. An entry is marked stale when the next-hop graceful restart neighbor disconnects and is unmarked when neighbor reconnects and refreshes the label.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chkpt</td>
<td>Status of the entry, checkpointed or not checkpointed.</td>
</tr>
<tr>
<td>path-id</td>
<td>Primary Path-id.</td>
</tr>
<tr>
<td>Backup-path-id</td>
<td>The backup path-id is the path-id of the path protecting a given primary path. A protecting path can be primary path or a non-primary path.</td>
</tr>
<tr>
<td>Peer</td>
<td>Displays next-hop LDP peer's LDP identifier.</td>
</tr>
<tr>
<td>Connected</td>
<td>Displays LDP connection state with LSD forwarding server.</td>
</tr>
<tr>
<td>Forwarding State Holdtime</td>
<td>Displays time that LDP has registered with LSD server to keep LDP forwarding state intact upon LDP disconnect event.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Number of LDP enabled MPLS interfaces.</td>
</tr>
<tr>
<td>Local Labels</td>
<td>Number of LDP allocated local labels from LSD.</td>
</tr>
<tr>
<td>Rewrites</td>
<td>Counts of Forwarding rewrites. Displays total number of known IPv4 prefixes alongwith information on number of prefixes with more than one ECMP path. This also displays number of prefixes with LFA-FRR protection. The labelled set prints the counts related to prefixes with none, all, partial labelled paths as shown by unlabeled, labelled, and partial keywords. This information is available for primary, backup, and complete path set.</td>
</tr>
<tr>
<td>Paths</td>
<td>Forwarding path counts. Displays count of total number of known forwarding paths, along with number of backup paths and number of FRR protected paths. It also displays the count of labelled paths indicating how many of non-primary paths are labelled.</td>
</tr>
</tbody>
</table>

2 Forwarding Equivalence Class.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>graceful-restart (MPLS LDP), on page 16</td>
<td>Configures the LDP graceful restart feature.</td>
</tr>
<tr>
<td>show mpls ldp bindings, on page 54</td>
<td>Displays the contents of LDP LIB.</td>
</tr>
</tbody>
</table>
show mpls ldp graceful-restart

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

```
show mpls ldp graceful-restart [{location node-id }] [{standby}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>location node-id</th>
<th>(Optional) Displays location information for the specified node ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>standby</td>
<td>(Optional) Displays standby-node-specific information.</td>
</tr>
</tbody>
</table>

**Command Default**
No default behavior or values

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read</td>
</tr>
</tbody>
</table>

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

```
RP/0/RP0/CPU0:router# show mpls ldp graceful-restart
Forwarding State Hold timer : Not Running
  GR Neighbors : 1
    Neighbor ID Up Connect Count Liveness Timer Recovery Timer
    ----------- -- -------------- ------------------ ------------------
    10.0.0.2     Y 1               -                 -
```

This table describes the significant fields shown in the display.

**Table 8: show mpls ldp graceful-restart Command Field Descriptions**

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>graceful-restart (MPLS LDP), on page 16</td>
<td>Configures the LDP graceful restart feature.</td>
</tr>
<tr>
<td>show mpls ldp neighbor, on page 76</td>
<td>Displays information about LDP neighbors.</td>
</tr>
</tbody>
</table>
show mpls ldp igp sync

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

```
show mpls ldp [[{}]] igp sync [interface type interface-path-id] [location node-id] [standby]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>(Optional) Displays the interface type.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>(Optional) Physical interface or a virtual interface.</td>
</tr>
<tr>
<td>location node-id</td>
<td>(Optional) Displays location information for the specified node ID.</td>
</tr>
<tr>
<td>standby</td>
<td>(Optional) Displays standby node-specific information.</td>
</tr>
</tbody>
</table>

**Note**

Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

LDP IGP synchronization addresses traffic loss issues as a result of synchronization between MPLS LDP and IP (IGP). For instance, upon a link up, IGP can advertise a link before MPLS converges on the link. Also, the IGP link is still used even when MPLS session goes down and MPLS LSP is broken on this link. The use of IGP link is determined based on MPLS LDP convergence synchronization status on the link.
Use the `show mpls ldp igp sync` command to display MPLS convergence status. The configuration for LDP IGP synchronization resides in IGPs (OSPF, ISIS); accordingly, LDP displays and advertises this information for all LDP-enabled interfaces (regardless if the interface is configured for LDP IGP).

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read</td>
</tr>
</tbody>
</table>

### Examples

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

```
RP/0/RP0/CPU0:router# show mpls ldp igp sync
POS0/3/0/2:  
  VRF: 'default' (0x60000000)  
  Sync delay: Disabled  
  Sync status: Ready  
  Peers:  
    192.168.0.1:0 (GR)
```

This table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF</td>
<td>VRF of the interface.</td>
</tr>
<tr>
<td>Sync status</td>
<td>MPLS LDP convergence status on a given link. Ready indicates that the link is converged and is ready to be used by IGP. Not Ready with Deferred means that the link fulfills LDP IGP synchronization requirements but is deferred by LDP IGP synchronization delay timeout configuration setting. Not Ready means that the link is not ready to be used by IGP.</td>
</tr>
<tr>
<td>Peers</td>
<td>List of peers converged on the given link. If the peer session is GR(^3)-enabled, output is tagged as GR. If GR-only reachability is indicated due to a GR neighbor record recovered from checkpoint after local start, then Chkpt-created flag is also set.</td>
</tr>
</tbody>
</table>

\(^3\) Graceful Restart.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>igp sync delay, on page 21</code></td>
<td>Configures LDP IGP sync delay timeout.</td>
</tr>
</tbody>
</table>
show mpls ldp interface

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

```
show mpls ldp interface [{[type interface-path-id | summary] | brief} | standby]
```

**Syntax Description**

- `type` (Optional) Interface type. For more information, use the question mark (?) online help function.

- `interface-path-id` Physical interface or a virtual interface.

- `summary` (Optional) Displays summary information about a specified LDP-enabled interface.

- `brief` (Optional) Displays concise information about a specified LDP-enabled interface.

- `detail` (Optional) Displays detailed information about a specified LDP-enabled interface.

- `location node-id` (Optional) Displays location information for the specified node ID.

- `standby` (Optional) Displays standby-node-specific information.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

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

```
RP/0/RP0/CPU0:router# show mpls ldp interface
```
Interface GigabitEthernet0/3/0/3
   No LDP config
Interface POS0/2/0/0
   No LDP config
   Auto-config items:
      ospf/100/0
Interface POS0/2/0/1
   No LDP config
   Auto-config items:
      ospf/100/0
Interface POS0/2/0/2
   No LDP config
   Auto-config items:
      ospf/100/0
Interface POS0/2/0/3
   No LDP config
   Auto-config items:
      ospf/100/0

This table describes the significant fields shown in the display.

Table 10: show mpls ldp interface Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-config items</td>
<td>Lists IGPs that specify an interface for MPLS LDP auto-configuration:</td>
</tr>
<tr>
<td></td>
<td>OSPF</td>
</tr>
<tr>
<td></td>
<td>ospf instance area</td>
</tr>
<tr>
<td></td>
<td>ISIS</td>
</tr>
<tr>
<td></td>
<td>isis instance</td>
</tr>
</tbody>
</table>

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

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>igp auto-config disable, on page 20</code></td>
<td>Enables LDP auto-configuration.</td>
</tr>
</tbody>
</table>
show mpls ldp neighbor

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

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

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

Usage Guidelines

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

- LDP neighbors with specific IP addresses
- LDP neighbors on a specific interface
- LDP neighbors that are graceful restartable
- LDP neighbors that are nongraceful restartable
- LDP neighbors enabled with session protection

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read</td>
</tr>
</tbody>
</table>

Examples

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

```
RP/0/RP0/CPU0:router# show mpls ldp neighbor 4.4.4.4

Peer LDP Identifier: 4.4.4.4:0
TCP connection: 14.1.0.41:38022 - 1.1.1.1:646
Graceful Restart: Yes (Reconnect Timeout: 120 sec, Recovery: 96 sec)
Session Holdtime: 180 sec
State: Oper; Msgs sent/rcvd: 1721/1716; Downstream-Unsolicited
Up time: 1d00h
LDP Discovery Sources:
  IPv4: (1)
    GigabitEthernet0/1/0/0
  IPv6: (0)
Addresses bound to this peer:
  IPv4: (3)
    4.4.4.4    14.1.0.41    24.1.0.4
  IPv6: (0)
```

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

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

Peer LDP Identifier: 10.44.44.4:0
TCP connection: 10.44.44.4:65535 - 10.33.33.33:646
Graceful Restart: No
State: Oper; Msgs sent/rcvd: 49/46
Up time: 00:33:33
LDP Discovery Sources:
  POS 0/1/0/0
```
Addresses bound to this peer:
10.44.44.44  10.10.3.2
Peer LDP Identifier: 10.22.22.22:0
TCP connection: 10.22.22.22:646 - 10.33.33.33:65530
Graceful Restart: No
State: Oper; Msgs sent/rcvd: 48/45
Up time: 00:33:11
LDP Discovery Sources:
POS 0/2/0/0
Addresses bound to this peer:
10.22.22.22  10.10.2.1

This table describes the significant fields shown in the display.

Table 11: show mpls ldp neighbor Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer LDP Identifier</td>
<td>LDP identifier of the neighbor (peer) for this session.</td>
</tr>
<tr>
<td>TCP connection</td>
<td>TCP connection used to support the LDP session, shown in the following format:</td>
</tr>
<tr>
<td></td>
<td>neighbor IP address</td>
</tr>
<tr>
<td></td>
<td>peer port</td>
</tr>
<tr>
<td></td>
<td>local IP address</td>
</tr>
<tr>
<td></td>
<td>local port</td>
</tr>
<tr>
<td>Graceful Restart</td>
<td>Graceful-restart status (Y or N).</td>
</tr>
<tr>
<td>State</td>
<td>State of the LDP session. Generally this is Oper (operational), but transient is another possible state.</td>
</tr>
<tr>
<td>Msgs sent/rcvd</td>
<td>Number of LDP messages sent to and received from the session peer. The count includes the transmission and receipt of periodic keepalive messages, which are required for maintenance of the LDP session.</td>
</tr>
<tr>
<td>Up time</td>
<td>The length of time that this session has been up for (in hh:mm:ss format).</td>
</tr>
<tr>
<td>LDP Discovery Sources</td>
<td>The source(s) of LDP discovery activity leading to the establishment of the LDP session.</td>
</tr>
</tbody>
</table>
| Addresses bound to this peer | The known interface addresses of the LDP session peer. These are addresses that might appear as “next hop” addresses in the local routing table. They are used to maintain the LFIB.

4 LFIB = Label Forwarding Information Base.

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

```
RP/0/RP0/CPU0:router# show mpls ldp neighbor brief
Peer   GR  NSR  Up Time  Discovery Addresses  Labels
       ipv4 ipv6 ipv4 ipv6 ipv4 ipv6 ipv4 ipv6
```
This table describes the significant fields shown in the display.

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

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

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

Peer LDP Identifier: 2.2.2.2:0
TCP connection: 2.2.2.2:11707 - 1.1.1.1:646
Graceful Restart: No
Session Holdtime: 180 sec
State: Oper; Mags sent/rcvd: 33/29
Up time: 00:13:37
LDP Discovery Sources:
  POS0/2/0/1
  Targeted Hello (1.1.1.1 -> 2.2.2.2, active)
Addresses bound to this peer:
  23.0.0.2
  20.0.0.2
  123.0.4.2
  10.42.37.119
  10.2.2.2
Peer holdtime: 180 sec; KA interval: 60 sec; Peer state: Estab
Clients: Dir Adj Client
Inbound label filtering: accept acl 'pfx_acl1'
Session Protection:
  Enabled, state: Ready
  Duration: 30 seconds
```

This table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer LDP Identifier</td>
<td>LDP identifier of the neighbor (peer) for this session.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TCP connection</td>
<td>TCP connection used to support the LDP session, shown in the following format: &lt;br&gt; &lt;b&gt;neighbor IP address&lt;/b&gt; &lt;br&gt; &lt;b&gt;peer port&lt;/b&gt; &lt;br&gt; &lt;b&gt;local IP address&lt;/b&gt; &lt;br&gt; &lt;b&gt;local port&lt;/b&gt;</td>
</tr>
<tr>
<td>Graceful Restart</td>
<td>Graceful-restart status (Y or N).</td>
</tr>
<tr>
<td>Session Holdtime</td>
<td>Session hold time, in seconds.</td>
</tr>
<tr>
<td>State</td>
<td>State of the LDP session (operational or transient).</td>
</tr>
<tr>
<td>Msgs sent/rcvd</td>
<td>Number of LDP messages sent to and received from the session peer. The count includes the transmission and receipt of periodic keepalive messages, which are required for maintenance of the LDP session.</td>
</tr>
<tr>
<td>Up time</td>
<td>Time the session has been up for (in &lt;i&gt;hh:mm:ss&lt;/i&gt; format).</td>
</tr>
<tr>
<td>Peer holdtime</td>
<td>Time to keep LDP peer session up without receipt of LDP protocol message from a peer.</td>
</tr>
<tr>
<td>Peer state</td>
<td>Peer session state.</td>
</tr>
<tr>
<td>Peer holdtime</td>
<td>Time to keep LDP peer session up without receipt of LDP protocol message from a peer.</td>
</tr>
<tr>
<td>Clients</td>
<td>LDP (internal) clients requesting session with a neighbor.</td>
</tr>
<tr>
<td>Inbound label filtering</td>
<td>LDP neighbor inbound filtering policy.</td>
</tr>
<tr>
<td>Session Protection</td>
<td>State of the session protection: &lt;br&gt; &lt;b&gt;Incomplete&lt;/b&gt; &lt;br&gt; Targeted discovery requested but not yet up.</td>
</tr>
<tr>
<td></td>
<td>&lt;b&gt;Ready&lt;/b&gt; &lt;br&gt; Targeted discovery and at least one link hello adjacency to the peer are up.</td>
</tr>
<tr>
<td></td>
<td>&lt;b&gt;Protecting&lt;/b&gt; &lt;br&gt; Targeted discovery is up and there is no link hello adjacency to the peer. Targeted discovery is protecting and backing up link discoveries.</td>
</tr>
<tr>
<td>Duration</td>
<td>Maximum time to maintain session through targeted discovery upon loss of primary link discovery.</td>
</tr>
<tr>
<td>Holdtimer</td>
<td>When in “protecting” state, time to keep LDP peer session up without receipt of LDP protocol message from a peer.</td>
</tr>
</tbody>
</table>
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>graceful-restart (MPLS LDP), on page 16</td>
<td>Configures the LDP graceful restart feature.</td>
</tr>
<tr>
<td>label accept, on page 27</td>
<td>Configures the LDP inbound label filtering feature.</td>
</tr>
<tr>
<td>session protection, on page 50</td>
<td>Configures the LDP session protection feature.</td>
</tr>
<tr>
<td>show mpls ldp discovery, on page 60</td>
<td>Displays the status of the LDP discovery process.</td>
</tr>
</tbody>
</table>
show mpls ldp parameters

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

```
show mpls ldp parameters [{location node-id | standby}]
```

**Syntax Description**

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

**Command Default**
No default behavior or values

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

- `mpls-ldp read`
- `network read`

**Examples**

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

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

LDP Parameters:
Protocol Version: 1
Router ID: 10.11.11.11
Null Label: Implicit
Session:
  Hold time: 180 sec
  Keepalive interval: 60 sec
  Backoff: Initial:15 sec, Maximum:120 sec
Discovery:
  Link Hellos: Holdtime:15 sec, Interval:5 sec
  Targeted Hellos: Holdtime:90 sec, Interval:10 sec
  (Accepting peer ACL 'peer_acl_10')
Graceful Restart:
  Enabled (Configured)
  Reconnect Timeout:120 sec, Forwarding State Holdtime:180 sec
Timeouts:
  Binding with no-route: 300 sec
```
This table describes the significant fields shown in the display.

**Table 14: show mpls ldp parameters Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td>Currently used router ID.</td>
</tr>
<tr>
<td>Null Label</td>
<td>LDP use of implicit-null or explicit-null as label for prefixes where it has to use a null label.</td>
</tr>
<tr>
<td>Session Hold time</td>
<td>Time LDP session is to be maintained with an LDP peer without receiving LDP traffic or an LDP keepalive message from the peer.</td>
</tr>
<tr>
<td>Session Keepalive interval</td>
<td>Time interval between consecutive transmissions of LDP keepalive messages to an LDP peer.</td>
</tr>
<tr>
<td>Session Backoff</td>
<td>Initial maximum backoff time for sessions.</td>
</tr>
<tr>
<td>Discovery Link Hellos</td>
<td>Time to remember that a neighbor platform wants an LDP session without receiving an LDP hello message from the neighbor (hold time), and the time interval between the transmission of consecutive LDP hello messages to neighbors (interval).</td>
</tr>
<tr>
<td>Discovery Targeted Hellos</td>
<td>Indicates the time:</td>
</tr>
<tr>
<td></td>
<td>• To remember that a neighbor platform wants an LDP session when the neighbor platform is not directly connected to the router or the neighbor platform has not sent an LDP hello message. This intervening interval is known as hold time.</td>
</tr>
<tr>
<td></td>
<td>• Interval between the transmission of consecutive hello messages to a neighbor not directly connected to the router and if targeted hellos are being accepted, displaying peer-acl (if any).</td>
</tr>
<tr>
<td>Graceful Restart</td>
<td>Status of graceful-restart status (Y or N).</td>
</tr>
<tr>
<td>Timeouts</td>
<td>Various timeouts (of interest) that the LDP is using. One timeout is binding no route, which indicates how long the LDP waits for an invalid route before deleting it. It also shows restart recovery time for LSD and LDP.</td>
</tr>
<tr>
<td>OOR state</td>
<td>Out of resource memory state: Normal, Major, or Critical.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_52</td>
<td>Configures the parameters for the LDP backoff mechanism.</td>
</tr>
</tbody>
</table>
### show mpls ldp parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_53</td>
<td>Configures the interval between transmission of LDP discovery messages.</td>
</tr>
<tr>
<td>explicit-null, on page 14</td>
<td>Configures a router to advertise an explicit-null label.</td>
</tr>
<tr>
<td>graceful-restart (MPLS LDP), on page 16</td>
<td>Configures the LDP graceful restart feature.</td>
</tr>
<tr>
<td>session holdtime (MPLS LDP), on page 18</td>
<td>Configures keepalive message hold time for LDP sessions.</td>
</tr>
<tr>
<td>neighbor targeted, on page 44</td>
<td>Specifies the preferred interface or IP address of a Loopback interface for determining the LDP router ID.</td>
</tr>
</tbody>
</table>
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 [{ lsr-id ldp-id }] [{ location node-id | standby }]
```

**Syntax Description**

- `lsr-id`  
  (Optional) LSR ID of neighbor in A.B.C.D format.

- `ldp-id`  
  (Optional) LDP ID of neighbor in A.B.C.D: format.

- `location node-id`  
  (Optional) Displays location information for the specified node ID.

- `standby`  
  (Optional) Displays standby-node-specific information.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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 shows a sample output from the `show mpls ldp statistics msg-counters` command:

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

Peer LDP Identifier: 10.33.33.33:0
Msg Sent: (90)  
  Init : 1  
  Address : 1  
  Address_Withdraw : 0  
  Label_Mapping : 5  
  Label_Withdraw : 0  
  Label_Release : 0  
  Notification : 0  
  KeepAlive : 73
```
Table 15: show mpls ldp statistics msg-counters Command Field Descriptions, on page 86 describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer LDP Identifier</td>
<td>LDP identifier of the neighbor (peer).</td>
</tr>
<tr>
<td>Msg Sent</td>
<td>Summary of messages sent to the LDP peer.</td>
</tr>
<tr>
<td>Msg Rcvd</td>
<td>Summary of messages received from the LDP peer.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_54</td>
<td>Clears MPLS LDP message counter values.</td>
</tr>
<tr>
<td>show mpls ldp bindings, on page 54</td>
<td>Displays the contents of LDP LIB.</td>
</tr>
<tr>
<td>show mpls ldp neighbor, on page 76</td>
<td>Displays LDP neighbor information.</td>
</tr>
</tbody>
</table>
show mpls ldp summary

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

```
show mpls ldp summary [{location node-id | standby}]
```

**Syntax Description**

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

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

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

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

AFIs : IPv4
Routes : 4
Neighbors : 1 (1 GR)
Hello Adj : 1
Addresses : 3
Interfaces: 4 LDP configured
```

The following example shows a sample output from the `show mpls ldp summary all` command:

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

VRFs     : 1 (1 oper)
AFIs     : IPv4
Routes   : 4
Neighbors : 1 (1 GR)
Hello Adj : 1
```
This table describes the significant fields shown in the display.

### Table 16: `show mpls ldp summary` Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routes</td>
<td>Number of known IP routes (prefixes).</td>
</tr>
<tr>
<td>Neighbors</td>
<td>Number of LDP neighbors, including targeted and graceful restartable neighbors.</td>
</tr>
<tr>
<td>Hello Adj</td>
<td>Number of discovered LDP discovery sources.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Number of known IP interfaces and number of LDP configured interfaces. LDP is configured on a forward-referenced interface which may not exist or for which no IP address is configured.</td>
</tr>
<tr>
<td>Addresses</td>
<td>Number of known local IP addresses.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mpls ldp bindings</code>, on page 54</td>
<td>Displays the contents of LDP LIB.</td>
</tr>
<tr>
<td><code>show mpls ldp discovery</code>, on page 60</td>
<td>Displays the status of the LDP discovery process.</td>
</tr>
<tr>
<td><code>show mpls ldp forwarding</code>, on page 64</td>
<td>Displays the contents of the LDP forwarding database.</td>
</tr>
<tr>
<td><code>show mpls ldp graceful-restart</code>, on page 68</td>
<td>Displays the status of the LDP graceful restart.</td>
</tr>
<tr>
<td><code>show mpls ldp parameters</code>, on page 82</td>
<td>Displays current LDP parameter settings.</td>
</tr>
</tbody>
</table>
**show lcc**

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

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

**Syntax Description**

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

**Command Default**

None

**Command Modes**

- IPv4 address family configuration
- IPv6 address family configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>read</td>
<td></td>
</tr>
<tr>
<td>IPv6</td>
<td>read</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

The following example shows an outcome of the label consistency checker information:
RP/RP0/CPU0:router# show lcc ipv4 unicast all

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

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

<table>
<thead>
<tr>
<th>Node</th>
<th>Checks Performed</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/2/CPU0</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>0/0/CPU0</td>
<td>6</td>
<td>0</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show rcc</td>
<td>Displays route consistency checker related information.</td>
</tr>
</tbody>
</table>
signalling dscp (LDP)

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

```
signalling dscp  dscp
no signalling dscp
```

**Syntax Description**

- `dscp` DSCP priority value. Range is 0 to 63.

**Command Default**

LDP control packets are sent with precedence 6 (`dscp: 48`)

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.0.0</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

DSCP marking improves signaling setup and teardown times.

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

**Note**

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

**Examples**

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

```
RP/0/RP0/CPU0:router(config-ldp)# signalling dscp 56
```
**snmp-server traps mpls ldp**

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>up</td>
<td>Displays the session-up notification.</td>
</tr>
<tr>
<td>down</td>
<td>Displays the session-down notification.</td>
</tr>
<tr>
<td>threshold</td>
<td>Displays the session-backoff-threshold crossed notification.</td>
</tr>
</tbody>
</table>

**Command Default**

LDP does not send SNMP traps.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

- **Session up**
  - Generated when sessions go up.

- **Session down**
  - Generated when sessions go down.

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
<tr>
<td>snmp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable LDP SNMP trap notifications for Session up:
RP/0/RP0/CPU0:router(config)# snmp-server traps mpls ldp up
snmp-server traps mpls ldp
MPLS Forwarding Commands

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

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

- mpls ip-ttl-propagate, on page 96
- mpls label range, on page 98
- show mpls forwarding, on page 100
- show mpls forwarding tunnels, on page 104
- show mpls forwarding exact-route, on page 106
- show mpls interfaces, on page 110
- show mpls label range, on page 113
- show mpls label table, on page 115
- show mpls lsd applications, on page 117
- show mpls lsd clients, on page 119
- show mpls traffic-eng fast-reroute database, on page 121
- show mpls traffic-eng fast-reroute log, on page 125
### mpls ip-ttl-propagate

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

```
mpls ip-ttl-propagate disable [forwarded | local]
no mpls ip-ttl-propagate
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>disable</th>
<th>Enables the propagation of IP TTL to and from the MPLS header for both forwarded and local packets.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>forwarded</td>
<td>(Optional) Enables the propagation of IP TTL to and from the MPLS header for only the forwarded packets. This prevents the <code>traceroute</code> command from displaying the MPLS-enabled nodes beyond the device under the configuration.</td>
</tr>
<tr>
<td></td>
<td>local</td>
<td>(Optional) Enables the propagation of IP TTL to the MPLS header for only locally generated packets. This prevents the <code>traceroute</code> command from displaying the MPLS-enabled nodes beyond the device under the configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Global configuration</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to disable IP TTL propagation:

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

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

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

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

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>table table-id</code></td>
<td>Identifies a specific label table; the global label table has table-id = 0. If no table is specified, the global table is assumed. Currently, you can specify table 0 only.</td>
</tr>
<tr>
<td><code>minimum</code></td>
<td>Smallest allowed label in the label space. Default is 16000.</td>
</tr>
<tr>
<td><code>maximum</code></td>
<td>Largest allowed label in the label space. Default is 1048575.</td>
</tr>
</tbody>
</table>

**Command Default**

- `table-id`: 0
- `minimum`: 16000
- `maximum`: 1048575

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

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

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

**Note**

- Labels outside the current range and which are allocated by MPLS applications remain in circulation until released.
- You must understand the maximum labels that are supported for each platform versus the labels that are supported for the CLI.
Restart the router after changing the mpls label range.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls label range, on page 113</td>
<td>Displays the range of the MPLS local label space.</td>
</tr>
</tbody>
</table>
show mpls forwarding

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

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

**Syntax Description**

- **detail** (Optional) Displays information in long form (includes length of encapsulation, length of Media Access Control [MAC] string, maximum transmission unit [MTU], Packet switched, and label stack).

- **hardware** (Optional) Displays the hardware location entry.

- **ingress** (Optional) Reads information from the ingress PSE.

- **egress** (Optional) Reads information from the egress PSE.

- **interface** (Optional) Displays information for the specified interface.

- **type** Interface type. For more information, use the `show interfaces` command to see a list of all possible interfaces currently configured on the router.

- **interface-path-id** Physical interface or a virtual interface.

  **Note** Use the `show interfaces` command to see a list of all possible interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

- **labels low-value [high-value]** (Optional) Entries with a local labels range. Ranges for both `low-value` and `high-value` are 0 to 1048575.

- **location node-id** (Optional) Displays hardware resource counters on the designated node.

- **prefix network/mask /length** (Optional) Displays the destination address and mask/prefix length.

  **Note** The forward slash (/) between `network` and `mask` is required.

- **ipv4 unicast** (Optional) Displays the IPv4 unicast address.

- **private** (Optional) Displays private information.

- **summary** (Optional) Displays summarized information.

- **tunnels tunnel-id** (Optional) Displays entries either for a specified label switch path (LSP) tunnel or all LSP tunnel entries.

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

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-static</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

```
RP/0/RP0/CP00:router# show mpls forwarding location 0/2/CPU0

Local  Outgoing  Outgoing  Next Hop  Bytes  Switched
Label   Label    Interface      Switched
-------- -------- --------------- ----------- -----------
16000  Unlabelled  ce01::ce01/128[V]  Gi0/1/0/0  ce01:10::2 0
16001  Aggregate  router: Per-VRF Aggr[V] \ router 0
         16021  16020  P2MP TE:10  Gi0/2/0/3  172.99.1.2 13912344
         16020  16040  P2MP TE:10  Gi0/2/0/3  172.99.2.2 13912344
         16045  16040  P2MP TE:10  Po0/1/0/4  172.16.1.2 13912344
```

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

```
RP/0/RP0/CP00:router# show mpls forwarding prefix 10.241.4.0/24 detail

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

16058  10.241.4.0/24  Te0/4/0/0  10.114.8.11 0
        Updated May 10 20:00:15.983
        MAC/Encaps: 14/18, MTU: 9086
```
The following sample output shows the number of P2MP TE heads and midpoints and the number of P2MP route updates that are received from the MRIB from the `summary` keyword:

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

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

This table describes the significant fields shown in the display.

**Table 17: show mpls forwarding Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Label</td>
<td>Label assigned by this router.</td>
</tr>
<tr>
<td>Outgoing Label</td>
<td>Label assigned by the next hop or downstream peer. Some of the entries that display in this column are:</td>
</tr>
<tr>
<td></td>
<td><strong>Unlabeled</strong></td>
</tr>
<tr>
<td></td>
<td>No label for the destination from the next hop, or label switching is not enabled on the outgoing interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Pop Label</strong></td>
</tr>
<tr>
<td></td>
<td>Next hop advertised an implicit-null label for the destination.</td>
</tr>
<tr>
<td>Prefix or Tunnel ID</td>
<td>Address or tunnel to which packets with this label are going.</td>
</tr>
<tr>
<td>Outgoing Interface</td>
<td>Interface through which packets with this label are sent.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>IP address of neighbor that assigned the outgoing label.</td>
</tr>
<tr>
<td>Bytes Switched</td>
<td>Number of bytes switched with this incoming label.</td>
</tr>
<tr>
<td>TO</td>
<td>Timeout: Indicated by an &quot;*&quot; if entry is being timed out in forwarding.</td>
</tr>
<tr>
<td>Mac/Encaps</td>
<td>Length in bytes of Layer 2 header, and length in bytes of packet encapsulation, including Layer 2 header and label header.</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU$^2$ of labeled packet.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Label Stack</td>
<td>All the outgoing labels on the forwarded packet.</td>
</tr>
<tr>
<td>Packets Switched</td>
<td>Number of packets switched with this incoming label.</td>
</tr>
<tr>
<td>Label switching</td>
<td>Number of Label switching LFIB(^5) forwarding entries.</td>
</tr>
<tr>
<td>IPv4 label imposition</td>
<td>Number of IPv4 label imposition forwarding entries (installed at ingress LSR).</td>
</tr>
<tr>
<td>MPLS TE tunnel head</td>
<td>Number of forwarding entries (installed at ingress LSR) on MPLS TE tunnel head.</td>
</tr>
<tr>
<td>MPLS TE fast-reroute</td>
<td>Number of forwarding entries (installed at PLR) for MPLS-TE fast reroute.</td>
</tr>
<tr>
<td>Forwarding updates</td>
<td>Number of forwarding updates sent from LSD (RP/DRP) to LFIB/MPLS (RP/DRP/LC) using BCDL mechanism, indicating the total number of updates and total number of BCDL messages.</td>
</tr>
<tr>
<td>Labels in use</td>
<td>Local labels in use (installed in LFIB). These usually indicate the lowest and highest label in use (allocated by applications). Furthermore, some reserved labels, such as explicit-nullv4, explicit-nullv6, are installed in the forwarding plane. The label range is 0 to 15.</td>
</tr>
</tbody>
</table>

\(^5\) MTU = Maximum Transmission Unit.
\(^6\) LFIB = Label Forwarding Information Base.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls forwarding exact-route, on page 106</td>
<td>Displays the exact path for the source and destination address pair.</td>
</tr>
</tbody>
</table>
show mpls forwarding tunnels

To display the contents of the MPLS forwarding tunnel, use the `show mpls forwarding tunnel` command in EXEC mode.

`show mpls forwarding tunnels [detail][tunnels tunnel-id] [vrf vrf-name]`

**Syntax Description**
- `detail` (Optional) Displays information in long form (includes length of encapsulation, length of Media Access Control [MAC] string, maximum transmission unit [MTU], Packet switched, and label stack).
- `tunnels tunnel-id` (Optional) Displays entries either for a specified label switch path (LSP) tunnel or all LSP tunnel entries.
- `vrf vrf-name` (Optional) Displays entries for VPN routing and forwarding (VRF).

**Command Modes**
- EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.3.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-static</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

```
show mpls forwarding tunnels
RP/0/RSP0/CPU0:PE1#sh mpls forwarding tunnels 1999 detail
```
Thu Jul 23 22:56:09.726 PDT
Tunnel Outgoing Outgoing Next Hop Bytes
Name Label Interface Switched
-------------- ----------- ------------ --------------- ------------
tt1999 50045 BE10 point2point 0
Updated: Jul 23 20:04:57.416
Version: 82681, Priority: 2
Label Stack (Top -> Bottom): { 50045 }
Local Label: 27972
NHID: 0x0, Path idx: 0, Backup path idx: 0, Weight: 0
MAC/Encaps: 14/18, MTU: 1500
Packets Switched: 0

Interface Handle: 0x0801f4a0, Local Label: 27972
Forwarding Class: 0, Weight: 0
Packets/Bytes Switched: 7045837/7116295370

RP/0/RSP0/CPU0:PE1#sh mpls forwarding tunnels 1999 detail location 0/0/CPU0
Thu Jul 23 22:56:14.526 PDT
Tunnel Outgoing Outgoing Next Hop Bytes
Name Label Interface Switched
-------------- ----------- ------------ --------------- ------------
tt1999 50045 BE10 point2point 0
Updated: Jul 23 20:04:57.640
Version: 82681, Priority: 2
Label Stack (Top -> Bottom): { 50045 }
Local Label: 27972
NHID: 0x0, Path idx: 0, Backup path idx: 0, Weight: 0
MAC/Encaps: 14/18, MTU: 1500
Packets Switched: 0

Interface Handle: 0x0801f4a0, Local Label: 27972
Forwarding Class: 0, Weight: 0
Packets/Bytes Switched: 7045837/7116295370

RP/0/RSP0/CPU0:PE1#sh mpls forwarding tunnels 1999
Thu Jul 23 22:56:19.717 PDT
Tunnel Outgoing Outgoing Next Hop Bytes
Name Label Interface Switched
-------------- ----------- ------------ --------------- ------------
tt1999 50045 BE10 point2point 0

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls forwarding exact-route, on page 106</td>
<td>Displays the exact path for the source and destination address pair.</td>
</tr>
</tbody>
</table>
show mpls forwarding exact-route

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

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

**Syntax Description**

- **label label-number** Displays the exact path for a source and destination address pair.
- **bottom-label value** Displays the bottom label value. Range is 0 to 1048575.
- **ipv4 source-address destination-address** Displays the exact path for IPv4 payload. The IPv4 source address in x.x.x.x format. The IPv4 destination address in x.x.x.x format.
- **ipv6 source-address destination-address** Displays the exact path for IPv6 payload. The IPv6 source address in x:x::x format. The IPv6 destination address in x:x::x format.
- **detail** (Optional) Displays detailed information.
- **protocol protocol** (Optional) Displays the specified protocol for the route.
- **source-port source-port** Sets the UDP source port. The range is from 0 to 65535.
- **destination-port destination-port** Sets the UDP destination port. The range is from 0 to 65535.
- **ingress-interface** Sets the ingress interface.
- **type** Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id** Physical interface or a virtual interface.

**Note**

Use the `show interfaces` command to see a list of all possible interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

- **location node-id** (Optional) Displays hardware resource counters on the designated node.
- **policy-class value** (Optional) Displays the policy-based tunnel selection (PBTS) to direct traffic into specific TE tunnels. The policy-class attribute maps the correct traffic class to this policy. The range for the policy-class value is from 1 to 7.
- **hardware** (Optional) Displays the hardware location entry.
- **ingress** (Optional) Reads information from the ingress PSE.
- **egress** (Optional) Reads information from the egress PSE.
Command Default

No default behavior or values

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

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

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

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

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-static</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

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

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

Local Outgoing Prefix Outgoing Next Hop Bytes
Label Label or ID Interface Switched
------ ----------- ------------------ ------------ --------------- ------------
16000 16001 5.5.5.32 PO0/1/5/1 1.24.1.192 N/A

Via: PO0/1/5/1, Next Hop: point2point
MAC/Encaps: 4/8, MTU: 1500
Label Stack (Top -> Bottom): ( 16001 )
```
This table describes the significant fields shown in the display.

**Table 18: show mpls forwarding exact-route Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Label</td>
<td>Label assigned by this router.</td>
</tr>
<tr>
<td>Outgoing Label</td>
<td>Label assigned by the next hop or downstream peer. Some of the entries that display in this column are:</td>
</tr>
<tr>
<td></td>
<td><strong>Unlabeled</strong> No label for the destination from the next hop, or label switching is not enabled on the outgoing interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Pop Label</strong> Next hop advertised an implicit-null label for the destination.</td>
</tr>
<tr>
<td>Prefix or Tunnel ID</td>
<td>Address or tunnel to which packets with this label are going.</td>
</tr>
<tr>
<td>Outgoing Interface</td>
<td>Interface through which packets with this label are sent.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>IP address of neighbor that assigned the outgoing label.</td>
</tr>
<tr>
<td>Bytes Switched</td>
<td>Number of bytes switched with this incoming label.</td>
</tr>
<tr>
<td>TO</td>
<td>Timeout: Indicated by an &quot;*&quot; if entry is being timed out in forwarding.</td>
</tr>
<tr>
<td>MAC/Encaps</td>
<td>Length in bytes of Layer 2 header, and length in bytes of packet encapsulation, including Layer 2 header and label header.</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU² of labeled packet.</td>
</tr>
<tr>
<td>Label Stack</td>
<td>All the outgoing labels on the forwarded packet.</td>
</tr>
<tr>
<td>Packets Switched</td>
<td>Number of packets switched with this incoming label.</td>
</tr>
<tr>
<td>Label switching</td>
<td>Number of Label switching LFIB³ forwarding entries.</td>
</tr>
<tr>
<td>IPv4 label imposition</td>
<td>Number of IPv4 label imposition forwarding entries (installed at ingress LSR).</td>
</tr>
<tr>
<td>MPLS TE tunnel head</td>
<td>Number of forwarding entries (installed at ingress LSR) on MPLS TE tunnel head.</td>
</tr>
<tr>
<td>MPLS TE fast-reroute</td>
<td>Number of forwarding entries (installed at PLR) for MPLS-TE fast reroute.</td>
</tr>
<tr>
<td>Forwarding updates</td>
<td>Number of forwarding updates sent from LSD (RP/DRP) to LFIB/MPLS (RP/DRP/LC) using BCDL mechanism, indicating the total number of updates and total number of BCDL messages.</td>
</tr>
<tr>
<td>Labels in use</td>
<td>Local labels in use (installed in LFIB). These usually indicate the lowest and highest label in use (allocated by applications). Furthermore, some reserved labels, such as explicit-nullv4, explicit-nullv6, are installed in the forwarding plane. The label range is 0 to 15.</td>
</tr>
</tbody>
</table>
MTU = Maximum Transmission Unit.
LFIB = Label Forwarding Information Base.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show mpls forwarding, on page 100</td>
<td>Displays the contents of the MPLS LFIB.</td>
</tr>
</tbody>
</table>
**show mpls interfaces**

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

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

**Syntax Description**

- **type** (Optional) Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id** Physical interface or a virtual interface.
- **location node-id** (Optional) Displays hardware resource counters on the designated node.
- **detail** (Optional) Displays detailed information for the designated node.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-static</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

```
RP/0/RP0/CPU0:router# show mpls interfaces
```
The following shows a sample output from the **show mpls interfaces** command using the **detail** keyword:

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

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

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

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

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

This table describes the significant fields in the sample display.

**Table 19: show mpls interfaces Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDP</td>
<td>State of LDP labelling.</td>
</tr>
<tr>
<td>Tunnel</td>
<td>State of LSP Tunnel labelling.</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU^2 of labeled packet.</td>
</tr>
<tr>
<td>Caps</td>
<td>Capsulation switching chains installed on an interface.</td>
</tr>
</tbody>
</table>
MPLS switching capsulation/switching chains are installed on the interface and are ready to switch MPLS traffic.

MTU = Maximum Transmission Unit.
show mpls label range

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

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-static</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

Range for dynamic labels: Min/Max: 16000/144000
```

This table describes the significant fields shown in the display.

**Table 20: show mpls label range Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range for dynamic labels</td>
<td>Minimum and maximum allowable range for local labels (which differs from the default range).</td>
</tr>
</tbody>
</table>
**show mpls label range**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls label range, on page 98</td>
<td>Configures a range of values for use as local labels.</td>
</tr>
</tbody>
</table>
show mpls label table

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

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

**Syntax Description**

- `table-index`  
  Index of the label table to display. The global label table is 0. Currently, you can specify table 0 only.

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

- `label label-value`  
  (Optional) Displays a selected label based on the label value. Range is 0 to 1048575.

- `summary`  
  (Optional) Displays a summary of local labels.

- `detail`  
  (Optional) Displays detailed information for the MPLS label table.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

- `mpls-te`  
  - read, write
- `mpls-ldp`  
  - read, write
- `mpls-static`  
  - read, write

**Examples**

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

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

<table>
<thead>
<tr>
<th>Table</th>
<th>Label</th>
<th>Owner</th>
<th>State</th>
<th>Rewrite</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>LSD</td>
<td>InUse</td>
<td>Yes</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>LSD</td>
<td>InUse</td>
<td>Yes</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>LSD</td>
<td>InUse</td>
<td>Yes</td>
</tr>
<tr>
<td>0</td>
<td>3</td>
<td>LSD</td>
<td>InUse</td>
<td>Yes</td>
</tr>
<tr>
<td>0</td>
<td>16</td>
<td>TE-Link</td>
<td>InUse</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

This table describes the significant fields shown in the display.

**Table 21: show mpls label table Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Table ID.</td>
</tr>
<tr>
<td>Label</td>
<td>Label index.</td>
</tr>
<tr>
<td>Owner</td>
<td>Application that allocated the label. All labels displaying “InUse” state have an owner.</td>
</tr>
<tr>
<td>State</td>
<td><strong>InUse</strong></td>
</tr>
<tr>
<td></td>
<td>Label allocated and in use by an application.</td>
</tr>
<tr>
<td></td>
<td><strong>Alloc</strong></td>
</tr>
<tr>
<td></td>
<td>Label allocated but is not yet in use by an application.</td>
</tr>
<tr>
<td></td>
<td><strong>Pend</strong></td>
</tr>
<tr>
<td></td>
<td>Label was in use by an application that has terminated unexpectedly, and the application has not reclaimed the label.</td>
</tr>
<tr>
<td></td>
<td><strong>Pend-S</strong></td>
</tr>
<tr>
<td></td>
<td>Label was in use by an application, but the MPLS LSD (Label Switching Database) server has recently restarted and the application has not reclaimed the label.</td>
</tr>
<tr>
<td>Rewrite</td>
<td>Number of initiated rewrites.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls forwarding, on page 100</td>
<td>Displays entries in the MPLS forwarding table. Label switching entries are indexed by their local label.</td>
</tr>
<tr>
<td>show mpls lsd applications, on page 117</td>
<td>Displays MPLS applications that are registered with the MPLS LSD server.</td>
</tr>
</tbody>
</table>
show mpls lsd applications

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

`show mpls lsd applications [application application]`

**Syntax Description**

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

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

Release 5.0.0 This command was introduced.

**Usage Guidelines**

MPLS applications include Traffic Engineering (TE) control, TE Link Management, and label distribution protocol (LDP). The application must be registered with MPLS LSD for its features to operate correctly. All applications are clients (see the `show mpls lsd clients`, on page 119 command), but not all clients are applications.

**Examples**

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

```
RP/0/RP0/CPU0:router# show mpls lsd applications
MPLS Type State RecoveryTime Node
------------ -------- ------------ ------------
LDP          Active 300       0/0/CPU0
TE-Control   Active 100       0/0/CPU0
TE-Link      Active 600       0/0/CPU0
```
This table describes the significant fields shown in the display.

**Table 22: show mpls lsd applications Command Field Descriptions**

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls lsd clients, on page 119</td>
<td>Displays MPLS clients connected to the MPLS LSD server.</td>
</tr>
</tbody>
</table>
show mpls lsd clients

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

**show mpls lsd clients**

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-static</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

<table>
<thead>
<tr>
<th>Id</th>
<th>Services</th>
<th>Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>BA (p-none)</td>
<td>0/0/CPU0</td>
</tr>
<tr>
<td>1</td>
<td>A (TE-Link)</td>
<td>0/0/CPU0</td>
</tr>
<tr>
<td>2</td>
<td>A (LDP)</td>
<td>0/0/CPU0</td>
</tr>
<tr>
<td>3</td>
<td>A (TE-Control)</td>
<td>0/0/CPU0</td>
</tr>
</tbody>
</table>
```

The following table describes the significant fields shown in the display.
### Table 23: `show mpls lsd clients` Command Field Descriptions

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mpls lsd applications</code></td>
<td>Displays MPLS applications registered with the MPLS LSD server.</td>
</tr>
</tbody>
</table>
**show mpls traffic-eng fast-reroute database**

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

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

**Syntax Description**

- **ip-address** (Optional) IP address of the destination network.
- **ip-address/length** (Optional) Bit combination indicating the portion of the IP address that is being used for the subnet address.
- **afi-all** (Optional) Returns data for all specified address family identifiers.
- **safi-all** (Optional) Returns data for all sub-address family identifiers.
- **unicast** (Optional) Returns unicast data only.
- **backup-interface** (Optional) Displays entries with the specified backup interface.
- **tunnel tunnel-id** (Optional) Tunnel and tunnel ID to which packets with this label are going. The **summary** suboption is available.
- **unresolved** (Optional) Displays entries whose backup interface has not yet been fully resolved.
- **interface** (Optional) Displays entries with this primary outgoing interface. The **summary** keyword is available.
- **type** (Optional) Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id** Physical interface or a virtual interface.

**Note**
Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

- **ipv4** (Optional) Displays only IPv4 data.
- **labels** (Optional) Displays database entries that possess in-labels assigned by this router (local labels). Specify either a starting value or a range of values. The **state** suboption is available.
show mpls traffic-eng fast-reroute database

<table>
<thead>
<tr>
<th>state</th>
<th>(Optional) Filters the database according to the state of the entry:</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>FRR rewrite is in the forwarding active database (where it can be placed onto appropriate incoming packets).</td>
</tr>
<tr>
<td>complete</td>
<td>FRR rewrite is assembled, ready or active.</td>
</tr>
<tr>
<td>partial</td>
<td>FRR rewrite is fully created; its backup routing information is still incomplete.</td>
</tr>
<tr>
<td>ready</td>
<td>FRR rewrite was created but is not in the forwarding active state.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>role</th>
<th>(Optional) Displays entries associated either with the tunnel head or tunnel midpoint. The summary suboption is available.</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>(Optional) Displays summarized information about the FRR database.</td>
</tr>
<tr>
<td>location</td>
<td>node-id (Optional) Displays hardware resource counters on the designated node.</td>
</tr>
</tbody>
</table>

Command Default
No default behavior or values

Command Modes
EXEC

Command History
Release Modification
5.0.0 This command was introduced.

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

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

Task ID
mpls-te read

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

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

Tunnel head FRR information:
Tunnel Out intf/label FRR intf/label Status
---------- ---------------- ---------------- -------
tt4000 PO0/3/0:0:34 tt1000:34 Ready
The Prefix field indicates the IP address where packets with this label are headed.

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

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

LSP midpoint FRR information:

<table>
<thead>
<tr>
<th>LSP Identifier</th>
<th>Out Intf/Label</th>
<th>FRR Intf/Label</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.10</td>
<td>Gi0/6/5/2:Pop</td>
<td>tt1060:Pop</td>
<td>Ready</td>
</tr>
</tbody>
</table>

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

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

Tunnel head FRR information:

<table>
<thead>
<tr>
<th>Tunnel</th>
<th>Out intf/lable</th>
<th>FRR intf/lable</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>tt4000</td>
<td>PO0/3/0/0:34</td>
<td>tt1000:34</td>
<td>Ready</td>
</tr>
<tr>
<td>tt4001</td>
<td>PO0/3/0/0:35</td>
<td>tt1001:35</td>
<td>Ready</td>
</tr>
<tr>
<td>tt4002</td>
<td>PO0/3/0/0:36</td>
<td>tt1001:36</td>
<td>Ready</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Status</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>0</td>
</tr>
<tr>
<td>Ready</td>
<td>3</td>
</tr>
<tr>
<td>Partial</td>
<td>0</td>
</tr>
</tbody>
</table>

The following sample output displays 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
```

<table>
<thead>
<tr>
<th>Status</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>0</td>
</tr>
<tr>
<td>Ready</td>
<td>2</td>
</tr>
<tr>
<td>Partial</td>
<td>0</td>
</tr>
</tbody>
</table>
This table describes the significant fields shown in the display.

**Table 24: show mpls traffic-eng fast-reroute database Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel</td>
<td>Short form of tunnel interface name.</td>
</tr>
<tr>
<td>Out intf/label</td>
<td><strong>Out interface</strong>&lt;br&gt;Short name of the physical interface through which traffic goes to the protected link.</td>
</tr>
<tr>
<td></td>
<td><strong>Out label</strong>&lt;br&gt;At a tunnel head, this is the label that the tunnel destination device advertises. The value “Unlabeled” indicates that no such label is advertised.&lt;br&gt;At a tunnel midpoint, this is the label selected by the next hop device. The value “Pop Label” indicates that the next hop is the final hop for the tunnel.</td>
</tr>
<tr>
<td>FRR intf/label</td>
<td><strong>Fast reroute interface</strong>&lt;br&gt;Backup tunnel interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Fast reroute label</strong>&lt;br&gt;At a tunnel head, this is the label that the tunnel tail selected to indicate the destination network. The value “Unlabeled” indicates that no label is advertised.&lt;br&gt;At a tunnel midpoint, this has the same value as the Out label.</td>
</tr>
<tr>
<td>Status</td>
<td>State of the rewrite: partial, ready, or active.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_70</td>
<td>Displays the contents of the FRR event log.</td>
</tr>
</tbody>
</table>
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 interface-path-id | location node-id ]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>interface</strong></td>
<td>(Optional) Displays all FRR events for the selected protected interface.</td>
</tr>
<tr>
<td><strong>type</strong></td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><strong>interface-path-id</strong></td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td><strong>location node-id</strong></td>
<td>(Optional) Displays all FRR events that occurred on the selected node.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

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

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

Node       Protected LSPs Rewrites When Switching Time Interface (usec)
------------ --------------- ------- ----------------- ----------------------
0/0/CPU0    PO0/1/0/1  1  1 Feb 27 19:12:29.064000 147
```
This table describes the significant fields shown in the display.

**Table 25: show mpls traffic-eng fast-reroute log Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>Node address.</td>
</tr>
<tr>
<td>Protected Interface</td>
<td>Type and interface-path-id that is being protected.</td>
</tr>
<tr>
<td>LSPs</td>
<td>LSP$^{10}$ associated with each interface being protected.</td>
</tr>
<tr>
<td>Rewrites</td>
<td>Number of rewrites initiated on the LSP.</td>
</tr>
<tr>
<td>When</td>
<td>Date the interface was protected.</td>
</tr>
<tr>
<td>Switching Time</td>
<td>Time required to switch the protected interface in microseconds.</td>
</tr>
</tbody>
</table>

$^{10}$ LSP = Link-state Packet.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls traffic-eng fast-reroute database, on page 121</td>
<td>Displays the contents of the FRR database.</td>
</tr>
</tbody>
</table>
MPLS Traffic Engineering Commands

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

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

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

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

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

- adjustment-threshold (MPLS-TE), on page 131
- admin-weight, on page 133
- affinity, on page 134
- affinity-map, on page 139
- application (MPLS-TE), on page 141
- attribute-flags, on page 143
- attribute-names, on page 145
- attribute-set, on page 146
- auto-bw (MPLS-TE), on page 149
- auto-bw collect frequency (MPLS-TE), on page 151
- autoroute announce, on page 153
- autoroute metric, on page 154
- auto-tunnel backup (MPLS-TE), on page 156
- backup-bw, on page 158
- backup-path tunnel-te, on page 160
- bw-limit (MPLS-TE), on page 162
- clear mpls traffic-eng auto-bw (MPLS-TE EXEC), on page 164
- clear mpls traffic-eng auto-tunnel backup unused, on page 166
- clear mpls traffic-eng auto-tunnel mesh, on page 167
- clear mpls traffic-eng counters auto-tunnel mesh, on page 168
• clear mpls traffic-eng counters auto-tunnel backup, on page 169
• clear mpls traffic-eng counters global, on page 170
• clear mpls traffic-eng counters signaling, on page 171
• clear mpls traffic-eng counters soft-preemption, on page 173
• clear mpls traffic-eng fast-reroute log, on page 174
• clear mpls traffic-eng link-management statistics, on page 175
• clear mpls traffic-eng pce, on page 176
• collect-bw-only (MPLS-TE), on page 177
• destination (MPLS-TE), on page 179
• disable (explicit-path), on page 181
• ds-te bc-model, on page 182
• ds-te mode, on page 184
• ds-te te-classes, on page 186
• exclude srlg (auto-tunnel backup), on page 188
• fast-reroute, on page 190
• fast-reroute protect, on page 192
• fast-reroute timers promotion, on page 193
• flooding threshold, on page 195
• flooding thresholds, on page 196
• forwarding-adjacency, on page 198
• index exclude-address, on page 200
• index exclude-srlg, on page 202
• index next-address, on page 203
• interface (MPLS-TE), on page 205
• interface (SRLG), on page 206
• interface tunnel-te, on page 207
• ipv4 unnumbered (MPLS), on page 209
• link-management timers bandwidth-hold, on page 210
• link-management timers periodic-flooding, on page 212
• link-management timers preemption-delay, on page 214
• maxabs (MPLS-TE), on page 215
• mpls traffic-eng, on page 216
• mpls traffic-eng auto-bw apply (MPLS-TE), on page 217
• mpls traffic-eng fast-reroute promote, on page 219
• mpls traffic-eng level, on page 220
• mpls traffic-eng link-management flood, on page 221
• mpls traffic-eng pce activate-pcep, on page 222
• mpls traffic-eng pce reoptimize, on page 223
• mpls traffic-eng reoptimize (EXEC), on page 224
• mpls traffic-eng resetup (EXEC), on page 225
• mpls traffic-eng router-id (MPLS-TE router), on page 226
• mpls traffic-eng repotimize mesh group, on page 228
• named-tunnels tunnel-te, on page 229
• nhop-only (auto-tunnel backup), on page 230
• overflow threshold (MPLS-TE), on page 232
• path-option (MPLS-TE), on page 234
• path-selection ignore overload (MPLS-TE), on page 237
• path-selection invalidation, on page 239
• path-selection loose-expansion affinity (MPLS-TE), on page 240
• path-selection loose-expansion domain-match, on page 242
• path-selection loose-expansion metric (MPLS-TE), on page 243
• path-selection metric (MPLS-TE), on page 245
• path-selection metric (interface), on page 247
• pce address (MPLS-TE), on page 248
• pce deadtimer (MPLS-TE), on page 250
• pce keepalive (MPLS-TE), on page 252
• pce peer (MPLS-TE), on page 254
• pce reoptimize (MPLS-TE), on page 256
• pce request-timeout (MPLS-TE), on page 258
• pce tolerance keepalive (MPLS-TE), on page 260
• priority (MPLS-TE), on page 262
• record-route, on page 264
• reoptimize timers delay (MPLS-TE), on page 265
• router-id secondary (MPLS-TE), on page 268
• show explicit-paths, on page 269
• show mpls traffic-eng affinity-map, on page 271
• show mpls traffic-eng attribute-set, on page 273
• show mpls traffic-eng autoroute, on page 275
• show mpls traffic-eng auto-tunnel backup, on page 277
• show mpls traffic-eng auto-tunnel mesh, on page 280
• show mpls traffic-eng collaborator-timers, on page 282
• show mpls traffic-eng counters signaling, on page 284
• show mpls traffic-eng ds-te te-class, on page 290
• show mpls traffic-eng forwarding, on page 292
• show mpls traffic-eng forwarding-adjacency, on page 294
• show mpls traffic-eng igp-areas, on page 295
• show mpls traffic-eng link-management admission-control, on page 296
• show mpls traffic-eng link-management advertisements, on page 299
• show mpls traffic-eng link-management bandwidth-allocation, on page 302
• show mpls traffic-eng link-management bfd-neighbors, on page 305
• show mpls traffic-eng link-management igp-neighbors, on page 307
• show mpls traffic-eng link-management interfaces, on page 309
• show mpls traffic-eng link-management statistics, on page 312
• show mpls traffic-eng link-management summary, on page 314
• show mpls traffic-eng maximum tunnels, on page 316
• show mpls traffic-eng pce peer, on page 319
• show mpls traffic-eng pce tunnels, on page 321
• show mpls traffic-eng preemption log, on page 323
• show mpls traffic-eng topology, on page 325
• show mpls traffic-eng tunnels, on page 335
• show mpls traffic-eng tunnels auto-bw brief, on page 363
• show mpls traffic-eng link-management soft-preemption, on page 365
• show srlg, on page 367
• signalled-bandwidth, on page 369
• signalled-name, on page 371
• signalling advertise explicit-null (MPLS-TE), on page 372
• snmp traps mpls traffic-eng, on page 373
• soft-preemption, on page 375
• srlg, on page 376
• timers loose-path (MPLS-TE), on page 377
• timers removal unused (auto-tunnel backup), on page 378
• timeout (soft-preemption), on page 380
• topology holddown sigerr (MPLS-TE), on page 381
• tunnel-id (auto-tunnel backup), on page 383
adjustment-threshold (MPLS-TE)

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

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

**Syntax Description**

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

**Command Default**

- **percentage**: 5
- **minimum bandwidth**: 10

**Command Modes**

MPLS-TE automatic bandwidth interface configuration

**Command History**

- **Release 5.0.0**: This command was introduced.

**Usage Guidelines**

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

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

**Examples**

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# auto-bw
RP/0/RP0/CPU0:router(config-if-tunte-autobw)# adjustment-threshold 20 min 500
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>application (MPLS-TE), on page 141</td>
<td>Configures the application frequency, in minutes, for the applicable tunnel.</td>
</tr>
</tbody>
</table>
### MPLS Traffic Engineering Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>auto-bw (MPLS-TE), on page 149</code></td>
<td>Configures automatic bandwidth on a tunnel interface and enters MPLS-TE automatic bandwidth interface configuration mode.</td>
</tr>
<tr>
<td><code>bw-limit (MPLS-TE), on page 162</code></td>
<td>Configures the minimum and maximum automatic bandwidth to set on a tunnel.</td>
</tr>
<tr>
<td><code>collect-bw-only (MPLS-TE), on page 177</code></td>
<td>Enables only the bandwidth collection without adjusting the automatic bandwidth.</td>
</tr>
<tr>
<td><code>overflow threshold (MPLS-TE), on page 232</code></td>
<td>Configures tunnel overflow detection.</td>
</tr>
<tr>
<td><code>show mpls traffic-eng tunnels, on page 335</code></td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
</tbody>
</table>
admin-weight

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

```
admin-weight weight
no admin-weight weight
```

### Syntax Description

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

### Command Default

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

### Command Modes

- MPLS-TE interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mplste</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

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

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface (MPLS-TE), on page 205</td>
<td>Enables MPLS-TE on an interface and enters MPLS-TE interface configuration mode.</td>
</tr>
<tr>
<td>mpls traffic-eng, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
<tr>
<td>path-selection metric (interface), on page 247</td>
<td>Specifies an MPLS-TE tunnel path-selection metric type.</td>
</tr>
</tbody>
</table>
## affinity

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

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

### Syntax Description

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>affinity-value</code></td>
<td>Attribute values that are required for links to carry this tunnel. A 32-bit decimal number. Range is from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.</td>
</tr>
<tr>
<td><code>mask</code></td>
<td>Checks the link attribute. A 32-bit decimal number. Range is 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute mask is 0 or 1.</td>
</tr>
<tr>
<td><code>exclude</code></td>
<td>Configures a particular affinity to exclude.</td>
</tr>
<tr>
<td><code>exclude-all</code></td>
<td>Excludes all affinities.</td>
</tr>
<tr>
<td><code>ignore</code></td>
<td>Ignore affinity attributes.</td>
</tr>
<tr>
<td><code>include</code></td>
<td>Configures the affinity to include in the loose sense.</td>
</tr>
<tr>
<td><code>include-strict</code></td>
<td>Configures the affinity to include in the strict sense.</td>
</tr>
</tbody>
</table>

### Command Default

- `affinity-value`: 0X00000000
- `mask-value`: 0x0000FFFF

### Interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Affinity determines the link attributes of the tunnel (that is, the attributes for which the tunnel has an affinity). The attribute mask determines which link attribute the router should check. If a bit in the mask is 0, the attribute value of a link or that bit is irrelevant. If a bit in the mask is 1, the attribute value of that link and the required affinity of the tunnel for that bit must match.

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

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

```
tunnel_affinity=tunnel_affinity and tunnel_affinity_mask
```

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

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

Include-strict

Specifies that a link is considered for CSPF if it contains only the colors associated with the include-strict statement. The link cannot have any additional colors. In addition, a link that does not have any attribute satisfies an exclude constraint.

Exclude

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

Exclude-all

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

Ignore

Ignores affinity attributes while considering links for CSPF.

You set one bit for each color; however, the sample output shows multiple bits at the same time. For example, you can configure red and orange colors on GigabitEthernet0/4/1/3 from the `interface` command. The sample output from the `show mpls traffic-eng link-management interfaces`, on page 309 command shows that the Attributes field is set to 0x21, which means that there are 0x20 and 0x1 bits on the link.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

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

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

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

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

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
```
This example shows how to configure a tunnel to ignore the affinity attributes on links.

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

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

Name: tunnel-te1 Destination: 0.0.0.0
Status:  
  Admin: up Oper: down Path: not valid Signalling: Down
  G-PID: 0x0800 (internally specified)
Config Parameters:
  Bandwidth: 0 kbps (CT0) Priority: 7 7
  Number of configured name based affinity constraints: 1
  Name based affinity constraints in use:
    Include bit map : 0x21
  Metric Type: TE (default)
  AutoRoute: disabled LockDown: disabled
  Loadshare: 0 equal loadshares
  Auto-bw: disabled (0/0) 0 Bandwidth Requested: 0
  Direction: unidirectional
  Endpoint switching capability: unknown, encoding type: unassigned
  Transit switching capability: unknown, encoding type: unassigned

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

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

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

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

Name: tunnel-te1 Destination: 0.0.0.0
Status:  
  Admin: up Oper: down Path: not valid Signalling: Down
  G-PID: 0x0800 (internally specified)
Config Parameters:
  Bandwidth: 0 kbps (CT0) Priority: 7 7
  Number of configured name based affinity constraints: 2
  Name based affinity constraints in use:
    Include bit map : 0x1
    Include bit map : 0x20
  Metric Type: TE (default)
AutoRoute: disabled  LockDown: disabled
Loadshare: 0 equal loadshares
Auto-bw: disabled(0/0) 0 Bandwidth Requested: 0
Direction: unidirectional
Endpoint switching capability: unknown, encoding type: unassigned
Transit switching capability: unknown, encoding type: unassigned

Reason for the tunnel being down: No destination is configured

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

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

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>affinity</strong></td>
<td>affinity-map, on page 139</td>
<td>Assigns a numerical value to each affinity name.</td>
</tr>
<tr>
<td></td>
<td>attribute-names, on page 145</td>
<td>Configures attribute names for the interface.</td>
</tr>
<tr>
<td></td>
<td>interface tunnel-te, on page 207</td>
<td>Configures an MPLS-TE tunnel interface.</td>
</tr>
<tr>
<td></td>
<td>show mpls traffic-eng affinity-map, on page 271</td>
<td>Displays the color name-to-value mappings configured on the router.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>show mpls traffic-eng tunnels, on page 335</td>
<td>Displays information about MPLS-TE tunnels.</td>
<td></td>
</tr>
</tbody>
</table>
affinity-map

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>affinity name</strong></td>
<td>Affinity map name-to-value designator (in hexadecimal, 0-ffffffff).</td>
</tr>
<tr>
<td><strong>affinity value</strong></td>
<td>Affinity map value designator. Range is from 1 to 80000000.</td>
</tr>
<tr>
<td><strong>bit-position</strong></td>
<td>Configures the value of an affinity map for the bit position of the 32-bit number.</td>
</tr>
<tr>
<td><strong>value</strong></td>
<td>Bit position value. Range is from 0 to 31.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- **Note**
  - The name-to-value mapping must represent a single bit of a 32-bit value.
  - Repeat the affinity-map command to define multiple colors up to a maximum of 256 colors.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

```
RP/0/RP0/CP00:router# configure
RP/0/RP0/CP00:router(config)# mpls traffic-eng
RP/0/RP0/CP00:router(config-mpls-te)# affinity-map red 1
RP/0/RP0/CP00:router(config-mpls-te)# affinity-map blue 2
```
The following example shows how to configure the value of 15 for an affinity map by bit position:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# affinity-map red2 bit-position 15
```
application (MPLS-TE)

To configure the application frequency, in minutes, for the applicable tunnel, use the `application` command in MPLS-TE automatic bandwidth interface configuration mode. To disable this feature, use the `no` form of this command.

```
application minutes
no application minutes
```

**Syntax Description**

- `minutes` Frequency, in minutes, for the automatic bandwidth application. The range is from 5 to 10080 (7 days). The default is 1440.

**Command Default**

- `minutes : 1440 (24 hours)`

**Command Modes**

MPLS-TE automatic bandwidth interface configuration

**Command History**

- **Release**
  - 5.0.0

**Modification**

- This command was introduced.

**Usage Guidelines**

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

If you configure and modify the application frequency, the application period can reset and restart for that tunnel. The next bandwidth application for the tunnel happens within the specified minutes.

**Task ID**

- **Task**
  - mpls-te

- **Operations**
  - read,
  - write

**Examples**

The following example shows how to configure application frequency to 1000 minutes for MPLS-TE interface 1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# auto-bw
RP/0/RP0/CPU0:router(config-if-tunte-autobw)# application 1000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adjustment-threshold (MPLS-TE), on page 131</td>
<td>Configures the tunnel-bandwidth change threshold to trigger an adjustment.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>auto-bw (MPLS-TE), on page 149</td>
<td>Configures automatic bandwidth on a tunnel interface and enters MPLS-TE automatic bandwidth configuration mode.</td>
</tr>
<tr>
<td>bw-limit (MPLS-TE), on page 162</td>
<td>Configures the minimum and maximum automatic bandwidth to set on a tunnel.</td>
</tr>
<tr>
<td>collect-bw-only (MPLS-TE), on page 177</td>
<td>Enables only the bandwidth collection without adjusting the automatic bandwidth.</td>
</tr>
<tr>
<td>interface tunnel-te, on page 207</td>
<td>Configures an MPLS-TE tunnel interface.</td>
</tr>
<tr>
<td>overflow threshold (MPLS-TE), on page 232</td>
<td>Configures tunnel overflow detection.</td>
</tr>
<tr>
<td>show mpls traffic-eng tunnels, on page 335</td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
</tbody>
</table>
attribute-flags

To configure attribute flags for an interface, use the `attribute-flags` command in MPLS-TE interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
attribute-flags  attribute-flags
no  attribute-flags  attribute-flags
```

### Syntax Description

- `attribute-flags`: Links attributes that are compared to the affinity bits of a tunnel during selection of a path. Range is 0x0 to 0xFFFFFFFF, representing 32 attributes (bits) where the value of an attribute is 0 or 1.

### Command Default

```
attributes : 0x0
```

### Command Modes

MPLS-TE interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `attribute-flags` command assigns attributes to a link so that tunnels with matching attributes (represented by their affinity bits) prefer this link instead of others that do not match.

The interface attribute is flooded globally so that it can be used as a tunnel headend path selection criterion.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to set attribute flags to 0x0101:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# interface POS 0/7/0/0
RP/0/RP0/CPU0:router(config-mpls-te-if)# attribute-flags 0x0101
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin-weight, on page 133</td>
<td>Overrides the IGP administrative weight of the link.</td>
</tr>
<tr>
<td>affinity, on page 134</td>
<td>Configures affinity (the properties that the tunnel requires in its links) for an MPLS-TE tunnel.</td>
</tr>
<tr>
<td>attribute-names, on page 145</td>
<td>Configures the attribute names for the interface.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>interface (MPLS-TE), on page 205</td>
<td>Enables MPLS-TE on an interface and enters MPLS-TE interface configuration mode.</td>
</tr>
<tr>
<td>mpls traffic-eng, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
</tbody>
</table>
attribute-names

To configure attributes for the interface, use the `attribute-names` command in MPLS-TE interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
attribute-names attribute name
no attribute-names attribute name
```

**Syntax Description**

- `attribute name` Attribute name expressed using alphanumeric or hexadecimal characters.

**Command Default**

No default behavior or values

**Command Modes**

MPLS-TE interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

- `mpls-te` read, write

**Examples**

The following example shows how to assign an attribute name (in this case, red) to a TE link:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# interface pos 0/2/0/1
RP/0/RP0/CPU0:router(config-mpls-te-if)# attribute-name red
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>affinity, on page 134</td>
<td>Configures affinity (the properties that the tunnel requires in its links) for an MPLS-TE tunnel.</td>
</tr>
<tr>
<td>attribute-flags, on page 143</td>
<td>Configures attribute flags for the interface.</td>
</tr>
<tr>
<td>interface (MPLS-TE), on page 205</td>
<td>Enables MPLS-TE on an interface and enters MPLS-TE interface configuration mode.</td>
</tr>
<tr>
<td>mpls traffic-eng, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
</tbody>
</table>
attribute-set

To configure attribute-set for auto-mesh tunnels, use the `attribute-set` command in MPLS-TE configuration mode.

```
attribute-set auto-mesh attribute-set-name {affinity [affinity-value mask mask-value] | exclude name | exclude-all | include name | include-strict name} | auto-bw collect-bw-only | autoroute announce | bandwidth bandwidth | fast-reroute [protect bandwidth node | node bandwidth] | logging events lsp-status | insufficient-bandwidth | reoptimize | reroute | state | priority setup-range hold-range | record-route | signalled-bandwidth bandwidth [class-type cl] | soft-preemption}
```

To configure attribute-set for a path-option, use the `attribute-set` command in MPLS-TE configuration mode.

```
attribute-set path-option attribute-set-name {affinity [affinity-value mask mask-value] | exclude name | exclude-all | include name | include-strict name} | signalled-bandwidth bandwidth [class-type cl]}
```

To disable this behavior, use the `no` form of this command.

```
no attribute-set
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-mesh</td>
<td>Specifies the values of an attribute set for the auto-mesh group.</td>
</tr>
<tr>
<td>path-option</td>
<td>Specifies the values of an attribute set for the path option.</td>
</tr>
<tr>
<td>attribute-set-name</td>
<td>A 32-bit character string, specifies the name of the attribute-set template.</td>
</tr>
<tr>
<td>affinity-value</td>
<td>Attribute values that are required for links to carry this tunnel. A 32-bit decimal number, representing 32 attributes (bits), where the value of an attribute is 0 or 1. Range is from 0x0 to 0xFFFF.</td>
</tr>
<tr>
<td>mask mask-value</td>
<td>Checks the link attribute. A 32-bit decimal number, representing 32 attributes (bits), where the value of an attribute mask is 0 or 1. Range is from 0x0 to 0xFFFF.</td>
</tr>
<tr>
<td>exclude name</td>
<td>Configures a specific affinity that is to be excluded.</td>
</tr>
<tr>
<td>exclude-all</td>
<td>Excludes all affinities.</td>
</tr>
<tr>
<td>include name</td>
<td>Configures the affinity to include in the loose sense.</td>
</tr>
<tr>
<td>include-strict name</td>
<td>Configures the affinity to include in the strict sense.</td>
</tr>
<tr>
<td>logging</td>
<td>Per-interface logging configuration.</td>
</tr>
<tr>
<td>events</td>
<td>Per-interface logging events.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>lsp-status</td>
<td>Enables interface LSP state change alarms.</td>
</tr>
<tr>
<td>reoptimize</td>
<td>Enables interface LSP REOPT change alarms.</td>
</tr>
<tr>
<td>state</td>
<td>Enables interface LSP UP/DOWN change alarms.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies the tunnel priority.</td>
</tr>
<tr>
<td>setup-range</td>
<td>Specifies setup priority. Range is 0 to 7.</td>
</tr>
<tr>
<td>hold-range</td>
<td>Specifies hold priority. Range is 0 to 7.</td>
</tr>
<tr>
<td>record-route</td>
<td>Records the route used by the tunnel.</td>
</tr>
<tr>
<td>signalled-bandwidth</td>
<td>Specifies the tunnel bandwidth requirement to be signalled.</td>
</tr>
<tr>
<td>bandwidth</td>
<td>Bandwidth required for an MPLS-TE tunnel, specified in kilobits per second. By default, bandwidth is reserved in the global pool. Range is from 0 to 4294967295.</td>
</tr>
<tr>
<td>class-type ct</td>
<td>(Optional) Configures the class type of the tunnel bandwidth request. Range is 0 to 1. Class-type 0 is equivalent to global-pool. Class-type 1 is equivalent to subpool.</td>
</tr>
<tr>
<td>soft-preemption</td>
<td>Enables the soft-preemption feature on this tunnel.</td>
</tr>
</tbody>
</table>

**Command Default**
- **affinity-value**: 0x0
- **mask-value**: 0xFFFF

**Command Modes**
- MPLS TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The values specified for an attribute within a path-option attribute-set does not prevent the configuration of the same attribute at the tunnel level. However, only one level is taken into consideration. The configuration at the path-option level is considered more specific than the one at the level of the tunnel, and is therefore used.

Attributes that are not specified within an attribute-set picks their default values, as usual, from the configuration at the tunnel level, the configuration at the global mpls level, or default values.

An XRO attribute-set can be specified as part of the path-option, if required. An empty XRO attribute set results in the GMPLS tunnel being signaled with no exclusions, and therefore no XRO.
This example shows how to configure an attribute-set to a TE interface for an auto-mesh tunnel:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# auto-tunnel mesh
RP/0/RP0/CPU0:router(config-te-auto-mesh)# group 1
RP/0/RP0/CPU0:router(config-te-mesh-group)# attribute-set am1
RP/0/RP0/CPU0:router(config-te-mesh-group)# destination-list dl1
```

This example shows how to configure the tunnel affinity and signalled-bandwidth for a path-option:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# attribute-set path-option myset
RP/0/RP0/CPU0:router(config-te-attribute-set)# affinity 0x3 mask 0x3
RP/0/RP0/CPU0:router(config-te-attribute-set)# signalled-bandwidth 2000
```
auto-bw (MPLS-TE)

To configure automatic bandwidth on a tunnel interface and to enter MPLS-TE automatic bandwidth interface configuration mode, use the auto-bw command in MPLS-TE interface configuration mode. To disable the automatic bandwidth on that tunnel, use the no form of this command.

auto-bw
no auto-bw

Syntax Description

This command has no arguments or keywords.

Command Default

By default, automatic bandwidth is not enabled.

Command Modes

MPLS-TE interface configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

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

Use the auto-bw command to enter MPLS-TE automatic bandwidth interface configuration mode.

The auto-bw and load-share unequal commands should not be used together.

The load-share unequal command determines the load-share for a tunnel based on the bandwidth. However, the MPLS-TE automatic bandwidth feature changes the bandwidth around. If you are configuring both the load-share unequal command and the MPLS-TE automatic bandwidth feature, we recommend that you specify an explicit load-share value configuration under each MPLS-TE automatic bandwidth tunnel.

The following automatic bandwidth scenarios are described:

• If you configure the automatic bandwidth on a tunnel, the automatic bandwidth is enabled on that tunnel. If no other configuration is specified, defaults for the various parameters are used, the operation stops.
• The automatic operation (for example, output rate collection) starts as soon as the automatic bandwidth is enabled on one tunnel. If automatic bandwidth is disabled from all tunnels, the operation stops.
• If the output rate collection is already active when the automatic bandwidth is configured on a tunnel, the statistics collection for that tunnel starts at the next collection configuration.

Note

Because the collection timer is already running, the first collection event for that tunnel happens in less than C minutes (for example, on an average of C/2 minutes).
auto-bw (MPLS-TE)

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enter MPLS-TE automatic bandwidth interface configuration mode:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adjustment-threshold (MPLS-TE), on page 131</td>
<td>Configures the tunnel-bandwidth change threshold to trigger an adjustment.</td>
</tr>
<tr>
<td>application (MPLS-TE), on page 141</td>
<td>Configures the application frequency, in minutes, for the applicable tunnel.</td>
</tr>
<tr>
<td>bw-limit (MPLS-TE), on page 162</td>
<td>Configures the minimum and maximum automatic bandwidth to set on a tunnel.</td>
</tr>
<tr>
<td>collect-bw-only (MPLS-TE), on page 177</td>
<td>Enables only the bandwidth collection without adjusting the automatic bandwidth.</td>
</tr>
<tr>
<td>interface tunnel-te, on page 207</td>
<td>Configures an MPLS-TE tunnel interface.</td>
</tr>
<tr>
<td>overflow threshold (MPLS-TE), on page 232</td>
<td>Configures tunnel overflow detection.</td>
</tr>
<tr>
<td>show mpls traffic-eng tunnels, on page 335</td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
</tbody>
</table>
auto-bw collect frequency (MPLS-TE)

To configure the automatic bandwidth collection frequency, use the `auto-bw collect frequency` command in MPLS-TE configuration mode. To reset the automatic bandwidth frequency to its default value, use the `no` form of this command.

```
auto-bw collect frequency minutes
no auto-bw collect frequency minutes
```

**Syntax Description**

- `minutes`: Interval between automatic bandwidth adjustments, in minutes. The range is from 1 to 10080. The default is 5.

**Command Default**

- `minutes`: 5

In addition, the `no` form of this command resets to the default.

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

The `auto-bw collect frequency` command configures the automatic bandwidth collection frequency for all the tunnels.

Modifying the global collection frequency does not restart the tunnel for the current application period. The application period continues with the modified collection frequency.

**Examples**

The following example configures a tunnel for an automatic bandwidth adjustment of 100 minutes:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config=mpls-te)# auto-bw collect frequency 100
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mpls traffic-eng</code>, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>mpls traffic-eng auto-bw apply (MPLS-TE), on page 217</td>
<td>Configures the highest bandwidth available on a tunnel without waiting for the current application period to end.</td>
</tr>
<tr>
<td>show mpls traffic-eng tunnels, on page 335</td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
</tbody>
</table>
autoroute announce

To specify that the Interior Gateway Protocol (IGP) should use the tunnel (if the tunnel is up) in its enhanced shortest path first (SPF) calculation, use the **autoroute announce** command in interface configuration mode. To return to the default behavior, use the no form of this command.

```
autoroute announce
no autoroute announce
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Announces IPv4 tunnel

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When more than one IGP is configured, the tunnel is announced as autoroute to the IGP that is used to compute the TE tunnel path.

When the **autoroute announce** command is configured, the route metric of the tunnel path to the destination equals the route metric of the shortest IGP path to that destination.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to configure IGP to use the tunnel in its enhanced SPF calculation when the tunnel is up:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface tunnel-te, on page 207</td>
<td>Configures an MPLS-TE tunnel interface.</td>
</tr>
</tbody>
</table>
**autoroute metric**

To specify the MPLS-TE tunnel metric that the Interior Gateway Protocol (IGP) enhanced Shortest Path First (SPF) calculation uses, use the `autoroute metric` command in interface configuration mode. If no specific metric is to be specified, use the `no` form of this command.

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

**Syntax Description**

- **absolute** Enables the absolute metric mode; you can enter a positive metric value.
- **relative** Enables the relative metric mode; you can enter a positive, negative, or zero value.
- **value** Metric that the IGP enhanced SPF calculation uses. Relative value range is from –10 to 10. Absolute value range is from 1 to 2147483647.

**Command Default**

The relative value is 0.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `autoroute metric` command overwrites the default tunnel route metric of the shortest IGP path to the destination.

**Task ID**

```
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>
```

**Examples**

The following example shows how to configure the IGP enhanced SPF calculation using MPLS-TE tunnel metric as relative negative 1:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>autoroute announce, on page 153</td>
<td>Instructs the IGP to use the tunnel (if it is up) in its enhanced SPF calculation.</td>
</tr>
<tr>
<td>interface tunnel-te, on page 207</td>
<td>Configures an MPLS-TE tunnel interface.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>show mpls traffic-eng autoroute, on page 275</code></td>
<td>Displays the tunnels announced to the IGP, including interface, destination, and bandwidth.</td>
</tr>
</tbody>
</table>
**auto-tunnel backup (MPLS-TE)**

To automatically build next-hop (NHOP) and next-next-hop (NNHOP) backup tunnels, and to enter auto-tunnel backup configuration mode, use the `auto-tunnel backup` command in MPLS-TE configuration mode. To clear the NHOP and NNHOP backup tunnels, use the `no` form of this command.

```
auto-tunnel backup
no auto-tunnel backup
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The range of `tunnel-ID` is required to be mentioned for the auto-tunnel backup tunnels; otherwise, none of the tunnels are created.

The `no` form of this command deletes both NHOP and NNHOP backup tunnelsthatare configured using either the `auto-tunnel backup` command or the `nhop-only` command.

**Example**

The following example automatically builds NHOP and NNHOP backup tunnels:

```
RP/0/RP0/CP00:router(config)# mpls traffic-eng
RP/0/RP0/CP00:router(config-mpls-te)# auto-tunnel backup
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear mpls traffic-eng auto-tunnel backup unused, on page 166</td>
<td>Clears the unused automatic backup tunnels.</td>
</tr>
<tr>
<td>mpls traffic-eng interface-path-id auto-tunnel backup</td>
<td>Configures the automatic backup tunnel for a specific interface.</td>
</tr>
<tr>
<td>show mpls traffic-eng tunnels, on page 335</td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>tunnel-id (auto-tunnel backup), on page 383</td>
<td>Configures range of tunnel interface numbers for automatic backup tunnels.</td>
</tr>
</tbody>
</table>
backup-bw

To configure the backup bandwidth for an MPLS-TE backup tunnel (that is used to protect a physical interface), use the backup-bw command in interface configuration mode. To return to the default behavior, use the no form of this command.

```
backup-bw {backup bandwidth {any-class-type | class-type ct} |
             global-pool {bandwidth | unlimited} |
             sub-pool {bandwidth | unlimited} |
            unlimited {any-class-type | class-type ct} }

no backup-bw {backup bandwidth {any-class-type | class-type ct} |
             global-pool {bandwidth | unlimited} |
             sub-pool {bandwidth | unlimited} |
            unlimited {any-class-type | class-type ct} }
```

**Syntax Description**

- `backup bandwidth` Backup bandwidth in any-pool provided by an MPLS-TE backup tunnel. Bandwidth is specified in kilobits per second (kbps). Range is 1 to 4294967295.
- `any-class-type` Displays the backup bandwidth assigned to any class-type protected tunnels.
- `class-type ct` Displays the class type of the backup bandwidth. Range is 0 to 1.
- `global-pool bandwidth` (In Prestandard DS-TE with RDM) Displays the backup bandwidth in global pool provided by an MPLS-TE backup tunnel. Bandwidth is specified in kilobits per second. Range is 1 to 4294967295.
- `unlimited` Displays the unlimited bandwidth.
- `sub-pool bandwidth` (In Prestandard DS-TE with RDM) Displays the backup bandwidth in sub-pool provided by an MPLS-TE backup tunnel. Bandwidth is specified in kilobits per second. Range bandwidth is 1 to 4294967295. Only label switched paths (LSPs) using bandwidth from the sub-pool can use the backup tunnel.

**Command Default**

Any class-type unlimited.

**Command Modes**

Interface configuration

**Command History**

Release 5.0.0 This command was introduced.

**Usage Guidelines**

Backup bandwidth can be limited or unlimited or specific to a global pool, sub-pool, or non-specific any-pool. Backup with backup-bw in global-pool protects global-pool LSPs only; backup-bw in sub-pool protects sub-pool LSPs only.

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

Backup bandwidth provides bandwidth protection for fast reroute (FRR). Bandwidth protection for FRR supports DiffServ-TE with two bandwidth pools (class-types).

Class-type 0 is strictly equivalent to global-pool; class-type 1 is strictly equivalent to sub-pool bandwidth using the Russian Doll Model (RDM).
### Example

The following example shows how to configure backup tunnel 1 for use only by LSPs that take their bandwidth from the global pool (class-type 0 tunnels). Backup tunnel 1 does not provide bandwidth protection.

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

or

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

In the following example, backup tunnel 2 is used by LSPs that take their bandwidth from the sub-pool (class-type 1 tunnels) only. Backup tunnel 2 provides bandwidth protection for up to 1000 units.

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

or

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 2
RP/0/RP0/CPU0:router(config-if)# backup-bw 1000 class-type 1
```

### Related Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>backup-path tunnel-te</code>, on page 160</td>
<td>Assigns one or more backup tunnels to a protected interface.</td>
</tr>
<tr>
<td><code>fast-reroute</code>, on page 190</td>
<td>Enables FRR protection for an MPLS-TE tunnel.</td>
</tr>
<tr>
<td><code>interface tunnel-te</code>, on page 207</td>
<td>Configures an MPLS-TE tunnel interface.</td>
</tr>
</tbody>
</table>
backup-path tunnel-te

To set an MPLS-TE tunnel to protect a physical interface against failure, use the `backup-path tunnel-te` command in MPLS-TE interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
backup-path tunnel-te  tunnel-number
no  backup-path tunnel-te  tunnel-number
```

Syntax Description

- `tunnel-number` Number of the tunnel protecting the interface. Range is 0 to 65535.

Command Default

No default behavior or values

Command Modes

MPLS-TE interface configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

When the protected interface is down (shut down or removed), the traffic it was carrying (for the other label switched paths [LSPs], referred to as the protected LSPs) is rerouted, using fast reroute (FRR) onto the backup tunnels.

The following guidelines pertain to the FRR process:

- Multiple (backup) tunnels can protect the same interface by entering this command multiple times for different tunnels. The same (backup) tunnel can protect multiple interfaces by entering this command for each interface.
- The backup tunnel used to protect a physical interface must have a valid IP address configured.
- The backup tunnel cannot pass through the same interface that it is protecting.
- TE tunnels that are configured with the FRR option, cannot be used as backup tunnels.
- For the backup tunnel to provide protection to the protected LSP, the backup tunnel must have a terminating-end node in the path of a protected LSP.
- The source IP address of the backup tunnel and the merge point (MP) address (the terminating-end address of the backup tunnel) must be reachable.

Note

You must configure record-route on TE tunnels that are protected by multiple backup tunnels merging at a single node.

Task ID

```
Task ID  Operations
mpls-te  read,
          write
```
The following example shows how to protect PoS interface 0/7/0/0 using tunnel 100 and tunnel 150:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# interface POS 0/7/0/0
RP/0/RP0/CPU0:router(config-mpls-te-if)# backup-path tunnel-te 100
RP/0/RP0/CPU0:router(config-mpls-te-if)# backup-path tunnel-te 150
```
bw-limit (MPLS-TE)

To configure the minimum and maximum automatic bandwidth to be set on a tunnel, use the `bw-limit` command in MPLS-TE automatic bandwidth interface configuration mode. To disable this feature, use the `no` form of this command.

```
bw-limit min bandwidth {max bandwidth}
no bw-limit
```

**Syntax Description**

- `min bandwidth` Configures the minimum automatic bandwidth, in kbps, on a tunnel. The range is from 0 to 4294967295. The default is 0.
- `max bandwidth` Configures the maximum automatic bandwidth, in kbps, on a tunnel. The range is from 0 to 4294967295. The default is 4294967295.

**Command Default**

- `min`: 0
- `max`: 4294967295

**Command Modes**

MPLS-TE automatic bandwidth interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

Both the `min` and `max` keywords must be configured.

The `bw-limit` command automatically sets the minimum bandwidth to the default value of 0, or the `bw-limit` command automatically sets the maximum to the default value of 4294967295 kbps.

If the value of the `min` keyword is greater than the `max` keyword, the `bw-limit` command is rejected. If you configure and modify the minimum or maximum bandwidth while the automatic bandwidth is already running, the next bandwidth application for that tunnel is impacted. For example, if the current tunnel requested bandwidth is 30 Mbps and the minimum bandwidth is modified to 50 Mbps, the next application sets the tunnel bandwidth to 50 Mbps.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the minimum and maximum bandwidth for the tunnel:
Configure the tunnel bandwidth change threshold to trigger an adjustment.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# auto-bw
RP/0/RP0/CPU0:router(config-if-tunte-autobw)# bw-limit min 30 max 80
```
clear mpls traffic-eng auto-bw (MPLS-TE EXEC)

To clear automatic bandwidth sampled output rates and to restart the application period for the specified tunnel, use the clear mpls traffic-eng auto-bw command in EXEC mode.

```
clear mpls traffic-eng auto-bw {all | internal | tunnel-te tunnel-number}
```

### Syntax Description
- **all**: Clears the automatic bandwidth sampled output rates for all tunnels.
- **internal**: Clears all the automatic bandwidth internal data structures.
- **tunnel-te tunnel-number**: Clears the automatic bandwidth sampled output rates for a specific tunnel. The `tunnel-number` argument is the tunnel ID used to clear the sampled output rates.

### Command Default
No default behavior or values

### Command Modes
EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

If no tunnel is specified, the `clear mpls traffic-eng auto-bw` command clears all the automatic bandwidth enabled tunnels.

For each tunnel in which the automatic bandwidth adjustment is enabled, information is maintained about the sampled output rates and the time remaining until the next bandwidth adjustment. The application period is restarted and values such as the largest collected bandwidth get reset. The tunnel continues to use the current bandwidth until the next application.

### Examples
The following example displays the information for the automatic bandwidth for tunnel number 0 from the `show mpls traffic-eng tunnels auto-bw brief` command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels 0 auto-bw brief

<table>
<thead>
<tr>
<th>Tunnel</th>
<th>LSP Name</th>
<th>Last appl ID</th>
<th>Requested BW (kbps)</th>
<th>Signalled BW (kbps)</th>
<th>Highest BW (kbps)</th>
<th>Application BW (kbps)</th>
<th>Time Left</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel-te0</td>
<td></td>
<td>278</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>150</td>
<td>12m 38s</td>
</tr>
</tbody>
</table>
```
The following example shows how to clear the automatic bandwidth sampled output rates for tunnel number 0:

RP/0/RP0/CPU0:router# clear mpls traffic-eng auto-bw tunnel-te 0

RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels 0 auto-bw brief

<table>
<thead>
<tr>
<th>Tunnel</th>
<th>LSP Name</th>
<th>Last appl ID</th>
<th>Requested BW(kbps)</th>
<th>Signalled BW(kbps)</th>
<th>Highest BW(kbps)</th>
<th>Time Left</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel-te0</td>
<td>278</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>0</td>
<td>24m 0s</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear mpls traffic-eng counters signaling,</td>
<td>Clears the automatic bandwidth configuration in a tunnel.</td>
</tr>
<tr>
<td>on page 171</td>
<td></td>
</tr>
<tr>
<td>show mpls traffic-eng tunnels auto-bw brief,</td>
<td>Displays the list of automatic-bandwidth-enabled tunnels, and indicates if</td>
</tr>
<tr>
<td>on page 363</td>
<td>the current signaled bandwidth of the tunnel is identical to the bandwidth</td>
</tr>
<tr>
<td></td>
<td>that is applied by the automatic bandwidth.</td>
</tr>
</tbody>
</table>
clear mpls traffic-eng auto-tunnel backup unused

To remove unused automatic backup tunnels, use the clear mpls traffic-eng auto-tunnel backup unused command in global configuration mode.

clear mpls traffic-eng auto-tunnel backup unused \{all | tunnel-te tunnel-number\}

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Clears all the unused automatic backup tunnels.</td>
</tr>
<tr>
<td>tunnel-te tunnel-number</td>
<td>Clears a specific unused automatic backup tunnel.</td>
</tr>
</tbody>
</table>

Command Default

No default behavior or values

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

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

The unused auto-tunnel backup tunnel is the tunnel that is not assigned to protect any FRR tunnel.

The behavior of this command is the same as the expiration of the timers removal unused command in which, when the timeout value is reached, the automatic backup tunnel is removed.

Example

The following example displays the information for the unused backup automatic tunnels from the show mpls traffic-eng tunnels unused command:

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

The following example shows how to clear the unused backup automatic tunnels:

RP/0/RP0/CPU0:router# clear mpls traffic-eng auto-tunnel backup unused all
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels unused

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls traffic-eng tunnels, on page 335</td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
</tbody>
</table>


clear mpls traffic-eng auto-tunnel mesh

To clear all unused auto-tunnel mesh destinations, use the `clear mpls traffic-eng auto-tunnel mesh` command in EXEC mode.

```
clear mpls traffic-eng auto-tunnel mesh unused \{all | tunnel-te\}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Clears all applicable unused auto-tunnel destinations.</td>
</tr>
<tr>
<td>tunnel-te id</td>
<td>Clears an unused auto-tunnel destinations identified by a tunnel identifier.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te execute</td>
</tr>
</tbody>
</table>

**Examples**

This is sample output from the `clear mpls traffic-eng auto-tunnel mesh` command:

```
clear mpls traffic-eng auto-tunnel mesh
```
clear mpls traffic-eng counters auto-tunnel mesh

To clear all auto-tunnel mesh counters, use the `clear mpls traffic-eng counters auto-tunnel mesh` command in EXEC mode.

`clear mpls traffic-eng counters auto-tunnel mesh`

This command has no arguments or keywords.

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

This is sample output from the `clear mpls traffic-eng counters auto-tunnel mesh` command:

```
RP/0/RP0/CPU0:router#clear mpls traffic-eng counters auto-tunnel mesh
```
clear mpls traffic-eng counters auto-tunnel backup

To clear MPLS-TE automatic tunnel backup counters, use the clear mpls traffic-eng counters auto-tunnel backup command in EXEC mode.

clear mpls traffic-eng counters auto-tunnel backup

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Example**

The following example removes all counters for the automatic backup tunnels:

```
RP/0/RP0/CPU0:router# clear mpls traffic-eng counters auto-tunnel backup
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls traffic-eng counters auto-tunnel backup</td>
<td>Displays the MPLS-TE automatic tunnel backup counters.</td>
</tr>
<tr>
<td>show mpls traffic-eng tunnels, on page 335</td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
</tbody>
</table>
clear mpls traffic-eng counters global

To clear the internal MPLS-TE tunnel counters, use the clear mpls traffic-eng counters global command in EXEC mode.

clear mpls traffic-eng counters global

Syntax Description
This command has no arguments or keywords.

Command Default
No default behavior or values

Command Modes
EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>execute</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to clear the internal MPLS-TE tunnel counters:

RP/0/RP0/CPU0:router# clear mpls traffic-eng counters global
clear mpls traffic-eng counters signaling

To clear (set to zero) the MPLS tunnel signaling counters, use the `clear mpls traffic-eng counters signaling` command in EXEC mode.

```
clear mpls traffic-eng counters signaling [all | [heads | mids | tails]] | name name | summary]
```

**Syntax Description**

- **all**  
  Clears counters for all MPLS-TE tunnels.
- **heads**  
  (Optional) Displays tunnels with their heads at this router.
- **mids**  
  (Optional) Displays tunnels with their midpoints at this router.
- **tails**  
  (Optional) Displays tunnels with their tails at this router.
- **name name**  
  Clears counters for an MPLS-TE tunnel with the specified name.
- **summary**  
  Clears the counter’s summary.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

**Task ID**

- **mpls-te**  
  read, write

**Examples**

The following example shows how to clear all counters:

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls traffic-eng counters signaling, on page 284</td>
<td>Displays tunnel signaling statistics.</td>
</tr>
</tbody>
</table>

clear mpls traffic-eng counters signaling
clear mpls traffic-eng counters soft-preemption

To clear (set to zero) the counters for soft-preemption statistics, use the `clear mpls traffic-eng counters soft-preemption` command in EXEC mode.

```
clear mpls traffic-eng counters {all | soft-preemption}
```

**Syntax Description**
- **all**: Clears counters for all MPLS-TE tunnels.
- **soft-preemption**: Clears the statistics for soft preemption counters.

**Command Default**
None

**Command Modes**
EXEC

**Command History**
- **Release 5.0.0**: This command was introduced.

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

When all counters are cleared using the `clear mpls traffic-eng counters all` command, the counters for soft-preemption statistics are automatically cleared.

**Task ID**
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**
This example shows how to clear all counters:

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

**Related Commands**
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls traffic-eng counters signaling, on page 284</td>
<td>Displays tunnel signaling statistics.</td>
</tr>
</tbody>
</table>
clear mpls traffic-eng fast-reroute log

To clear the log of MPLS fast reroute (FRR) events, use the clear mpls traffic-eng fast-reroute log command in EXEC mode.

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

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

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows sample output before clearing the log of FRR events:

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

Node              Protected LSPs Rewrites When            Switching Time (usec)
--------  ---------  ----------------------  ----------------------
0/0/CPU0 PO0/1/0/1 1  1          Feb 27 19:12:29.064000  147
0/1/CPU0 PO0/1/0/1 1  1          Feb 27 19:12:29.060093  165
0/2/CPU0 PO0/1/0/1 1  1          Feb 27 19:12:29.063814  129
0/3/CPU0 PO0/1/0/1 1  1          Feb 27 19:12:29.062861  128

RP/0/RP0/CPU0:router# clear mpls traffic-eng fast-reroute log
```
clear mpls traffic-eng link-management statistics

To clear all the MPLS-TE admission control statistics, use the clear mpls traffic-eng link-management statistics command in EXEC mode.

clear mpls traffic-eng link-management statistics

Syntax Description
This command has no arguments or keywords.

Command Default
No default behavior or values

Command Modes
EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

Task ID

<table>
<thead>
<tr>
<th>Task</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td></td>
</tr>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples
The following example shows how to clear all the MPLS-TE statistics for admission control:

RP/0/RP0/CPU0:router# clear mpls traffic-eng link-management statistics
clear mpls traffic-eng pce

To clear the path computation element (PCE) statistics, use the `clear mpls traffic-eng pce` command in EXEC mode.

```
clear mpls traffic-eng pce [peer  ipv4  address]
```

**Syntax Description**

- **peer**: (Optional) Clears the statistics for one peer.
- **ipv4 address**: (Optional) Configures the IPv4 address for PCE.

**Command Default**

Clears statistics for all the PCE peers.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear the statistics for the PCE:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mpls traffic-eng pce peer</code>, on page 319</td>
<td>Displays the status of the PCE peer address and state.</td>
</tr>
</tbody>
</table>
collect-bw-only (MPLS-TE)

To configure only the bandwidth collection without adjusting the bandwidth automatically, use the `collect-bw-only` command in MPLS-TE automatic bandwidth interface configuration mode. To disable this feature, use the `no` form of this command.

```
collect-bw-only
no  collect-bw-only
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Bandwidth collection is either enabled or disabled.

**Command Modes**

MPLS-TE automatic bandwidth interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

If you enable the `collect-bw-only` command while the automatic bandwidth is already running on a tunnel, the bandwidth application is disabled from that moment. Before you enable the actual bandwidth application, you can get the status of the automatic bandwidth behavior.

If you disable the `collect-bw-only` command on a tunnel from which the automatic bandwidth is already running, the actual bandwidth application takes place on the tunnel at the next application period.

It is also possible to manually activate a bandwidth application regardless of the collect bandwidth only flag that is being specified on a tunnel. To activate the bandwidth application, use the `mpls traffic-eng auto-bw apply` command in EXEC mode.

```
Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable only the bandwidth collection without adjusting the automatic bandwidth:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# auto-bw
RP/0/RP0/CPU0:router(config-if-tunte-autobw)# collect-bw-only
```
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adjustment-threshold (MPLS-TE), on page 131</td>
<td>Configures the tunnel-bandwidth change threshold to trigger an adjustment.</td>
</tr>
<tr>
<td>application (MPLS-TE), on page 141</td>
<td>Configures the application frequency, in minutes, for the applicable tunnel.</td>
</tr>
<tr>
<td>auto-bw (MPLS-TE), on page 149</td>
<td>Configures automatic bandwidth on a tunnel interface and enters MPLS-TE automatic bandwidth interface configuration mode.</td>
</tr>
<tr>
<td>bw-limit (MPLS-TE), on page 162</td>
<td>Configures the minimum and maximum automatic bandwidth to set on a tunnel.</td>
</tr>
<tr>
<td>interface tunnel-te, on page 207</td>
<td>Configures an MPLS-TE tunnel interface.</td>
</tr>
<tr>
<td>overflow threshold (MPLS-TE), on page 232</td>
<td>Configures tunnel overflow detection.</td>
</tr>
<tr>
<td>show mpls traffic-eng tunnels, on page 335</td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
</tbody>
</table>
destination (MPLS-TE)

To configure the destination address of a TE tunnel, use the destination command in interface configuration mode. To return to the default behavior, use the no form of this command.

```
destination ip-address
no destination ip-address
```

**Syntax Description**

- `ip-address`  Destination address of the MPLS-TE router ID.

**Command Default**

No default behavior or values

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Note**

The tunnel destination address must be a unique MPLS-TE router ID; it cannot be an MPLS-TE link address on a node.

For Point-to-Point (P2P) tunnels, the destination command is used as a single-line command.

**Task ID**

- Task ID
  - mpls-te read, write

**Examples**

The following example shows how to set the destination address for tunnel-te1 to 10.10.10.10:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te1
RP/0/RP0/CPU0:router(config-if)# destination 10.10.10.10
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface tunnel-te, on page 207</td>
<td>Configures an MPLS-TE tunnel interface.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>show mpls traffic-eng tunnels, on page 335</code></td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
</tbody>
</table>
disable (explicit-path)

To prevent the path from being used by MPLS-TE tunnels while it is configured, use the `disable` command in explicit path configuration mode. To return to the default behavior, use the `no` form of this command.

```
disable
no disable
```

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

**Command Default**
Explicit path is enabled.

**Command Modes**
Explicit path configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to disable explicit path 200:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>index exclude-address, on page 200</td>
<td>Specifies the next IP address to exclude from the explicit path.</td>
</tr>
<tr>
<td>index next-address, on page 203</td>
<td>Specifies path entries at a specific index.</td>
</tr>
<tr>
<td>show explicit-paths, on page 269</td>
<td>Displays the configured IP explicit paths.</td>
</tr>
</tbody>
</table>
ds-te bc-model

To enable a specific bandwidth constraint model (Maximum Allocation Model or Russian Doll Model) on the entire label switched router (LSR), use the `ds-te bc-model` command in MPLS-TE configuration mode. To return to the default behavior, use the `no` form of this command.

```
ds-te bc-model mam
no ds-te bc-model mam
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mam</code></td>
<td>Enables the Maximum Allocation Model (MAM) bandwidth constraints model.</td>
</tr>
</tbody>
</table>

**Command Default**

RDM is the default bandwidth constraint model.

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

You can configure both the MAM and RDM bandwidth values on a single interface before swapping to an alternate global MPLS-TE BC model.

If you configure bandwidth constraints without configuring the corresponding bandwidth constraint values, the router uses default bandwidth constraint values.

MAM is not supported in prestandard DS-TE mode. MAM and RDM are supported in IETF DS-TE mode; RDM is supported in prestandard DS-TE mode.

**Note**

Changing the bandwidth constraints model affects the entire router and may have a major impact on system performance as nonzero-bandwidth tunnels are torn down.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable the MAM bandwidth constraints model:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
```
RP/0/RP0/CPU0:router(config-mpls-te)# ds-te bc-model mam

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ds-te mode, on page 184</td>
<td>Configures standard DS-TE mode.</td>
</tr>
<tr>
<td>ds-te te-classes, on page 186</td>
<td>Enters DS-TE te-class map configuration mode.</td>
</tr>
<tr>
<td>mpls traffic-eng, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
<tr>
<td>show mpls traffic-eng ds-te te-class, on page 290</td>
<td>Displays the Diff-Serv TE-class map in use.</td>
</tr>
</tbody>
</table>
ds-te mode

To configure standard differentiated-service TE mode (DS-TE), use the `ds-te mode` command in MPLS-TE configuration mode. To return to the default behavior, use the `no` form of this command.

```
no ds-te mode ietf
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ietf</code></td>
<td>Enables IETF standard mode.</td>
</tr>
</tbody>
</table>

### Command Default

Prestandard DS-TE is the default differentiated service mode.

### Command Modes

MPLS-TE configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

The following two DS-TE modes are supported:

- **Prestandard mode**
  - The Cisco proprietary mechanism for IGPs and RSVP signalling are used and DS-TE does not interoperate with third-party vendor equipment.

- **IETF mode**
  - Standard defined extensions are used for IGPs and RSVP signalling and DS-TE in this mode interoperates with third-party equipment.
  - IETF mode supports two bandwidth constraint models: the Russian Doll Model (RDM) and Maximum Allocation Model (MAM).
  - RDM is the default model.
  - Router advertises variable-length bandwidth constraints, max-reservable-bandwidth, and unreserved bandwidths in TE-classes.
  - tunnels must have valid class-type and priority configured as per TE-class map in use; otherwise, tunnels remain down.
  - TE-class map (a set of tunnel priority and class-type values) is enabled to interpret unreserved bandwidth values advertised in IGP; therefore, TE-class map must be identical on all nodes for TE tunnels to be successfully established.

For DS-TE to function properly, DS-TE modes must be configured identically on all MPLS-TE nodes.
If you need to change the DS-TE mode, you must bring down all tunnel interfaces and after the change, you should flood the updated bandwidth values through the network.

---

**Note**

Changing the DS-TE mode affects the entire LSR and can have a major impact on system performance when tunnels are torn down.

---

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to enable IETF standard mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# ds-te mode ietf
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ds-te bc-model, on page 182</td>
<td>Enables a specific bandwidth constraint model (Maximum Allocation Model or Russian Doll Model) on the LSR.</td>
</tr>
<tr>
<td>ds-te te-classes, on page 186</td>
<td>Configures MPLS DS-TE TE-class maps.</td>
</tr>
<tr>
<td>mpls traffic-eng, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
<tr>
<td>mpls traffic-eng fast-reroute promote, on page 219</td>
<td>Configures the router to assign new or more efficient backup MPLS-TE tunnels to protected MPLS-TE tunnels.</td>
</tr>
<tr>
<td>show mpls traffic-eng ds-te te-class, on page 290</td>
<td>Displays the Diff-Serv TE-class map in use.</td>
</tr>
</tbody>
</table>
ds-te te-classes

To enter DS-TE te-class map configuration mode, use the `ds-te te-classes` command in MPLS-TE configuration mode. To return to the default behavior, use the `no` form of this command.

```
ds-te te-classes te-class te_class_index {class-type class_type_number {priority pri_number} | unused}
no ds-te te-classes te-class te_class_index {class-type class_type_number {priority pri_number} | unused}
```

**Syntax Description**

- **te-class** Configures the te-class map.
- **te_class_index** TE class-map index. Range is 0 to 7.
- **class-type** Configures the class type.
- **class_type_number** Class type value in the te-class map. Range is 0 to 1.
- **priority** Configures the TE tunnel priority.
- **pri_number** TE tunnel priority value. Range is 0 to 7.
- **unused** Marks the TE-class as unused.

**Command Default**

The following default te-class maps are used in IETF DS-TE mode:

<table>
<thead>
<tr>
<th>te-class index</th>
<th>class-type</th>
<th>priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>7</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>UNUSED</td>
<td>—</td>
</tr>
<tr>
<td>3</td>
<td>UNUSED</td>
<td>—</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>UNUSED</td>
<td>—</td>
</tr>
<tr>
<td>7</td>
<td>UNUSED</td>
<td>—</td>
</tr>
</tbody>
</table>

**Note**

The default mapping has 4 TE-classes used with 2 class-types and, 4 TE-classes are unused. TE-class map is not used in prestandard DS-TE mode.
MPLS-TE configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

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

In IETF DS-TE mode, modified semantic of the unreserved bandwidth TLV is used. Each of the eight available bandwidth values advertised in the IGP corresponds to a TE class. Because IGP advertises only eight bandwidth values, only eight TE-Classes can be supported in a IETF DS-TE network. The TE-Class mapping must be configured the same way on every router in a DS-TE domain. There is, however, no method to automatically detect or enforce this required consistency.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to configure a TE-class 7 parameter:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# ds-te te-classes te-class 7 class-type 0 priority 4
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ds-te bc-model, on page 182</td>
<td>Enables a specific bandwidth constraint model (Maximum Allocation Model or Russian Doll Model) on the LSR.</td>
</tr>
<tr>
<td>ds-te mode, on page 184</td>
<td>Configures standard DS-TE mode.</td>
</tr>
<tr>
<td>mpls traffic-eng, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
<tr>
<td>show mpls traffic-eng ds-te-class, on page 290</td>
<td>Displays the Diff-Serv TE-class map in use.</td>
</tr>
</tbody>
</table>
exclude srlg (auto-tunnel backup)

To specify that automatic backup tunnels should avoid Shared Risk Link Groups (SRLGs) of protected interface, use the `exclude srlg` command in auto-tunnel backup configuration mode. To disable this feature, use the `no` form of this command.

```
exclude srlg [preferred]
no exclude srlg [preferred]
```

**Syntax Description**

- **preferred** (Optional) Causes the backup tunnel to avoid SRLGs of its protected interface(s); however, the backup tunnel is created if SRLGs are not avoided.

**Command Default**

Strict SRLG

**Command Modes**

Auto-tunnel backup configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

Strict SRLG configuration of this command means that the path computed for the backup tunnel that is automatically created, must not contain any links that are part of the excluded SRLG groups. If such a path cannot be found, the backup tunnel does not come up.

Configuration of the preferred option allows the automatic backup tunnel to come up even if a path that excludes SRLGs can not be found.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

In the following example, automatic backup tunnels must avoid SRLGs of the protected interface.

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# interface pos 0/1/0/1
RP/0/RP0/CPU0:router(config-mpls-te-if)# auto-tunnel backup
RP/0/RP0/CPU0:router(config-mpls-te-if-auto-backup)# exclude srlg preferred
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-tunnel backup (MPLS-TE), on page 156</td>
<td>Builds automatic next-hop and next-next-hop tunnels, and enters auto-tunnel configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>
To enable fast-reroute (FRR) protection for an MPLS-TE tunnel, use the `fast-reroute` command in interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
fast-reroute
no fast-reroute
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

FRR is disabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When a protected link used by the fast-reroutable label switched path (LSP) fails, the traffic is rerouted to a previously assigned backup tunnel. Configuring FRR on the tunnel informs all the nodes that the LSP is traversing that this LSP desires link/node/bandwidth protection.

You must allow sufficient time after an switchover before triggering FRR on standby to synchronize with the active (verified using the `show redundancy` command). All TE tunnels must be in the recovered state and the database must be in the ready state for all ingress and egress line cards. To verify this information, use the `show mpls traffic-eng tunnels` and `show mpls traffic-eng fast-reroute database` commands.

**Note**

Wait approximately 60 seconds before triggering FRR after verifying the database state.

**Task ID**

- **mpls-te** read, write

**Examples**

The following example shows how to enable FRR on an MPLS-TE tunnel:

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fast-reroute protect, on page 192</td>
<td>Configures node and bandwidth protection for an MPLS-TE tunnel.</td>
</tr>
<tr>
<td>interface tunnel-te, on page 207</td>
<td>Configures an MPLS-TE tunnel interface.</td>
</tr>
<tr>
<td>show mpls traffic-eng forwarding, on page 292</td>
<td>Displays the contents of the FRR database.</td>
</tr>
<tr>
<td>show mpls traffic-eng tunnels, on page 335</td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
</tbody>
</table>
**fast-reroute protect**

To enable node and bandwidth protection for an MPLS-TE tunnel, use the `fast-reroute protect` command in interface configuration mode. To return to the default behavior, use the no form of this command.

```
fast-reroute protect {bandwidth | node}
no fast-reroute protect
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth</td>
<td>Enables bandwidth protection request.</td>
</tr>
<tr>
<td>node</td>
<td>Enables node protection request.</td>
</tr>
</tbody>
</table>

**Command Default**

FRR is disabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpl-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable bandwidth protection for a specified TE tunnel:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>fast-reroute</code>, on page 190</td>
<td>Enables FRR protection for an MPLS-TE tunnel.</td>
</tr>
<tr>
<td><code>interface tunnel-te</code>, on page 207</td>
<td>Configures an MPLS-TE tunnel interface.</td>
</tr>
<tr>
<td><code>show mpls traffic-eng tunnels</code>, on page 335</td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
</tbody>
</table>
fast-reroute timers promotion

To configure how often the router considers switching a protected MPLS-TE tunnel to a new backup tunnel if additional backup-bandwidth or a better backup tunnel becomes available, use the `fast-reroute timers promotion` command in MPLS-TE configuration mode. To return to the default behavior, use the `no` form of this command.

```
fast-reroute timers promotion interval
no fast-reroute timers promotion
```

**Syntax Description**

| interval | Interval, in seconds, between scans to determine if a label switched path (LSP) should use a new, better backup tunnel. Range is 0 to 604800. A value of 0 disables backup tunnel promotions. |

**Command Default**

```
interval: 300
```

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

Setting the interval to a low value puts more load on the CPU because it has to scan all protected LSPs more frequently. It is not recommended that the timer be configured below the default value of 300 seconds.

Pacing mechanisms have been implemented to distribute the load on the CPU when backup promotion is active. Because of this, when a large number of protected LSPs are promoted, some delay is noticeable in backup promotion. If the promotion timer is configured to a very low value (depending on the number of protected LSPs) some protected LSPs may never get promoted.

To disable the timer, set the value to zero.

**Task ID**

```
Task ID

mpls-te read, write
```

**Examples**

The following example shows how to specify that LSPs are scanned every 600 seconds (10 minutes) to determine if they should be promoted to a better backup tunnel:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# fast-reroute timers promotion 600
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls traffic-eng, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
<tr>
<td>mpls traffic-eng fast-reroute promote, on page 219</td>
<td>Configures the router to use a new or more efficient backup MPLS-TE tunnel when a current tunnel is overloaded.</td>
</tr>
</tbody>
</table>
flooding threshold

To set the reserved bandwidth thresholds for a link as a percentage of the total bandwidth change, use the `flooding threshold` command in MPLS-TE configuration mode. To return to the default behavior, use the `no` form of this command.

```
flooding threshold {up | down} percent
do floo ding thresholds {up | down} percent
```

**Syntax Description**

- **up**: Configures the upward flooding threshold as a percentage of the total link bandwidth change.
- **down**: Configures the downward flooding threshold as a percentage of the total link bandwidth change.
- **percent**: Bandwidth threshold level. Range is 0 to 100.

**Command Default**

No default behavior or values.

**Command Modes**

MPLS-TE configuration

**Command History**

```
Release      Modification
5.3.4        This command was introduced.
```

**Usage Guidelines**

Use the `flooding threshold` command to set the up and down thresholds as a percentage of the total bandwidth change. If the `flooding threshold` command is configured, flooding occurs only if the change from the previous flooding is greater than the configured thresholds.

**Examples**

The following example shows how to set the reserved bandwidth thresholds as a percentage of the total bandwidth change. Flooding occurs only if the change from the previous flooding is greater than the configured thresholds. In this example, the up and down thresholds are configured as 10 percent. That means, if the last flooded bandwidth percentage is 50 percent, then the flooding occurs only if the bandwidth goes below 40 percent, or if the bandwidth goes above 60 percent.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# flooding threshold up 10 down 10
```
flooding thresholds

To set the reserved bandwidth thresholds for a link, use the `flooding thresholds` command in MPLS-TE interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
flooding thresholds {down | up} percent [{percent1 percent2 percent3 ... percent 15}] 
no flooding thresholds {down | up}
```

**Syntax Description**
- **down** Configures the threshold for decreased resource availability.
- **up** Configures the threshold for increased resource availability.
- **percent** [ percent ] Bandwidth threshold level. Range is 0 to 100 for all 16 levels.

**Command Default**
- **down**: 100, 99, 98, 97, 96, 95, 90, 85, 80, 75, 60, 45, 30, 15
- **up**: 5, 30, 45, 60, 75, 80, 85, 90, 95, 97, 98, 99, 100

**Command Modes**
- MPLS-TE interface configuration

**Command History**
```
Release     Modification
5.0.0        This command was introduced.
```

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

You can configure up to 16 flooding threshold values. The first value is mandatory; the next 15 are optional.

When a threshold is crossed, MPLS-TE link management advertises updated link information. If no thresholds are crossed, changes can be flooded periodically unless periodic flooding was disabled.

**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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface (MPLS-TE), on page 205</td>
<td>Enables MPLS-TE on an interface and enters MPLS-TE interface configuration mode.</td>
</tr>
<tr>
<td>mpls traffic-eng, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
<tr>
<td>link-management timers periodic-flooding, on page 212</td>
<td>Sets the length of the interval used for periodic flooding.</td>
</tr>
<tr>
<td>show mpls traffic-eng link-management advertisements, on page 299</td>
<td>Displays local link information currently being flooded by MPLS-TE link management into the global TE topology.</td>
</tr>
<tr>
<td>show mpls traffic-eng link-management bandwidth-allocation, on page 302</td>
<td>Displays current local link information.</td>
</tr>
</tbody>
</table>
forwarding-adjacency

To configure an MPLS-TE forwarding adjacency, use the `forwarding-adjacency` command in interface configuration mode. By configuring forwarding adjacency, the MPLS-TE tunnels are considered to be links by the IGP. If no forwarding adjacency is to be defined, use the `no` form of this command.

```
forwarding-adjacency [holdtime time]
no forwarding-adjacency [holdtime time]
```

**Syntax Description**

`holdtime time` (Optional) Configures the hold time value, in milliseconds, that is associated with each forwarding-adjacency LSP. The hold time is the duration after which the state change of LSP is advertised to IGP. The default value is 0.

**Command Default**

`holdtime time: 0`

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

If you do not specify a `holdtime time` value, a delay is introduced with the following results:

- When forwarding-adjacency is configured on a tunnel that is up, TE notifies IGP without any additional delay.
- When forwarding-adjacency is configured on a tunnel that is down, TE does not notify IGP.
- When a tunnel on which forwarding-adjacency has been configured comes up, TE holds the notification to IGP for the period of holdtime (assuming non-zero holdtime). When the holdtime elapses, TE notifies IGP if the tunnel is still up.

The paths that traffic is taking to the destination can be manipulated by adjusting the forwarding adjacency link metric. To do that, use the `bandwidth` command. The unit of possible bandwidth values is in kbps.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to configure forwarding adjacency with a holdtime value of 60 milliseconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 888
```
Related Commands | Command | Description |
--- | --- | --- |
 | bandwidth (RSVP), on page 389 | Configures RSVP bandwidth on an interface using prestandard DS-TE mode. |
 | interface tunnel-te, on page 207 | Configures an MPLS-TE tunnel interface. |
 | show mpls traffic-eng forwarding-adjacency, on page 294 | Displays forwarding-adjacency information. |
index exclude-address

To exclude an address from a tunnel path entry at a specific index, use the `index exclude-address` command in explicit path configuration mode. To return to the default behavior, use the `no` form of this command.

```
index index-id exclude-address { ipv4 unicast IP address }
no index index-id
```

**Syntax Description**

| `index-id` | Index number at which the path entry is inserted or modified. Range is 1 to 65535. |
| `ipv4 unicast IP address` | Excludes the IPv4 unicast address. |

**Command Default**

No default behavior or values

**Command Modes**

Explicit path configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You cannot include or exclude addresses from an IP explicit path unless explicitly configured using the `exclude-address` keyword.

Use the `exclude-address` keyword only after entering the explicit path configuration mode.

If you use the `exclude-address` keyword and specify the IP address of a link, the constraint-based routine does not consider that link when it sets up MPLS-TE paths. If the excluded address is a flooded MPLS-TE router ID, the constraint-based shortest path first (SPF) routine does not consider that entire node.

**Note**

The person who performs the configuration must know the IDs of the routers, as it may not be apparent if the value refers to the link or to the node.

MPLS-TE accepts IP explicit paths composed of all excluded addresses configured using the `exclude-address` keyword.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to exclude address 192.168.3.2 at index 3 of the explicit path 200:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# explicit-path identifier 200
```
RP/RP0/CPU0:router(config-expl-path)# index 3 exclude-address ipv4 unicast 192.168.3.2

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>index next-address, on page 203</td>
<td>Specifies path entries at a specific index.</td>
</tr>
<tr>
<td></td>
<td>show explicit-paths, on page 269</td>
<td>Displays the configured IP explicit paths.</td>
</tr>
</tbody>
</table>
index exclude-srlg

To exclude an address to get SRLGs from a tunnel path entry at a specific index, use the index exclude-srlg command in explicit path configuration mode. To return to the default behavior, use the no form of this command.

index  index-id  exclude-srlg  ipv4  unicast  IP address

no  index  index-id

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>index-id</td>
<td>Index number at which the path entry is inserted or modified. Range is 1 to 65535.</td>
</tr>
<tr>
<td>exclude-srlg</td>
<td>Specifies an IP address to get SRLG values from for exclusion.</td>
</tr>
<tr>
<td>ipv4 unicast IP address</td>
<td>Excludes the IPv4 unicast address.</td>
</tr>
</tbody>
</table>

Command Default

No default behavior or values

Command Modes

Explicit path configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

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

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Example

The following example shows how to exclude the SRLG values from the IP address 192.168.3.2 at index 1 of the explicit path 100:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# explicit-path identifier 100
RP/0/RP0/CPU0:router(config-expl-path)# index 1 exclude-srlg ipv4 unicast 192.168.3.2
**index next-address**

To include a path entry at a specific index, use the `index next-address` command in explicit path configuration mode. To return to the default behavior, use the `no` form of this command.

```
index index-id next-address [{loose | strict}] ipv4 unicast IP-address
no index index-id
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>index-id</code></td>
<td>Index number at which the path entry is inserted or modified. Range is 1 to 65535.</td>
</tr>
<tr>
<td><code>ipv4 unicast IP-address</code></td>
<td>Includes the IPv4 unicast address (strict address).</td>
</tr>
<tr>
<td><code>loose ipv4 unicast IP-address</code></td>
<td>(Optional) Specifies the next unicast address in the path as a loose hop.</td>
</tr>
<tr>
<td><code>strict ipv4 unicast IP-address</code></td>
<td>(Optional) Specifies the next unicast address in the path as a strict hop.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

Explicit path configuration

**Command History**

```
Release 5.0.0
```

This command was introduced.

**Usage Guidelines**

You cannot include addresses from an IP explicit path unless explicitly configured using the `next-address` keyword.

Use the `next-address` keyword only after entering the explicit path configuration mode.

**Note**

The person who performs the configuration must know the IDs of the routers, as it may not be apparent if the value refers to the link or to the node.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to insert the `next-address` 192.168.3.2 at index 3 of the explicit path 200:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# explicit-path identifier 200
```
RP/0/RP0/CPU0:router(config-expl-path)# **index 3 next-address ipv4 unicast 192.168.3.2**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>index exclude-address, on page 200</td>
<td>Specifies the next IP address to exclude from the explicit path.</td>
</tr>
<tr>
<td>show explicit-paths, on page 269</td>
<td>Displays the configured IP explicit paths.</td>
</tr>
</tbody>
</table>
interface (MPLS-TE)

To enable MPLS-TE on an interface and to enter MPLS-TE interface configuration mode, use the `interface` command in global configuration mode. To return to the default behavior, use the `no` form of this command.

```
interface type interface-path-id
no interface type interface-path-id
```

**Syntax Description**

- **type**: Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id**: Physical interface or virtual interface.

**Note**

Use the `show interfaces` command to see a list of all possible interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No default behavior or values

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must enter MPLS-TE interface mode to configure specific interface parameters on physical interfaces. Configuring MPLS-TE links or a tunnel TE interface begins the TE-control process on.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**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 0/0/1
```

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 0/0/1
```
interface (SRLG)

To enable Shared Risk Link Groups (SRLGs) on an interface and to enter SRLG interface configuration mode, use the `interface` command in SRLG configuration mode. To return to the previous configuration mode, use the `no` form of this command.

```
interface type interface-path-id
no interface type interface-path-id
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note**

Use the `show interfaces` command to see a list of all possible interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

---

**Command Default**

No default behavior or values

**Command Modes**

SRLG configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

The following example shows how to enter SRLG interface configuration mode:

```
RP/0/RP0/CPU0:router(config)# srlg
RP/0/RP0/CPU0:router(config-srlg)# interface POS 0/1/0/1
RP/0/RP0/CPU0:router(config-srlg-if)# value 10
RP/0/RP0/CPU0:router(config-srlg-if)# value 50
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface (MPLS-TE), on page 205</td>
<td>Enables MPLS-TE on an interface and enters MPLS-TE interface configuration mode.</td>
</tr>
<tr>
<td>mpls traffic-eng, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
</tbody>
</table>
interface tunnel-te

To configure an MPLS-TE tunnel interface, use the `interface tunnel-te` command in XR Config mode. To return to the default behavior, use the `no` form of this command.

```
interface tunnel-te  tunnel-id
no  interface tunnel-te  tunnel-id
```

**Syntax Description**
- `tunnel-id` Tunnel number. Range is 0 to 65535.

**Command Default**
Tunnel interfaces are disabled.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
You cannot have two tunnels using the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and to use the loopback interface address as the source address of the tunnel.

Configuring MPLS-TE links or Tunnel-TE interface begins the TE-control process on .

The `interface tunnel-te` command indicates that the tunnel interface is for an MPLS-TE tunnel and enables the various tunnel MPLS configuration options.

**Note**
You must configure record-route on TE tunnels that are protected by multiple backup tunnels merging at a single node.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface  read,</td>
</tr>
<tr>
<td>write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to configure tunnel interface 1:

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

The following example shows how to set the tunnel-class attribute to map the correct traffic class to the tunnel:

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>affinity, on page 134</td>
<td>Configures affinity (the properties that the tunnel requires in its links) for an MPLS-TE tunnel.</td>
</tr>
<tr>
<td>autoroute metric, on page 154</td>
<td>Instructs the IGP to use the tunnel in its enhanced SPF calculation, if the tunnel is in an up state.</td>
</tr>
<tr>
<td>backup-bw, on page 158</td>
<td>Configures backup bandwidth for FRR.</td>
</tr>
<tr>
<td>fast-reroute, on page 190</td>
<td>Enables FRR protection for an MPLS-TE tunnel.</td>
</tr>
<tr>
<td>path-option (MPLS-TE), on page 234</td>
<td>Configures a path option for an MPLS tunnel.</td>
</tr>
<tr>
<td>path-selection metric (interface), on page 247</td>
<td>Configures a path selection metric—TE or IGP.</td>
</tr>
<tr>
<td>policy-class</td>
<td>Configures PBTS to direct traffic into specific TE tunnels.</td>
</tr>
<tr>
<td>priority (MPLS-TE), on page 262</td>
<td>Configures setup and reservation priority for an MPLS-TE tunnel.</td>
</tr>
<tr>
<td>record-route, on page 264</td>
<td>Configures record-route on an MPLS-TE tunnel.</td>
</tr>
</tbody>
</table>
ipv4 unnumbered (MPLS)

To specify the MPLS-TE tunnel Internet Protocol Version 4 (IPv4) address, use the `ipv4 unnumbered` command in interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
ipv4 unnumbered type interface-path-id
no ipv4 unnumbered type interface-path-id
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>type</code></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note**

Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No IP address is set.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

Tunnel-te is not signaled until an IP address is configured on the tunnel interface; therefore, the tunnel state stays down without IP address configuration.

Loopback is commonly used as the interface type.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>network</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the MPLS-TE tunnel to use the IPv4 address used on loopback interface 0:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# ipv4 unnumbered loopback0
```
link-management timers bandwidth-hold

To set the length of time that bandwidth is held for a Resource Reservation Protocol (RSVP) Path (setup) message to wait for the corresponding RSVP Resv message to return, use the link-management timers bandwidth-hold command in MPLS-TE configuration mode. To return to the default behavior, use the no form of this command.

```
link-management timers bandwidth-hold  holdtime
no link-management timers bandwidth-hold  holdtime
```

**Syntax Description**

| holdtime | Number of seconds that bandwidth can be held. Range is 1 to 300. Default is 15. |

**Command Default**

```
holdtime: 15
```

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

The link-management timers bandwidth-hold command determines the time allowed for an RSVP message to return from a neighbor RSVP node.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>link-management timers periodic-flooding, on page 212</td>
<td>Sets the length of the interval used for periodic flooding.</td>
</tr>
<tr>
<td>mpls traffic-eng, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>show mpls traffic-eng link-management</code></td>
<td>Displays current local link information and bandwidth hold time.</td>
</tr>
<tr>
<td><code>bandwidth-allocation</code>, on page 302</td>
<td></td>
</tr>
</tbody>
</table>
**link-management timers periodic-flooding**

To set the length of the interval for periodic flooding, use the `link-management timers periodic-flooding` command in MPLS-TE configuration mode. To return to the default behavior, use the `no` form of this command.

```plaintext
link-management timers periodic-flooding interval
no link-management timers periodic-flooding
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interval</code></td>
<td>Length of the interval, in seconds, for periodic flooding. Range is 0 to 3600. A value of 0 turns off periodic flooding. The minimum value is 30.</td>
</tr>
</tbody>
</table>

**Command Default**

`interval`: 180

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

The `link-management timers periodic-flooding` command advertises the link state information changes that do not trigger immediate action, such as a change to the allocated bandwidth that does not cross a threshold.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flooding thresholds, on page 196</td>
<td>Sets the reserved bandwidth flooding thresholds for a link.</td>
</tr>
<tr>
<td>link-management timers bandwidth-hold, on page 210</td>
<td>Sets the length of time that bandwidth is held for a RSVP Path (setup) message to wait for the corresponding RSVP Resv message to return.</td>
</tr>
</tbody>
</table>
### MPLS Traffic Engineering Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls traffic-eng, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
<tr>
<td>show mpls traffic-eng link-management summary, on page 314</td>
<td>Displays the current periodic flooding interval.</td>
</tr>
</tbody>
</table>
link-management timers preemption-delay

To set the length of the interval for delaying LSP preemption, use the `link-management timers preemption-delay` command in MPLS-TE configuration mode. To disable this behavior, use the `no` form of this command.

`link-management timers preemption-delay bundle-capacity sec`

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bundle-capacity sec</code></td>
<td>Specifies the bundle-capacity preemption timer value in seconds.</td>
</tr>
</tbody>
</table>

| Command Default | None |

| Command Modes | MPLS-TE configuration |

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
<td></td>
</tr>
</tbody>
</table>

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

The value 0 as bundle-capacity value in the `link-management timers preemption-delay` command disables this timer. This means there is no delay before preemption sets in when the bundle capacity goes down. |

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
<td></td>
</tr>
</tbody>
</table>

This example shows how to set the interval length for preemption-delay:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# link-management timers preemption-delay bundle-capacity 180
```
maxabs (MPLS-TE)

To specify the maximum number of MPLS-TE tunnels that can be configured, use the `maxabs` command in MPLS-TE configuration mode. To return to the default behavior, use the `no` form of this command.

```
maxabs tunnels tunnel-limit destinations dest-limit
no maxabs tunnels tunnel-limit destinations dest-limit
```

**Syntax Description**
- `tunnels` Configures all tunnels for MPLS-TE.
- `tunnel-limit` Maximum number of tunnel TE interfaces. Range is 1 to 65536.
- `destinations` Configures all destinations for MPLS-TE.
- `dest-limit` Maximum total number of destinations that can be configured. Range is 1 to 65536.

**Command Default**
- `tunnel-limit`: 4096
- `dest-limit`: 4096

**Command Modes**
- MPLS-TE configuration

**Command History**
- **Release 5.0.0** This command was introduced.

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

**Task ID**
- `mpls-te` read, write

**Examples**
The following example shows how to set the tunnel-te configuration limit to 1000:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# maxabs tunnels 1000 destinations 1000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls traffic-eng maximum tunnels, on page 316</td>
<td>Displays the configuration of the maximum tunnel-te interfaces allowed.</td>
</tr>
</tbody>
</table>
**mpls traffic-eng**

To enter MPLS-TE configuration mode, use the `mpls traffic-eng` command in global configuration mode.

### Syntax Description

This command has no arguments or keywords.

### Command Default

No default behavior or values

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to enter MPLS-TE configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)#
```
mpls traffic-eng auto-bw apply (MPLS-TE)

To apply the highest bandwidth collected on a tunnel without waiting for the current application period to end, use the `mpls traffic-eng auto-bw apply` command in EXEC mode.

```
mpls traffic-eng auto-bw apply {all | tunnel-te tunnel-number}
```

**Syntax Description**
- `all`: Applies the highest bandwidth collected instantly on all the automatic bandwidth-enabled tunnels.
- `tunnel-te tunnel-number`: Applies the highest bandwidth instantly to the specified tunnel. The range is from 0 to 65535.

**Command Default**
No default behavior or values

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

The `mpls traffic-eng auto-bw apply` command can forcefully expire the current application period on a specified tunnel and immediately apply the highest bandwidth recorded so far instead of waiting for the application period to end on its own.

**Note**

The predefined threshold check still applies on the configuration, and if the delta is not significant enough, the automatic bandwidth functionality overrides this command.

The bandwidth application is performed only if at least one output rate sample has been collected for the current application period.

To guarantee the application of a specific signaled bandwidth value when triggering a manual bandwidth application, follow these steps:

1. Configure the minimum and maximum automatic bandwidth to the bandwidth value that you want to apply by using the `bw-limit (MPLS-TE), on page 162` command.
2. Trigger a manual bandwidth application by using the `mpls traffic-eng auto-bw apply` command.
3. Revert the minimum and maximum automatic bandwidth value back to their original value.
The following example applies the highest bandwidth to a specified tunnel:

```
RP/0/RP0/CPU0:router# mpls traffic-eng auto-bw apply tunnel-te 1
```
mpls traffic-eng fast-reroute promote

To configure the router to assign new or more efficient backup MPLS-TE tunnels to protected MPLS-TE tunnels, use the `mpls traffic-eng fast-reroute promote` command in EXEC mode. To return to the default behavior, use the `no` form of this command.

```
mpls traffic-eng fast-reroute promote
no  mpls traffic-eng fast-reroute promote
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

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

**Usage Guidelines**

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

**Task ID**

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

**Examples**

The following example shows how to initiate backup tunnel promote and assignment:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fast-reroute, on page 190</td>
<td>Enables FRR protection for an MPLS-TE tunnel.</td>
</tr>
</tbody>
</table>
**mpls traffic-eng level**

To configure a router running Intermediate System-to-System (IS-IS) MPLS-TE at IS-IS Level 1 and Level 2, use the `mpls traffic-eng level` command in router configuration mode. To return to the default behavior, use the `no` form of this command.

```
mpls traffic-eng level  isis-level
no  mpls traffic-eng level  isis-level
```

**Syntax Description**

<table>
<thead>
<tr>
<th>isis-level</th>
<th>IS-IS level (1, 2, or both) where MPLS-TE is enabled.</th>
</tr>
</thead>
</table>

**Command Default**

No default behavior or values

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

The `mpls traffic-eng level` command is supported for IS-IS and affects the operation of MPLS-TE only if MPLS-TE is enabled for that routing protocol instance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>isis</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router isis 1
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-af)# mpls traffic-eng level 1
RP/0/RP0/CPU0:router(config-isis-af)# metric-style wide
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls traffic-eng router-id (MPLS-TE router), on page 226</td>
<td>Specifies that the TE router identifier for the node is the IP address associated with a given interface.</td>
</tr>
</tbody>
</table>
mpls traffic-eng link-management flood

To enable immediate flooding of all the local MPLS-TE links, use the `mpls traffic-eng link-management flood` command in EXEC mode. To return to the default behavior, use the `no` form of this command.

```
no mpls traffic-eng link-management flood
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Note**

If there is no change in the LSA since last flooding, IGP may dampen the advertisement.

**Task ID**

```
Task ID: mpls-te
Operations: read, write
```

**Examples**

The following example shows how to initiate flooding of the local MPLS-TE links:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mpls traffic-eng link-management advertisements</code>, on page 299</td>
<td>Displays MPLS-TE link-management advertisements.</td>
</tr>
</tbody>
</table>
**mpls traffic-eng pce activate-pcep**

To force idle peers to be reestablished without waiting for a timer, use the `mpls traffic-eng pce activate-pcep` command in EXEC mode. To return to the default behavior, use the `no` form of this command.

```plaintext
mpls traffic-eng pce activate-pcep {address | all}
no mpls traffic-eng pce activate-pcep {address | all}
```

**Syntax Description**
- `address` Address of the idle peer.
- `all` Activates all the idle peers.

**Command Default**
No default behavior or values

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

**Task ID**
- `mpls-te` read, write, execute

**Examples**
The following example shows how to trigger a path computation client (PCC) or PCE to activate an idle path computation element protocol (PCEP) session:

```plaintext
RP/0/RP0/CPU0:router# mpls traffic-eng pce activate-pcep all
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mpls traffic-eng pce reoptimize, on page 223</code></td>
<td>Triggers reoptimization manually either for all tunnels or a specific PCE-based tunnel.</td>
</tr>
</tbody>
</table>
mpls traffic-eng pce reoptimize

To trigger reoptimization manually either for all or a specific PCE-based tunnel, use the `mpls traffic-eng pce reoptimize` command in EXEC mode. To disable this feature, use the `no` form of this command.

```
mpls traffic-eng pce reoptimize [tunnel ID] [force]
no mpls traffic-eng pce reoptimize [tunnel ID] [force]
```

**Syntax Description**

- `tunnel ID` (Optional) Tunnel ID to be reoptimized. Range is from 0 to 65535.
- `force` (Optional) Forces the router to start using the newly calculated route even if the used path has a better metric.

**Command Default**

Reoptimizes all the PCE tunnels.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

If you do not run the `mpls traffic-eng pce reoptimize` command, the system tries to reoptimize at an interval of 3600 seconds.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write, execute</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to trigger reoptimization for all PCE-based tunnels:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls traffic-eng pce activate-pcep, on page 222</td>
<td>Forces idle peers to be re-established without waiting for a timer.</td>
</tr>
</tbody>
</table>
**mpls traffic-eng reoptimize (EXEC)**

To trigger the reoptimization interval of all TE tunnels, use the `mpls traffic-eng reoptimize` command in EXEC mode.

```
mpls traffic-eng reoptimize [tunnel-id] [tunnel-name] [p2p|all tunnel-id]
```

**Syntax Description**

- **tunnel-id** (Optional) MPLS-TE tunnel identification expressed as a number. Range is from 0 to 65535.
- **tunnel-name** (Optional) TE tunnel identification expressed as a name.
- **p2p** (Optional) Forces an immediate reoptimization of all P2P TE tunnels.
- **all** (Optional) Forces an immediate reoptimization for all P2P tunnels.
- **tunnel-id** P2P TE tunnel identification to be reoptimized. Range is from 0 to 65535.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

- **Task ID**
- **Operations**
- **mpls-te** execute

**Examples**

The following example shows how to immediately reoptimize all TE tunnels:

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

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

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

The following example shows how to immediately reoptimize all P2P TE tunnels:

```
RP/0/RP0/CPU0:router# mpls traffic-eng reoptimize p2p all
```
# mpls traffic-eng resetup (EXEC)

To trigger the re-setup of TE tunnels, clearing the LSP states, use the `mpls traffic-eng resetup` command in XR EXEC mode.

```bash
doesn't work
```

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>mpls traffic-eng resetup</strong></td>
<td>**{P2MP</td>
</tr>
<tr>
<td><strong>name</strong></td>
<td>Re-setup a specific tunnel by the given name.</td>
</tr>
</tbody>
</table>

## Command Default

No default behavior or values

## Command Modes

XR EXEC mode

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Task ID

```bash
doesn't work
```

### Examples

The following example shows how to re-setup a specific tunnel by the given name (tunnel-te1):

```bash
RP/0/RP0/CPU0:router# mpls traffic-eng resetup name tunnel-te1
```

The following example shows how to re-setup a specific P2P tunnel based on the specified tunnel-id (tunnel-id 1):

```bash
RP/0/RP0/CPU0:router# mpls traffic-eng resetup P2P tunnel-id 1
```

The following example shows how to re-setup a P2MP tunnel based on the specified tunnel-id (tunnel-id 2):

```bash
RP/0/RP0/CPU0:router# mpls traffic-eng resetup P2MP tunnel-id 2
```
mpls traffic-eng router-id (MPLS-TE router)

To specify that the TE router identifier for the node is the IP address associated with a given interface, use the `mpls traffic-eng router-id` command in the appropriate mode. To return to the default behavior, use the `no` form of this command.

```
mpls traffic-eng router-id  type interface-path-id
no  mpls traffic-eng router-id  type interface-path-id
```

**Syntax Description**

- `type` Interface type. For more information, use the question mark (?) online help function.
- `interface-path-id` Physical interface or virtual interface.

**Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No default behavior or values

**Command Modes**

- OSPF configuration
- IS-IS address family configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

A routers identifier acts as a stable IP address for the TE configuration. This IP address is flooded to all nodes. You must set the destination on the destination node TE router identifier for all affected tunnels. This router ID is the address that the TE topology database at the tunnel head uses for its path calculation.

**Note**

When the `mpls traffic-eng router-id` command is not configured, global router ID is used by MPLS-TE if there is one configured.
Examples

The following examples show how to specify the TE router identifier as the IP address associated with loopback interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router ospf CORE_AS
RP/0/RP0/CPU0:router(config-ospf)# mpls traffic-eng router-id 7.7.7.7
```

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# router isis 811
RP/0/RP0/CPU0:router(config-isis)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-af)# mpls traffic-eng router-id 8.8.8.8
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls traffic-eng level, on page 220</td>
<td>Configures a router running OSPF MPLS so that it floods TE for the indicated IS-IS level.</td>
</tr>
</tbody>
</table>
mpls traffic-eng reoptimize mesh group

To reoptimize all tunnels of a mesh group, use the **mpls traffic-eng reoptimize mesh group** command in EXEC mode.

```
mpls traffic-eng reoptimize auto-tunnel mesh group group_id
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group_id</td>
<td>Defines auto-tunnel mesh group ID that is to be reoptimized. Range is 0 to 4294967295.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>MPLS Transport profile configuration</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Release</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>4.1.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Release</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>5.0.0</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>mpls-te execute</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Examples</th>
<th>This is sample out from the <strong>mpls traffic-eng reoptimize mesh group</strong> command:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RP/0/RP0/CPU0:router mpls traffic-eng reoptimize mesh group 10</td>
</tr>
</tbody>
</table>
named-tunnels tunnel-te

To name the TE (Traffic Engineering) tunnels in the network with unique tunnel IDs (STRING names), use the `named-tunnels tunnel-te` command in MPLS-TE configuration mode. To delete the named tunnels, use the `no` form of this command.

```
named-tunnels tunnel-te  tunnel-name
no  named-tunnels
```

**Syntax Description**

- `tunnel-name`  
  Configures the given name to the TE tunnel.
  
  **Note**  
  If the tunnel name contains more than one word, use hyphens to separate the words.

**Command Default**

None

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

The following example shows how to name a TE tunnel:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# named-tunnels
RP/0/RP0/CPU0:router(config-mpls-te-named-tunnels)# tunnel-te FROM-NY-TO-LA
```
nhop-only (auto-tunnel backup)

To configure only a next-hop automatic backup tunnel with only link protection, use the nhop-only command in MPLS-TE auto-tunnel backup interface configuration mode. To return to the default configuration setting for automatic backup tunnels, use the no form of this command.

```
  nhop-only
  no nhop-only
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Both NHOP and NNHOP protection are enabled.

**Command Modes**

Auto-tunnel backup configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

If you configure the nhop-only command, you destroy any next-next-hop (NNHOP) tunnel created to provide node protection for tunnels running over the specified interface.

If you unconfigure the nhop-only command, you trigger a backup assignment on primary tunnels running over that link. The automatic backup tunnel feature attempts to create NNHOP backup tunnels to provide node protection for the specified tunnels.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

In the following example, NNHOP automatic backup tunnels are destroyed and only NHOP tunnels with link protection is configured:

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# interface pos 0/1/0/1
RP/0/RP0/CPU0:router(config-mpls-te-if)# auto-tunnel backup
RP/0/RP0/CPU0:router(config-mpls-te-if-auto-backup)# nhop-only
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-tunnel backup (MPLS-TE), on page 156</td>
<td>Builds automatic NHOP and NNHOP backup tunnels.</td>
</tr>
</tbody>
</table>
overflow threshold (MPLS-TE)

To configure the tunnel overflow detection, use the **overflow threshold** command in MPLS-TE automatic bandwidth interface configuration mode. To disable the overflow detection feature, use the **no** form of this command.

```
overflow threshold  percentage  [min  bandwidth]  limit  limit
no  overflow threshold
```

**Syntax Description**
- **percentage**: Bandwidth change percent to trigger an overflow. The range is from 1 to 100.
- **min bandwidth**: (Optional) Configures the bandwidth change value, in kbps, to trigger an overflow. The range is from 10 to 4294967295. The default is 10.
- **limit limit**: Configures the number of consecutive collection intervals that exceeds the threshold. The bandwidth overflow triggers an early tunnel bandwidth update. The range is from 1 to 10. The default is none.

**Command Default**
The default value is disabled.

**Command Modes**
MPLS-TE automatic bandwidth interface configuration

**Command History**

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

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

If you modify the **limit** keyword, the consecutive overflows counter for the tunnel is also reset.

If you enable or modify the minimum value, the current consecutive overflows counter for the tunnel is also reset, which effectively restarts the overflow detection from scratch.

Several number of consecutive bandwidth samples are greater than the overflow threshold (bandwidth percentage) and the minimum bandwidth configured, then a bandwidth application is updated immediately instead of waiting for the end of the application period.

Overflow detection applies only to bandwidth increase. For example, an overflow can not be triggered even if bandwidth decreases by more than the configured overflow threshold.

**Task ID**

```
Task ID  Operations
mpls-te  read,
          write
```
The following example shows how to configure the tunnel overflow detection for tunnel-te 1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# auto-bw
RP/0/RP0/CPU0:router(config-if-tunte-autobw)# overflow threshold 50 limit 3
```
**path-option (MPLS-TE)**

To configure a path option for an MPLS-TE tunnel, use the `path-option` command in tunnel-te interface configuration mode. To return to the default behavior, use the `no` form of this command.

```plaintext
path-option preference-priority {dynamic [pce [address ipv4 address]]| explicit {name path-name | identifier path-number}} [attribute-set name] [isis instance-name level level] [lockdown] [ospf instance-name area {value address}] [verbatim]
no path-option preference-priority {dynamic [pce [address ipv4 address]]| explicit {name path-name [identifier path-number]}} [isis instance-name level level] [lockdown] [ospf instance-name area {value address}] [verbatim]
```

### Syntax Description

- **preference-priority**: Path option number. Range is from 1 to 1000.
- **dynamic**: Specifies that label switched paths (LSP) are dynamically calculated.
- **pce**: (Optional) Specifies that the LSP is computed by a Path Computation Element (PCE).
- **address**: (Optional) Configures the address for the PCE.
- **ipv4 address**: Configures the IPv4 address for the PCE.
- **explicit**: Specifies that LSP paths are IP explicit paths.
- **name path-name**: Specifies the path name of the IP explicit path.
- **identifier path-number**: Specifies a path number of the IP explicit path.
- **isis instance-name**: (Optional) Limits CSPF to a single IS-IS instance and area.
- **attribute-set name**: (Optional) Specifies the attribute set for the LSP.
- **level level**: Configures the level for IS-IS. The range is from 1 to 2.
- **lockdown**: (Optional) Specifies that the LSP cannot be reoptimized.
- **ospf instance-name**: (Optional) Limits CSPF to a single OSPF instance and area.
- **area**: Configures the area for OSPF.
- **value**: Decimal value for the OSPF area ID.
- **address**: IP address for the OSPF area ID.
- **verbatim**: (Optional) Bypasses the Topology/CSPF check for explicit paths.

### Command Default

No default behavior or values

### Command Modes

Tunnel-te interface configuration
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

You can configure several path options for a single tunnel. For example, there can be several explicit path options and a dynamic option for one tunnel. The path setup preference is for lower (not higher) numbers, so option 1 is preferred.

When the lower number path option fails, the next path option is used to set up a tunnel automatically (unless using the lockdown option).

You specify the backup path for the path-option command in case of the primary path failure.

CSPF areas are configured on a per-path-option basis.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following examples show how to configure the tunnel to use a named IPv4 explicit path as verbatim and lockdown options for the tunnel. This tunnel cannot reoptimize when the FRR event goes away, unless you manually reoptimize it:

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

The following example shows how to enable path protection on a tunnel to configure an explicit path:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# path-option 1 explicit name po4
RP/0/RP0/CPU0:router(config-if)# path-option protecting 1 explicit name po6
```

The following example shows how to limit CSPF to a single OSPF instance and area:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# path-option 1 explicit name router1 ospf 3 area 7 verbatim
```

The following example shows how to limit CSPF to a single IS-IS instance and area:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# path-option 1 dynamic isis mtbf level 1 lockdown
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show explicit-paths, on page 269</td>
<td>Displays the configured IP explicit paths.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>show mpls traffic-eng tunnels, on page 335</code></td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
</tbody>
</table>
path-selection ignore overload (MPLS-TE)

To ignore the Intermediate System-to-Intermediate System (IS-IS) overload bit setting for MPLS-TE, use the `path-selection ignore overload` command in MPLS-TE configuration mode. To return to the default behavior, use the `no` form of this command.

```
path-selection ignore overload  {head | mid | tail}
no  path-selection ignore overload  {head | mid | tail}
```

**Syntax Description**

- **head**
  - The tunnel stays up if `set-overload-bit` is set by ISIS on the head router. Ignores overload node during CSPF for the head node.

- **mid**
  - The tunnel stays up if `set-overload-bit` is set by ISIS on the mid router. Ignores overload node during CSPF for the mid node.

- **tail**
  - The tunnel stays up if `set-overload-bit` is set by ISIS on the tail router. Ignores overload node during CSPF for the tail node.

**Command Default**

None

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

Use the `path-selection ignore overload` command to ensure that label switched paths (LSPs) are not broken because of routers that have IS-IS overload bit as enabled.

When the IS-IS overload bit avoidance (OLA) feature is activated, all nodes with the overload bit set, which includes head nodes, mid nodes, and tail nodes, are ignored. This means that they are still available for use with label switched paths (LSPs). This feature allows you to include an overloaded node in constraint-based shortest path first (CSPF).

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to use the `path-selection ignore overload head` command:

```
RP/0/RP0/CP00:router# configure
RP/0/RP0/CP00:router(config)# mpls traffic-eng
```
path-selection ignore overload (MPLS-TE)

RP/0/RP0/CPU0:router(config-mpls-te)# path-selection ignore overload
RP/0/RP0/CPU0:router(config-mpls-te)# path-selection ignore overload head
path-selection invalidation

To configure the path invalidation timer such that when the timer expires, the path is either removed or the data is dropped, use the `path-selection invalidation` command in MPLS-TE configuration mode. To remove the path invalidation timer, use the `no` form of this command.

```
path-selection invalidation path-invalidation-timer-value{drop | tear}
```

**Syntax Description**

- `path-invalidation-timer-value`: Configures the path invalidation timer value in milliseconds. The range is from 0 to 60000.
- `drop`: The data is dropped after the path invalidation timer expires.
- `tear`: The path is torn down after the path invalidation timer expires.

**Command Default**

None

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to set the `path-selection invalidation` timer in MPLS TE configuration mode.

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)#path-selection invalidation 1 drop
```
path-selection loose-expansion affinity (MPLS-TE)

To specify the affinity value to be used to expand a path to the next loose hop for a tunnel on an area border router, use the path-selection loose-expansion affinity command in MPLS-TE configuration mode. To return to the default behavior, use the no form of this command.

```
path-selection loose-expansion affinity affinity-value mask affinity-mask [class-type type]
no path-selection loose-expansion affinity affinity-value mask affinity-mask [class-type type]
```

**Syntax Description**

- **affinity-value**: Attribute values required for links carrying this tunnel. A 32-bit decimal number. Range is 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.

- **mask affinity-mask**: Checks the link attribute, a 32-bit decimal number. Range is 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute mask is 0 or 1.

- **class-type type**: (Optional) Requests the class-type of the tunnel bandwidth. Range is 0 to 1.

**Command Default**

- **affinity-value**: 0X00000000
- **mask-value**: 0XFFFFFFFF

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Note**

The new affinity scheme (based on names) is not supported for loose-hop expansion. New configuration does not affect the already up tunnels.

**Task ID**

- **Task ID**
  - mpls-te read, write

**Examples**

The following example shows how to configure affinity 0x55 with mask 0xFFFFFFFF:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>path-selection loose-expansion metric (MPLS-TE), on page 243</td>
<td>Configures a metric type to be used to expand a path to the next loose hop for a tunnel on an area border router.</td>
</tr>
<tr>
<td>path-selection metric (MPLS-TE), on page 245</td>
<td>Configures the MPLS-TE tunnel path-selection metric.</td>
</tr>
</tbody>
</table>
**path-selection loose-expansion domain-match**

To match the domain of the subsequent auto-discovered ABR (Area Border Router) with the domain of the incoming interface where the Path message is received, use the `path-selection loose-expansion domain-match` command in MPLS-TE configuration mode. To return to the default behavior, use the `no` form of this command.

```
path-selection loose-expansion domain-match
no path-selection loose-expansion domain-match
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

None

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.5</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

The following example shows how to configure domain-match:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# path-selection loose-expansion domain-match
```
path-selection loose-expansion metric (MPLS-TE)

To configure a metric type to be used to expand a path to the next loose hop for a tunnel on an area border router, use the path-selection loose-expansion metric command in MPLS-TE configuration mode. To return to the default behavior, use the no form of this command.

```
path-selection loose-expansion metric {igp | te} [class-type type]
no path-selection loose-expansion metric {igp | te} [class-type type]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igp</td>
<td>Configures an Interior Gateway Protocol (IGP) metric.</td>
</tr>
<tr>
<td>te</td>
<td>Configures a TE metric. This is the default.</td>
</tr>
<tr>
<td>class-type type</td>
<td>(Optional) Requests the class type of the tunnel bandwidth. Range is 0 to 1.</td>
</tr>
</tbody>
</table>

### Command Default

The default is TE metric.

### Command Modes

MPLS-TE configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

**Note**

New configurations do not affect tunnels that are already up.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# path-selection loose-expansion metric igp
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>path-selection loose-expansion affinity (MPLS-TE), on page 240</td>
<td>Specifies the affinity value to be used to expand a path to the next loose hop for a tunnel on an area border router.</td>
</tr>
</tbody>
</table>
path-selection metric (MPLS-TE)

To specify the MPLS-TE tunnel path-selection metric, use the `path-selection metric` command in MPLS-TE configuration mode. To return to the default behavior, use the `no` form of this command.

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

**Syntax Description**
- `igp` Configures an Interior Gateway Protocol (IGP) metric.
- `te` Configures a TE metric.

**Command Default**
The default is TE metric.

**Command Modes**
MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

The metric type to be used for path calculation for a given tunnel is determined as follows:

- If the `path-selection metric` command was entered to specify a metric type for the tunnel, use that metric type.
- Otherwise, use the default (TE) metric.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>path-selection loose-expansion affinity (MPLS-TE), on page 240</td>
<td>Specifies the affinity value to be used to expand a path to the next loose hop for a tunnel on an area border router.</td>
</tr>
</tbody>
</table>
path-selection metric (interface)

To configure an MPLS-TE tunnel path-selection metric type, use the `path-selection metric` command in interface configuration mode. To return to the default behavior, use the `no` form of this command.

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

**Syntax Description**
- `igp` Configures Interior Gateway Protocol (IGP) metrics.
- `te` Configures TE metrics. This is the default.

**Command Default**
The default is TE metrics.

**Command Modes**
Interface configuration

**Command History**
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.0.0</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The metric type to be used for path calculation for a given tunnel is determined as follows:

- If the `path-selection metric` command was entered to either a metric type for the tunnel or only a metric type, use that metric type.
- Otherwise, use the default (TE) metric.

**Task ID**
- `mpls-te` read, write

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# path-selection metric igp
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls traffic-eng topology</td>
<td>Displays the tunnel path used.</td>
</tr>
</tbody>
</table>
pce address (MPLS-TE)

To configure the IPv4 self address for Path Computation Element (PCE), use the `pce address` command in MPLS-TE configuration mode. To return to the default behavior, use the `no` form of this command.

```
pce address ipv4 address
no pce address ipv4 address
```

**Syntax Description**

- `ipv4 address` Configures the IPv4 address for PCE.

**Command Default**

No default behavior or values

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

The IP address is used in the TCP communication with the other PCEs or PCCs. In addition, this address is advertised using IGP.

**Task ID**

- Task ID: `mpls-te`
  - Operations: `read, write`

**Examples**

The following example shows how to configure the IPv4 self address for PCE:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# pce address ipv4 10.10.10.10
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pce keepalive (MPLS-TE), on page 252</td>
<td>Configures a PCEP keepalive interval.</td>
</tr>
<tr>
<td>path-option (MPLS-TE), on page 234</td>
<td>Configures a path option for an MPLS-TE tunnel.</td>
</tr>
<tr>
<td>pce peer (MPLS-TE), on page 254</td>
<td>Configures an IPv4 self address for a PCE peer.</td>
</tr>
<tr>
<td>pce reoptimize (MPLS-TE), on page 256</td>
<td>Configures a periodic reoptimization timer.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>pce request-timeout (MPLS-TE), on page 258</td>
<td>Configures a PCE request-timeout.</td>
</tr>
<tr>
<td>pce tolerance keepalive (MPLS-TE), on page 260</td>
<td>Configures a PCE tolerance keepalive (which is the minimum acceptable peer proposed keepalive).</td>
</tr>
</tbody>
</table>
pce deadtimer (MPLS-TE)

To configure a path computation element (PCE) deadtimer, use the `pce deadtimer` command in MPLS-TE configuration mode. To return to the default behavior, use the `no` form of this command.

```
pce deadtimer value
no pce deadtimer value
```

**Syntax Description**

- `value` Keepalive dead interval, in seconds. The range is 0 to 255.

**Command Default**

- `value`: 120

**Command Modes**

- MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

When the dead interval is 0, the LSR does not timeout a PCEP session to a remote peer.

**Task ID**

- `mpls-te` read, write

**Examples**

The following example shows how to configure a PCE deadtimer:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# pce deadtimer 50
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls traffic-eng, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
<tr>
<td>path-option (MPLS-TE), on page 234</td>
<td>Configures a path option for an MPLS-TE tunnel.</td>
</tr>
<tr>
<td>pce address (MPLS-TE), on page 248</td>
<td>Configures the IPv4 self address for a PCE.</td>
</tr>
<tr>
<td>pce keepalive (MPLS-TE), on page 252</td>
<td>Configures a PCEP keepalive interval.</td>
</tr>
</tbody>
</table>
### Command Reference

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>pce peer (MPLS-TE), on page 254</code></td>
<td>Configures an IPv4 self address for a PCE peer.</td>
</tr>
<tr>
<td><code>pce reoptimize (MPLS-TE), on page 256</code></td>
<td>Configures a periodic reoptimization timer.</td>
</tr>
<tr>
<td><code>pce request-timeout (MPLS-TE), on page 258</code></td>
<td>Configures a PCE request-timeout.</td>
</tr>
<tr>
<td><code>pce tolerance keepalive (MPLS-TE), on page 260</code></td>
<td>Configures a PCE tolerance keepalive (which is the minimum acceptable peer proposed keepalive).</td>
</tr>
</tbody>
</table>
**pce keepalive (MPLS-TE)**

To configure a path computation element protocol (PCEP) keepalive interval, use the `pce keepalive` command in MPLS-TE configuration mode. To disable this command, use the `no` form of this command.

```
pce keepalive interval
no pce keepalive interval
```

**Syntax Description**

`interval` Keepalive interval, in seconds. The range is 0 to 255.

**Command Default**

`interval`: 30

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

When the keepalive interval is 0, the LSR does not send keepalive messages.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure PCEP keepalive interval for 10 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# pce keepalive 10
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls traffic-eng, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
<tr>
<td>path-option (MPLS-TE), on page 234</td>
<td>Configures a path option for an MPLS-TE tunnel.</td>
</tr>
<tr>
<td>pce address (MPLS-TE), on page 248</td>
<td>Configures the IPv4 self address for a PCE.</td>
</tr>
<tr>
<td>pce deadtimer (MPLS-TE), on page 250</td>
<td>Configures a PCE deadtimer.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>pce peer (MPLS-TE), on page 254</td>
<td>Configures an IPv4 self address for a PCE peer.</td>
</tr>
<tr>
<td>pce reoptimize (MPLS-TE), on page 256</td>
<td>Configures a periodic reoptimization timer.</td>
</tr>
<tr>
<td>pce request-timeout (MPLS-TE), on page 258</td>
<td>Configures a PCE request-timeout.</td>
</tr>
<tr>
<td>pce tolerance keepalive (MPLS-TE), on page 260</td>
<td>Configures a PCE tolerance keepalive (which is the minimum acceptable peer proposed keepalive).</td>
</tr>
</tbody>
</table>
pce peer (MPLS-TE)

To configure an IPv4 self address for a path computation element (PCE) peer, use the `pce peer` command in MPLS-TE configuration mode. To return to the default behavior, use the `no` form of this command.

```
pce peer ipv4 address
no pce peer ipv4 address
```

**Syntax Description**
- `ipv4 address` Configures the IPv4 address for PCE.

**Command Default**
- TE metric

**Command Modes**
- MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure an IPv4 self address for a PCE peer:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# pce peer ipv4 11.11.11.11
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls traffic-eng, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
<tr>
<td>path-option (MPLS-TE), on page 234</td>
<td>Configures a path option for an MPLS-TE tunnel.</td>
</tr>
<tr>
<td>pce address (MPLS-TE), on page 248</td>
<td>Configures the IPv4 self address for a PCE.</td>
</tr>
<tr>
<td>pce deadtimer (MPLS-TE), on page 250</td>
<td>Configures a PCE deadtimer.</td>
</tr>
<tr>
<td>pce keepalive (MPLS-TE), on page 252</td>
<td>Configures a PCEP keepalive interval.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>pce reoptimize (MPLS-TE), on page 256</td>
<td>Configures a periodic reoptimization timer.</td>
</tr>
<tr>
<td>pce request-timeout (MPLS-TE), on page 258</td>
<td>Configures a PCE request-timeout.</td>
</tr>
<tr>
<td>pce tolerance keepalive (MPLS-TE), on page 260</td>
<td>Configures a PCE tolerance keepalive (which is the minimum acceptable peer proposed keepalive).</td>
</tr>
</tbody>
</table>
pce reoptimize (MPLS-TE)

To configure a periodic reoptimization timer, use the `pce reoptimize` command in MPLS-TE configuration mode. To disable this feature, use the `no` form of this command.

```
pce reoptimize value
no pce reoptimize value
```

**Syntax Description**

- `value` Periodic reoptimization timer value, in seconds. The range is 60 to 604800.

**Command Default**

- `value: 3600`

**Command Modes**

- MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

When the dead interval is 0, the LSR does not time out a path computation element protocol (PCEP) session to a remote peer.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a periodic reoptimization timer for 200 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# pce reoptimize 200
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls traffic-eng, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
<tr>
<td>path-option (MPLS-TE), on page 234</td>
<td>Configures a path option for an MPLS-TE tunnel.</td>
</tr>
<tr>
<td>pce address (MPLS-TE), on page 248</td>
<td>Configures the IPv4 self address for a PCE.</td>
</tr>
<tr>
<td>pce deadtimer (MPLS-TE), on page 250</td>
<td>Configures a PCE deadtimer.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>pce keepalive (MPLS-TE), on page 252</code></td>
<td>Configures a PCEP keepalive interval.</td>
</tr>
<tr>
<td><code>pce peer (MPLS-TE), on page 254</code></td>
<td>Configures an IPv4 self address for a PCE peer.</td>
</tr>
<tr>
<td><code>pce request-timeout (MPLS-TE), on page 258</code></td>
<td>Configures a PCE request-timeout.</td>
</tr>
<tr>
<td><code>pce tolerance keepalive (MPLS-TE), on page 260</code></td>
<td>Configures a PCE tolerance keepalive (which is the minimum acceptable peer proposed keepalive).</td>
</tr>
</tbody>
</table>
pce request-timeout (MPLS-TE)

To configure a path computation element (PCE) request-timeout, use the `pce request-timeout` command in MPLS-TE configuration mode. To disable this feature, use the `no` form of this command.

```
pce request-timeout  value
no  pce request-timeout  value
```

**Syntax Description**

- `value` PCE request-timeout, in seconds. The range is 5 to 100.

**Command Default**

- `value`: 10

**Command Modes**

- MPLS-TE configuration

**Command History**

- **Release**: 5.0.0  
  This command was introduced.

**Usage Guidelines**

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

PCC or PCE keeps a pending path request only for the request-timeout period.

**Examples**

The following example shows how to configure a PCE request-timeout for 10 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# pce request-timeout 10
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls traffic-eng, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
<tr>
<td>path-option (MPLS-TE), on page 234</td>
<td>Configures a path option for an MPLS-TE tunnel.</td>
</tr>
<tr>
<td>pce address (MPLS-TE), on page 248</td>
<td>Configures the IPv4 self address for a PCE.</td>
</tr>
<tr>
<td>pce deadtimer (MPLS-TE), on page 250</td>
<td>Configures a PCE deadtimer.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>pce keepalive (MPLS-TE), on page 252</td>
<td>Configures a PCEP keepalive interval.</td>
</tr>
<tr>
<td>pce peer (MPLS-TE), on page 254</td>
<td>Configures an IPv4 self address for a PCE peer</td>
</tr>
<tr>
<td>pce reoptimize (MPLS-TE), on page 256</td>
<td>Configures a periodic reoptimization timer.</td>
</tr>
<tr>
<td>pce tolerance keepalive (MPLS-TE), on page 260</td>
<td>Configures a PCE tolerance keepalive (which is the minimum acceptable peer proposed keepalive).</td>
</tr>
</tbody>
</table>
pce tolerance keepalive (MPLS-TE)

To configure a path computation element (PCE) tolerance keepalive (which is the minimum acceptable peer proposed keepalive), use the `pce tolerance keepalive` command in MPLS-TE configuration mode. To disable this feature, use the `no` form of this command.

```
pce tolerance keepalive  value
no  pce tolerance keepalive  value
```

**Syntax Description**

- `value`  
  PCE tolerance keepalive value, in seconds. The range is 0 to 255.

**Command Default**

- `value`: 10

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

- `mpls-te`  
  read,  
  write

**Examples**

The following example shows how to configure a PCE tolerance keepalive for 10 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# pce tolerance keepalive 10
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mpls traffic-eng</code>, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
<tr>
<td><code>path-option (MPLS-TE)</code>, on page 234</td>
<td>Configures a path option for an MPLS-TE tunnel.</td>
</tr>
<tr>
<td><code>pce address (MPLS-TE)</code>, on page 248</td>
<td>Configures the IPv4 self-address for a PCE.</td>
</tr>
<tr>
<td><code>pce deadtimer (MPLS-TE)</code>, on page 250</td>
<td>Configures a PCE deadtimer.</td>
</tr>
<tr>
<td><code>pce keealpalive (MPLS-TE)</code>, on page 252</td>
<td>Configures a PCEP keepalive interval.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>pce peer (MPLS-TE), on page 254</td>
<td>Configures an IPv4 self address for a PCE peer</td>
</tr>
<tr>
<td>pce reoptimize (MPLS-TE), on page 256</td>
<td>Configures a periodic reoptimization timer.</td>
</tr>
<tr>
<td>pce request-timeout (MPLS-TE), on page 258</td>
<td>Configures a PCE request-timeout.</td>
</tr>
</tbody>
</table>
To configure the setup and reservation priority for an MPLS-TE tunnel, use the **priority** command in interface configuration mode. To return to the default behavior, use the **no** form of this command.

```
priority  setup-priority  hold-priority
no  priority  setup-priority  hold-priority
```

**Syntax Description**

- **setup-priority**  Priority used when signaling a label switched path (LSP) for this tunnel to determine which existing tunnels can be preempted. Range is 0 to 7 (in which a lower number indicates a higher priority). Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non-0 priority.

- **hold-priority**  Priority associated with an LSP for this tunnel to determine if it should be preempted by other LSPs that are being signaled. Range is 0 to 7 (in which a lower number indicates a higher priority).

**Command Default**

```
setup-priority: 7
hold-priority: 7
```

**Command Modes**

Interface configuration

**Command History**

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

**Usage Guidelines**

When an LSP is signaled and an interface does not currently have enough bandwidth available for that LSP, the call admission software (if necessary) preempts lower-priority LSPs to admit the new LSP. Accordingly, the new LSP priority is the setup priority and the existing LSP priority is the hold priority. The two priorities make it possible to signal an LSP with a low setup priority (so that the LSP does not preempt other LSPs on setup) and a high hold priority (so that the LSP is not preempted after it is established). Setup priority and hold priority are typically configured to be equal, and setup priority cannot be numerically smaller than the hold priority.

**Examples**

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# priority 1 1
```
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface tunnel-te, on page 207</td>
<td>Configures an MPLS-TE tunnel interface.</td>
</tr>
</tbody>
</table>
record-route

To record the route used by a tunnel, use the `record-route` command in interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
record-route
no record-route
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must configure record-route on TE tunnels that are protected by multiple backup tunnels merging at a single node.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable record-route on the TE tunnel:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mpls traffic-eng tunnels</code> on page 335</td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
</tbody>
</table>
reoptimize timers delay (MPLS-TE)

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

```
reoptimize timers delay {after-frr seconds | cleanup delay-time | installation delay-time | path-protection seconds}
no reoptimize timers delay {after-frr seconds | cleanup delay-time | installation delay-time | path-protection seconds}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>after-frr</code></td>
<td>Delays the LSP reoptimization in the event of the FRR.</td>
</tr>
<tr>
<td><code>seconds</code></td>
<td>Reoptimization initiation delay time of the tunnel, in seconds, after an FRR event. Range is from 0 to 120.</td>
</tr>
<tr>
<td><code>cleanup</code></td>
<td>Delays removal of the old LSPs after tunnel reoptimization.</td>
</tr>
<tr>
<td><code>delay-time</code></td>
<td>Reoptimization delay time, in seconds. A value of 0 disables delay. The valid range is from 0 to 300 for cleanup time.</td>
</tr>
<tr>
<td><code>installation</code></td>
<td>Delays installation of a new label after tunnel reoptimization.</td>
</tr>
<tr>
<td><code>delay-time</code></td>
<td>Reoptimization delay time, in seconds. A value of 0 disables delay. The valid range is 0 to 3600 for installation time.</td>
</tr>
<tr>
<td><code>path-protection</code></td>
<td>Delays the time between path protection switchover event and tunnel reoptimization.</td>
</tr>
<tr>
<td><code>seconds</code></td>
<td>Time, in seconds, between path protection switchover event and tunnel reoptimization. A value of 0 disables delay. Range is from 0 to 604800.</td>
</tr>
</tbody>
</table>

### Command Default

- `after-frr delay: 0`
- `cleanup delay: 20`
- `delay-time: 20`
- `installation delay: 20`
**reoptimize timers delay (MPLS-TE)**

### Command Modes

- **MPLS-TE configuration**

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

A device with Multiprotocol Label Switching traffic engineering (MPLS-TE) tunnels periodically examines tunnels with established LSPs to discover whether more efficient LSPs (paths) are available. If a better LSP is available, the device signals the more efficient LSP; if the signaling is successful, the device replaces the older LSP with the new, more efficient LSP.

Sometimes the slower router-point nodes may not yet utilize the new label’s forwarding plane. In this case, if the headend node replaces the labels quickly, it can result in brief packet loss. By delaying the cleanup of the old LSP using the `reoptimize timers delay cleanup` command, packet loss is avoided.

### Task ID

- **mpls-te**
  - read, write

### Examples

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

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

The following example shows how to set the reoptimization installation delay time to 40 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# reoptimize timers delay installation 40
```

The following example shows how to set the reoptimization delay time after the event of the FRR to 50 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# reoptimize timers delay after-frr 50
```

The following example shows how to set the reoptimization delay time between path protection switchover event and tunnel reoptimization to 80:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# reoptimize timers delay path-protection 80
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls traffic-eng reoptimize (EXEC), on page 224</td>
<td>Reoptimizes all traffic engineering tunnels immediately.</td>
<td></td>
</tr>
</tbody>
</table>
**router-id secondary (MPLS-TE)**

To configure a secondary TE router identifier in MPLS-TE to be used locally (not advertised through IGP), use the `router-id secondary` command in MPLS-TE configuration mode. To return to the default behavior, use the `no` form of this command.

```
router-id secondary  IP address
no router-id secondary  IP address
```

**Syntax Description**

| IP address | IPv4 address to be used as secondary TE router ID. |

**Command Default**

No default behavior or values

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

Use the `router-id secondary` command on tail end nodes to terminate verbatim tunnels to secondary TE RIDs as destinations.

You can configure up to 32 IPv4 addresses as TE secondary router IDs.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a secondary TE router identifier in MPLS-TE:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# router-id secondary 1.1.1.1
RP/0/RP0/CPU0:router(config-mpls-te)# router-id secondary 2.2.2.2
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls traffic-eng router-id (MPLS-TE router), on page 226</td>
<td>Specifies that the TE router identifier for the node is the IP address associated with a given interface.</td>
</tr>
</tbody>
</table>
show explicit-paths

To display the configured IP explicit paths, use the show explicit-paths command in EXEC mode.

```
show explicit-paths [{name path-name | identifier number}]
```

**Syntax Description**
- **name path-name**: (Optional) Displays the name of the explicit path.
- **identifier number**: (Optional) Displays the number of the explicit path. Range is 1 to 65535.

**Command Default**
No default behavior or values

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
An IP explicit path is a list of IP addresses that represent a node or link in the explicit path.

**Task ID**
- **Task ID**: Operations
- **Operations ID**: mpls-te

**Examples**
The following shows a sample output from the show explicit-paths command:

```
RP/0/RP0/CPU0:router# show explicit-paths
Path ToR2 status enabled
  0x1: next-address 192.168.1.2
  0x2: next-address 10.20.20.20
Path ToR3 status enabled
  0x1: next-address 192.168.1.2
  0x2: next-address 192.168.2.2
  0x3: next-address 10.30.30.30
Path 100 status enabled
  0x1: next-address 192.168.1.2
  0x2: next-address 10.20.20.20
Path 200 status enabled
  0x1: next-address 192.168.1.2
  0x2: next-address 192.168.2.2
  0x3: next-address 10.30.30.30
```
This table describes the significant fields shown in the display.

**Table 26: show explicit-paths Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>Pathname or number, followed by the path status.</td>
</tr>
<tr>
<td>1:</td>
<td>First IP address in the path.</td>
</tr>
<tr>
<td>next-address</td>
<td></td>
</tr>
<tr>
<td>2:</td>
<td>Second IP address in the path.</td>
</tr>
<tr>
<td>next-address</td>
<td></td>
</tr>
</tbody>
</table>

The following shows a sample output from the `show explicit-paths` command using a specific path name:

```
RP/0/RP0/CPU0:router# show explicit-paths name ToR3
Path ToR3  status enabled
  0x1:  next-address 192.168.1.2
  0x2:  next-address 192.168.2.2
  0x3:  next-address 10.30.30.30
```

The following shows a sample output from the `show explicit-paths` command using a specific path number:

```
RP/0/RP0/CPU0:router# show explicit-paths identifier 200
Path 200  status enabled
  0x1:  next-address 192.168.1.2
  0x2:  next-address 192.168.2.2
  0x3:  next-address 10.30.30.30
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>index exclude-address, on page 200</td>
<td>Specifies the next IP address to exclude from the explicit path.</td>
</tr>
<tr>
<td>index next-address, on page 203</td>
<td>Specifies path entries at a specific index.</td>
</tr>
</tbody>
</table>
show mpls traffic-eng affinity-map

To display the color name-to-value mappings configured on the router, use the show mpls traffic-eng affinity-map command in EXEC mode.

Syntax Description
This command has no arguments or keywords.

Command Default
No default behavior or values

Command Modes
EXEC

Command History
Modification Release
This command was introduced. 5.0.0

Usage Guidelines
If the affinity value of an affinity associated with an affinity constraint is unknown, the show mpls traffic-eng affinity-map command output displays: "(refers to undefined affinity name)"

Task ID
Task Operations
ID
mpls te read

Examples
The following shows a sample output from the show mpls traffic-eng affinity-map command:

RP/0/RP0/CPU0:router# show mpls traffic-eng affinity-map

<table>
<thead>
<tr>
<th>Affinity Name</th>
<th>Bit-position</th>
<th>Affinity Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>bcdefghabcdefghabcdefghabcdefgh</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>red1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>red2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>red3</td>
<td>3</td>
<td>8</td>
</tr>
<tr>
<td>red4</td>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>red5</td>
<td>5</td>
<td>20</td>
</tr>
<tr>
<td>red6</td>
<td>6</td>
<td>40</td>
</tr>
<tr>
<td>red7</td>
<td>7</td>
<td>80</td>
</tr>
<tr>
<td>red8</td>
<td>8</td>
<td>100</td>
</tr>
<tr>
<td>red9</td>
<td>9</td>
<td>200</td>
</tr>
<tr>
<td>red10</td>
<td>10</td>
<td>400</td>
</tr>
<tr>
<td>red11</td>
<td>11</td>
<td>800</td>
</tr>
<tr>
<td>red12</td>
<td>12</td>
<td>1000</td>
</tr>
<tr>
<td>red13</td>
<td>13</td>
<td>2000</td>
</tr>
<tr>
<td>red14</td>
<td>14</td>
<td>4000</td>
</tr>
<tr>
<td>red15</td>
<td>15</td>
<td>8000</td>
</tr>
<tr>
<td>red16</td>
<td>16</td>
<td>10000</td>
</tr>
<tr>
<td>cdefghabcdefghabcdefghabcdefgh</td>
<td>17</td>
<td>20000</td>
</tr>
<tr>
<td>red18</td>
<td>18</td>
<td>40000</td>
</tr>
<tr>
<td>red19</td>
<td>19</td>
<td>80000</td>
</tr>
<tr>
<td>red20</td>
<td>20</td>
<td>100000</td>
</tr>
</tbody>
</table>
show mpls traffic-eng affinity-map

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affinity Name</td>
<td>Affinity name associated with the tunnel affinity constraints.</td>
</tr>
<tr>
<td>Bit-position</td>
<td>Bit position set in the 32-bit affinity value</td>
</tr>
<tr>
<td>Affinity Value</td>
<td>Affinity value associated with the affinity name.</td>
</tr>
</tbody>
</table>

Table 27: show mpls traffic-eng affinity-map Field Descriptions, on page 272 describes the significant fields shown in the display.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>affinity, on page 134</td>
<td>Configures an affinity (the properties the tunnel requires in its links) for an MPLS-TE tunnel.</td>
</tr>
<tr>
<td>affinity-map, on page 139</td>
<td>Assigns a numerical value to each affinity name.</td>
</tr>
</tbody>
</table>
show mpls traffic-eng attribute-set

To display the attribute set for MPLS-TE, use the `show mpls traffic-eng attribute-set` command in EXEC mode.

```
show mpls traffic-eng attribute-set [ { auto-backup | auto-mesh | path-option [ attribute-set-name ] } ]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-backup</td>
<td>Displays information for the auto-backup attribute type.</td>
</tr>
<tr>
<td>auto-mesh</td>
<td>Displays information for the auto-mesh attribute type.</td>
</tr>
<tr>
<td>path-option</td>
<td>Displays information for the path-option attribute type.</td>
</tr>
<tr>
<td>attribute-set-name</td>
<td>Specifies the name of the attribute set to be displayed.</td>
</tr>
</tbody>
</table>

### Command Default

Displays information about all types of attribute sets.

### Command Modes

EXEC mode

### Command History

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

### Usage Guidelines

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

To use this command, first enable the MPLS-TE application.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
</tbody>
</table>

### Example

The following command shows the attribute set for auto-backup attribute type.

```
RP/0/RP0/CPU0:router# show mpls traffic-eng attribute-set auto-backup auto1
```

Attribute Set Name: auto1 (Type: auto-backup)
Affinity: 0x0/0xffff (Default)
Priority: 7 7 (Default)
Record-route: Enabled
Policy-class: 0 (Not configured)
Logging: None
The following command shows the attribute set for auto-mesh attribute type.

```
RP/0/RP0/CPU0:router# show mpls traffic-eng attribute-set auto-mesh mesh1
```

Attribute Set Name: mesh1 (Type: auto-mesh)
- Bandwidth: 0 kbps (CT0) (Default)
- Affinity: 0x0/0xffff (Default)
- Priority: 7 7 (Default)
- Interface Bandwidth: 0 kbps (Default)
- AutoRoute Announce: Disabled
- Auto-bw: Disabled
- Soft Preemption: Disabled
- Fast Reroute: Disabled, Protection Desired: None
- Record-route: Disabled
- Policy-class: 0 (Not configured)
- Logging: None
- List of Mesh Groups (count 0)

The following command shows the attribute set for path-option attribute type.

```
RP/0/RP0/CPU0:router# show mpls traffic-eng attribute-set path-option path1
```

Attribute Set Name: path1 (Type: path option)
- Bandwidth: 0 kbps (CT0) (Default)
- Affinity: 0x0/0xffff (Default)
- List of tunnel IDs (count 0)
show mpls traffic-eng autoroute

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

```
show mpls traffic-eng autoroute [IP-address]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>IP-address</code></td>
<td>(Optional) Tunnel leading to this address.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The traffic-engineering tunnels are taken into account for the enhanced shortest path first (SPF) calculation of the IGP. The `show mpls traffic-eng autoroute` command displays those tunnels that IGP is currently using in its enhanced SPF calculation (that is, those tunnels that are up and have autoroute configured).

Tunnels are organized by destination. All tunnels to a destination carry a share of the traffic tunneled to that destination.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
</tbody>
</table>

Examples

The following shows a sample output from the `show mpls traffic-eng autoroute` command:

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

Destination 103.0.0.3 has 2 tunnels in OSPF 0 area 0
tunnel-te1 (traffic share 1, nexthop 103.0.0.3)
tunnel-te2 (traffic share 1, nexthop 103.0.0.3)
```

This table describes the significant fields shown in the display.

```
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Multiprotocol Label Switching (MPLS) TE tail-end router ID.</td>
</tr>
</tbody>
</table>
```
A factor, based on bandwidth, indicating how much traffic this tunnel should carry, relative to other tunnels, to the same destination. If two tunnels go to a single destination, one with a traffic share of 200 and the other with a traffic share of 100, the first tunnel carries two-thirds of the traffic.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>traffic share</td>
<td>A factor, based on bandwidth, indicating how much traffic this tunnel should carry, relative to other tunnels, to the same destination.</td>
</tr>
<tr>
<td>NeXthop</td>
<td>Next-hop router ID of the MPLS-TE tunnel.</td>
</tr>
<tr>
<td>absolute metric</td>
<td>Metric with mode absolute for the MPLS-TE tunnel.</td>
</tr>
<tr>
<td>relative metric</td>
<td>Metric with mode relative for the MPLS-TE tunnel.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>autoroute metric, on page 154</td>
<td>Specifies the MPLS-TE tunnel metric that the IGP-enhanced SPF calculation uses.</td>
</tr>
<tr>
<td>show mpls traffic-eng tunnels, on page 335</td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
<tr>
<td>topology holddown sigerr (MPLS-TE), on page 381</td>
<td>Specifies the time that a router should ignore a link in its TE topology database in tunnel path CSPF computations following a TE tunnel signalling error on the link.</td>
</tr>
</tbody>
</table>
show mpls traffic-eng auto-tunnel backup

To display information about automatically build MPLS-TE backup tunnels, use the `show mpls traffic-eng auto-tunnel backup` command in EXEC mode.

```
show mpls traffic-eng auto-tunnel backup {backup [{private | summary | unused}]}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup</td>
<td>Displays information about auto-tunnel backup.</td>
</tr>
<tr>
<td>private</td>
<td>(Optional) Displays private information about the automatically build MPLS-TE backup tunnels.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays the automatically build MPLS-TE backup tunnels summary information.</td>
</tr>
<tr>
<td>unused</td>
<td>(Optional) Displays only unused MPLS-TE backup tunnels.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

```
Task ID  Operation ID
mpls-te read
```

**Example**

This is sample output from the `show mpls traffic-eng auto-tunnel backup` command:

```
AutoTunnel Backup Configuration:
  Interfaces count: 4
  Unused removal timeout: 1h 0m 0s
  Configured tunnel number range: 2000-2500

AutoTunnel Backup Summary:
  AutoTunnel Backups:
    1 created, 1 up, 0 down, 0 unused
    1 NHOP, 0 NNHOP, 0 SRLG strict, 0 SRLG preferred
  Protected LSPs:
    1 NHOP, 0 NHOP+SRLG
    0 NNHOP, 0 NNHOP+SRLG
```
Protected S2L Sharing Families:
  0 NHOP, 0 NHOP+SRLG
  0 NNHOP, 0 NNHOP+SRLG

Protected S2Ls:
  0 NHOP, 0 NHOP+SRLG
  0 NNHOP, 0 NNHOP+SRLG

Cumulative Counters (last cleared 05:17:19 ago):

<table>
<thead>
<tr>
<th></th>
<th>Total</th>
<th>NHOP</th>
<th>NNHOP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Connected</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Removed (down)</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Removed (unused)</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Range exceeded</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

AutoTunnel Backups:

<table>
<thead>
<tr>
<th>Tunnel Name</th>
<th>State</th>
<th>Protection</th>
<th>Prot. Flows*</th>
<th>Protected Interface</th>
<th>Protected Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel-te2000</td>
<td>up NHOP</td>
<td>1</td>
<td></td>
<td>G10/2/0/2</td>
<td>N/A</td>
</tr>
</tbody>
</table>

*Prot. Flows = Total Protected LSPs, S2Ls and S2L Sharing Families

This is sample output from the `show mpls traffic-eng auto-tunnel mesh` command:

```
RP/0/RP0/CP00:router# show mpls traffic-eng auto-tunnel mesh

Auto-tunnel Mesh Global Configuration:
  Unused removal timeout: 2h
  Configured tunnel number range: 10000-12000

Auto-tunnel Mesh Groups Summary:
  Mesh Groups count: 5
  Mesh Groups Destinations count: 50

Mesh Group 40 (2 Destinations, 1 Up, 1 Down):
  Destination-list: dl-40
  Attribute-set: ta_name
  Destination: 40.40.40.40, tunnel-id: 10000, State: Up
  Destination: 10.10.10.10, tunnel-id: 10001, State: Down

Mesh Group 41 (3 Destinations, 2 Up, 1 Down):
  Destination-list: dl-40
  Attribute-set: ta_name
  Destination: 4.4.4.4, tunnel-id: 10005, State: Up
  Destination: 3.3.3.3, tunnel-id: 10006, State: Up
  Destination: 1.1.1.1, tunnel-id: 10007, State: Down

Mesh Group 51 (0 Destinations, 0 Up, 0 Down):
  Destination-list: Not configured
  Attribute-set: Not configured

Mesh Group 52 (0 Destinations, 0 Up, 0 Down):
  Destination-list: NAME1 (Not defined)
  Attribute-set: NAME2 (Not defined)

Mesh Group 53 (2 Destinations, 1 Up, 1 Down):
  Destination-list: dl-53
  Attribute-set: Not configured
  Destination: 40.40.40.40, tunnel-id: 10000, State: Up
  Destination: 10.10.10.10, tunnel-id: 10001, State: Down

Cumulative Counters (last cleared 7h ago):
  Total
  Created: 100
  Connected: 50
```
Removed (unused): 50
Removed (in use): 0
Range exceeded: 0

This is sample output from the `show mpls traffic-eng auto-tunnel private` command:

Auto-tunnel Mesh Private Information:
ID allocator overall maximum ID: 4096
ID allocator last allocated ID: 50999
ID allocator number IDs allocated: 1000
show mpls traffic-eng auto-tunnel mesh

To display information about automatically built MPLS-TE mesh tunnels, use the show mpls traffic-eng auto-tunnel mesh command in EXEC mode.

```
show mpls traffic-eng auto-tunnel mesh {mesh-value | unused | summary | attribute-set name | destination address | destination-list name | down | up | tunnel {created | not-created} | onehop}
```

**Syntax Description**

- **mesh mesh-value**: Displays the tunnels that belong to the specified auto-tunnel mesh group. The range of mesh group ID is from 0 to 4294967295.
- **attribute-set name**: Displays mesh-groups configured with a specific attribute set.
- **destination address**: Displays only the destinations with a specified address.
- **destination-list name**: Displays mesh-groups configured with a specified prefix-list.
- **down**: Displays only those tunnels that are down.
- **up**: Displays only those tunnels that are up.
- **summary**: Displays auto-tunnel mesh summary information.
- **unused**: Displays only the down tunnels with no destination in the topology.
- **tunnel created | not-created**: Specifies either created destinations with tunnels, or not-created destinations without tunnels.

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS-TE</td>
<td>read</td>
</tr>
</tbody>
</table>

This is sample output from the show mpls traffic-eng auto-tunnel mesh command:

```
RP/0/RP0/CPU0:router show mpls traffic-eng auto-tunnel mesh

Auto-tunnel Mesh Global Configuration:
Unused removal timeout: 1h 0m 0s
```
Configured tunnel number range: 1000-1200

Auto-tunnel Mesh Groups Summary:
- Mesh Groups count: 1
- Mesh Groups Destinations count: 3
- Mesh Groups Tunnels count:
  - 3 created, 0 up, 3 down, 0 FRR enabled

Mesh Group: 65 (3 Destinations)
- Status: Enabled
- Attribute-set: am-65
- Destination-list: dl-65 (Not a prefix-list)
- Recreate timer: Not running

<table>
<thead>
<tr>
<th>Destination</th>
<th>Tunnel ID</th>
<th>State</th>
<th>Unused timer</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.2</td>
<td>1000</td>
<td>up</td>
<td>Not running</td>
</tr>
<tr>
<td>192.168.0.3</td>
<td>1001</td>
<td>up</td>
<td>Not running</td>
</tr>
<tr>
<td>192.168.0.4</td>
<td>1002</td>
<td>up</td>
<td>Not running</td>
</tr>
</tbody>
</table>

Displayed 3 tunnels, 0 up, 3 down, 0 FRR enabled

Auto-mesh Cumulative Counters:
  - Total
    - Created: 3
    - Connected: 0
    - Removed (unused): 0
    - Removed (in use): 0
    - Range exceeded: 0

This shows how to configure the auto-tunnel mesh command with destination-list and attribute-set keywords:

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# auto-tunnel mesh
RP/0/RP0/CPU0:router(config-te-auto-mesh)# group 65
RP/0/RP0/CPU0:router(config-te-mesh-group)# disable
RP/0/RP0/CPU0:router(config-te-mesh-group)# destination-list dl-65
RP/0/RP0/CPU0:router(config-te-mesh-group)# attribute-set am-65
```

This attribute-set is an optional configuration. Without this configuration, all tunnels use default tunnel attribute values. If you configure an non-existent attribute-set, this mesh group does not create any tunnel.

---

**Note**

This destination-list configuration is mandatory. If there is no IPv4 prefix-list by this name on this router, this mesh group create tunnels with all routers in the network.
show mpls traffic-eng collaborator-timers

To display the current status of the MPLS-TE collaborator timers, use the show mpls traffic-eng collaborator-timers command in EXEC mode.

show mpls traffic-eng collaborator-timers

Syntax Description
This command has no arguments or keywords.

Command Default
No default behavior or values

Command Modes
EXEC

Command History
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

The MPLS-TE process maintains the timers for all of the collaborators such as RSVP, LSD, and so forth. The show mpls traffic-eng collaborator-timers command shows the status of these timers.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
</tbody>
</table>

Examples
The following sample output shows the current status of the collaborator timers:

RP/0/RP0/CPU0:router# show mpls traffic-eng collaborator-timers

Collaborator Timers
-------------------
Timer Name: [LMRIB Restart] Index:[0]  
Duration: [60] Is running: NO  
Last start time: 02/09/2009 11:57:59  
Last stop time: 02/09/2009 11:58:00  
Last expiry time: Never expired  
Timer Name: [LMRIB Recovery] Index:[1]  
Duration: [60] Is running: YES  
Last start time: 02/09/2009 11:58:00  
Last stop time: Never Stopped  
Last expiry time: 19/08/2009 17:45:24  
Timer Name: [RSVP Restart] Index:[2]  
Duration: [180] Is running: NO  
Last start time: 26/08/2009 18:59:18  
Last stop time: 26/08/2009 18:59:20  
Last expiry time: Never expired  
Timer Name: [RSVP Recovery] Index:[3]  
Duration: [1800] Is running: NO
This table describes the significant fields shown in the display.

**Table 29: show mpls traffic-eng collaborator-timers Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timer Name</td>
<td>Timer name that is associated to a collaborator.</td>
</tr>
<tr>
<td>Index</td>
<td>Identification number of the timer.</td>
</tr>
<tr>
<td>Duration</td>
<td>Expiry delay of the timer, in seconds. For example, the duration indicates</td>
</tr>
<tr>
<td></td>
<td>the timer interval.</td>
</tr>
<tr>
<td>Is running</td>
<td>Timer is running low or not.</td>
</tr>
<tr>
<td>Last start time</td>
<td>Last time that the collaborator process for MPLS LSD was restarted.</td>
</tr>
<tr>
<td>Last stop time</td>
<td>Time TE was able to reconnect to the MPLS LSD process.</td>
</tr>
<tr>
<td>Last expiry time</td>
<td>Time that timer expired.</td>
</tr>
</tbody>
</table>
# show mpls traffic-eng counters signaling

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

```
show mpls traffic-eng counters signaling {signaling | soft-preemption} {tunnel-number | all | [heads | mids | tails]} | name tunnel-name | summary
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>signaling</td>
<td>Displays signaling counters.</td>
</tr>
<tr>
<td>soft-preemption</td>
<td>Displays the statistics for the soft-preemption.</td>
</tr>
<tr>
<td>tunnel-number</td>
<td>Statistics for the input tunnel number. The range is from 0 to 65535.</td>
</tr>
<tr>
<td>all</td>
<td>Displays statistics for all tunnels.</td>
</tr>
<tr>
<td>heads</td>
<td>(Optional) Displays statistics for all tunnel heads.</td>
</tr>
<tr>
<td>mids</td>
<td>(Optional) Displays statistics for all tunnel midpoints.</td>
</tr>
<tr>
<td>tails</td>
<td>(Optional) Displays statistics for all tunnel tails.</td>
</tr>
<tr>
<td>name</td>
<td>Displays statistics for a specified tunnel.</td>
</tr>
<tr>
<td>tunnel-name</td>
<td>Name of the specified tunnel.</td>
</tr>
<tr>
<td>summary</td>
<td>Displays a summary of signaling statistics.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
This is a sample output from the `show mpls traffic-eng counters signaling` command, using the `all` keyword, which displays tunnel signaling statistics for all tunnels:

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

Tunnel Head: tunnel-te100
Cumulative Tunnel Counters:
<table>
<thead>
<tr>
<th>Signalling Events</th>
<th>Recv</th>
<th>Xmit</th>
<th>ResvCreate</th>
<th>Recv</th>
<th>Xmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>PathCreate</td>
<td>1</td>
<td>1</td>
<td>ResvCreate</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>PathChange</td>
<td>0</td>
<td>0</td>
<td>ResvChange</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathError</td>
<td>0</td>
<td>0</td>
<td>ResvError</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
<td>18</td>
<td>ResvTear</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BackupAssign</td>
<td>0</td>
<td>1</td>
<td>BackupError</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathQuery</td>
<td>0</td>
<td>0</td>
<td>Unknown</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Destination 100.0.0.4
Cumulative counters
<table>
<thead>
<tr>
<th>Signalling Events</th>
<th>Recv</th>
<th>Xmit</th>
<th>ResvCreate</th>
<th>Recv</th>
<th>Xmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>PathCreate</td>
<td>1</td>
<td>1</td>
<td>ResvCreate</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>PathChange</td>
<td>0</td>
<td>0</td>
<td>ResvChange</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathError</td>
<td>0</td>
<td>0</td>
<td>ResvError</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
<td>18</td>
<td>ResvTear</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BackupAssign</td>
<td>0</td>
<td>1</td>
<td>BackupError</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathQuery</td>
<td>0</td>
<td>0</td>
<td>Unknown</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

S2L LSP ID: 2 Sub-Grp ID: 0
Destination: 100.0.0.4
<table>
<thead>
<tr>
<th>Signalling Events</th>
<th>Recv</th>
<th>Xmit</th>
<th>ResvCreate</th>
<th>Recv</th>
<th>Xmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>PathCreate</td>
<td>1</td>
<td>1</td>
<td>ResvCreate</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>PathChange</td>
<td>0</td>
<td>0</td>
<td>ResvChange</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathError</td>
<td>0</td>
<td>0</td>
<td>ResvError</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
<td>20</td>
<td>ResvTear</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BackupAssign</td>
<td>0</td>
<td>1</td>
<td>BackupError</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathQuery</td>
<td>0</td>
<td>0</td>
<td>Unknown</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Tunnel Head: tunnel-mte200
Cumulative Tunnel Counters:
<table>
<thead>
<tr>
<th>Signalling Events</th>
<th>Recv</th>
<th>Xmit</th>
<th>ResvCreate</th>
<th>Recv</th>
<th>Xmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>PathCreate</td>
<td>2</td>
<td>2</td>
<td>ResvCreate</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>PathChange</td>
<td>0</td>
<td>0</td>
<td>ResvChange</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathError</td>
<td>0</td>
<td>0</td>
<td>ResvError</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
<td>20</td>
<td>ResvTear</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BackupAssign</td>
<td>0</td>
<td>2</td>
<td>BackupError</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathQuery</td>
<td>0</td>
<td>0</td>
<td>Unknown</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Destination 100.0.0.4
Cumulative counters
<table>
<thead>
<tr>
<th>Signalling Events</th>
<th>Recv</th>
<th>Xmit</th>
<th>ResvCreate</th>
<th>Recv</th>
<th>Xmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>PathCreate</td>
<td>2</td>
<td>2</td>
<td>ResvCreate</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>PathChange</td>
<td>0</td>
<td>0</td>
<td>ResvChange</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathError</td>
<td>0</td>
<td>0</td>
<td>ResvError</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
<td>20</td>
<td>ResvTear</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BackupAssign</td>
<td>0</td>
<td>2</td>
<td>BackupError</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathQuery</td>
<td>0</td>
<td>0</td>
<td>Unknown</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

S2L LSP ID: 10021 Sub-Grp ID: 1
Destination: 100.0.0.4
<table>
<thead>
<tr>
<th>Signalling Events</th>
<th>Recv</th>
<th>Xmit</th>
<th>ResvCreate</th>
<th>Recv</th>
<th>Xmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>PathCreate</td>
<td>2</td>
<td>2</td>
<td>ResvCreate</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>PathChange</td>
<td>0</td>
<td>0</td>
<td>ResvChange</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathError</td>
<td>0</td>
<td>0</td>
<td>ResvError</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
<td>20</td>
<td>ResvTear</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BackupAssign</td>
<td>0</td>
<td>2</td>
<td>BackupError</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathQuery</td>
<td>0</td>
<td>0</td>
<td>Unknown</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Tunnel Mid/Tail: router Source: 100.0.0.1 P2MP ID: 1677721603 Tunnel ID: 1 LSP ID: 21</td>
<td>Cumulative LSP Counters:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Signalling Events</strong></td>
<td><strong>Recv</strong></td>
<td><strong>Xmit</strong></td>
<td><strong>Recv</strong></td>
<td><strong>Xmit</strong></td>
<td></td>
</tr>
<tr>
<td>PathCreate</td>
<td>1</td>
<td>1</td>
<td>ResvCreate</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>PathChange</td>
<td>0</td>
<td>0</td>
<td>ResvChange</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathError</td>
<td>0</td>
<td>0</td>
<td>ResvError</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
<td>0</td>
<td>ResvTear</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BackupAssign</td>
<td>0</td>
<td>1</td>
<td>BackupError</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathQuery</td>
<td>0</td>
<td>0</td>
<td>Unknown</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tunnel Mid/Tail: router Source: 100.0.0.1 P2MP ID: 1677721603 Tunnel ID: 2 LSP ID: 21</th>
<th>Cumulative LSP Counters:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Signalling Events</strong></td>
<td><strong>Recv</strong></td>
</tr>
<tr>
<td>PathCreate</td>
<td>2</td>
</tr>
<tr>
<td>PathChange</td>
<td>0</td>
</tr>
<tr>
<td>PathError</td>
<td>0</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
</tr>
<tr>
<td>BackupAssign</td>
<td>0</td>
</tr>
<tr>
<td>PathQuery</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tunnel Mid/Tail: router Source: 100.0.0.1 P2MP ID: 1677721603 Tunnel ID: 3 LSP ID: 18</th>
<th>Cumulative LSP Counters:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Signalling Events</strong></td>
<td><strong>Recv</strong></td>
</tr>
<tr>
<td>PathCreate</td>
<td>2</td>
</tr>
<tr>
<td>PathChange</td>
<td>0</td>
</tr>
<tr>
<td>PathError</td>
<td>0</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
</tr>
<tr>
<td>BackupAssign</td>
<td>0</td>
</tr>
<tr>
<td>PathQuery</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tunnel Mid/Tail: router-1_t3 Source: 100.0.0.1 P2MP ID: 1677721603 Tunnel ID: 3 LSP ID: 18</th>
<th>Cumulative LSP Counters:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Signalling Events</strong></td>
<td><strong>Recv</strong></td>
</tr>
<tr>
<td>PathCreate</td>
<td>2</td>
</tr>
<tr>
<td>PathChange</td>
<td>0</td>
</tr>
<tr>
<td>PathError</td>
<td>0</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
</tr>
<tr>
<td>BackupAssign</td>
<td>0</td>
</tr>
<tr>
<td>PathQuery</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tunnel Mid/Tail: router-3_t33 Source: 100.0.0.3 P2MP ID: 1677721605 Tunnel ID: 33 LSP ID: 2</th>
<th>Cumulative LSP Counters:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Signalling Events</strong></td>
<td><strong>Recv</strong></td>
</tr>
<tr>
<td>PathCreate</td>
<td>2</td>
</tr>
<tr>
<td>PathChange</td>
<td>0</td>
</tr>
<tr>
<td>PathError</td>
<td>0</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
</tr>
<tr>
<td>BackupAssign</td>
<td>0</td>
</tr>
<tr>
<td>PathQuery</td>
<td>0</td>
</tr>
</tbody>
</table>
Cumulative LSP Counters:

<table>
<thead>
<tr>
<th>Signalling Events</th>
<th>Recv</th>
<th>Xmit</th>
<th>Recv</th>
<th>Xmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>PathCreate</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>PathChange</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathError</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BackupAssign</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathQuery</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

S2L LSP ID: 2 Sub-Grp ID: 0 Destination: 100.0.0.5

<table>
<thead>
<tr>
<th>Signalling Events</th>
<th>Recv</th>
<th>Xmit</th>
<th>Recv</th>
<th>Xmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>PathCreate</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>PathChange</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathError</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BackupAssign</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathQuery</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Signaling Counter Summary:

<table>
<thead>
<tr>
<th>Signalling Events</th>
<th>Recv</th>
<th>Xmit</th>
<th>Recv</th>
<th>Xmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>PathCreate</td>
<td>11</td>
<td>7</td>
<td>11</td>
<td>4</td>
</tr>
<tr>
<td>PathChange</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathError</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
<td>38</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BackupAssign</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathQuery</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

This is a sample output from the show mpls traffic-eng counters signaling command using the tunnel number argument, which displays statistics for the input tunnel number:

RP/0/RP0/CPU0:router# show mpls traffic-eng counters signaling 200

Tunnel Head: tunnel-te200

Cumulative Tunnel Counters:

<table>
<thead>
<tr>
<th>Signalling Events</th>
<th>Recv</th>
<th>Xmit</th>
<th>Recv</th>
<th>Xmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>PathCreate</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>PathChange</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathError</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BackupAssign</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathQuery</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Destination 3.3.3.3

Cumulative counters

<table>
<thead>
<tr>
<th>Signalling Events</th>
<th>Recv</th>
<th>Xmit</th>
<th>Recv</th>
<th>Xmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>PathCreate</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>PathChange</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathError</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BackupAssign</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathQuery</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

S2L LSP ID: 3 Sub-Grp ID: 0 Destination: 3.3.3.3

<table>
<thead>
<tr>
<th>Signalling Events</th>
<th>Recv</th>
<th>Xmit</th>
<th>Recv</th>
<th>Xmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>PathCreate</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>PathChange</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathError</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BackupAssign</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathQuery</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
This table describes the significant fields shown in the display.

**Table 30: show mpls traffic-eng counters signaling Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Head</td>
<td>Tunnel head identifier.</td>
</tr>
<tr>
<td>Match Resv Create</td>
<td>Number of RSVP Reservation create messages received.</td>
</tr>
<tr>
<td>Sender Create</td>
<td>Number of Sender Create messages sent by TE to RSVP.</td>
</tr>
<tr>
<td>Path Error</td>
<td>Number of RSVP Path Error messages received.</td>
</tr>
<tr>
<td>Match Resv Change</td>
<td>Number of RSVP Reservation change messages received.</td>
</tr>
<tr>
<td>Sender Modify</td>
<td>Number of Sender Modify messages sent by TE to RSVP.</td>
</tr>
<tr>
<td>Path Change</td>
<td>Number of RSVP Path Change messages received.</td>
</tr>
<tr>
<td>Match Resv Delete</td>
<td>Number of RSVP Reservation delete messages received.</td>
</tr>
<tr>
<td>Sender Delete</td>
<td>Number of Sender Delete messages sent by TE to RSVP.</td>
</tr>
<tr>
<td>Path Delete</td>
<td>Number of RSVP Path Delete messages received.</td>
</tr>
<tr>
<td>Total</td>
<td>Total signaling messages received from RSVP.</td>
</tr>
<tr>
<td>Unknown</td>
<td>Unknown messages include fast reroute events and internal messages related to process restart.</td>
</tr>
</tbody>
</table>

This is sample output from the `show mpls traffic-eng counters soft-preemption` command, which displays statistics for the soft preempted LSPs:

```
RP/0/RP0/CPU0:router#show mpls traffic-eng counters soft-preemption

Soft Preemption Global Counters:
Last Cleared: Never
Preemption Node Stats:
  Number of soft preemption events: 1
  Number of soft preempted LSPs: 1
  Number of soft preempted LSPs that timed out: 0
  Number of soft preempted LSPs that were torn down: 0
  Number of soft preempted LSPs that were fast rerouted: 0
  Minimum Time in Soft Preemption Pending State (sec): 0
  Maximum Time in Soft Preemption Pending State (sec): 0
  Average Time in Soft Preemption Pending State (sec): 0
Headend Stats:
  Number of soft preempted LSPs: 1
  Number of reoptimized soft preempted headend-LSPs: 0
  Number of path protected switchover soft preempted headend-LSPs: 0
  Number of torn down soft preempted headend-LSPs: 0
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear mpls traffic-eng counters signaling, on page 171</td>
<td>Clears the counters for MPLS-TE tunnels.</td>
</tr>
<tr>
<td>clear mpls traffic-eng fast-reroute log, on page 174</td>
<td>Clears the counters for MPLS-TE tunnels.</td>
</tr>
<tr>
<td>soft-preemption</td>
<td>Enables soft-preemption on a head-end for the MPLS TE tunnel.</td>
</tr>
</tbody>
</table>
show mpls traffic-eng ds-te te-class

To display the Diff-Serv TE-class map in use, use the `show mpls traffic-eng ds-te te-class` command in EXEC mode.

```text
show show mpls traffic-eng ds-te te-class
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Note**

TE-class is used only in IETF DS-TE mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following shows a sample output from the `show mpls traffic-eng ds-te te-class` command:

```text
RP/0/RP0/CPU0:router# show mpls traffic-eng ds-te te-class

  te-class 0: class-type 0 priority 7 status default
  te-class 1: class-type 1 priority 7 status default
  te-class 2: unused
  te-class 3: unused
  te-class 4: class-type 0 priority 0 status default
  te-class 5: class-type 1 priority 0 status default
  te-class 6: unused
  te-class 7: unused
```
This table describes the significant fields shown in the display.

*Table 31: show mpls traffic-eng ds-te te-class Command Field Descriptions*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>te-class</td>
<td>TE-class map, pair of class-type, and priority.</td>
</tr>
<tr>
<td>class-type</td>
<td>class-type of the tunnel.</td>
</tr>
<tr>
<td>status</td>
<td>Source of the TE-class map, either default or user configured.</td>
</tr>
</tbody>
</table>
show mpls traffic-eng forwarding

To display forwarding information on tunnels that were admitted locally, use the `show mpls traffic-eng forwarding` command in EXEC mode.

```
show mpls traffic-eng forwarding [backup-name tunnel-name] [signalled-name tunnel-name] [source source-address] [tunnel-id tunnel-id] [interface {in | inout | out} type interface-path-id] [detail]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup-name tunnel-name</td>
<td>(Optional) Restricts tunnels with this backup tunnel name.</td>
</tr>
<tr>
<td>signalled-name tunnel-name</td>
<td>(Optional) Restricts tunnels with this signalled tunnel name.</td>
</tr>
<tr>
<td>source source-address</td>
<td>(Optional) Restricts tunnels for this specified tunnel source IPv4 address.</td>
</tr>
<tr>
<td>tunnel-id tunnel-id</td>
<td>(Optional) Restricts tunnels for this tunnel identifier. Range for the <code>tunnel-id</code> argument is from 0 to 65535.</td>
</tr>
<tr>
<td>interface</td>
<td>(Optional) Displays information on the specified interface.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or a virtual interface.</td>
</tr>
<tr>
<td>in</td>
<td>Displays information for the input interface.</td>
</tr>
<tr>
<td>inout</td>
<td>Displays information for either the input or output interface.</td>
</tr>
<tr>
<td>out</td>
<td>Displays information for the output interface.</td>
</tr>
<tr>
<td>p2p</td>
<td>(Optional) Displays only Point-to-Point (P2P) information.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays detailed forwarding information.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values
Command Modes

**EXEC**

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Task ID

**Task ID**

<table>
<thead>
<tr>
<th>Operations Task ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>read</td>
</tr>
</tbody>
</table>

Examples

The following shows a sample output from the `show mpls traffic-eng forwarding` command:

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

Tue Sep 15 14:22:39.609 UTC P2P tunnels

<table>
<thead>
<tr>
<th>Tunnel ID</th>
<th>Ingress IF</th>
<th>Egress IF</th>
<th>In lbl</th>
<th>Out lbl</th>
<th>Backup tunnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.2.2 2_2</td>
<td>Gi0/0/0/3</td>
<td>Gi0/0/0/4</td>
<td>16004</td>
<td>16020</td>
<td>unknown</td>
</tr>
<tr>
<td>6.6.6.6 1_23</td>
<td>-</td>
<td>Gi0/0/0/3</td>
<td>16000</td>
<td>3</td>
<td>tt1300</td>
</tr>
<tr>
<td>6.6.6.6 1100_9</td>
<td>-</td>
<td>Gi0/0/0/3</td>
<td>16002</td>
<td>16001</td>
<td>unknown</td>
</tr>
<tr>
<td>6.6.6.6 1200_9</td>
<td>-</td>
<td>Gi0/0/0/3</td>
<td>16001</td>
<td>16000</td>
<td>unknown</td>
</tr>
<tr>
<td>6.6.6.6 1300_2</td>
<td>-</td>
<td>Gi0/0/0/4</td>
<td>16005</td>
<td>16021</td>
<td>unknown</td>
</tr>
<tr>
<td>6.6.6.6 1400_9</td>
<td>-</td>
<td>Gi0/0/0/3</td>
<td>16003</td>
<td>16002</td>
<td>unknown</td>
</tr>
</tbody>
</table>
```

This table describes the significant fields shown in the display.

**Table 32: show mpls traffic-eng forwarding Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TUNNEL ID</td>
<td>Tunnel identification.</td>
</tr>
<tr>
<td>Ingress IF</td>
<td>Ingress interface of the tunnel.</td>
</tr>
<tr>
<td>Egress IF</td>
<td>Egress interface of the tunnel.</td>
</tr>
<tr>
<td>In lbl</td>
<td>Incoming label associated with the tunnel.</td>
</tr>
<tr>
<td>Out lbl</td>
<td>Outgoing label associated with the tunnel.</td>
</tr>
<tr>
<td>Backup tunnel</td>
<td>Fast Reroute backup tunnel</td>
</tr>
</tbody>
</table>
show mpls traffic-eng forwarding-adjacency

To display forwarding-adjacency information for an IPv4 address, use the `show mpls traffic-eng forwarding-adjacency` command in EXEC mode.

**Syntax Description**

`IP-address` (Optional) Destination IPv4 address for forwarding adjacency.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

This is a sample output from the `show mpls traffic-eng forwarding-adjacency` command:

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

destination 3.3.3.3 has 1 tunnels
tunnel-te1 (traffic share 0, next-hop 3.3.3.3)
(Adjacency Announced: yes, holdtime 0)
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>forwarding-adjacency, on page 198</td>
<td>Configures an MPLS-TE forwarding adjacency.</td>
</tr>
</tbody>
</table>
show mpls traffic-eng igp-areas

To display MPLS-TE internal area storage, use the show mpls traffic-eng igp-areas command in EXEC mode.

show mpls traffic-eng igp-areas  [detail]

Syntax Description

<table>
<thead>
<tr>
<th>Detail</th>
<th>(Optional) Displays detailed information about the configured MPLS-TE igp-areas and communication statistics with IGPs.</th>
</tr>
</thead>
</table>

Command Default

No default behavior or values

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

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

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
</tbody>
</table>

Examples

This table describes the significant fields shown in the display.

Table 33: show mpls traffic-eng igp-areas Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global router-id</td>
<td>Global router ID on this node.</td>
</tr>
<tr>
<td>IGP ID</td>
<td>IGP System ID.</td>
</tr>
<tr>
<td>area</td>
<td>IGP area.</td>
</tr>
<tr>
<td>TE index</td>
<td>Internal index in the IGP area table.</td>
</tr>
<tr>
<td>IGP config for TE</td>
<td>Whether the IGP configuration is complete or missing.</td>
</tr>
</tbody>
</table>
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.

```plaintext
show mpls traffic-eng link-management admission-control [interface type interface-path-id]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>(Optional) Displays information on the specified interface.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note**

Use the `show interfaces` command to see a list of all possible interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following shows a sample output from the `show mpls traffic-eng link-management admission-control` command:

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

System Information:
  Tunnels Count : 2
  Tunnels Selected : 2
Bandwidth descriptor legend:
  B0 = bw from pool 0, B1 = bw from pool 1, R = bw locked, H = bw held

TUNNEL ID | UP IF | DOWN IF | PRI STATE | BW (kbits/sec) |
----------|-------|---------|-----------|----------------|
```
This table describes the significant fields shown in the display.

Table 34: show mpls traffic-eng link-management admission-control Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnels Count</td>
<td>Total number of tunnels admitted.</td>
</tr>
<tr>
<td>Tunnels Selected</td>
<td>Number of tunnels displayed.</td>
</tr>
<tr>
<td>Bandwidth descriptor legend</td>
<td>BW pool type and status displayed with the tunnel entry. Shown as RG (Locked BW in global pool) in the preceding sample output.</td>
</tr>
<tr>
<td>TUNNEL ID</td>
<td>Tunnel identification.</td>
</tr>
<tr>
<td>UP IF</td>
<td>Upstream interface used by the tunnel.</td>
</tr>
<tr>
<td>DOWN IF</td>
<td>Downstream interface used by the tunnel.</td>
</tr>
<tr>
<td>PRI</td>
<td>Tunnel setup priority and hold priority.</td>
</tr>
<tr>
<td>STATE</td>
<td>Tunnel admission status.</td>
</tr>
<tr>
<td>BW (kbps)</td>
<td>Tunnel bandwidth in kilobits per second. If an R follows the bandwidth number, the bandwidth is reserved. If an H follows the bandwidth number, the bandwidth is temporarily being held for a Path message. If a G follows the bandwidth number, the bandwidth is from the global pool. If an S follows the bandwidth number the bandwidth is from the sub-pool.</td>
</tr>
</tbody>
</table>

The following shows a sample output from the `show mpls traffic-eng link-management interface` command:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng link-management interface pos 0/2/0/1

System Information::
   Links Count: 1

Link ID:: POS0/2/0/1 (35.0.0.5)
   Local Intf ID: 7
   Link Status:
      Link Label Type : PSC (inactive)
      Physical BW : 155520 kbits/sec
      BCID : RDM
      Max Reservable BW : 0 kbits/sec (reserved: 100% in, 100% out)
      BC0 (Res. Global BW): 0 kbits/sec (reserved: 100% in, 100% out)
      BC1 (Res. Sub BW) : 0 kbits/sec (reserved: 100% in, 100% out)
      MPLS-TE Link State : MPLS-TE on, RSVP on
      Inbound Admission : allow-all
      Outbound Admission : allow-if-room
      IGP Neighbor Count : 0
      Max Res BW (RDM) : 0 kbits/sec
      BC0 (RDM) : 0 kbits/sec
      BC1 (RDM) : 0 kbits/sec
```
show mpls traffic-eng link-management admission-control

Max Res BW (MAM) : 0 kbits/sec
BC0 (MAM) : 0 kbits/sec
BC1 (MAM) : 0 kbits/sec
Admin Weight : 1 (OSPF), 10 (ISIS)
Attributes : 0x5 (name-based)
Flooding Status: (1 area)
IGP Area[1]: ospf 100 area 0, not flooded
(Reason: Interface has been administratively disabled)

This table describes the significant fields shown in the display.

Table 35: show mpls traffic-eng link-management interface Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Links Count</td>
<td>Number of links configured for MPLS-TE.</td>
</tr>
<tr>
<td>Link ID</td>
<td>Index of the link described.</td>
</tr>
<tr>
<td>Local IntfID</td>
<td>Local interface ID.</td>
</tr>
<tr>
<td>Link Label Type</td>
<td>Label type of the link, for instance: PSC(^{11}), TDM(^ {12}), FSC(^ {13}).</td>
</tr>
<tr>
<td>Physical BW</td>
<td>Link bandwidth capacity (in kilobits per second).</td>
</tr>
<tr>
<td>BCID</td>
<td>Bandwidth constraint model ID (RDM or MAM).</td>
</tr>
<tr>
<td>Max Reservable BW</td>
<td>Maximum reservable bandwidth on this link.</td>
</tr>
<tr>
<td>BC0 (Res. Global BW)</td>
<td>Bandwidth constraint value for class-type 0.</td>
</tr>
<tr>
<td>BC1 (Res. Sub BW)</td>
<td>Bandwidth constraint value for class-type 1.</td>
</tr>
<tr>
<td>MPLS-TE Link State</td>
<td>Status of the link MPLS-TE-related functions.</td>
</tr>
<tr>
<td>Inbound Admission</td>
<td>Link admission policy for incoming tunnels.</td>
</tr>
<tr>
<td>Outbound Admission</td>
<td>Link admission policy for outgoing tunnels.</td>
</tr>
<tr>
<td>IGP Neighbor Count</td>
<td>IGP neighbors directly reachable over this link.</td>
</tr>
<tr>
<td>Max Res BW (RDM)</td>
<td>Maximum reservable bandwidth on this link for RDM.</td>
</tr>
<tr>
<td>BC0 (RDM)</td>
<td>Bandwidth constraint value for RDM.</td>
</tr>
<tr>
<td>BC1 (RDM)</td>
<td>Bandwidth constraint value for RDM.</td>
</tr>
<tr>
<td>Admin Weight</td>
<td>Administrative weight associated with this link.</td>
</tr>
<tr>
<td>Attributes</td>
<td>Interface attributes referring to one or more affinity names.</td>
</tr>
<tr>
<td>IGP Area[1]</td>
<td>IGP type and area and level used for TE flooding.</td>
</tr>
</tbody>
</table>

\(^{11}\) PSC = Packet switch capable.
\(^{12}\) TDM = Time-division multiplexing.
\(^{13}\) FSC = Fiber switch capable.
show mpls traffic-eng link-management advertisements

To display local link information that MPLS-TE link management is currently flooding into the global TE topology, use the **show mpls traffic-eng link-management advertisements** command in EXEC mode.

**show mpls traffic-eng link-management advertisements**

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

**Command Default**
No default behavior or values

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

The **show mpls traffic-eng link-management advertisements** command has two output formats depending on the Diff-Serv TE Mode: one for prestandard mode and one for IETF mode.

The SRLG values are advertised for the link.

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

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

Link ID: 0 (GigabitEthernet0/2/0/1)
  Link IP Address : 12.9.0.1
  O/G Intf ID : 28
  Designated Router : 12.9.0.2
  TE Metric : 1
  IGF Metric : 1
  Physical BW : 1000000 kbits/sec
  BCID : RDM
  Max Reservable BW : 10000 kbits/sec
  Res Global BW : 10000 kbits/sec
  Res Sub BW : 0 kbits/sec
  SRLGs : 10, 20

  Downstream:
```

---

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
</tbody>
</table>

---

**MPLS Command Reference for Cisco NCS 6000 Series Routers**

299
This table describes the significant fields shown in the display.

**Table 36: show mpls traffic-eng link-management advertisements Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link ID</td>
<td>Index of the link described.</td>
</tr>
<tr>
<td>Link IP Address</td>
<td>Local IP address of the link.</td>
</tr>
<tr>
<td>TE Metric</td>
<td>Metric value for the TE link configured under MPLS-TE.</td>
</tr>
<tr>
<td>IGP Metric</td>
<td>Metric value for the TE link configured under IGP.</td>
</tr>
<tr>
<td>Physical BW</td>
<td>Link bandwidth capacity (in kilobits per second).</td>
</tr>
<tr>
<td>BCID</td>
<td>Bandwidth constraint model ID (RDM or MAM).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Max Reservable BW</td>
<td>Maximum reservable bandwidth on this link.</td>
</tr>
<tr>
<td>Res Global BW</td>
<td>Maximum reservable of global pool/BC0 bandwidth on this link.</td>
</tr>
<tr>
<td>Res Sub BW</td>
<td>Reservable sub-bandwidth for sub-pool /BC1 bandwidth on this link.</td>
</tr>
<tr>
<td>SRLGs(^{14})</td>
<td>Links that share a common fiber or a common physical attribute. If one link fails, other links in the group may also fail. Links in the group have a shared risk.</td>
</tr>
<tr>
<td>Downstream</td>
<td>Direction of the LSP path message.</td>
</tr>
<tr>
<td>Reservable BW([x])</td>
<td>Bandwidth available for reservations in the global TE topology and subpools.</td>
</tr>
<tr>
<td>Attribute Flags</td>
<td>Link attribute flags being flooded.</td>
</tr>
<tr>
<td>Attribute Names</td>
<td>Name of the affinity attribute of a link.</td>
</tr>
<tr>
<td>BC0</td>
<td>Bandwidth constraint value for class-type 0</td>
</tr>
<tr>
<td>BC1</td>
<td>Bandwidth constraint value for class-type 1</td>
</tr>
<tr>
<td>TE-class [index]</td>
<td>TE-class configured on this router at given index (mapping of class-type and priority), shows available bandwidth in that class.</td>
</tr>
</tbody>
</table>

\(^{14}\) SRLGs = Shared Risk Link Groups.
show mpls traffic-eng link-management bandwidth-allocation

To display current local link information, use the show mpls traffic-eng link-management bandwidth-allocation command in EXEC mode.

show mpls traffic-eng link-management bandwidth-allocation [interface type interface-path-id]

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>(Optional) Displays information on the specified interface.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or a virtual interface.</td>
</tr>
</tbody>
</table>

Note: Use the show interfaces command to see a list of all possible interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

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

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

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
</tbody>
</table>

Examples

The following shows a sample output from the show mpls traffic-eng link-management bandwidth-allocation command:

RP/0/RP0/CPU0:router# show mpls traffic-eng link bandwidth-allocation interface POS 0/2/0/1

System Information:
  Links Count : 4
  Bandwidth Hold time : 15 seconds
Link ID:: POS0/2/0/1 (7.2.2.1)
Local Intf ID: 4

Link Status:
- Link Label Type : PSC
- Physical BW : 155520 kbits/sec
- BCID : MAM
- Max Reservable BW : 1000 kbits/sec (reserved: 0% in, 0% out)
- BC0 : 600 kbits/sec (reserved: 2% in, 2% out)
- BC1 : 400 kbits/sec (reserved: 0% in, 0% out)
- MPLS-TE Link State : MPLS-TE on, RSVP on, admin-up, flooded
- Inbound Admission : allow-all
- Outbound Admission : allow-if-room
- IGP Neighbor Count : 2
- BW Descriptors : 1 (including 0 BC1 descriptors)
- Admin Weight : 1 (OSPF), 10 (ISIS)

Up Thresholds : 15 30 45 60 75 80 85 90 95 96 98 99 100 (default)
Down Thresholds : 100 99 98 97 96 95 90 85 80 75 60 45 30 15 (default)

Bandwidth Information:

Downstream BC0 (kbits/sec):

<table>
<thead>
<tr>
<th>KEEP PRIORITY</th>
<th>BW HELD</th>
<th>BW TOTAL HELD</th>
<th>BW LOCKED</th>
<th>BW TOTAL LOCKED</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>10</td>
</tr>
</tbody>
</table>

Downstream BC1 (kbits/sec):

<table>
<thead>
<tr>
<th>KEEP PRIORITY</th>
<th>BW HELD</th>
<th>BW TOTAL HELD</th>
<th>BW LOCKED</th>
<th>BW TOTAL LOCKED</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

This table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Links Count</td>
<td>Number of links configured for MPLS-TE.</td>
</tr>
<tr>
<td>Bandwidth Hold Time</td>
<td>Time, in seconds, that bandwidth can be held.</td>
</tr>
<tr>
<td>Link ID</td>
<td>Interface name and IP address of the link.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Link Label type</td>
<td>Label type of the link, for example:</td>
</tr>
<tr>
<td></td>
<td>• PSC(^{15})</td>
</tr>
<tr>
<td></td>
<td>• TDM(^{16})</td>
</tr>
<tr>
<td></td>
<td>• FSC(^{17})</td>
</tr>
<tr>
<td>Physical BW</td>
<td>Link bandwidth capacity (in bits per second).</td>
</tr>
<tr>
<td>BCID</td>
<td>Bandwidth constraint model ID (RDM or MAM).</td>
</tr>
<tr>
<td>Max Reservable BW</td>
<td>Maximum reservable bandwidth on this link.</td>
</tr>
<tr>
<td>BC0</td>
<td>Maximum RSVP bandwidth in BC0.</td>
</tr>
<tr>
<td>BC1</td>
<td>Maximum RSVP bandwidth in BC1.</td>
</tr>
<tr>
<td>BW Descriptors</td>
<td>Number of bandwidth allocations on this link.</td>
</tr>
<tr>
<td>MPLS-TE Link State</td>
<td>Status of the link MPLS-TE-related functions.</td>
</tr>
<tr>
<td>Inbound Admission</td>
<td>Link admission policy for incoming tunnels.</td>
</tr>
<tr>
<td>Outbound Admission</td>
<td>Link admission policy for outgoing tunnels.</td>
</tr>
<tr>
<td>IGP Neighbor Count</td>
<td>IGP neighbors directly reachable over this link.</td>
</tr>
<tr>
<td>BW Descriptors</td>
<td>Internal bandwidth descriptors created when tunnels are admitted.</td>
</tr>
<tr>
<td>Admin Weight</td>
<td>Administrative weight associated with this link.</td>
</tr>
<tr>
<td>Up Thresholds</td>
<td>Threshold values used to determine link advertisement when available bandwidth increases.</td>
</tr>
<tr>
<td>Down Thresholds</td>
<td>Threshold values used to determine link advertisement when available bandwidth decreases.</td>
</tr>
</tbody>
</table>

\(^{15}\) PSC = Packet switch capable.  
\(^{16}\) TDM = Time-division multiplexing.  
\(^{17}\) FSC = Fiber switch capable.
show mpls traffic-eng link-management bfd-neighbors

To display TE-enabled Bidirectional Forwarding Detection (BFD) neighbors, use the `show mpls traffic-eng link-management bfd-neighbors` command in EXEC mode.

```
show mpls traffic-eng link-management bfd-neighbors [interface type interface-path-id]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface</code></td>
<td>(Optional) Displays information about the specified interface.</td>
</tr>
<tr>
<td><code>type</code></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note**: Use the `show interfaces` command to see a list of all possible interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**: No default behavior or values

**Command Modes**: EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**: The following shows a sample output from the `show mpls traffic-eng link-management bfd-neighbors` command:

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

Link ID:: POS0/6/0/0
BFD Neighbor Address: 7.3.3.1, State: Up
Link ID:: POS0/6/0/1
No BFD Neighbor
Link ID:: POS0/6/0/2
BFD Neighbor Address: 7.4.4.1, State: Down
```
This table describes the significant fields shown in the display.

**Table 38: show mpls traffic-eng link-management bfd Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link ID</td>
<td>Link by which the neighbor is reached.</td>
</tr>
<tr>
<td>BFD Neighbor Address</td>
<td>Neighbor address and Up/Down state.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bfd fast-detect (MPLS-TE)</td>
<td>Enables BFD for communication failure detection.</td>
</tr>
<tr>
<td>bfd minimum-interval (MPLS-TE)</td>
<td>Sets the BFD interval.</td>
</tr>
<tr>
<td>bfd multiplier (MPLS-TE)</td>
<td>Sets the BFD multiplier.</td>
</tr>
</tbody>
</table>
show mpls traffic-eng link-management igp-neighbors

To display Interior Gateway Protocol (IGP) neighbors, use the `show mpls traffic-eng link-management igp-neighbors` command in EXEC mode.

```
show mpls traffic-eng link-management igp-neighbors  [igp-id  {isis  isis-address | ospf  ospf-id}  
[interface  type  interface-path-id  IP-address]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igp-id</td>
<td>(Optional) Displays the IGP neighbors that are using a specified IGP identification.</td>
</tr>
<tr>
<td>isis  isis-address</td>
<td>Displays the specified Intermediate System-to-Intermediate System (IS-IS) neighbor system ID when neighbors are displayed by IGP ID.</td>
</tr>
<tr>
<td>ospf  ospf-id</td>
<td>Displays the specified Open Shortest Path first (OSPF) neighbor OSPF router ID when neighbors are displayed by IGP ID.</td>
</tr>
<tr>
<td>interface</td>
<td>(Optional) Displays information on the specified interface.</td>
</tr>
<tr>
<td>type</td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or a virtual interface.</td>
</tr>
</tbody>
</table>

**Note**

Use the `show interfaces` command to see a list of all possible interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-address</td>
<td>(Optional) IGP neighbors that are using a specified IGP IP address.</td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following shows a sample output from the `show mpls traffic-eng link-management igp-neighbors` command:
show mpls traffic-eng link-management igp-neighbors

Link ID: POS0/7/0/0
No Neighbors

Link ID: POS0/7/0/1
Neighbor ID: 10.90.90.90 (area: ospf area 0, IP: 10.15.12.2)

This table describes the significant fields shown in the display.

Table 39: show mpls traffic-eng link-management igp-neighbors Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link ID</td>
<td>Link by which the neighbor is reached.</td>
</tr>
<tr>
<td>Neighbor ID</td>
<td>IGP identification information for the neighbor.</td>
</tr>
</tbody>
</table>
show mpls traffic-eng link-management interfaces

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

**show mpls traffic-eng link-management interfaces [type interface-path-id]**

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>type</strong></td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><strong>interface-path-id</strong></td>
<td>Physical interface or a virtual interface.</td>
</tr>
</tbody>
</table>

**Note**

Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You cannot configure more than 250 links under MPLS-TE.

**Examples**

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

```
RP/0/RP0/CPU0:router# show mpls traffic-eng link-management interfaces GigabitEthernet0/1/1/0

System Information::
  Links Count : 16 (Maximum Links Supported 800)
Link ID:: GigabitEthernet0/1/1/0 (10.12.110.1)
  Local Intf ID: 22
  Link Status:
    Link Label Type : PSC
    Physical BW : 1000000 kbits/sec
    BCID : RDM
    Max Reservable BW : 743346 kbits/sec (reserved: 40% in, 40% out)
    BC0 (Res. Global BW) : 743346 kbits/sec (reserved: 40% in, 40% out)
```
BC1 (Res. Sub BW) : 0 kbits/sec (reserved: 100% in, 100% out)
MPLS TE Link State : MPLS TE on, RSVP on, admin-up
IGP Neighbor Count : 1
Max Res BW (RDM) : 900000 kbits/sec
BC0 (RDM) : 900000 kbits/sec
BC1 (RDM) : 0 kbits/sec
Max Res BW (MAM) : 0 kbits/sec
BC0 (MAM) : 0 kbits/sec
BC1 (MAM) : 0 kbits/sec
Attributes : 0x0
Ext Admin Group :
Length : 256 bits
Value : 0x::
Attribute Names :
Flooding Status: (1 area)
IGP Area[1]: IS-IS 0 level 2, flooded
Nbr: ID 0000.0000.0002.00, IP 10.12.110.2 (Up)
Admin weight: not set (TE), 10 (IGP)
Lockout Status: Never

This table describes the significant fields shown in the display.

Table 40: show mpls traffic-eng link-management interfaces Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Links Count</td>
<td>Number of links configured for MPLS-TE. Maximum number of links supported is 100.</td>
</tr>
<tr>
<td>Link ID</td>
<td>Link identification index.</td>
</tr>
<tr>
<td>Link Label Type</td>
<td>Label type assigned to the link.</td>
</tr>
<tr>
<td>Physical Bandwidth</td>
<td>Link bandwidth capacity (in kilobits per second).</td>
</tr>
<tr>
<td>BCID</td>
<td>Bandwidth constraint model ID (RDM or MAM).</td>
</tr>
<tr>
<td>Max Reservable BW</td>
<td>Maximum reservable bandwidth on this link.</td>
</tr>
<tr>
<td>BC0</td>
<td>Reservable bandwidth (in kbps) on this link in BC0.</td>
</tr>
<tr>
<td>BC1</td>
<td>Reservable bandwidth (in kbps) on this link in BC1.</td>
</tr>
<tr>
<td>Attributes</td>
<td>TE link attribute in hexadecimal.</td>
</tr>
<tr>
<td>Attribute Names</td>
<td>Name of the affinity attribute of a link.</td>
</tr>
<tr>
<td>MPLS-TE Link State</td>
<td>Status of the MPLS link.</td>
</tr>
<tr>
<td>Inbound Admission</td>
<td>Link admission policy for inbound tunnels.</td>
</tr>
<tr>
<td>Outbound Admission</td>
<td>Link admission policy for outbound tunnels.</td>
</tr>
<tr>
<td>IGP Neighbor Count</td>
<td>IGP neighbors directly reachable over this link.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>Admin. Weight</td>
<td>Administrative weight associated with this link.</td>
</tr>
<tr>
<td>Flooding Status</td>
<td>Status for each configured area or Flooding status for the configured area.</td>
</tr>
<tr>
<td>IGP Area</td>
<td>IGP type and area and level used for TE flooding.</td>
</tr>
</tbody>
</table>

18 IGP = Interior Gateway Protocol.
show mpls traffic-eng link-management statistics

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

`show mpls traffic-eng link-management statistics [summary | interface type interface-path-id]`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>(Optional) Displays the statistics summary.</td>
</tr>
<tr>
<td>interface</td>
<td>(Optional) Displays the interface for which information is requested.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note** Use the `show interfaces` command to see a list of all possible interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

The `show mpls traffic-eng link-management statistics` command displays resource and configuration information for all configured interfaces.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following shows a sample output from the `show mpls traffic-eng link-management statistics` command using the `summary` keyword:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng link-management statistics summary
LSP Admission Statistics:
```
Table 41: show mpls traffic-eng link-management statistics summary Command Field Descriptions, on page 313 describes the significant fields shown in the display.

Table 41: show mpls traffic-eng link-management statistics summary Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>Path information.</td>
</tr>
<tr>
<td>Resv</td>
<td>Reservation information.</td>
</tr>
<tr>
<td>Setup Requests</td>
<td>Number of requests for a setup.</td>
</tr>
<tr>
<td>Setup Admits</td>
<td>Number of admitted setups.</td>
</tr>
<tr>
<td>Setup Rejects</td>
<td>Number of rejected setups.</td>
</tr>
<tr>
<td>Setup Errors</td>
<td>Number of setup errors.</td>
</tr>
<tr>
<td>Tear Requests</td>
<td>Number of tear requests.</td>
</tr>
<tr>
<td>Tear Preempts</td>
<td>Number of paths torn down due to preemption.</td>
</tr>
<tr>
<td>Tear Errors</td>
<td>Number of tear errors.</td>
</tr>
</tbody>
</table>
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.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

You cannot configure more than 250 links for MPLS-TE/FRR.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

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

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

System Information::
    Links Count : 6 (Maximum Links Supported 100)
    Flooding System : enabled
    IGP Areas Count : 2

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

IGP Area[1]:  isis  level-2
    Flooding Protocol : ISIS
    Flooding Status : flooded
    Periodic Flooding : enabled (every 180 seconds)
    Flooded Links : 4
    IGP System ID : 0000.0000.0002.00
    MPLS-TE Router ID : 20.20.20.20
    IGP Neighbors : 8

IGP Area[2]:  ospf  area 0
    Flooding Protocol : OSPF
```
Flooding Status : flooded
Periodic Flooding : enabled (every 180 seconds)
Flooded Links : 4
IGP System ID : 20.20.20.20
MPLS-TE Router ID : 20.20.20.20
IGP Neighbors : 8

This table describes the significant fields shown in the display.

Table 42: show mpls traffic-eng link-management summary Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Links Count</td>
<td>Number of links configured for MPLS-TE. Maximum number of links supported is 100.</td>
</tr>
<tr>
<td>Flooding System</td>
<td>Enable status of the MPLS-TE flooding system.</td>
</tr>
<tr>
<td>IGP Areas Count</td>
<td>Number of IGP(^{19}) areas described.</td>
</tr>
<tr>
<td>IGP Area</td>
<td>IGP type and area and level used for TE flooding.</td>
</tr>
<tr>
<td>Flooding Protocol</td>
<td>IGP flooding information for this area.</td>
</tr>
<tr>
<td>Flooding Status</td>
<td>Status of flooding for this area.</td>
</tr>
<tr>
<td>Periodic Flooding</td>
<td>Status of periodic flooding for this area.</td>
</tr>
<tr>
<td>Flooded Links</td>
<td>Links that were flooded.</td>
</tr>
<tr>
<td>IGP System ID</td>
<td>IGP for the node associated with this area.</td>
</tr>
<tr>
<td>MPLS-TE Router ID</td>
<td>MPLS-TE router ID for this node.</td>
</tr>
<tr>
<td>IGP Neighbors</td>
<td>Number of reachable IGP neighbors associated with this area.</td>
</tr>
</tbody>
</table>

\(^{19}\) IGP = Interior Gateway Protocol.
**show mpls traffic-eng maximum tunnels**

To display the maximum number of MPLS-TE tunnels that you can configure, use the **show mpls traffic-eng maximum tunnels** command in EXEC mode.

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

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

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

Maximum Global Tunnel Count:

<table>
<thead>
<tr>
<th>Maximum</th>
<th>Current Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>4096</td>
<td>2</td>
</tr>
</tbody>
</table>

Maximum Global Destination Count:

<table>
<thead>
<tr>
<th>Maximum</th>
<th>Current Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>4096</td>
<td>2</td>
</tr>
</tbody>
</table>

Maximum AutoTunnel Backup Count:

<table>
<thead>
<tr>
<th>Maximum</th>
<th>Current Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>122</td>
</tr>
</tbody>
</table>
```
This is sample output of the automatic mesh tunnels from the `show mpls traffic-eng maximum tunnels` command:

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

Maximum Global Tunnel Count:

<table>
<thead>
<tr>
<th>Maximum</th>
<th>Current Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>4096</td>
<td>12</td>
</tr>
</tbody>
</table>

Maximum Static Tunnel Count:

<table>
<thead>
<tr>
<th>Maximum</th>
<th>Current Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>4096</td>
<td>8</td>
</tr>
</tbody>
</table>

Maximum Auto-tunnel Mesh Count:

<table>
<thead>
<tr>
<th>Maximum</th>
<th>Current Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>3</td>
</tr>
</tbody>
</table>

Maximum P2MP Tunnel Count:

<table>
<thead>
<tr>
<th>Maximum</th>
<th>Current Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>500</td>
<td>1</td>
</tr>
</tbody>
</table>

Maximum Global Destination Count:

<table>
<thead>
<tr>
<th>Maximum</th>
<th>Current Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>4096</td>
<td>13</td>
</tr>
</tbody>
</table>

Maximum GMPLS-UNI Tunnel Count:

<table>
<thead>
<tr>
<th>Maximum</th>
<th>Current Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>500</td>
<td>39</td>
</tr>
</tbody>
</table>

Table 43: `show mpls traffic-eng maximum tunnels` Command Field Descriptions, on page 317 describes the significant fields shown in the display.

Table 43: `show mpls traffic-eng maximum tunnels` Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum P2MP Tunnel Count</td>
<td>Maximum number of P2MP tunnels that can be configured.</td>
</tr>
<tr>
<td>Maximum Global Destination Count</td>
<td>Maximum number of tunnel destinations that can be configured.</td>
</tr>
<tr>
<td>Maximum</td>
<td>Table heading for the maximum number in each category.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Current Count</td>
<td>Table heading for the current count in each category.</td>
</tr>
<tr>
<td>Maximum AutoTunnel Backup Count</td>
<td>Maximum number of automatic backup tunnels that can be configured.</td>
</tr>
<tr>
<td>Maximum GMPLS UNI Tunnel Count</td>
<td>Maximum number of Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI) tunnels that can be configured and the current tunnel count.</td>
</tr>
<tr>
<td>Maximum AutoTunnel Mesh Count</td>
<td>Maximum number of automatic mesh tunnels that can be configured.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>maxabs (MPLS-TE), on page 215</code></td>
<td>Specifies the maximum number of tunnel TE interfaces that can be configured.</td>
</tr>
<tr>
<td><code>tunnel-id (auto-tunnel backup), on page 383</code></td>
<td>Configures the range of tunnel interface numbers used for automatic backup tunnels.</td>
</tr>
</tbody>
</table>
show mpls traffic-eng pce peer

To display the status of the path computation element (PCE) peer address and state, use the show mpls traffic-eng pce peer command in EXEC mode.

show mpls traffic-eng pce peer [ { address | all } ]

Syntax Description

address  (Optional) IPv4 peer address for the PCE.

all      (Optional) Displays all the peers for the PCE.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release      Modification
Release 5.0.0    This command was introduced.

Usage Guidelines

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

Task ID

Task Operations ID

mpls-te read

Examples

The following sample output shows the status of both the PCE peer and state:

RP/0/RP0/CPU0:router# show mpls traffic-eng pce peer

PCE Address 202.202.88.8
State Up
  PCEP has been up for: 04:18:31
  Learned through:
    OSPF 1
  Sending KA every 30 s
  Time out peer if no KA received for 120 s
  Tolerance: Minimum KA 10 s
  KA messages rxed 518 txed 517
  PCEReq messages rxed 0, txed 0
  PCERep messages rxed 0, txed 0
  PCEErr messages rxed 0, txed 0
  Last error received: None
  Last error sent: None
  PCE OPEN messages: rxed 1, txed 2
  PCEP session ID: local 0, remote 0

  Average reply time from peer: 0 ms
Minimum reply time from peer: 0 ms
Maximum reply time from peer: 0 ms
0 requests timed out with this peer
Transmit TCP buffer: Current 0, Maximum 12
Receive TCP buffer: Current 0, Maximum 12

This table describes the significant fields shown in the display.

Table 44: show mpls traffic-eng pce peer Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KA</td>
<td>PCEP keepalive.</td>
</tr>
<tr>
<td>Learned through</td>
<td>Learned through is how the peer was learned which is either through a static configuration or an IGP.</td>
</tr>
<tr>
<td>Average reply time from peer</td>
<td>Average reply time for the peer to respond to PCEReq request messages with PCERep response messages.</td>
</tr>
<tr>
<td>Minimum reply time from peer</td>
<td>Minimum reply time for the peer to respond to PCEReq request messages with PCERep response messages.</td>
</tr>
<tr>
<td>Maximum reply time from peer</td>
<td>Maximum reply for the peer to respond to PCEReq request messages with PCERep response messages.</td>
</tr>
<tr>
<td>Transmit TCP buffer</td>
<td>Number of messages that are in the TCP buffer with the peer waiting to be sent or processed locally.</td>
</tr>
<tr>
<td>Receive TCP Buffer</td>
<td>Number of PCEReq messages that timed out waiting for a response from this peer.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear mpls traffic-eng pce, on page 176</td>
<td>Clears the PCE statistics.</td>
</tr>
<tr>
<td>pce address (MPLS-TE), on page 248</td>
<td>Configures the IPv4 self address for a PCE.</td>
</tr>
<tr>
<td>pce peer (MPLS-TE), on page 254</td>
<td>Configures an IPv4 self address for a PCE peer.</td>
</tr>
</tbody>
</table>
show mpls traffic-eng pce tunnels

To display the status of the path computation element (PCE) tunnels, use the `show mpls traffic-eng pce tunnels` command in EXEC mode.

```
show mpls traffic-eng pce tunnels [tunnel-id]
```

**Syntax Description**

```
tunnel-id  (Optional) Tunnel identifier. The range is 0 to 4294967295.
```

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following sample output shows the status of the PCE tunnels:

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

Tunnel : tunnel-te10
  Destination : 205.205.10.10
  State : down, PCE failed to find path

Tunnel : tunnel-te30
  Destination : 3.3.3.3
  State : up
  Current path option: 10, path obtained from dynamically learned PCE 1.2.3.4
  Admin weight : 15
  Hop Count : 3
```

This table describes the significant fields shown in the display.

**Table 45: show mpls traffic-eng pce tunnels Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel</td>
<td>Tunnel number for the MPLS-TE tunnel interface.</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address of the destination of the tunnel.</td>
</tr>
<tr>
<td>State</td>
<td>State of the tunnel. Values are up, down, or admin-down.</td>
</tr>
</tbody>
</table>
show mpls traffic-eng pce tunnels

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin weight</td>
<td>Administrative weight (cost) of the link.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pce address (MPLS-TE), on page 248</td>
<td>Configures the IPv4 self address for a PCE.</td>
</tr>
</tbody>
</table>
show mpls traffic-eng preemption log

To display the log of preemption events, use the `show mpls traffic-eng preemption log` command in EXEC mode.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>log</code></td>
<td>Displays a log of preemption events.</td>
</tr>
</tbody>
</table>

Command Default

None

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 5.1.2</td>
<td>The command output was modified to display the log of soft-preemption over FRR backup tunnels events.</td>
</tr>
</tbody>
</table>

Usage Guidelines

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

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
</tbody>
</table>

This is sample output from the `show mpls traffic-eng preemption log` command displaying the log of preemption events:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng preemption log
Bandwidth Change on GigabitEthernet0/0/0/0
  Old BW (BC0/BC1): 200000/100000, New BW (BC0/BC1): 1000/500 kbps
  BW Overshoot (BC0/BC1): 1000/0 kbps
  Preempted BW (BC0/BC1): 35000/0 kbps; Soft 30000/0 kbps; Hard 5000/0 kbps;
  Preempted 2 tunnels; Soft 1 tunnel; Hard 1 tunnel
------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>TunID</th>
<th>LSP ID</th>
<th>Source</th>
<th>Destination</th>
<th>Preempt Pri</th>
<th>Bandwidth (in kbps)</th>
<th>BW Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10002</td>
<td>192.168.0.1</td>
<td>1.0.0.0</td>
<td>Hard 7/7</td>
<td>5000</td>
<td>BC0</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>192.168.0.1</td>
<td>192.168.0.4</td>
<td>Soft 7/7</td>
<td>30000</td>
<td>BC0</td>
</tr>
</tbody>
</table>
```

This sample output displays the log of soft-preemption over FRR backup tunnels events:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng preemption log
Thu Apr 25 13:12:04.863 EDT
```
Bandwidth Change on GigabitEthernet0/0/0/1 at 04/25/2013 12:56:14
Old BW (BC0/BC1): 200000/100000, New BW (BC0/BC1): 100000/0 kbps
BW Overshoot (BC0/BC1): 30000/0 kbps
Preempted BW (BC0/BC1): 130000/0 kbps; Soft 60000/0 kbps; Hard 0/0 kbps; FRRSoft 70000/0

Preempted 2 tunnel, 2 LSP; Soft 1 tunnel, 1 LSP; Hard 0 tunnels, 0 LSPs; FRRSoft 1 tunnel, 1 LSP

<table>
<thead>
<tr>
<th>TunID</th>
<th>LSP ID</th>
<th>Source</th>
<th>Destination</th>
<th>Preempt Type</th>
<th>Pri</th>
<th>Bandwidth (in kbps)</th>
<th>BW Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>13</td>
<td>192.168.0.1</td>
<td>192.168.0.3</td>
<td>FRRSoft</td>
<td>7/7</td>
<td>70000</td>
<td>BC0</td>
</tr>
<tr>
<td>2</td>
<td>22</td>
<td>192.168.0.1</td>
<td>192.168.0.3</td>
<td>Soft</td>
<td>7/7</td>
<td>60000</td>
<td>BC0</td>
</tr>
</tbody>
</table>
show mpls traffic-eng topology

To display the current MPLS-TE network topology for the node, use the `show mpls traffic-eng topology` command in EXEC mode.

```
show mpls traffic-eng topology [IP-address] [affinity] [brief] [link-only] [bandwidth number | exclude-srlg exclude-srlg-interface-address] explicit-path [identifier explicit-path-id-number | name explicit-path-name] [priority level] [isis nsap-address | ospf ospf-address | path {destination IP-address | tunnel P2P-tunnel-number}] [router | network] [model-type {rdm | mam}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP-address</strong></td>
<td>(Optional) Node IP address (router identifier to interface address).</td>
</tr>
<tr>
<td><strong>destination IP-address</strong></td>
<td>Displays the LSP destination IPv4 address.</td>
</tr>
<tr>
<td><strong>exclude-srlg</strong></td>
<td>Specifies an IP address to get SRLG values from for exclusion.</td>
</tr>
<tr>
<td><strong>explicit-path</strong></td>
<td>Displays the explicit LSP path.</td>
</tr>
<tr>
<td><strong>tunnel</strong></td>
<td>Displays the topology path that is based on the Point-to-Point (P2P) tunnel number.</td>
</tr>
<tr>
<td><strong>P2P-tunnel-number</strong></td>
<td>P2P tunnel number. Range is 0 to 65535.</td>
</tr>
<tr>
<td><strong>affinity</strong></td>
<td>(Optional) Displays the attribute values that are required for links carrying this tunnel. A 32-bit decimal number. Range is 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.</td>
</tr>
<tr>
<td><strong>bandwidth number</strong></td>
<td>(Optional) Displays the bandwidth value that is required by this label switched path (LSP).</td>
</tr>
<tr>
<td><strong>priority level</strong></td>
<td>(Optional) Displays the priority used when signaling a LSP for this tunnel, to determine which existing tunnels can be preempted.</td>
</tr>
<tr>
<td><strong>isis nsap-address</strong></td>
<td>(Optional) Displays the node router identification, if Intermediate System-to-Intermediate System (IS-IS) is enabled.</td>
</tr>
</tbody>
</table>
**Command Default**
No default behavior or values

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following shows a sample output from the `show mpls traffic-eng topology` command specifying the tunnel number in brief form:

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

Tunnel160 Path Setup to 10.10.10.10: FULL_PATH
bw 100 (CT0), min_bw 0, metric: 10
setup_pri 7, hold_pri 7
affinity_bits 0x0, affinity_mask 0xffff
Hop0:10.2.2.1
Hop1:10.10.10.10
```
The following shows a sample output from the `show mpls traffic-eng topology` command specifying the destination IP address:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng topology path destination 10.10.10
Path Setup to 10.10.10:
  bw 0 (CT0), min_bw 999900, metric: 10
  setup_pri 7, hold_pri 7
  affinity_bits 0x0, affinity_mask 0xffffffff
  Hop0:10.2.2.1
  Hop1:10.10.10.10
```

The following sample output shows the MPLS-TE network topology with the name of the affinity attribute of the link:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng topology
Link[1]:Point-to-Point, Nbr IGP Id:3.3.3.3, Nbr Node Id:9, gen:23
  Frag Id:25, Intf Address:13.9.1.1, Intf Id:0
  Nbr Intf Address:13.9.1.3, Nbr Intf Id:0
  TE Metric:1, IGP Metric:1, Attribute Flags:0x0
  Attribute Names: Switching Capability:, Encoding:
  BC Model ID:RDM
  Physical BW:155520 (kbps), Max Reservable BW Global:116640 (kbps)
  Max Reservable BW Sub:0 (kbps)
```

<table>
<thead>
<tr>
<th>Total Allocated</th>
<th>Global Pool</th>
<th>Sub Pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>BW (kbps)</td>
<td>Reservable</td>
<td>Reservable</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>bw[0]:</td>
<td>0</td>
<td>116640</td>
</tr>
<tr>
<td>bw[1]:</td>
<td>0</td>
<td>116640</td>
</tr>
<tr>
<td>bw[2]:</td>
<td>0</td>
<td>116640</td>
</tr>
<tr>
<td>bw[3]:</td>
<td>0</td>
<td>116640</td>
</tr>
<tr>
<td>bw[4]:</td>
<td>0</td>
<td>116640</td>
</tr>
<tr>
<td>bw[5]:</td>
<td>0</td>
<td>116640</td>
</tr>
<tr>
<td>bw[6]:</td>
<td>0</td>
<td>116640</td>
</tr>
<tr>
<td>bw[7]:</td>
<td>0</td>
<td>116640</td>
</tr>
</tbody>
</table>

```
Link[2]:Broadcast, DR:12.9.0.2, Nbr Node Id:1, gen:23
  Frag Id:28, Intf Address:12.9.0.1, Intf Id:0
  Nbr Intf Address:0.0.0.0, Nbr Intf Id:0
  TE Metric:1, IGP Metric:1, Attribute Flags:0x4
  Attribute Names: red2
  Switching Capability:, Encoding:
  BC Model ID:RDM
  Physical BW:1000000 (kbps), Max Reservable BW Global:10000 (kbps)
  Max Reservable BW Sub:0 (kbps)
```

<table>
<thead>
<tr>
<th>Total Allocated</th>
<th>Global Pool</th>
<th>Sub Pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>BW (kbps)</td>
<td>Reservable</td>
<td>Reservable</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>bw[0]:</td>
<td>0</td>
<td>10000</td>
</tr>
<tr>
<td>bw[1]:</td>
<td>0</td>
<td>10000</td>
</tr>
<tr>
<td>bw[2]:</td>
<td>0</td>
<td>10000</td>
</tr>
<tr>
<td>bw[3]:</td>
<td>0</td>
<td>10000</td>
</tr>
<tr>
<td>bw[4]:</td>
<td>0</td>
<td>10000</td>
</tr>
<tr>
<td>bw[5]:</td>
<td>0</td>
<td>10000</td>
</tr>
<tr>
<td>bw[6]:</td>
<td>0</td>
<td>10000</td>
</tr>
<tr>
<td>bw[7]:</td>
<td>0</td>
<td>10000</td>
</tr>
</tbody>
</table>
The following shows a sample output from the `show mpls traffic-eng topology` command in detail form in prestandard DS-TE mode:

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

My_System_id: 0000.0000.0002.00 (isis level-2)
My_System_id: 20.20.20.20 (ospf area 0)
My_BC_Model_Type: RDM

Signalling error holddown: 10 sec Global Link Generation 36

IGP Id: 0000.0000.0002.00, MPLS-TE Id: 20.20.20.20 Router Node (isis level-2)
Link[0]:Point-to-Point, Nbr IGP Id:0000.0000.0003.00, Nbr Node Id:3, gen:36
   Frag Id:0, Intf Address:7.3.3.1, Intf Id:0
   Nbr Intf Address:7.3.3.2, Nbr Intf Id:0
   TE Metric:10, IGP Metric:10, Attribute Flags:0x0

BC Model ID: RDM
Physical BW:155520 (kbps), Max Reservable BW Global:100000 (kbps)
   Max Reservable BW Sub:50000 (kbps)
   Total Allocated Reservable Reservable
   BW (kbps) BW (kbps) BW (kbps)
   \--------------- ----------- ----------
   bw[0]: 0 100000 50000
   bw[1]: 0 100000 50000
   bw[2]: 0 100000 50000
   bw[3]: 0 100000 50000
   bw[4]: 0 100000 50000
   bw[5]: 0 100000 50000
   bw[6]: 0 100000 50000
   bw[7]: 0 100000 50000
```

The following shows a sample output from the `show mpls traffic-eng topology` command in detail form in IETF DS-TE mode.

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

My_System_id: 0000.0000.0001.00 (isis 1 level-2)
My_System_id: 10.10.10.10 (ospf 100 area 0)
My_BC_Model_Type: MAM

Signalling error holddown: 10 sec Global Link Generation 84

IGP Id: 0000.0000.0001.00, MPLS-TE Id: 10.10.10.10 Router Node (isis 1 level-2)
Link[0]:Point-to-Point, Nbr IGP Id:0000.0000.0003.00, Nbr Node Id:6, gen:84
   Frag Id:0, Intf Address:7.2.2.1, Intf Id:0
   Nbr Intf Address:7.2.2.2, Nbr Intf Id:0
   TE Metric:10, IGP Metric:10, Attribute Flags:0x0

Switching Capability:, Encoding:
BC Model ID: MAM
Physical BW:155520 (kbps), Max Reservable BW:1000 (kbps)
   BC0:600 (kbps) BC1:400 (kbps)
   Total Allocated Reservable
   BW (kbps) BW (kbps)
   \--------------- -----------
   TE-class[0]: 10 590
```
The following shows a sample output for the `show mpls traffic-eng topology` command in brief form:

```plaintext
RP/0/RP0/CPU0:router# show mpls traffic-eng topology 192.168.0.145 brief

IGP Id: 0000.0000.0010.00, MPLS TE Id: 192.168.0.145 Router Node  (ISIS test level-1)
Link[0]:Point-to-Point, Nbr IGP Id:192.168.0.143, Nbr Node Id:6, gen:84
  Frag Id:0, Intf Address:7.1.1.1, Intf Id:0
  Nbr Intf Address:7.1.1.2, Nbr Intf Id:0

Switching Capability:, Encoding:
  BC Model ID:MAM
  Physical BW:155520 (kbps), Max Reservable BW:1000 (kbps) BC0:600 (kbps) BC1:400

<table>
<thead>
<tr>
<th>TE-class</th>
<th>Total Allocated BW (kbps)</th>
<th>Reservable BW (kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>class[0]</td>
<td>10</td>
<td>590</td>
</tr>
<tr>
<td>class[1]</td>
<td>0</td>
<td>400</td>
</tr>
<tr>
<td>class[2]</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>class[3]</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>class[4]</td>
<td>0</td>
<td>600</td>
</tr>
<tr>
<td>class[5]</td>
<td>0</td>
<td>400</td>
</tr>
<tr>
<td>class[6]</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>class[7]</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

The following sample output shows a brief topology for the affinity attributes:

```plaintext
RP/0/RP0/CPU0:router# show mpls traffic-eng topology affinity

affinity
Mon Mar 23 13:25:47.236 EST EST
  My_System_id: 1.1.1.1 (OSPF 100 area 0)
  My_System_id: 0000.0000.0001.00 (IS-IS 100 level-2)
  My_BC_Model_Type: RDM

  Signalling error holddown: 10 sec Global Link Generation 233

IGP Id: 0000.0000.0001.00, MPLS TE Id: 11.11.1.1 Router Node  (IS-IS 100 level-2)

IGP Id: 1.1.1.1, MPLS TE Id: 1.1.1.1 Router Node  (OSPF 100 area 0)
Link[0]: Intf Address: 12.9.1.1, Nbr Intf Address: 12.9.1.2
  Attribute Flags: 0x0
  Attribute Names:
```

MPLS Command Reference for Cisco NCS 6000 Series Routers
The following sample output for the `show mpls traffic-eng topology` command that shows the output to a single link:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng topology 12.9.1.1 link-only

Wed Sep 2 13:24:48.821 EST

IGP Id: 0000.0000.0002.00, MPLS TE Id: 2.2.2.2 Router Node (IS-IS 100 level-2)

Link[0]:Point-to-Point, Nbr IGP Id:0000.0000.0001.00, Nbr Node Id:-1, gen:277740
Frag Id:0, Intf Address:12.9.1.2, Intf Id:0
Nbr Intf Address:12.9.1.1, Nbr Intf Id:0
TE Metric:10, IGP Metric:10, Attribute Flags:0x0
Attribute Names:
Switching Capability:, Encoding:
BC Model ID:RDM
Physical BW:155520 (kbps), Max Reservable BW Global:116640 (kbps)
Max Reservable BW Sub:0 (kbps)

<table>
<thead>
<tr>
<th>Total Allocated</th>
<th>Global Pool Reservable</th>
<th>Sub Pool Reservable</th>
</tr>
</thead>
<tbody>
<tr>
<td>BW (kbps)</td>
<td>BW (kbps)</td>
<td>BW (kbps)</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>bw[0]: 0</td>
<td>116640</td>
<td>0</td>
</tr>
<tr>
<td>bw[1]: 0</td>
<td>116640</td>
<td>0</td>
</tr>
<tr>
<td>bw[2]: 0</td>
<td>116640</td>
<td>0</td>
</tr>
<tr>
<td>bw[3]: 0</td>
<td>116640</td>
<td>0</td>
</tr>
<tr>
<td>bw[4]: 0</td>
<td>116640</td>
<td>0</td>
</tr>
<tr>
<td>bw[5]: 0</td>
<td>116640</td>
<td>0</td>
</tr>
<tr>
<td>bw[6]: 0</td>
<td>116640</td>
<td>0</td>
</tr>
<tr>
<td>bw[7]: 0</td>
<td>116640</td>
<td>0</td>
</tr>
</tbody>
</table>
```
IGP Id: 2.2.2.2, MPLS TE Id: 2.2.2.2 Router Node (OSPF 100 area 0)

Link[3]: Point-to-Point, Nbr IGP Id: 1.1.1.1, Nbr Node Id: -1, gen: 277737
Frag Id: 29, Intf Address: 12.9.1.2, Intf Id: 0
Nbr Intf Address: 12.9.1.1, Nbr Intf Id: 0
TE Metric: 1, IGP Metric: 1, Attribute Flags: 0x0
Attribute Names:
- Switching Capability:
- Encoding:
- BC Model ID: RDM
Physical BW: 155520 (kbps), Max Reservable BW Global: 116640 (kbps)
Max Reservable BW Sub: 0 (kbps)

<table>
<thead>
<tr>
<th>Total Allocated BW (kbps)</th>
<th>Global Pool Reservable BW (kbps)</th>
<th>Sub Pool Reservable BW (kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>bw[0]: 0</td>
<td>0</td>
<td>116640</td>
</tr>
<tr>
<td>bw[1]: 0</td>
<td>0</td>
<td>116640</td>
</tr>
<tr>
<td>bw[2]: 0</td>
<td>0</td>
<td>116640</td>
</tr>
<tr>
<td>bw[3]: 0</td>
<td>0</td>
<td>116640</td>
</tr>
<tr>
<td>bw[4]: 0</td>
<td>0</td>
<td>116640</td>
</tr>
<tr>
<td>bw[5]: 0</td>
<td>0</td>
<td>116640</td>
</tr>
<tr>
<td>bw[6]: 0</td>
<td>0</td>
<td>116640</td>
</tr>
<tr>
<td>bw[7]: 0</td>
<td>0</td>
<td>116640</td>
</tr>
</tbody>
</table>

The following shows a sample output for the `show mpls traffic-eng topology model-type mam` command:

RP/0/RP0/CPU0:router# show mpls traffic-eng topology model-type mam

IGP Id: 0000.0000.0001.00, MPLS-TE Id: 10.10.10.10 Router Node (isis 1 level-2)
Link[0]: Intf Address: 7.2.2.1, Nbr Intf Address: 7.2.2.2
Link[1]: Intf Address: 7.1.1.1, Nbr Intf Address: 7.1.1.2

IGP Id: 0000.0000.0002.00, MPLS-TE Id: 20.20.20.20 Router Node (isis 1 level-2)
Link[0]: Intf Address: 7.2.2.2, Nbr Intf Address: 7.2.2.1
Link[1]: Intf Address: 7.1.1.2, Nbr Intf Address: 7.1.1.1
Link[2]: Intf Address: 7.3.3.1, Nbr Intf Address: 7.3.3.2

IGP Id: 0000.0000.0003.00, MPLS-TE Id: 30.30.30.30 Router Node (isis 1 level-2)
Link[0]: Intf Address: 7.3.3.2, Nbr Intf Address: 7.3.3.1

The following shows a sample output from the `show mpls traffic-eng topology srlg` command specifying the topology for the SRLG interfaces:

RP/0/RP0/CPU0:router# show mpls traffic-eng topology srlg

Tue Oct 6 13:10:30.342 UTC
My_System_id: 0000.0000.0005.00 (IS-IS 1 level-2)

<table>
<thead>
<tr>
<th>SRLG</th>
<th>Interface Addr</th>
<th>TE Router ID</th>
<th>IGP Area ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>51.1.2.1</td>
<td>100.0.0.1</td>
<td>IS-IS 1 level-2</td>
</tr>
<tr>
<td>2</td>
<td>51.1.2.1</td>
<td>100.0.0.1</td>
<td>IS-IS 1 level-2</td>
</tr>
<tr>
<td>3</td>
<td>51.1.2.1</td>
<td>100.0.0.1</td>
<td>IS-IS 1 level-2</td>
</tr>
<tr>
<td>4</td>
<td>51.1.2.1</td>
<td>100.0.0.1</td>
<td>IS-IS 1 level-2</td>
</tr>
<tr>
<td>5</td>
<td>51.1.2.1</td>
<td>100.0.0.1</td>
<td>IS-IS 1 level-2</td>
</tr>
<tr>
<td>6</td>
<td>51.1.2.1</td>
<td>100.0.0.1</td>
<td>IS-IS 1 level-2</td>
</tr>
<tr>
<td>7</td>
<td>51.1.2.1</td>
<td>100.0.0.1</td>
<td>IS-IS 1 level-2</td>
</tr>
<tr>
<td>8</td>
<td>51.1.2.1</td>
<td>100.0.0.1</td>
<td>IS-IS 1 level-2</td>
</tr>
<tr>
<td>10</td>
<td>50.4.5.5</td>
<td>100.0.0.5</td>
<td>IS-IS 1 level-2</td>
</tr>
<tr>
<td>30</td>
<td>50.4.5.5</td>
<td>100.0.0.5</td>
<td>IS-IS 1 level-2</td>
</tr>
</tbody>
</table>
The following shows a sample output from the `show mpls traffic-eng topology path destination` command specifying the topological path with SRLG exclusion:

```
Tue Oct 6 13:13:44.053 UTC
Path Setup to 100.0.0.2:
  bw 0 (CT0), min_bw 0, metric: 20
  setup_pri 7, hold_pri 7
  affinity_bits 0x0, affinity_mask 0xffff
  Exclude SRLG Intf Addr : 50.4.5.5
  SRLGs Excluded: 10, 30, 77, 88, 1500, 10000000
       4294967290, 4294967295
  Hop0:50.5.1.5
  Hop1:50.5.1.1
  Hop2:50.1.2.1
  Hop3:50.1.2.2
  Hop4:100.0.0.2
```

The following shows a sample output from the `show mpls traffic-eng topology path destination` command specifying the topological path based on a given explicit path:

```
Tue Oct 6 13:16:44.233 UTC
Path Setup to 100.0.0.2:
  bw 0 (CT0), min_bw 0, metric: 20
  setup_pri 7, hold_pri 7
  affinity_bits 0x0, affinity_mask 0xffff
  SRLGs Excluded: 10, 30, 77, 88, 1500, 10000000
       1, 2, 3, 4
       5, 6, 7, 8
  Hop0:50.5.1.5
  Hop1:50.5.1.1
  Hop2:50.5.1.2
  Hop3:50.5.1.2
  Hop4:100.0.0.2
```

This table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>My_System_id</td>
<td>IGP system or IGP router ID.</td>
</tr>
<tr>
<td>Signalling error holddown</td>
<td>Link hold-down timer configured to handle path error events to exclude link from topology.</td>
</tr>
<tr>
<td>IGP Id</td>
<td>Identification of the advertising router.</td>
</tr>
</tbody>
</table>

---

**Table 46: show mpls traffic-eng topology Field Descriptions**
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link</td>
<td>MPLS-TE link.</td>
</tr>
<tr>
<td>Frag Id</td>
<td>GP LSA^21_21 fragment identifier.</td>
</tr>
<tr>
<td>Nbr Intf Address</td>
<td>Neighbor Interface address of this link.</td>
</tr>
<tr>
<td>TE Metric</td>
<td>TE cost of link.</td>
</tr>
<tr>
<td>Switching Capability</td>
<td>Switching capability: packet, optical, lambda.</td>
</tr>
<tr>
<td>Physical BW</td>
<td>Physical line rate.</td>
</tr>
<tr>
<td>BC Model ID</td>
<td>Bandwidth constraint model ID (RDM or MAM).</td>
</tr>
<tr>
<td>Max Reservable BW</td>
<td>Maximum bandwidth (in kilobits per second) that you can reserve on a link.</td>
</tr>
<tr>
<td>Max Reservable BW Global</td>
<td>Maximum bandwidth (in kilobits per second) that you can reserve on a link in global-pool (prestandard and RDM).</td>
</tr>
<tr>
<td>Max Reservable BW Sub</td>
<td>Maximum bandwidth (in kilobits per second) that you can reserve on a link in subpool (prestandard and RDM).</td>
</tr>
<tr>
<td>BC0</td>
<td>Maximum bandwidth (in kilobits per second) that you can reserve on a link in BC0.</td>
</tr>
<tr>
<td>BC1</td>
<td>Maximum bandwidth (in kilobits per second) that you can reserve on a link in BC1.</td>
</tr>
<tr>
<td>TE-class[index]</td>
<td>Available bandwidth in TE-class (map of class-type and priority) at given index.</td>
</tr>
<tr>
<td>Total Allocated BW</td>
<td>Bandwidth (in Kbps) allocated at that priority.</td>
</tr>
<tr>
<td>Global Pool Reservable BW</td>
<td>Available bandwidth (in kbps) reservable at that priority in global pool (prestandard RDM).</td>
</tr>
<tr>
<td>Sub Pool Reservable BW</td>
<td>Available bandwidth (in kbps) reservable at that priority in sub-pool (prestandard RDM).</td>
</tr>
<tr>
<td>Attribute Names</td>
<td>Brief topology and the associated affinity attributes. The names of the affinity attribute of the link are displayed.</td>
</tr>
</tbody>
</table>

---

20 IGP = Interior Gateway Protocol.

21 LSA = link-state advertisement.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls traffic-eng tunnels, on page 335</td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
<tr>
<td>interface (SRLG), on page 206</td>
<td>Enables SRLG on an interface and enters SRLG interface configuration mode.</td>
</tr>
</tbody>
</table>
### Command Reference

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>srlg, on page 376</td>
<td>Configures an MPLS traffic engineering SRLG values for a link on an interface.</td>
</tr>
<tr>
<td>show srlg, on page 367</td>
<td>Displays the SRLG interface and configuration information.</td>
</tr>
</tbody>
</table>
**show mpls traffic-eng tunnels**

To display information about MPLS-TE tunnels, use the `show mpls traffic-eng tunnels` command in XR EXEC mode.

```
show mpls traffic-eng tunnels [tunnel-number] [affinity] [all] [auto-bw] [auto-tunnel] [backup
promotion-timer] [protected-interface type interface-path-id | {static | auto}] [brief]
[destination destination-address] [detail] [down] [interface (in | out | inout) type interface-path-id] [name
tunnel-name] [p2p] [property { backup-tunnel | fast-reroute}] [promotion-timer]
(protection [unused]) [reoptimized within-last interval] [role {all | head | tail | middle}]
[soft-preemption {desired | triggered}] [source source-address] [suboptimal constraints {current | max | none}]
[summary] [tabular] [unused] [up] [class-type ct] [igp {isis | ospf}] [within-last interval]
```

**Syntax Description**

- **tunnel-number**
  (Optional) Number of the tunnel. Range is from 0 to 65535.

- **attribute-set**
  (Optional) Restricts the display of tunnels with an attribute set.

- **affinity**
  (Optional) Displays the affinity attributes for all outgoing links. The links, which are used by the tunnel, display color information.

- **all**
  (Optional) Displays all MPLS-TE tunnels.

- **auto-bw**
  (Optional) Restricts the display to tunnels when the automatic bandwidth is enabled.

- **auto-tunnel**
  (Optional) Restricts the display of automatically created tunnels.

- **mesh mesh-value**
  (Optional) Displays the tunnels that belong to the specified auto-tunnel mesh group.

- **backup**
  (Optional) Displays FRR backup tunnels information. The information includes the physical interface protected by the tunnel, the number of TE LSPs protected, and the bandwidth protected.

- **name tunnel-name**
  (Optional) Displays the tunnel with given name.

- **promotion-timer promotion-timer**
  (Optional) Displays the configured FRR backup tunnel promotion timer value, in seconds.

- **protected-interface**
  (Optional) Displays FRR protected interfaces.

- **static**
  (Optional) Displays static backup tunnels.
**show mpls traffic-eng tunnels**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-tunnel</td>
<td>(Optional) Displays protected automatic backup tunnels.</td>
</tr>
<tr>
<td>brief</td>
<td>(Optional) Displays the brief form of this command.</td>
</tr>
<tr>
<td>destination destination-address</td>
<td>(Optional) Restricts the display to tunnels destined for the specified IP address.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays detail information about headend tunnels.</td>
</tr>
<tr>
<td>down</td>
<td>(Optional) Displays tunnels that are down.</td>
</tr>
<tr>
<td>interface in</td>
<td>(Optional) Displays tunnels that use the specified input interface.</td>
</tr>
<tr>
<td>interface out</td>
<td>(Optional) Displays tunnels that use the specified output interface.</td>
</tr>
<tr>
<td>interface inout</td>
<td>(Optional) Displays tunnels that use the specified interface as an input or output interface.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or a virtual interface.</td>
</tr>
<tr>
<td>Note</td>
<td>Use the show interfaces command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>p2p</td>
<td>(Optional) Displays only P2P tunnels.</td>
</tr>
<tr>
<td>property backup-tunnel</td>
<td>(Optional) Displays tunnels with property of backup tunnel. Selects MPLS-TE tunnels used to protect physical interfaces on this router. A tunnel configured to protect a link against failure is a backup tunnel and has the backup tunnel property.</td>
</tr>
<tr>
<td>property fast-reroute</td>
<td>(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.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>protection</td>
<td>(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.</td>
</tr>
<tr>
<td>reoptimized within-last interval</td>
<td>(Optional) Displays tunnels reoptimized within the last given time interval.</td>
</tr>
<tr>
<td>role all</td>
<td>(Optional) Displays all tunnels.</td>
</tr>
<tr>
<td>role head</td>
<td>(Optional) Displays tunnels with their heads at this router.</td>
</tr>
<tr>
<td>role middle</td>
<td>(Optional) Displays tunnels at the middle of this router.</td>
</tr>
<tr>
<td>role tail</td>
<td>(Optional) Displays tunnels with their tails at this router.</td>
</tr>
<tr>
<td>soft-preemption</td>
<td>Displays tunnels on which the soft-preemption feature is enabled.</td>
</tr>
<tr>
<td>source source-address</td>
<td>(Optional) Restricts the display to tunnels with a matching source IP address.</td>
</tr>
<tr>
<td>suboptimal constraints current</td>
<td>(Optional) Displays tunnels whose path metric is greater than the current shortest path constrained by the tunnel’s configured options.</td>
</tr>
<tr>
<td>suboptimal constraints max</td>
<td>(Optional) Displays tunnels whose path metric is greater than the current shortest path, constrained by the configured options for the tunnel, and taking into consideration only the network capacity.</td>
</tr>
<tr>
<td>suboptimal constraints none</td>
<td>(Optional) Displays tunnels whose path metric is greater than the shortest unconstrained path.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays summary of configured tunnels.</td>
</tr>
<tr>
<td>tabular</td>
<td>(Optional) Displays a table showing TE LSPs, with one entry per line.</td>
</tr>
<tr>
<td>unused</td>
<td>(Optional) Displays only unused backup tunnels.</td>
</tr>
<tr>
<td>up</td>
<td>(Optional) Displays tunnels when the tunnel interface is up.</td>
</tr>
<tr>
<td>class-type ct</td>
<td>(Optional) Displays tunnels using the given class-type value configuration.</td>
</tr>
</tbody>
</table>
### Command Default

None

### Command Modes

EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 5.1.2</td>
<td>These changes were made to support the path-selection cost-limit feature:</td>
</tr>
<tr>
<td></td>
<td>• The command output was modified to show the configured cost-limit.</td>
</tr>
<tr>
<td></td>
<td>• The shown PCALC error was modified to show cost-limit failure: applies for</td>
</tr>
<tr>
<td></td>
<td>new paths and verification of existing paths.</td>
</tr>
<tr>
<td></td>
<td>• The 'Reopt Reason' field in the show output was modified to show the</td>
</tr>
<tr>
<td></td>
<td>cost-limit.</td>
</tr>
<tr>
<td></td>
<td>• The path-protection switchover reason in the show output was modified to</td>
</tr>
<tr>
<td></td>
<td>show the cost-limit.</td>
</tr>
</tbody>
</table>

The command output was modified to display the 'Traffic switched to FRR backup tunnel-te' message as part of Soft-preemption over FRR backup tunnels feature implementation.

### Usage Guidelines

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

Use the **brief** form of the `show mpls traffic-eng tunnels` command to display information specific to a tunnel interface. Use the command without the **brief** keyword to display information that includes the destination address, source ID, role, name, suboptimal constraints, and interface.

The **affinity** keyword is available for only the source router.

Selected tunnels would have a shorter path if they were reoptimized immediately.
This sample output is not changed when no area is specified for the active path-option. If the area is specified, it is added on a line of its own after the existing path-option information.

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels 20 detail
```

```
Signalling Summary:
LSP Tunnels Process: running
RSVP Process: running
Forwarding: enabled
Periodic reoptimization: every 3600 seconds, next in 2400 seconds
Periodic FRR Promotion: every 300 seconds, next in 16 seconds
Auto-bw enabled tunnels: 6

Name: tunnel-te20 Destination: 130.130.130.130
Status: Admin: up Oper: up Path: valid Signalling: connected

path option 1, type explicit r1r2r3gig_path (Basis for Setup, path weight 200)
G-PID: 0x0800 (derived from egress interface properties)
Bandwidth Requested: 113 kbps CT0

Config Parameters:
Bandwidth: 100 kbps (CT0) Priority: 7 7 Affinity: 0x0/0xffffffff
Metric Type: TE (interface)
AutoRoute: enabled LockDown: disabled Policy class: not set
Forwarding-Adjacency: disabled
Loadshare: 0 equal loadshares
Auto-bw: enabled
Last BW Applied: 113 kbps CT0 BW Applications: 1
Last Application Trigger: Periodic Application
Bandwidth Min/Max: 0-4294967295 kbps
Application Frequency: 5 min Jitter: 0s Time Left: 4m 19s
Collection Frequency: 1 min
Samples Collected: 0 Next: 14s
Highest BW: 0 kbps Underflow BW: 0 kbps
Adjustment Threshold: 10% 10 kbps
Overflow Detection disabled
Underflow Detection disabled
Fast Reroute: Disabled, Protection Desired: None
Path Protection: Not Enabled

History:
Tunnel has been up for: 00:18:54 (since Sun Mar 14 23:48:23 UTC 2010)
Current LSP:
Uptime: 00:05:41 (since Mon Mar 15 00:01:36 UTC 2010)
Prior LSP:
ID: path option 1 [3]
Removal Trigger: reoptimization completed

Current LSP Info:
Instance: 4, Signaling Area: IS-IS 1 level-2
Uptime: 00:05:41 (since Mon Mar 15 00:01:36 UTC 2010)
Outgoing Interface: GigabitEthernet0/5/0/21, Outgoing Label: 16009
Router-IDs: local 110.110.110.110
downstream 120.120.120.120

Path Info:
```
Outgoing:
Explicit Route:
  Strict, 61.10.1.2
  Strict, 61.15.1.1
  Strict, 61.15.1.2
  Strict, 130.130.130.130
Record Route: Disabled
Tspec: avg rate=113 kbits, burst=1000 bytes, peak rate=113 kbits
Session Attributes: Local Prot: Not Set, Node Prot: Not Set, BW Prot: Not Set
Resv Info: None
Record Route: Disabled
Fspec: avg rate=113 kbits, burst=1000 bytes, peak rate=113 kbits
Displayed 1 (of 6) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads

This is a sample output from the `show mpls traffic-eng tunnels` command using the `property` keyword:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels property backup interface out pos 0/6/0/0
```

Signalling Summary:
  LSP Tunnels Process: running, not registered with RSVP
  RSVP Process: not running
  Forwarding: enabled
  Periodic reoptimization: every 3600 seconds, next in 3595 seconds
  Periodic FRR Promotion: every 300 seconds, next in 295 seconds
  Periodic auto-bw collection: disabled

Name: tunnel-te1 Destination: 1.1.1.1
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 1, type dynamic (Basis for Setup, path weight 1)
  G-PID: 0x0800 (derived from egress interface properties)

Config Parameters:
  Bandwidth: 1000 kbps (CT0) Priority: 7 7 Affinity: 0x0/0xffff
  Metric Type: TE (default)
  AutoRoute: disabled LockDown: disabled
  Loadshare: 10000 bandwidth-based
  Auto-bw: disabled(0/0) 0 Bandwidth Requested: 0
  Direction: unidirectional
  Endpoint switching capability: unknown, encoding type: unassigned
  Transit switching capability: unknown, encoding type: unassigned
  Backup FRR EXP Demotion: 1 ' 7, 2 ' 1
  Class-Attributes: 1, 2, 7
  Bandwidth-Policer: off

History:
  Tunnel has been up for: 00:00:08
  Current LSP:
    Uptime: 00:00:08

Path info (ospf 0 area 0):
  Hop0: 10.0.0.2
  Hop1: 102.0.0.2
Displayed 1 (of 1) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 0 up, 1 down, 0 recovering, 0 recovered heads
This table describes the significant fields shown in the display.

**Table 47: show mpls traffic-eng tunnels Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP Tunnels Process</td>
<td>Status of the LSP tunnels process.</td>
</tr>
<tr>
<td>RSVP Process</td>
<td>Status of the RSVP process.</td>
</tr>
<tr>
<td>Forwarding</td>
<td>Status of forwarding (enabled or disabled).</td>
</tr>
<tr>
<td>Periodic reoptimization</td>
<td>Time, in seconds, until the next periodic reoptimization.</td>
</tr>
<tr>
<td>Periodic FRR Promotion</td>
<td>Time, in seconds, till the next periodic FRR promotion.</td>
</tr>
<tr>
<td>Periodic auto-bw collection</td>
<td>Time, in seconds, till the next periodic auto-bw collection.</td>
</tr>
<tr>
<td>Name</td>
<td>Interface configured at the tunnel head.</td>
</tr>
<tr>
<td>Destination</td>
<td>Tail-end router identifier.</td>
</tr>
<tr>
<td>Admin/STATUS</td>
<td>Configured up or down.</td>
</tr>
<tr>
<td>Oper/STATE</td>
<td>Operationally up or down.</td>
</tr>
<tr>
<td>Signalling</td>
<td>Signaling connected or down or proceeding.</td>
</tr>
<tr>
<td>Config Parameters</td>
<td>Configuration parameters provided by tunnel mode MPLS traffic-eng, including those specific to unequal load-balancing functionality (bandwidth, load-share, backup FRR EXP demotion, class-attributes, and bandwidth-policer).</td>
</tr>
<tr>
<td>History: Current LSP: Uptime</td>
<td>Time LSP has been up.</td>
</tr>
<tr>
<td>Path Info</td>
<td>Hop list of current LSP.</td>
</tr>
</tbody>
</table>

24 LSP = Link-State Packet.
25 FRR = Fast Reroute.

This sample output shows the link attributes of links that are traversed by the tunnel (color information):

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels 11 affinity

Signalling Summary:
  LSP Tunnels Process: running
  RSVP Process: running
  Forwarding: enabled
  Periodic reoptimization: every 3600 seconds, next in 2710 seconds
  Periodic FRR Promotion: every 300 seconds, next in 27 seconds

Auto-bw enabled tunnels: 0 (disabled)

Name: tunnel-te11 Destination: 3.3.3.3
Status:
  Admin: up Oper: up Path: valid Signalling: connected
```
path option 1, type explicit gige_1_2_3 (Basis for Setup, path weight 2)
G-PID: 0x0800 (derived from egress interface properties)
Bandwidth Requested: 200 kbps CT0

Config Parameters:
Bandwidth: 200 kbps (CT0) Priority: 2 2
Number of affinity constraints: 1
Include bit map : 0x4
Include name : red2

Metric Type: TE (default)
AutoRoute: disabled LockDown: disabled Policy class: not set
Forwarding-Adjacency: disabled Loadshare: 0 equal loadshares
Auto-bw: disabled
Fast Reroute: Enabled, Protection Desired: Any
Path Protection: Not Enabled

History:
Tunnel has been up for: 02:55:27
Current LSP:
    Uptime: 02:02:19
Prior LSP:
    ID: path option 1 [8]
    Removal Trigger: reoptimization completed

Path info (OSPF 100 area 0):
    Link0: 12.9.0.1
    Attribute flags: 0x4
    Attribute names: red2
    Link1: 23.9.0.2
    Attribute flags: 0x4
    Attribute names: red2

Displayed 1 (of 8) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads

This sample output shows the brief summary of the tunnel status and configuration:

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

Signalling Summary:
    LSP Tunnels Process: running
    RSVP Process: running
    Forwarding: enabled
    Periodic reoptimization: every 3600 seconds, next in 2538 seconds
    Periodic FRR Promotion: every 300 seconds, next in 38 seconds
    Auto-bw enabled tunnels: 0 (disabled)

<table>
<thead>
<tr>
<th>TUNNEL NAME</th>
<th>DESTINATION</th>
<th>STATUS</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel-te1060</td>
<td>10.6.6.6</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>PE6_C12406_t607</td>
<td>10.7.7.7</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>PE6_C12406_t608</td>
<td>10.8.8.8</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>PE6_C12406_t609</td>
<td>10.9.9.9</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>PE6_C12406_t610</td>
<td>10.10.10.10</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>PE6_C12406_t621</td>
<td>10.21.21.21</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>PE7_C12406_t706</td>
<td>10.6.6.6</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>PE7_C12406_t721</td>
<td>10.21.21.21</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Tunnel_PE8-PE6</td>
<td>10.6.6.6</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Tunnel_PE8-PE21</td>
<td>10.21.21.21</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Tunnel_PE9-PE6</td>
<td>10.6.6.6</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Tunnel_PE9-PE21</td>
<td>10.21.21.21</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Tunnel_PE10-PE6</td>
<td>10.6.6.6</td>
<td>up</td>
<td>up</td>
</tr>
</tbody>
</table>
This section shows a sample output that results when automatic backup tunnels are created:

RP/0/RP0/CPU0# show mpls traffic-eng tunnels brief

TUNNEL NAME DESTINATION STATUS STATE
  tunnel-te0 200.0.0.3 up up
  tunnel-te1 200.0.0.3 up up
  tunnel-te2 200.0.0.3 up up
  *tunnel-te50 200.0.0.3 up up
  *tunnel-te60 200.0.0.3 up up
  *tunnel-te70 200.0.0.3 up up
  *tunnel-te80 200.0.0.3 up up

* = automatically created backup tunnel

This is sample output that shows a summary of configured tunnels by using the summary keyword:

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

LSP Tunnels Process: not running, disabled
RSVP Process: running
Forwarding: enabled
Periodic reoptimization: every 3600 seconds, next in 2706 seconds
Periodic FRR Promotion: every 300 seconds, next in 81 seconds
Periodic auto-bw collection: disabled

Signalling Summary:
  Head: 1 interfaces, 1 active signalling attempts, 1 established
  0 explicit, 1 dynamic
  1 activations, 0 deactivations
  0 recovering, 0 recovered
Mids: 0
Tails: 0

Fast ReRoute Summary:
  Head: 0 FRR tunnels, 0 protected, 0 rerouted
  Mid: 0 FRR tunnels, 0 protected, 0 rerouted
  Summary: 0 protected, 0 link protected, 0 node protected, 0 bw protected
AutoTunnel Backup Summary:

AutoTunnel Backups:
- 50 created, 50 up, 0 down, 8 unused
- 25 NHOP, 25 NNHOP, 10 SRLG strict, 10 SRLG pref

Protected LSPs:
- 10 NHOP, 20 NHOP+SRLG
- 15 NNHOP, 5 NNHOP+SRLG

Protected S2L Sharing Families:
- 10 NHOP, 20 NHOP+SRLG
- 15 NNHOP, 5 NNHOP+SRLG

Protected S2Ls:
- 10 NHOP, 20 NHOP+SRLG
- 15 NNHOP, 5 NNHOP+SRLG

This table describes the significant fields shown in the display.

**Table 48: show mpls traffic-eng tunnels protection Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel#</td>
<td>Number of the MPLS-TE backup tunnel.</td>
</tr>
<tr>
<td>LSP Head/router</td>
<td>Node is either head or router for this LSP.</td>
</tr>
<tr>
<td>Instance</td>
<td>LSP ID.</td>
</tr>
<tr>
<td>Backup tunnel</td>
<td>Backup tunnel protection for NHOP/NNHOP.</td>
</tr>
<tr>
<td>out if</td>
<td>Backup tunnel's outgoing interface</td>
</tr>
<tr>
<td>Original</td>
<td>Outgoing interface, label, and next-hop of the LSP when not using backup.</td>
</tr>
<tr>
<td>With FRR</td>
<td>Outgoing interface and label when using backup tunnel.</td>
</tr>
<tr>
<td>LSP BW</td>
<td>Signaled bandwidth of the LSP.</td>
</tr>
<tr>
<td>Backup level</td>
<td>Type of bandwidth protection provided—pool type and limited/unlimited bandwidth.</td>
</tr>
<tr>
<td>LSP Tunnels Process</td>
<td>Status of the TE process.</td>
</tr>
</tbody>
</table>

26 LSP = Link-State Packet.
27 LSP = Label Switched Path

This is sample output from the `show mpls traffic-eng tunnels` command using the `backup` keyword. This command selects every MPLS-TE tunnel known to the router, and displays information about the FRR protection that each selected tunnel provides for interfaces on this route. The command does not generate output for tunnels that do not provide FRR protection of interfaces on this router:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels backup
tunnel160
   Admin: up, Oper: up
   Src: 10.20.20.20, Dest: 10.10.10.10, Instance: 28
   Fast Reroute Backup Provided:
      Protected I/fs: POS0/7/0/0
```
Protected lsps: 0
Backup BW: any-class unlimited, Inuse: 0 kbps

This table describes the significant fields shown in the display.

Table 49: show mpls traffic-eng tunnels backup Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel#</td>
<td>MPLS-TE backup tunnel number.</td>
</tr>
<tr>
<td>Dest</td>
<td>IP address of backup tunnel destination.</td>
</tr>
<tr>
<td>State</td>
<td>State of the backup tunnel. Values are up, down, or admin-down.</td>
</tr>
<tr>
<td>Instance</td>
<td>LSP ID of the tunnel.</td>
</tr>
<tr>
<td>Protected I/fs</td>
<td>List of interfaces protected by the backup tunnel.</td>
</tr>
<tr>
<td>Protected lsps</td>
<td>Number of LSPs currently protected by the backup tunnel.</td>
</tr>
<tr>
<td>Backup BW</td>
<td>Configured backup bandwidth type and amount. Pool from which bandwidth is acquired. Values are any-class, CT0, and CT1. Amount is either unlimited or a configured limit in kbps.</td>
</tr>
<tr>
<td>Inuse</td>
<td>Backup bandwidth currently in use on the backup tunnel.</td>
</tr>
</tbody>
</table>

This shows a sample output from the `show mpls traffic-eng tunnels` command using the `backup` and `protected-interface` keywords:

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

Interface: POS0/5/0/1
  Tunnel100 UNUSED : out I/f: Admin: down Oper: down

Interface: POS0/7/0/0
  Tunnel160 NHOP : out I/f: POS0/6/0/0 Admin: up Oper: up
```

This table describes the significant fields shown in the display.

Table 50: show mpls traffic-eng tunnels backup protected-interface Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>MPLS-TE-enabled FRR protected interface.</td>
</tr>
<tr>
<td>Tunnel#</td>
<td>FRR protected tunnel on the interface.</td>
</tr>
<tr>
<td>NHOP/NNHOP/UNUSED</td>
<td>State of Protected tunnel. Values are unused, next hop, next-next hop.</td>
</tr>
<tr>
<td>out I/f</td>
<td>Outgoing interface of the backup tunnel providing the protection.</td>
</tr>
</tbody>
</table>

This shows a sample output from the `show mpls traffic-eng tunnels up` command using the `igp ospf` keywords:
show mpls traffic-eng tunnels up igp ospf

Signalling Summary:
- LSP Tunnels Process: running
- RSVP Process: running
- Forwarding: enabled
- Periodic reoptimization: every 3600 seconds, next in 3381 seconds
- Periodic FRR Promotion: every 300 seconds, next in 81 seconds
- Periodic auto-bw collection: disabled

Name: tunnel-te11 Destination: 30.30.30.30
Status:
- Admin: up
- Oper: up
- Path: valid
- Signalling: connected
  path option 1, type explicit back (Basis for Setup, path weight 1)
  G-PID: 0x0800 (derived from egress interface properties)

Config Parameters:
- Bandwidth: 0 kbps (CT0)
- Priority: 7 7
- Affinity: 0x0/0xffffffff
- Number of configured name based affinities: 2
- Name based affinity constraints in use:
  - Include bit map: 0x4 (refers to undefined affinity name)
  - Include-strict bit map: 0x4
- Metric Type: TE (default)
- AutoRoute: disabled
- LockDown: disabled
- Loadshare: 0 bw-based
- Auto-bw: disabled
- Bandwidth Requested: 0
- Direction: unidirectional
- Endpoint switching capability: unknown, encoding type: unassigned
- Transit switching capability: unknown, encoding type: unassigned

History:
- Tunnel has been up for: 00:00:21
  - Current LSP:
    - Uptime: 00:00:21
  - Prior LSP:
    - ID: path option 1 [4]
    - Removal Trigger: tunnel shutdown

Path info (ospf area 0):
- Hop0: 7.4.4.2
- Hop1: 30.30.30.30
- Displayed 1 (of 3) heads, 0 (of 0) midpoints, 0 (of 0) tails
  Displayed 1 up, 0 down, 0 recovering, 0 recovered heads

This shows a sample output from the `show mpls traffic-eng tunnels` command using the `up within-last` keywords:

show mpls traffic-eng tunnels up within-last 200

Signalling Summary:
- LSP Tunnels Process: running
- RSVP Process: running
- Forwarding: enabled
- Periodic reoptimization: every 3600 seconds, next in 3381 seconds
- Periodic FRR Promotion: every 300 seconds, next in 81 seconds
- Periodic auto-bw collection: disabled

Name: tunnel-te11 Destination: 30.30.30.30
Status:
Admin: up Oper: up Path: valid Signalling: connected
path option 1, type explicit back (Basis for Setup, path weight 1)
G-PID: 0x0800 (derived from egress interface properties)

Config Parameters:
Bandwidth: 0 kbps (CT0) Priority: 7 7 Affinity: 0x0/0xffff
Number of configured name based affinities: 2
Name based affinity constraints in use:
  Include bit map : 0x4 (refers to undefined affinity name)
  Include-strict bit map: 0x4
Metric Type: TE (default)
AutoRoute: disabled LockDown: disabled Loadshare: 0 bw-based
Auto-bw: disabled(0/0) 0 Bandwidth Requested: 0
Direction: unidirectional
Endpoint switching capability: unknown, encoding type: unassigned
  Transit switching capability: unknown, encoding type: unassigned

History:
Tunnel has been up for: 00:00:21
Current LSP:
  Uptime: 00:00:21
Prior LSP:
  ID: path option 1 [4]
    Removal Trigger: tunnel shutdown

Path info (ospf area 0):
  Hop0: 7.4.4.2
  Hop1: 30.30.30.30

Displayed 1 (of 3) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads

This shows a sample output from the show mpls traffic-eng tunnels command using the reoptimized within-last keywords:

RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels reoptimized within-last 600

Signalling Summary:
  LSP Tunnels Process: running
  RSVP Process: running
  Forwarding: enabled
  Periodic reoptimization: every 60000 seconds, next in 41137 seconds
  Periodic FRR Promotion: every 300 seconds, next in 37 seconds
  Periodic auto-bw collection: disabled

Name: tunnel-te1 Destination: 30.30.30.30
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 1, type explicit prot1 (Basis for Setup, path weight 1)
  G-PID: 0x0800 (derived from egress interface properties)

Config Parameters:
  Bandwidth: 66 kbps (CT0) Priority: 7 7 Affinity: 0x0/0xffff
  Metric Type: IGP (global)
  AutoRoute: enabled LockDown: disabled Loadshare: 66 bw-based
  Auto-bw: disabled(0/0) 0 Bandwidth Requested: 66
  Direction: unidirectional
  Endpoint switching capability: unknown, encoding type: unassigned
    Transit switching capability: unknown, encoding type: unassigned
This is a sample output from the `show mpls traffic-eng tunnels` command using the `detail` keyword:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels 100 detail

Name: tunnel-te1 Destination: 24.24.24.24
Status:
   Admin: up Oper: up
   Working Path: valid Signalling: connected
   Protecting Path: valid Protect Signalling: connected
   Working LSP is carrying traffic
   path option 1, type explicit po4 (Basis for Setup, path weight 1)
     (Basis for Standby, path weight 2)
   G-PID: 0x001d (derived from egress interface properties)
   Path protect LSP is present.
   path option 1, type explicit po6 (Basis for Setup, path weight 1)
Config Parameters:
   Bandwidth: 10 kbps (CT0) Priority: 7 7 Affinity: 0x0/0xffff
   Metric Type: TE (default)
   AutoRoute: enabled LockDown: disabled Loadshare: 10 bw-based
   Auto-bw: disabled(0/0) 0 Bandwidth Requested: 10
   Direction: unidirectional
   Endpoint switching capability: unknown, encoding type: unassigned
   Transit switching capability: unknown, encoding type: unassigned

History:
   Tunnel has been up for: 00:04:06
   Current LSP:
      Uptime: 00:04:06
      Prior LSP:
         ID: path option 1 [5452]
         Removal Trigger: path verification failed
Current LSP Info:
   Instance: 71, Signaling Area: ospf optical area 0
   Uptime: 00:10:41
   Incoming Label: explicit-null
   Outgoing Interface: POS0/4/0/0, Outgoing Label: implicit-null
   Path Info:
      Explicit Route:
         Strict, 100.0.0.3
         Strict, 24.24.24.24
      Record Route: None
      Tspec: avg rate=2488320 kbits, burst=1000 bytes, peak rate=2488320 kbits
```
This is a sample output from the `show mpls traffic-eng tunnels` command using the `role mid` keyword:

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

Signalling Summary:
    LSP Tunnels Process: running
    RSVP Process: running
    Forwarding: enabled
    Periodic reoptimization: every 3600 seconds, next in 1166 seconds
    Periodic FRR Promotion: every 300 seconds, next in 90 seconds
    Periodic auto-bw collection: disabled
LSP Tunnel 10.10.10.10 1 [5508] is signalled, connection is up
Tunnel Name: FRR1_t1 Tunnel Role: Mid
InLabel: POS0/2/0/1, 33
OutLabel: POS0/3/0/0, implicit-null
Signalling Info:
   Src 10.10.10.10 Dst 30.30.30.30, Tunnel ID 1, Tunnel Instance 5508
Path Info:
   Incoming Address: 7.3.3.1
      Strict, 7.3.3.1
      Loose, 30.30.30.30
ERO Expansion Info:
   ospf 100 area 0, Metric 1 (TE), Affinity 0x0, Mask 0xffff, Queries 0
Outgoing Explicit Route:
   Strict, 7.2.2.1
   Strict, 30.30.30.30
Record Route: None
Resv Info:
   InLabel: POS0/2/0/1, 33
   OutLabel: POS0/3/0/0, implicit-null
   Tspec: avg rate=10 kbits, burst=1000 bytes, peak rate=10 kbits
   Resv Info:
       InLabel: POS0/2/0/1, 33
       OutLabel: POS0/3/0/0, implicit-null
This sample output shows a tabular table for TE LSPs by using the `tabular` keyword:
```
This sample output shows a tabular table indicating automatic backup tunnels when using the `tabular` keyword:

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

<table>
<thead>
<tr>
<th>Tunnel Name</th>
<th>LSP ID</th>
<th>Destination Address</th>
<th>Source Address</th>
<th>Tun State</th>
<th>FRR State</th>
<th>Role</th>
<th>Prot</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel-te1060</td>
<td>2</td>
<td>10.6.6.6</td>
<td>10.1.1.1</td>
<td>up</td>
<td>Inact</td>
<td>Head</td>
<td></td>
</tr>
<tr>
<td>PE6_C12406_t607</td>
<td>2</td>
<td>10.7.7.7</td>
<td>10.6.6.6</td>
<td>up</td>
<td>Inact</td>
<td>Mid</td>
<td></td>
</tr>
<tr>
<td>PE6_C12406_t608</td>
<td>2</td>
<td>10.8.8.8</td>
<td>10.6.6.6</td>
<td>up</td>
<td>Inact</td>
<td>Mid</td>
<td></td>
</tr>
<tr>
<td>PE6_C12406_t609</td>
<td>2</td>
<td>10.9.9.9</td>
<td>10.6.6.6</td>
<td>up</td>
<td>Inact</td>
<td>Mid</td>
<td></td>
</tr>
<tr>
<td>PE6_C12406_t610</td>
<td>2</td>
<td>10.10.10.10</td>
<td>10.6.6.6</td>
<td>up</td>
<td>Inact</td>
<td>Mid</td>
<td></td>
</tr>
<tr>
<td>PE6_C12406_t621</td>
<td>2</td>
<td>10.21.21.21</td>
<td>10.6.6.6</td>
<td>up</td>
<td>Inact</td>
<td>Mid</td>
<td></td>
</tr>
<tr>
<td>PE7_C12406_t706</td>
<td>835</td>
<td>10.6.6.6</td>
<td>10.7.7.7</td>
<td>up</td>
<td>Inact</td>
<td>Mid</td>
<td></td>
</tr>
<tr>
<td>PE7_C12406_t721</td>
<td>603</td>
<td>10.21.21.21</td>
<td>10.7.7.7</td>
<td>up</td>
<td>Inact</td>
<td>Mid</td>
<td></td>
</tr>
<tr>
<td>Tunnel_PE8-PE6</td>
<td>4062</td>
<td>10.6.6.6</td>
<td>10.8.8.8</td>
<td>up</td>
<td>Inact</td>
<td>Mid</td>
<td></td>
</tr>
<tr>
<td>Tunnel_PE9-PE6</td>
<td>4062</td>
<td>10.6.6.6</td>
<td>10.9.9.9</td>
<td>up</td>
<td>Inact</td>
<td>Mid</td>
<td></td>
</tr>
<tr>
<td>Tunnel_PE9-PE21</td>
<td>6795</td>
<td>10.6.6.6</td>
<td>10.9.9.9</td>
<td>up</td>
<td>Inact</td>
<td>Mid</td>
<td></td>
</tr>
<tr>
<td>Tunnel_PE10-PE6</td>
<td>4091</td>
<td>10.6.6.6</td>
<td>10.10.10.10</td>
<td>up</td>
<td>Inact</td>
<td>Mid</td>
<td></td>
</tr>
<tr>
<td>Tunnel_PE10-PE21</td>
<td>6821</td>
<td>10.6.6.6</td>
<td>10.10.10.10</td>
<td>up</td>
<td>Inact</td>
<td>Mid</td>
<td></td>
</tr>
<tr>
<td>PE21_C12406_t2106</td>
<td>2</td>
<td>10.6.6.6</td>
<td>10.21.21.21</td>
<td>up</td>
<td>Ready</td>
<td>Mid</td>
<td></td>
</tr>
<tr>
<td>PE21_C12406_t2107</td>
<td>2</td>
<td>10.7.7.7</td>
<td>10.21.21.21</td>
<td>up</td>
<td>Inact</td>
<td>Mid</td>
<td></td>
</tr>
<tr>
<td>PE21_C12406_t2108</td>
<td>2</td>
<td>10.8.8.8</td>
<td>10.21.21.21</td>
<td>up</td>
<td>Inact</td>
<td>Mid</td>
<td></td>
</tr>
<tr>
<td>PE21_C12406_t2109</td>
<td>2</td>
<td>10.9.9.9</td>
<td>10.21.21.21</td>
<td>up</td>
<td>Inact</td>
<td>Mid</td>
<td></td>
</tr>
<tr>
<td>PE21_C12406_t2110</td>
<td>2</td>
<td>10.10.10.10</td>
<td>10.21.21.21</td>
<td>up</td>
<td>Inact</td>
<td>Mid</td>
<td></td>
</tr>
<tr>
<td>PE6_C12406_t6070</td>
<td>626</td>
<td>10.6.6.6</td>
<td>10.7.7.7</td>
<td>up</td>
<td>Inact</td>
<td>Mid</td>
<td></td>
</tr>
<tr>
<td>PE7_C12406_t7060</td>
<td>626</td>
<td>10.6.6.6</td>
<td>10.7.7.7</td>
<td>up</td>
<td>Inact</td>
<td>Mid</td>
<td></td>
</tr>
</tbody>
</table>

* = automatically created backup tunnel

This table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Name</td>
<td>MPLS-TE tunnel name.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LSP ID</td>
<td>LSP ID of the tunnel.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Destination address of the TE tunnel (identified in Tunnel Name).</td>
</tr>
<tr>
<td>Source Address</td>
<td>Source address for the filtered tunnels.</td>
</tr>
<tr>
<td>Tunnel State</td>
<td>State of the tunnel. Values are up, down, or admin-down.</td>
</tr>
<tr>
<td>FRR State</td>
<td>FRR state identifier.</td>
</tr>
<tr>
<td>LSP Role</td>
<td>Role identifier. Values are All, Head, or Tail.</td>
</tr>
</tbody>
</table>

This sample output shows the MPLS-TE tunnel information only for tunnels in which the automatic bandwidth is enabled using the `auto-bw` keyword:

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

**Signalling Summary:**
- LSP Tunnels Process: running
- RSVP Process: running
- Forwarding: enabled
- Periodic reoptimization: every 3600 seconds, next in 636 seconds
- Periodic FRR Promotion: every 300 seconds, next in 276 seconds
- Auto-bw enabled tunnels: 1

**Name:** tunnel-te1  **Destination:** 0.0.0.0

**Status:**
- Admin: up  Oper: down  Path: not valid  Signalling: Down
- G-PID: 0x0800 (internally specified)
- Bandwidth Requested: 0 kbps  CT0

**Config Parameters:**
- Bandwidth: 0 kbps (CT0)  Priority: 7 7  Affinity: 0x0/0xffff
- Metric Type: TE (default)
- AutoRoute: disabled  LockDown: disabled  Policy class: not set
- Loadshare: 0 equal loadshares

**Auto-bw:** (collect bw only)
- Last BW Applied: 500 kbps (CT0)  BW Applications: 25
- Last Application Trigger: Periodic Application
- Bandwidth Min/Max: 10-10900 kbps
- Application Frequency: 10 min (Cfg: 10 min)  Time Left: 5m 34s
- Collection Frequency: 2 min
- Samples Collected: 2  Highest BW: 450 kbps  Next: 1m 34s
- Adjustment Threshold: 5%
- Overflow Threshold: 15%  Limit: 1/4  Early BW Applications: 0
- Direction: unidirectional
- Endpoint switching capability: unknown, encoding type: unassigned
- Transit switching capability: unknown, encoding type: unassigned
- Fast Reroute: Disabled, Protection Desired: None

**Reason for the tunnel being down:** No destination is configured

**History:**
- Displayed 1 (of 1) heads, 0 (of 0) midpoints, 0 (of 0) tails
- Displayed 0 up, 1 down, 0 recovering, 0 recovered heads
This table describes the significant fields shown in the display.

### Table 52: show mpls traffic-eng tunnels auto-bw Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>collect bw only</td>
<td>Field is displayed only if the bandwidth collection is configured in the tunnel automatic bandwidth configuration.</td>
</tr>
<tr>
<td>Last BW Applied</td>
<td>Last bandwidth change that is requested by the automatic bandwidth for the tunnel. In addition, this field indicates which pool is used for the bandwidth.</td>
</tr>
<tr>
<td>BW Applications</td>
<td>Total number of bandwidth applications that is requested by the automatic bandwidth, which includes the applications triggered by an overflow condition.</td>
</tr>
<tr>
<td>Last Application Trigger</td>
<td>These last application options are displayed:</td>
</tr>
<tr>
<td></td>
<td>• Periodic Application</td>
</tr>
<tr>
<td></td>
<td>• Overflow Detected</td>
</tr>
<tr>
<td></td>
<td>• Manual Application</td>
</tr>
<tr>
<td>Bandwidth Min/Max</td>
<td>Bandwidth configured is either minimum or maximum.</td>
</tr>
<tr>
<td>Application Frequency</td>
<td>Configured application frequency. The Time Left field indicates the time left before the next application executes.</td>
</tr>
<tr>
<td>Collection Frequency</td>
<td>Globally configured collection frequency, which is the same value for all the tunnels.</td>
</tr>
<tr>
<td>Samples Collected</td>
<td>Number of samples that are collected during the current application period. This field is replaced by the Collection Disabled field if Collection Frequency is not currently configured.</td>
</tr>
<tr>
<td>Highest BW</td>
<td>Highest bandwidth that is collected for the application period.</td>
</tr>
<tr>
<td>Next</td>
<td>Time left before the next collection event.</td>
</tr>
<tr>
<td>Overflow Threshold</td>
<td>Overflow threshold that is configured. The Overflow field appears only if the overflow detection is configured in the tunnel automatic bandwidth configuration.</td>
</tr>
<tr>
<td>Limit</td>
<td>Consecutive overflow detected or configured limit.</td>
</tr>
<tr>
<td>Early BW Applications</td>
<td>Number of early bandwidth applications that are triggered by an overflow condition.</td>
</tr>
</tbody>
</table>

This is sample output from the `show mpls traffic-eng tunnels` command after the NNHOP SRLG preferred automatic backup tunnel is configured:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels 1

Signalling Summary:
  LSP Tunnels Process: running
  RSVP Process: running
  Forwarding: enabled
  Periodic reoptimization: every 3600 seconds, next in 2524 seconds
  Periodic FRR Promotion: every 300 seconds, next in 49 seconds
  Auto-bw enabled tunnels: 1
```
Name: tunnel-te1  Destination: 200.0.0.3 (auto backup)
Status:
  Admin:  up  Oper:  up  Path:  valid  Signalling: connected
   path option 10,  type explicit (autob_nnhop_srlg_tunnel1) (Basis for Setup, path weight 11)
   path option 20,  type explicit (autob_nnhop_tunnel1)
G-PID: 0x0800 (derived from egress interface properties)
Bandwidth Requested: 0 kbps  CT0
Creation Time: Fri Jul 10 01:53:25.581 PST  (1h 25m 17s ago)

Config Parameters:
  Bandwidth:  0 kbps  (CT0)  Priority:  7  7  Affinity: 0x0/0xffffffff
  Metric Type:  TE  (default)
  AutoRoute:  disabled  LockDown:  disabled  Policy class:  not set
  Forwarding-Adjacency:  disabled

Loadshare:  0 equal loadshares
  Auto-bw:  disabled
  Fast Reroute:  Disabled, Protection Desired: None
  Path Protection:  Not Enabled

Auto Backup:
  Protected LSPs: 4
  Protected S2L Sharing Families: 0
  Protected S2Ls: 0
  Protected i/f:  Gi0/1/0/0  Protected node: 20.0.0.2
  Protection:  NNHOP+SRLG
  Unused removal timeout: not running

History:
  Tunnel has been up for: 00:00:08
  Current LSP:
    Uptime: 00:00:08
    Prior LSP:
      ID:  path option 1 [545]
      Removal Trigger: configuration changed

Path info (OSPF 0 area 0):
  Hop0: 10.0.0.2
  Hop1: 100.0.0.2
  Hop2: 100.0.0.3
  Hop3: 200.0.0.3

This table describes the significant fields shown in the display.

Table 53: show mpls traffic-eng tunnels Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Backup</td>
<td>Auto backup section header.</td>
</tr>
<tr>
<td>Creation Time</td>
<td>Time when the tunnel was created and for what period was the tunnel created.</td>
</tr>
<tr>
<td>Protected LSPs</td>
<td>Number of ready and active LSPs protected by this backup.</td>
</tr>
<tr>
<td>Protected S2L Sharing Familes</td>
<td>Number of ready and active sharing families protected by this backup.</td>
</tr>
<tr>
<td>Protected S2Ls</td>
<td>Number of ready and active primary tunnels protected by this backup.</td>
</tr>
</tbody>
</table>
### Field Description

| Protected i/f | Interface and NNHOP node protected by this backup. |
| Protected node | |

| Protection: NNHOP+SRLG | Type of protection provided by this backup. |
| Note | Protection can be different when a preferred SRLG is configured and an SRLG path is not found. |

| Example when backup is in use: | Amount of time left before the unused removal timeout expires. This timer only runs when the backup is in the unused state. After the timer expires, the automatic backup tunnel is removed. |
| Unused removal timeout: not running | |
| Unused removal timeout: 1h26m | |

This is sample output from the `show mpls traffic-eng tunnels` command using the `detail` keyword:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels 999 detail

Name: tunnel-te999  Destination: 1.1.1.1
Status:
  Admin: up  Oper: up  Path: valid  Signalling: connected

  path option 1, type dynamic  (Basis for Setup, path weight 2)
  Path-option attribute: po
    Number of affinity constraints: 2
      Include bit map : 0x4
      Include name : blue
      Exclude bit map : 0x2
      Exclude name : red

  Bandwidth: 300 (CT0)
  G-PID: 0x0800 (derived from egress interface properties)
  Bandwidth Requested: 300 kbps CT0
  Creation Time: Tue Aug 14 23:35:58 2012 (00:00:42 ago)

Config Parameters:
  Bandwidth: 100 kbps (CT0)  Priority: 7 7  Affinity: 0x0/0xffffffff
  Metric Type: TE (default)
  Hop-limit: disabled
  AutoRoute: disabled  LockDown: disabled  Policy class: not set
  Forwarding-Adjacency: disabled
  Loadshare: 0 equal loadshares
  Auto-bw: disabled
  Fast Reroute: Enabled, Protection Desired: Any
  Path Protection: Not Enabled
  Soft Preemption: Disabled
SNMP Index: 42
History:
  Tunnel has been up for: 00:00:30 (since Tue Aug 14 23:36:10 EST 2012)
  Current LSP:
    Uptime: 00:00:30 (since Tue Aug 14 23:36:10 EST 2012)
  Current LSP Info:
    Instance: 2, Signaling Area: OSPF 100 area 16909060
    Uptime: 00:00:30 (since Tue Aug 14 23:36:10 EST 2012)
    Outgoing Interface: GigabitEthernet0/2/0/2, Outgoing Label: 16005
    Router-IDs: local 3.3.3.3  downstream 2.2.2.2
    Soft Preemption: None
```
This is sample output from the `show mpls traffic-eng tunnels` command using the `auto-tunnel backup` keywords:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels auto-tunnel backup

AutoTunnel Backup Configuration:
  Interfaces count: 30
  Unused removal timeout: 2h
  Configured tunnel number range: 0-100
AutoTunnel Backup Summary:
  50 created, 50 up, 0 down, 8 unused
  25 NHOP, 25 NNHOP, 10 SRLG strict, 10 SRLG pref
Protected LSPs:
  10 NHOP, 20 NHOP+SRLG
  15 NNHOP, 5 NNHOP+SRLG
Protected S2L Sharing Families:
  10 NHOP, 20 NHOP+SRLG
  15 NNHOP, 5 NNHOP+SRLG
Protected S2Ls:
  10 NHOP, 20 NHOP+SRLG
  15 NNHOP, 5 NNHOP+SRLG

Cumulative Counters (last cleared 1h ago):

<table>
<thead>
<tr>
<th>Total</th>
<th>NHOP</th>
<th>NNHOP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created:</td>
<td>550 100 150</td>
<td></td>
</tr>
<tr>
<td>Connected:</td>
<td>300 250 250</td>
<td></td>
</tr>
<tr>
<td>Removed (down):</td>
<td>0 0 0</td>
<td></td>
</tr>
<tr>
<td>Removed (unused):</td>
<td>200 100 100</td>
<td></td>
</tr>
<tr>
<td>Removed (in use):</td>
<td>0 0 0</td>
<td></td>
</tr>
<tr>
<td>Range exceeded:</td>
<td>0 0 0</td>
<td></td>
</tr>
</tbody>
</table>
```
This table describes the significant fields shown in the display.

**Table 54: show mpls traffic-eng tunnels auto-tunnel backup Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoTunnel Backup Configuration</td>
<td>Header for the automatic tunnel backup configuration.</td>
</tr>
<tr>
<td>Interfaces count</td>
<td>Number of interfaces that have automatic tunnel backup enabled.</td>
</tr>
<tr>
<td>Unused removal timeout</td>
<td>Configured value and time left before expiration of the unused removal timeout attribute.</td>
</tr>
<tr>
<td>Configured tunnel number range</td>
<td>Configured tunnel number range.</td>
</tr>
<tr>
<td>AutoTunnel Backup Summary</td>
<td>Header for the automatic tunnel backup summary information.</td>
</tr>
<tr>
<td>50 created</td>
<td>Number of automatic backup tunnels created.</td>
</tr>
<tr>
<td>50 up</td>
<td>Number of automatic backup tunnels in the up state.</td>
</tr>
<tr>
<td>0 down</td>
<td>Number of automatic backup tunnels in the down state.</td>
</tr>
<tr>
<td>8 unused</td>
<td>Number of automatic backup tunnels in the unused state.</td>
</tr>
<tr>
<td>25 NHOP</td>
<td>Number of automatic backup tunnels created for NHOP protection.</td>
</tr>
<tr>
<td>25 NNHOP</td>
<td>Number of automatic backup tunnels created for NNHOP protection.</td>
</tr>
<tr>
<td>10 SRLG strict</td>
<td>Number of automatic backup tunnels created with the SRLG preferred attribute.</td>
</tr>
<tr>
<td>10 SRLG pref</td>
<td>Number of automatic backup tunnels created with the SRLG preferred attribute.</td>
</tr>
<tr>
<td>Protected LSPs</td>
<td>Headings for summary information showing current status of LSPs, S2L Sharing Families, and S2Ls that are protected by the automatic tunnel backups. Numbers include primary tunnels in FRR ready and active state.</td>
</tr>
<tr>
<td>Protected S2L Sharing Families</td>
<td></td>
</tr>
<tr>
<td>Protected S2Ls</td>
<td></td>
</tr>
<tr>
<td>10 NHOP</td>
<td>Number of automatic backup tunnels that are link protected.</td>
</tr>
<tr>
<td>20 NHOP+SRLG</td>
<td>Number of automatic backup tunnels that are link protected and using an SRLG diverse backup path.</td>
</tr>
<tr>
<td>15 NNHOP</td>
<td>Number of automatic backup tunnels that are node protected.</td>
</tr>
<tr>
<td>20 NNHOP+SRLG</td>
<td>Number of automatic backup tunnels that are node protected and use an SRLG diverse backup path.</td>
</tr>
</tbody>
</table>
Cumulative counters for automatic backuptunnels. CumulativeCounters(lastcleared1hago):
Total number of counters and breakdown of NHOP and NNHOP counters.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cumulative Counters (last cleared 1h ago):</td>
<td>Cumulative counters for automatic backup tunnels.</td>
</tr>
<tr>
<td>Headers: Total, NHOP, NNHOP</td>
<td>Total number of counters and breakdown of NHOP and NNHOP counters.</td>
</tr>
<tr>
<td>Created:</td>
<td>Cumulative number of created automatic backup tunnels since the last counter was cleared.</td>
</tr>
<tr>
<td>Connected:</td>
<td>Cumulative number of the connected automatic backup tunnels since the last counter was cleared.</td>
</tr>
<tr>
<td>Note</td>
<td>Counter increments only the first time that a tunnel connects.</td>
</tr>
<tr>
<td>Removed (down_UNUSED/in use)</td>
<td>Number of automatic backup tunnels that are removed based on state.</td>
</tr>
<tr>
<td>Range exceeded</td>
<td>Number of automatic backup tunnels attempted and later rejected when the total number exceeds the configured range.</td>
</tr>
</tbody>
</table>

This is sample output from the `show mpls traffic-eng tunnels name tunnel-te1 detail` command, which displays the soft preemption information for the tunnel-te1 tunnel:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels name tunnel-te1 detail
Name: tunnel-te1 Destination: 192.168.0.4
Status:
    Admin: up Oper: up Path: valid Signalling: connected
    path option 1, type explicit ABC1 (Basis for Setup, path weight 2)
    Last FCAIC Error [Reopt]: Thu Oct 13 16:40:24 2011
        Info: Can’t reach 10.10.10.2 on 192.168.0.2, from node 192.168.0.1 (bw)
        Info: [2] PathErr(34,1)-(reroute, flow soft-preempted) at 10.10.10.1
        G-PID: 0x0800 (derived from egress interface properties)
        Bandwidth Requested: 30000 kbps CT0
        Creation Time: Thu Oct 13 15:46:45 2011 (00:53:44 ago)
Config Parameters:
    Bandwidth: 30000 kbps (CT0) Priority: 7 7 Affinity: 0x0/0xffff
    Metric Type: TE (default)
    Hop-limit: disabled
    AutoRoute: enabled LockDown: disabled Policy class: not set
    Forwarding-Adjacency: disabled
    Loadshare: 0 equal loadshares
    Auto-bw: disabled
    Fast Reroute: Enabled, Protection Desired: Any
    Path Protection: Not Enabled
    Soft Preemption: Enabled
Soft Preemption:
    Current Status: Preemption pending
    Last Soft Preemption: Thu Oct 13 16:38:53 2011 (00:01:36 ago)
    Addresses of preempting links:
        10.10.10.1: Thu Oct 13 16:38:53 2011 (00:01:36 ago)
    Duration in preemption pending: 96 seconds
    Preemption Resolution: Pending
```
Stats:
Number of preemption pending events: 1
Min duration in preemption pending: 0 seconds
Max duration in preemption pending: 0 seconds
Average duration in preemption pending: 0 seconds
Resolution Counters: 0 reopt complete, 0 torn down
0 path protection switchover

SNMP Index: 9

History:
Tunnel has been up for: 00:52:46 (since Thu Oct 13 15:47:43 EDT 2011)
Current LSP:
Uptime: 00:52:46 (since Thu Oct 13 15:47:43 EDT 2011)
Reopt. LSP:
Last Failure:
LSP not signalled, has no S2Ls
Date/Time: Thu Oct 13 16:40:24 EDT 2011 [00:00:05 ago]
Prior LSP:
ID: path option 1 [2]
Removal Trigger: path error
Current LSP Info:
Instance: 2, Signaling Area: OSPF ring area 0
Uptime: 00:52:46 (since Thu Oct 13 15:47:43 EDT 2011)
Outgoing Interface: GigabitEthernet0/0/0/0, Outgoing Label: 16002
Router-IDs: local 192.168.0.1
downstream 192.168.0.2
Soft Preemption: Pending
Preemption Link: GigabitEthernet0/0/0/0; Address: 10.10.10.1
Preempted at: Thu Oct 13 16:38:53 2011 (00:01:36 ago)
Time left before hard preemption: 204 seconds
Path Info:
Outgoing:
Explicit Route:
Strict, 10.10.10.2
Strict, 14.14.14.4
Strict, 192.168.0.4
Record Route: Empty
Tspec: avg rate=30000 kbits, burst=1000 bytes, peak rate=30000 kbits
Session Attributes: Local Prot: Set, Node Prot: Not Set, BW Prot: Not Set
Soft Preemption Desired: Set

Resv Info:
Record Route:
IPv4 192.168.0.2, flags 0x20
Label 16002, flags 0x1
IPv4 10.10.10.2, flags 0x0
Label 16002, flags 0x1
IPv4 192.168.0.4, flags 0x20
Label 3, flags 0x1
IPv4 14.14.14.4, flags 0x0
Label 3, flags 0x1
Fspec: avg rate=30000 kbits, burst=1000 bytes, peak rate=30000 kbits
Displayed 1 (of 4) heads, 0 (of 0) midpoints, 0 (of 2) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads

This is sample output from the `show mpls traffic-eng tunnels` command with the mesh keyword:

RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels auto-tunnel
Signalling Summary:
LSP Tunnels Process: running
RSVP Process: running
Forwarding: enabled
Periodic reoptimization: every 3600 seconds, next in 3098 seconds
Periodic FRR Promotion: every 300 seconds, next in 238 seconds
Auto-bw enabled tunnels: 1000
Name: tunnel-te9000  Destination: 20.20.20.20 (auto-tunnel mesh)
Status:
  Admin: up  Oper: up  Path: valid  Signalling: connected
  path option 10, type dynamic (Basis for Setup, path weight 11)
  O-PID: 0x0800 (derived from egress interface properties)
Bandwidth Requested: 0 kbps  CT0
Creation Time: Thu Jan 14 09:09:31 2010 (01:41:20 ago)
Config Parameters:
  Bandwidth: 0 kbps (CT0)  Priority: 7 7  Affinity: 0x0/0xffff
  Metric Type: TE (default)
  AutoRoute: disabled  LockDown: disabled  Policy class: not set
  Forwarding-Adjacency: disabled
  Loadshare: 0 equal loadshares
  Auto-bw: disabled
  Fast Reroute: Disabled, Protection Desired: None
Path Protection: Not Enabled
Attribute-set: TA-NAME (type auto-mesh)

Auto-tunnel Mesh:
  Group 40: Destination-list dl-40
Unused removal timeout: not running

History:
  Tunnel has been up for: 01:40:53 (since Thu Jan 14 09:09:58 EST 2010)
  Current LSP:
    Uptime: 01:41:00 (since Thu Jan 14 09:09:51 EST 2010)
  Reopt. LSP:
    Last Failure:
      LSP not signalled, identical to the [CURRENT] LSP
      Date/Time: Thu Jan 14 09:42:30 EST 2010 [01:08:21 ago]

Path info (OSPF 100 area 0):
  Hop0: 7.0.15.1
  Hop1: 20.20.20.20

This shows an auto-tunnel mesh summary sample output from the `show mpls traffic-eng tunnels` command using the `summary` keyword:

```
RP0/RP0/CP00:router# show mpls traffic-eng tunnels summary
Thu Jan 14 10:46:34.677 EST

  LSP Tunnels Process: running
  RSVP Process: running
  Forwarding: enabled
  Periodic reoptimization: every 3600 seconds, next in 3354 seconds
  Periodic FRR Promotion: every 300 seconds, next in 193 seconds
  Periodic auto-bw collection: 1000

  Signalling Summary:
    Head: 2000 interfaces, 2000 active signalling attempts, 2000 established
    2000 explicit, 0 dynamic
    9250 activations, 7250 deactivations
    0 recovering, 2000 recovered
    Mids: 0
    Tails: 0

  Fast ReRoute Summary:
    Head: 1000 FRR tunnels, 1000 protected, 0 rerouted
    Mid: 0 FRR tunnels, 0 protected, 0 rerouted
    Summary: 1000 protected, 500 link protected, 500 node protected, 0 bw protected

  P2MP Summary:
    Tunnel Head: 250 total, 250 connected
    Destination Head: 500 total, 500 connected
    S2L Head: 500 established, 0 proceeding
    S2L Mid: 0 established, 0 proceeding
```
P2MP Fast ReRoute Summary:
- Tunnel Head: 250 FRR enabled
- S2L Head: 500 FRR, 500 protected, 0 rerouted
- S2L Mid: 0 FRR, 0 protected, 0 rerouted
- Summary: 500 protected, 500 link protected, 0 node protected, 0 bw protected

Auto-tunnel Mesh Summary:
- Auto-mesh Tunnels: 50 created, 50 up, 0 down, 25 FRR, 20 FRR enabled
- Mesh Groups: 4 groups, 50 destinations

This shows an auto-tunnel mesh summary sample output from the `show mpls traffic-eng tunnels` command using the `auto-mesh` keyword:
This example includes output for Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI) configuration for the `show mpls traffic-eng tunnels` command using the `summary` keyword:

```
RP/0/RP0/CPU0#show mpls traffic-eng tunnels auto-tunnel
Thu Jan 14 10:46:34.677 EST
   LSP Tunnels Process: running
   RSVP Process: running
   Forwarding: enabled
   Periodic reoptimization: every 3600 seconds, next in 3354 seconds
   Periodic FRR Promotion: every 300 seconds, next in 193 seconds
   Periodic auto-bw collection: 1000

Signalling Summary:
   Head: 2000 interfaces, 2000 active signalling attempts, 2000 established
         2000 explicit, 0 dynamic
         9250 activations, 7250 deactivations
         0 recovering, 2000 recovered
   Mids: 0
   Tails: 0

Fast ReRoute Summary:
   Head: 1000 FRR tunnels, 1000 protected, 0 rerouted
   Mid: 0 FRR tunnels, 0 protected, 0 rerouted
   Summary: 1000 protected, 500 link protected, 500 node protected, 0 bw protected

P2MP Summary:
   Tunnel Head: 250 total, 250 connected
   Destination Head: 500 total, 500 connected
   S2L Head: 500 established, 0 proceeding
   S2L Mid: 0 established, 0 proceeding
   S2L Tail: 0 established

P2MP Fast ReRoute Summary:
   Tunnel Head: 250 FRR enabled
   S2L Head: 500 FRR, 500 protected, 0 rerouted
   S2L Mid: 0 FRR, 0 protected, 0 rerouted
   Summary: 500 protected, 500 link protected, 0 node protected, 0 bw protected
```

This sample output displays the cost-limit configuration information:

```
RP/0/RP0/CPU0#show mpls traffic-eng tunnels detail
Name: tunnel-te1
   Signalled-Name: ios_t1
   Status: Admin: up Oper: down Path: not valid Signalling: Down
   G-PID: 0x0800 (derived from egress interface properties)
   Bandwidth Requested: 0 kbps CT0
   Creation Time: Tue Apr 15 13:00:29 2014 (5d06h ago)
   Config Parameters:
      Bandwidth: 0 kbps (CT0) Priority: 7 7 Affinity: 0x0/0xffff
      Metric Type: TE (default)
      Hop-limit: disabled
      Cost-limit: 2
      AutoRoute: disabled LockDown: disabled Policy class: not set
```
Forward class: 0 (default)
Forwarding-Adjacency: disabled
Loadshare: 0 equal loadshares
Auto-bw: disabled
Fast Reroute: Disabled, Protection Desired: None
Path Protection: Not Enabled
BFD Fast Detection: Disabled
Reoptimization after affinity failure: Enabled
Soft Preemption: Disabled
Reason for the tunnel being down: No destination is configured
SNMP Index: 10
Displayed 1 (of 1) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 0 up, 1 down, 0 recovering, 0 recovered heads

This sample output displays the 'Traffic switched to FRR backup tunnel' message, when the FRR backup is activated as part of soft-preemption:

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

Soft Preemption: Pending
  Preemption Link: GigabitEthernet0/0/0/1; Address: 14.14.14.2
  Traffic switched to FRR backup tunnel-te 1000
  Preempted at: Thu Apr 25 12:56:14 2013 (00:00:03 ago)
  Time left before hard preemption: 96 seconds

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-tunnel backup (MPLS-TE)</td>
<td>Builds automatic NHOP and NNHOP backup tunnels.</td>
</tr>
<tr>
<td>backup-bw</td>
<td>Specifies the bandwidth type that LSPs can use for a backup tunnel, whether the backup tunnel should provide bandwidth protection, and if yes, how much and in which bandwidth pool.</td>
</tr>
<tr>
<td>srlg</td>
<td>Configures an SRLG membership for a link on a given interface.</td>
</tr>
<tr>
<td>soft-preemption</td>
<td>Enables soft-preemption on a head-end for the MPLS TE tunnel.</td>
</tr>
</tbody>
</table>
show mpls traffic-eng tunnels auto-bw brief

To display the list of automatic bandwidth enabled tunnels, and to indicate if the current signaled bandwidth of the tunnel is identical to the bandwidth that is applied by the automatic bandwidth, use the `show mpls traffic-eng tunnels auto-bw brief` command in XR EXEC mode.

show mpls traffic-eng tunnels auto-bw brief

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

Use the `show mpls traffic-eng tunnels auto-bw brief` command to determine if the automatic bandwidth application has been applied on a specified tunnel. If a single tunnel is specified, only the information for that tunnel is displayed.

**Examples**

The following sample output shows the list of automatic bandwidth enabled tunnels:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels auto-bw brief

Tunnel LSP Last appl Requested Signalled Highest Application
Name ID BW(kbps) BW(kbps) BW(kbps) BW(kbps) Time Left
-------------- ------ ---------- ---------- ---------- ---------- --------------
tunnel-te0 1 10 10 50 2h 5m

tunnel-te1 5 500 300 420 1h 10m
```

This table describes the significant fields shown in the display.

**Table 55: show mpls traffic-eng tunnels auto-bw brief Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel Name</td>
<td>Name for the tunnel.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
LSP ID | ID of the Label Switched Path that is used by the tunnel.
Last appl BW (kbps) | Last bandwidth applied (for example, requested) by the automatic-bandwidth feature for the tunnel.
Requested BW (kbps) | Bandwidth that is requested for the tunnel.
Signalled BW (kbps) | Bandwidth that is actually signalled for the tunnel.
Highest BW (kbps) | Highest bandwidth measured since the last start of the application interval.
Application Time Left | Time left until the application period ends for this tunnel.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls traffic-eng tunnels, on page 335</td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
</tbody>
</table>
show mpls traffic-eng link-management soft-preemption

To display information about soft-preemption activity on a MPLS TE link, use the **show mpls traffic-eng link-management soft-preemption** command in EXEC mode.

**show mpls traffic-eng link-management soft-preemption** [interface*type*interface-path-id]

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Displays information on the specified interface.</td>
</tr>
<tr>
<td>type</td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or a virtual interface.</td>
</tr>
</tbody>
</table>

**Note**

Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.2.0</td>
<td>This command was introduced .</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

This is sample output from the **show mpls traffic-eng link-management soft-preemption** command:
**show mpls traffic-eng link-management soft-preemption interface**

POS0/1/0/1

Name: POS0/1/0/1; IPv4 Address: 1.2.3.10

Total Soft Preempted Bandwidth (BC0/BC1) kbps: 1500/1000

Currently Soft Preempted Bandwidth (BC0/BC1) kbps: 1200/800

Released Soft Preempted Bandwidth (BC0/BC1) kbps: 300/200

Currently Over-subscribed Bandwidth (BC0/BC1) kbps: 1000/600

Currently Soft Preempted Tunnels: 5 tunnels

<table>
<thead>
<tr>
<th>TunID</th>
<th>LSPID</th>
<th>Source</th>
<th>Destination</th>
<th>Pri</th>
<th>BW</th>
<th>Class</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>10</td>
<td>4.4.4.40</td>
<td>1.1.1.10</td>
<td>2/2</td>
<td>400</td>
<td>BC0</td>
<td>100</td>
</tr>
<tr>
<td>51</td>
<td>11</td>
<td>4.4.4.40</td>
<td>1.1.1.10</td>
<td>2/2</td>
<td>600</td>
<td>BC0</td>
<td>100</td>
</tr>
<tr>
<td>52</td>
<td>12</td>
<td>4.4.4.40</td>
<td>1.1.1.10</td>
<td>3/3</td>
<td>200</td>
<td>BC0</td>
<td>80</td>
</tr>
<tr>
<td>53</td>
<td>11</td>
<td>4.4.4.40</td>
<td>1.1.1.10</td>
<td>3/3</td>
<td>500</td>
<td>BC1</td>
<td>90</td>
</tr>
<tr>
<td>54</td>
<td>12</td>
<td>4.4.4.40</td>
<td>1.1.1.10</td>
<td>4/4</td>
<td>300</td>
<td>BC1</td>
<td>90</td>
</tr>
</tbody>
</table>
To show the SRLG interface and configuration information, use the `show srlg` command in EXEC mode.

```
show srlg [interface type interface-path-id] [location {node-id | all | mgmt-nodes}] [value value-number] [trace {file filename original | hexdump | last entries | reverse | stats | tailf | unique | verbose | wrapping}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface type</code></td>
<td>(Optional) Displays information on the specific interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or virtual interface. Note: Use the <code>show interfaces</code> command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>location</code></td>
<td>(Optional) Specifies a node.</td>
</tr>
<tr>
<td><code>node-id</code></td>
<td>Node ID. The <code>node-id</code> argument is entered in the <code>rack/slot/module</code> notation.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Specifies all locations.</td>
</tr>
<tr>
<td><code>mgmt-nodes</code></td>
<td>Specifies all management nodes.</td>
</tr>
<tr>
<td><code>value value-number</code></td>
<td>(Optional) Displays SRLG value numbers.</td>
</tr>
<tr>
<td><code>trace</code></td>
<td>(Optional) Displays trace information for SRLG.</td>
</tr>
<tr>
<td><code>file filename</code></td>
<td>(Optional) Displays trace information for a specific file name.</td>
</tr>
<tr>
<td><code>original</code></td>
<td>Displays the original location of the file.</td>
</tr>
<tr>
<td><code>hexdump</code></td>
<td>(Optional) Displays traces in hexadecimal format.</td>
</tr>
<tr>
<td><code>last</code></td>
<td>(Optional) Displays trace information for a specific number of entries.</td>
</tr>
<tr>
<td><code>entries</code></td>
<td>Number of entries. Replace entries with the number of entries you want to display. For example, if you enter 5, the display shows the last 5 entries in the trace data. Range is 1 to 4294967295.</td>
</tr>
<tr>
<td><code>reverse</code></td>
<td>(Optional) Displays the latest traces first.</td>
</tr>
<tr>
<td><code>stats</code></td>
<td>(Optional) Displays the statistics in the command output.</td>
</tr>
</tbody>
</table>
show srlg

Output Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tailf</td>
<td>(Optional) Displays the new traces as they are added in the command output.</td>
</tr>
<tr>
<td>unique</td>
<td>(Optional) Displays the unique entries with counts in the command output.</td>
</tr>
<tr>
<td>verbose</td>
<td>(Optional) Displays the information for internal debugging in the command output.</td>
</tr>
<tr>
<td>wrapping</td>
<td>(Optional) Displays the wrapping entries in the command output.</td>
</tr>
</tbody>
</table>

Command Default

No default behavior or values

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-services</td>
<td>read</td>
</tr>
</tbody>
</table>

Example

The following sample output is from the `show srlg value` command.

```
System Information::
 Interface Count : 2 (Maximum Interfaces Supported 250)

Interface : POS0/1/0/0, Value Count : 2
 SRLG Values : 10,20
Interface : POS0/1/0/1, Value Count : 2
 SRLG Values : 10,30
Interface : POS0/1/0/2, Value Count : 2
 SRLG Values : 10,40
Interface : POS0/2/0/0, Value Count : 1
 SRLG Values : 100
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface (MPLS-TE), on page 205</td>
<td>Enables MPLS-TE on an interface and enters MPLS-TE interface configuration mode.</td>
</tr>
<tr>
<td>mpls traffic-eng, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
</tbody>
</table>
signalled-bandwidth

To configure the bandwidth required for an MPLS-TE tunnel, use the `signalled-bandwidth` command in interface configuration mode. To disable the behavior, use the `no` form of this command.

```
signalled-bandwidth {bandwidth [class-type ct] | sub-pool bandwidth}
no signalled-bandwidth {bandwidth [class-type ct] | sub-pool bandwidth}
```

**Syntax Description**

- `bandwidth` (Optional) Bandwidth required for an MPLS-TE tunnel. Bandwidth is specified in kilobits per second. By default, bandwidth is reserved in the global pool. Range is from 0 to 4294967295.

- `class-type ct` (Optional) Configures the class type of the tunnel bandwidth request. Range is from 0 to 1. Class-type 0 is strictly equivalent to global-pool. Class-type 1 is strictly equivalent to subpool.

- `sub-pool bandwidth` Reserves the bandwidth in the subpool instead of the global pool. Range is 1 to 4294967295. A subpool bandwidth value of 0 is not allowed.

**Command Default**

The default is 0 in class-type 0.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `signalled-bandwidth` command supports two bandwidth pools (class-types) for the Diff-Serv Aware TE (DS-TE) feature.

**Note**

The Cisco Diff-serve Aware TE feature is compliant to IETF standard and will interoperate with third party vendor DS-TE. Both Russian Doll Model and Maximum Allocation Model for bandwidth allocation are supported. We recommended that IETF terminology be used in DS-TE bandwidth configurations, namely, Class-type (CT) and Bandwidth Constraints (BC).

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to set the bandwidth required for an MPLS-TE tunnel to 1000 in the global pool (class-type 0):
This example shows how to set the bandwidth required for an MPLS-TE tunnel to 1000 in the sub-pool (class-type 1):

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls traffic-eng</td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
</tbody>
</table>
**signalled-name**

To configure the name of the tunnel required for an MPLS-TE tunnel, use the `signalled-name` command in interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
signalled-name  name
no  signalled-bandwidth  name
```

**Syntax Description**

- `name`: Name used to signal the tunnel.

**Command Default**

Default name is the hostname_tID, where ID is the tunnel interface number.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the tunnel name:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# signalled-name tunnel-from-NY-to-NJ
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls traffic-eng tunnels, on page 335</td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
</tbody>
</table>
signalling advertise explicit-null (MPLS-TE)

To specify that tunnels terminating on a router use explicit-null labels, use the `signalling advertise explicit-null` command in MPLS-TE configuration mode. To return to the default behavior, use the `no` form of this command.

```
signalling advertise explicit-null
no signalling advertise explicit-null
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Implicit-null labels are advertised.

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

Use the `signalling advertise explicit-null` command to specify that tunnels terminating on this router use explicit-null labels. This command applies to tunnel labels advertised to next to last (penultimate) hop.

The explicit label is used to carry quality-of-service (QoS) information up to the terminating-end router of the label switched path (LSP).

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure explicit null tunnel labels:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls traffic-eng, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
<tr>
<td>path-selection loose-expansion metric (MPLS-TE), on page 243</td>
<td>Configures a metric type to be used to expand a path to the next loose hop for a tunnel on an area border router.</td>
</tr>
</tbody>
</table>
snmp traps mpls traffic-eng

To enable the router to send Multiprotocol Label Switching traffic engineering (MPLS-TE) Simple Network Management Protocol (SNMP) notifications or informs, use the `snmp traps mpls traffic-eng` command in global configuration mode. To disable this behavior, use the `no` form of this command.

```
snmp traps mpls traffic-eng [notification-option] preempt
no  snmp traps mpls traffic-eng [notification-option]
```

**Syntax Description**

- `notification-option` (Optional) Notification option to enable the sending of notifications to indicate changes in the status of MPLS-TE tunnels. Use one of these values:
  - `up`
  - `down`
  - `reoptimize`
  - `reroute`
  - `cisco-ext`

- `preempt` Enables MPLS-TE tunnel preempt trap.

**Command Default**

None

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

If the command is entered without the `notification-option` argument, all MPLS-TE notification types are enabled.

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

The `snmp-server enable traps mpls traffic-eng` command enables both traps and inform requests for the specified notification types. To specify whether the notifications should be sent as traps or informs, use the `snmp-server host` command and specify the keyword `trap` or `informs`.

If you do not enter the `snmp traps mpls traffic-eng` command, no MPLS-TE notifications controlled by this command are sent. To configure the router to send these MPLS-TE SNMP notifications, you must enter at least one `snmp enable traps mpls traffic-eng` command. If you enter the command with no keywords, all MPLS-TE notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. To enable multiple types of MPLS-TE notifications, you must issue a separate `snmp traps mpls traffic-eng` command for each notification type and notification option.
The `snmp traps mpls traffic-eng` command is used in conjunction with the `snmp host` command. Use the `snmp host` command to specify which host or hosts receive MPLS-TE SNMP notifications. To send notifications, you must configure at least one `snmp host` command.

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

### Examples

This example shows how to configure a router to send MPLS-TE tunnel up SNMP notifications when a configured MPLS-TE tunnel leaves the down state and enters the up state:

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snmp-server host</code></td>
<td>Specifies the recipient of a SNMP notification operation.</td>
</tr>
<tr>
<td><code>soft-preemption</code></td>
<td>Enables soft-preemption on a head-end for the MPLS TE tunnel.</td>
</tr>
</tbody>
</table>
soft-preemption

To enable soft-preemption with default timeout on a head-end for the MPLS TE tunnel, use the `soft-preemption` command in MPLS TE mode. To disable this feature, use the `no` form of this command.

```
soft-preemption  timeout  seconds
```

```
no soft-preemption
```

<table>
<thead>
<tr>
<th><strong>timeout seconds</strong></th>
<th>Defines the timeout for soft-preempted LSP, in seconds. The default timeout is 60. Range is from 30 to 300.</th>
</tr>
</thead>
</table>

**Command Default**

The default `timeout seconds` is 60 seconds.

**Command Modes**

MPLS TE configuration

Tunnel Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS-TE</td>
<td>write</td>
</tr>
</tbody>
</table>

This example shows how to enable soft-preemption on a specific tunnel:

```
RP/0/RP0/CPU0:router(config)#interface tunnel-te 50
RP/0/RP0/CPU0:router(config-if)#soft-preemption
```

This example shows how to enable soft-preemption on a node:

```
RP/0/RP0/CPU0:router(config)#mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)#soft-preemption
RP/0/RP0/CPU0:router(config-soft-preemption)#
```
srlg

To configure an MPLS traffic engineering shared-risk link group (SRLG) value for a link on a given interface, use the `srlg` command in global configuration mode. To disable this configuration, use the `no` form of this command.

```
srlg value
no srlg value
```

**Syntax Description**

- `value`: Value number that identifies the SRLG. Range is 0 to 4294967295.

**Command Default**

Shared Risk Link Group memberships are not configured.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can enter up to 30 SRLG entries on the ingress and egress ports of the interface. SRLG entries configured over 30 are silently dropped.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure an SRLG with 10 member links:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router#(config)# srlg
RP/0/RP0/CPU0:router#(config-srlg)# interface POS 0/3/0/2
RP/0/RP0/CPU0:router#(config-srlg-if)# value 10
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface (MPLS-TE), on page 205</td>
<td>Enables MPLS-TE on an interface and enters MPLS-TE interface configuration mode.</td>
</tr>
<tr>
<td>mpls traffic-eng, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
</tbody>
</table>
timers loose-path (MPLS-TE)

To configure the period between the headend retries after path errors, use the `timers loose-path` command in MPLS-TE configuration mode. To return to the default behavior, use the `no` form of this command.

```
timers loose-path retry-period value
no timers loose-path retry-period value
```

**Syntax Description**
- `retry-period value` Configures the time, in seconds, between retries upon a path error. Range is 30 to 600.

**Command Default**
- `value`: 120

**Command Modes**
- MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to change the period between retries after path errors to 300 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# timers loose-path retry-period 300
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls traffic-eng, on page 216</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
<tr>
<td>path-selection loose-expansion affinity (MPLS-TE), on page 240</td>
<td>Specifies the affinity value to be used to expand a path to the next loose hop for a tunnel on an area border router.</td>
</tr>
</tbody>
</table>
timers removal unused (auto-tunnel backup)

To configure the frequency at which a timer scans backup autotunnels and removes tunnels that are not in use, use the `timers removal unused (auto-tunnel backup)` command in auto-tunnel backup configuration mode. To return to the default behavior, use the `no` form of this command.

```
timers removal unused frequency
no timers removal unused frequency
```

**Syntax Description**

- **frequency**: Frequency, in minutes, between backup autotunnel scans to remove tunnels that are not used. Range is 0; 5 to 10080 minutes (7 days). A value of 0 disables the scanning and removal of tunnels.

**Command Default**

`frequency`: 60

**Command Modes**

auto-tunnel backup configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

The `unused` auto-tunnel backup tunnel is the tunnel that is not assigned to protect any FRR tunnel.

**Task ID**

- `mpls-te` read, write

**Example**

The following example shows that unused automatic backup tunnels are removed after the 10 minute timer scan is reached.

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# auto-tunnel backup
RP/0/RP0/CPU0:router(config-te-auto-bk)# timers removal unused 10
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls traffic-eng auto-tunnel backup unused</td>
<td>Displays the unused backup tunnels only.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>auto-tunnel backup (MPLS-TE), on page 156</td>
<td>Builds automatic next-hop and next-next-hop tunnels, and enters auto-tunnel configuration mode.</td>
</tr>
</tbody>
</table>
timeout (soft-preemption)

To override the soft-preemption default timeout, use the `timeout` command in MPLS TE mode. To remove this configuration, use the `no` form of this command.

```
soft-preemption timeout seconds
```

```
no soft-preemption
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>timeout seconds</code></td>
<td>Defines the timeout for soft-preempted LSP, in seconds. The default timeout is 60. Range is from 30 to 300.</td>
</tr>
</tbody>
</table>

**Command Default**

The default `timeout seconds` is 60 seconds.

**Command Modes**

MPLS TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS-TE</td>
<td>write</td>
</tr>
</tbody>
</table>

This example shows how to override the soft-preemption default timeout:

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# soft-preemption
RP/0/RP0/CPU0:router(config-soft-preemption)# timeout 60
```
**topology holddown sigerr (MPLS-TE)**

To specify the time that a router should ignore a link in its TE topology database in tunnel path constrained shortest path first (CSPF) computations following a TE tunnel signaling error on the link, use the `topology holddown sigerr` command in MPLS-TE configuration mode. To return to the default behavior, use the `no` form of this command.

```
topology holddown sigerr  seconds
no topology holddown sigerr  seconds
```

**Syntax Description**
- **seconds** Time that the router ignores a link during tunnel path calculations, following a TE tunnel error on the link, specified in seconds. Range is 0 to 300. Default is 10.

**Command Default**
- **seconds**: 10

**Command Modes**
- MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A router at the headend for TE tunnels can receive a Resource Reservation Protocol (RSVP) No Route error message before the router receives a topology update from the IGP routing protocol announcing that the link is down. When this happens, the headend router ignores the link in subsequent tunnel path calculations to avoid generating paths that include the link and are likely to fail when signaled. The link is ignored until the router receives a topology update from its IGP or a link holddown timeout occurs. Use the `topology holddown sigerr` command to change the link holddown time from its 10-second default value.

**Task ID**

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

**Examples**

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

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls traffic-eng</td>
<td>Enters MPLS-TE configuration mode.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>show mpls traffic-eng topology</td>
<td>Displays the current MPLS-TE global topology of this node as well as the signaling error holddown time.</td>
</tr>
</tbody>
</table>
tunnel-id (auto-tunnel backup)

To configure the range of tunnel interface numbers to be used for automatic backup tunnels, use the `tunnel-id` command in auto-tunnel backup configuration mode. To delete the automatic backup tunnels, use the `no` form of this command.

```
tunnel-id
min  number
max  number
no   tunnel-id
```

**Syntax Description**
- `min` (Optional) Minimum number for automatic backup tunnels.
- `number` Valid values are from 0 to 65535.
- `max` (Optional) Maximum number for automatic backup tunnels.

**Command Default**
No default behavior or values

**Command Modes**
Auto-tunnel backup configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

If you increase the tunnel ID range, the automatic backup tunnels that failed earlier will get created the next time automatic backup assignments are processed.

**Restrictions:**
- Command is rejected if the `max` value minus `min` value is >= 1K.
- Command is rejected if `min` value > `max` value.
- Command is rejected if `min` value is greater than the tunnel ID of an existing automatic backup tunnel.
- Command is rejected if `max` value is smaller than the tunnel ID of an existing automatic backup tunnel.
- Command is rejected if a statically configured tunnel ID matches with the configured `min` and `max` range of values.
- Command is rejected if a static backup assignment is already configured to a tunnel with an ID within the `min` value `/` `max` value range.
### Example

The following example allows 800 automatic backup tunnels to be created:

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# auto-tunnel backup
RP/0/RP0/CPU0:router(config-te-auto-bk)# tunnel-id min 1200 max 2000
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-tunnel backup (MPLS-TE), on page 156</td>
<td>Builds automatic next-hop and next-next-hop tunnels, and enters auto-tunnel configuration mode.</td>
</tr>
</tbody>
</table>
RSVP Infrastructure Commands

This module describes the commands to configure and use Resource Reservation Protocol (RSVP). RSVP is a signaling protocol used to set up, maintain, and control end-to-end quality-of-service (QoS) reservations over IP. RSVP is specified in Internet Engineering Task Force (IETF) RFC 2205 (ftp://ftp.isi.edu/in-notes/rfc2205.txt).

The protocol has been extended to signal Multiprotocol Label Switching traffic engineering (MPLS-TE) tunnels, as specified in the IETF RFC 3209, RSVP-TE: Extensions to RSVP for LSP Tunnels. The RSVP implementation supports fault handling as specified in IETF RFC 3473, Generalized Multiprotocol Label Switching (GMPLS) Signaling RSVP-TE extensions. The RSVP implementation also supports cryptographic authentication and refresh overhead reduction as specified in the RFC2747, RSVP Cryptographic Authentication and RFC2961, RSVP Refresh Overhead Reduction Extensions respectively.

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

Disable or Enable RSVP Message Checksum

Starting from Cisco IOS XR Release 4.0 RSVP computes and sets the checksum field on all outgoing RSVP messages, by default. RSVP also verifies the received checksum on all RSVP received messages to ensure its integrity.

A CLI is provided to override this default behavior and revert to the behavior exhibited in prior releases, whereby RSVP neither computes or sets the RSVP checksum field on outgoing RSVP messages, nor does it verify the checksum on received RSVP messages. This CLI is:

RP/0/RP0/CPU0:router(config)#rsvp signalling checksum disable

When the rsvp signalling checksum disable command is configured, RSVP sets a zero checksum on all outgoing RSVP messages and ignores the checksum on all received RSVP incoming messages.

Note

- authentication (RSVP), on page 387
- bandwidth (RSVP), on page 389
- bandwidth mam (RSVP), on page 391
- bandwidth rdm (RSVP), on page 393
- clear rsvp authentication, on page 395
- clear rsvp counters authentication, on page 397
RSVP Infrastructure Commands

- clear rsvp counters all, on page 399
- clear rsvp counters chkpt, on page 400
- clear rsvp counters events, on page 401
- clear rsvp counters messages, on page 402
- clear rsvp counters oor, on page 403
- clear rsvp counters prefix-filtering, on page 404
- key-source key-chain (RSVP), on page 406
- life-time (RSVP), on page 408
- rsvp, on page 410
- rsvp interface, on page 411
- rsvp neighbor, on page 413
- show rsvp authentication, on page 415
- show rsvp counters, on page 420
- show rsvp counters oor, on page 424
- show rsvp counters prefix-filtering, on page 426
- show rsvp fast-reroute, on page 429
- show rsvp graceful-restart, on page 431
- show rsvp hello instance, on page 434
- show rsvp hello instance interface-based, on page 436
- show rsvp interface, on page 438
- show rsvp request, on page 441
- show rsvp reservation, on page 443
- show rsvp sender, on page 446
- show rsvp session, on page 449
- signalling dscp (RSVP), on page 452
- signalling graceful-restart, on page 454
- signalling hello graceful-restart interface-based, on page 456
- signalling hello graceful-restart refresh interval, on page 457
- signalling hello graceful-restart refresh misses, on page 459
- signalling prefix-filtering access-list, on page 460
- signalling prefix-filtering default-deny-action, on page 462
- signalling rate-limit, on page 463
- signalling refresh interval, on page 465
- signalling refresh missed, on page 467
- signalling refresh reduction bundle-max-size, on page 469
- signalling refresh reduction disable, on page 470
- signalling refresh reduction reliable, on page 472
- signalling refresh reduction summary, on page 475
- window-size (RSVP), on page 477
authentication (RSVP)

To enter RSVP authentication mode, use the `authentication` command in global configuration mode, RSVP interface configuration mode, or RSVP neighbor configuration mode. To remove authentication parameters in the applicable mode, use the `no` form of this command.

```
authentication
no authentication
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The default value is no authentication, which means that the feature is disabled.

**Command Modes**

- Global configuration
- RSVP interface configuration
- RSVP neighbor configuration

**Command History**

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

**Task ID**

```
mpls-te  read, write
```

**Examples**

The following example shows how to enter RSVP authentication configuration mode from global configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp authentication
```

The following example shows how to activate the RSVP on an interface and enter RSVP authentication configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/2/1/0
RP/0/RP0/CPU0:router(config-rsvp-if)# authentication
```

The following example shows how to configure the RSVP neighbor with IP address 1.1.1.1 and enter neighbor authentication configuration mode:

```
RP/0/RP0/CPU0:router# configure
```
RP/0/RP0/CPU0:router(config)# rsvp neighbor 1.1.1.1 authentication
RP/0/RP0/CPU0:router(config-rsvp-nbor-auth)#

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>key-source key-chain (RSVP), on page 406</td>
<td>Specifies the source of the key information to authenticate RSVP signaling messages.</td>
</tr>
<tr>
<td></td>
<td>life-time (RSVP), on page 408</td>
<td>Controls how long RSVP maintains idle security associations with trusted neighbors.</td>
</tr>
<tr>
<td></td>
<td>window-size (RSVP), on page 477</td>
<td>Specifies the tolerance to accept out-of-sequence messages.</td>
</tr>
</tbody>
</table>
bandwidth (RSVP)

To configure RSVP bandwidth on an interface using prestandard DS-TE mode, use the `bandwidth` command in RSVP interface configuration mode. To reset the RSVP bandwidth on that interface to its default value, use the `no` form of this command.

`bandwidth [total-reservable-bandwidth [largest-reservable-flow] [sub-pool reservable-bw]] [global-pool bandwidth [sub-pool reservable-bw]] [bc0 bandwidth [bc1 reservable-bw]]`

`no bandwidth`

**Syntax Description**

- `total-reservable-bandwidth` (Optional) Total reservable bandwidth (in Kbps, Mbps or Gbps) that RSVP accepts for reservations on this interface. Range is 0 to 4294967295.

- `largest-reservable-flow` (Optional) Largest reservable flow (in Kbps, Mbps or Gbps) that RSVP accepts for reservations on this interface. Range is 0 to 4294967295.

- `sub-pool reservable-bw` (Optional) Configures the total reservable bandwidth in the sub-pool (in Kbps, Mbps, or Gbps). Range is 0 to 4294967295.

- `bc0 bandwidth` (Optional) Configures the total reservable bandwidth in the bc0 pool (in Kbps, Mbps or Gbps). The default is Kbps. Range is 0 to 4294967295.

- `bc1 reservable-bw` (Optional) Configures the total reservable bandwidth in the bc1 pool (in Kbps, Mbps or Gbps).

- `global-pool bandwidth` (Optional) Configures the total reservable bandwidth in the global-pool. Range is 0 to 4294967295 Kbps.

**Command Default**

`sub-pool-bw: 0`

**Note**

If the command is entered without the optional arguments, the total bandwidth is set to 75 percent of the intrinsic bandwidth of the interface. (If the interface has zero intrinsic bandwidth, none are reserved.)

**Command Modes**

RSVP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

RSVP is enabled either using the `rsvp interface` command or when MPLS is configured on the interface. In addition, there are other instances in which RSVP is enabled automatically; for example, when an RSVP message is received on an interface that is not configured under RSVP or MPLS (such as out-of-band signaling for an Optical User Network Interface application).

If RSVP reservation messages are received on an interface different from the one through which the corresponding Path message was sent out, the interfaces are adjusted such that all resource reservations, such as bandwidth, are done on the outgoing interface of the Path message.
Prestandard DS-TE uses the Cisco proprietary mechanisms for RSVP signaling and IGP advertisements. This DS-TE mode does not interoperate with third-party vendor equipment. Note that prestandard DS-TE is enabled only after configuring the sub-pool bandwidth values on MPLS-enabled interfaces.

---

**Note**

You can also configure RSVP bandwidth on an interface using IETF DS-TE mode. This mode supports multiple bandwidth constraint models, including the Russian Doll Model (RDM) and the Maximum Allocation Model (MAM) both with two bandwidth pools.

---

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to limit the total of all RSVP reservations on POS interface 0/3/0/0 to 5000 Kbps:

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bandwidth mam (RSVP)</code></td>
<td>Configures RSVP bandwidth on an interface using the MAM bandwidth constraints model.</td>
</tr>
<tr>
<td><code>bandwidth rdm (RSVP)</code></td>
<td>Configures RSVP bandwidth on an interface using the RDM bandwidth constraints model.</td>
</tr>
</tbody>
</table>
bandwidth mam (RSVP)

To configure RSVP bandwidth on an interface using the Maximum Allocation Model (MAM) bandwidth constraints model, use the `bandwidth mam` command in RSVP interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
bandwidth mam {total-reservable-bandwidth | max-reservable-bw maximum-reservable-bw}
[largest-reservable-flow [bc0 reservable-bandwidth] [bc1 reservable-bw]]
no bandwidth mam
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>total-reservable-bandwidth</code></td>
<td>Total reservable bandwidth (in Kbps, Mbps or Gbps) that RSVP accepts for reservations on this interface. Range is 0 to 4294967295.</td>
</tr>
<tr>
<td><code>max-reservable-bw</code></td>
<td>Configures the maximum reservable bandwidth (in Kbps, Mbps or Gbps) that RSVP accepts for reservations on this interface. Range is 0 to 4294967295.</td>
</tr>
<tr>
<td><code>maximum-reservable-bw</code></td>
<td></td>
</tr>
<tr>
<td><code>largest-reservable-flow</code></td>
<td>(Optional) Largest reservable flow (in Kbps, Mbps or Gbps) that RSVP accepts for reservations on this interface. Range is 0 to 4294967295.</td>
</tr>
<tr>
<td><code>bc0 reservable-bandwidth</code></td>
<td>(Optional) Configures the total reservable bandwidth in the bc0 pool (in Kbps, Mbps or Gbps).</td>
</tr>
<tr>
<td><code>bc1 reservable-bw</code></td>
<td>(Optional) Configures the total reservable bandwidth in the bc1 pool (in Kbps, Mbps or Gbps).</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values.

### Command Modes

RSVP interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Both the MAM and RDM models can be configured on a single interface to allow switching between each model.

___

**Note**

Non-stop forwarding (NSF) is not guaranteed when the bandwidth constraint model is changed.

---

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>
Examples

The following example shows how to limit the total of all RSVP reservations on POS interface 0/3/0/0 to 7500 kbps:

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

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth (RSVP), on page 389</td>
<td>Configures RSVP bandwidth on an interface using prestandard DS-TE mode.</td>
</tr>
<tr>
<td>bandwidth rdm (RSVP), on page 393</td>
<td>Configures RSVP bandwidth on an interface using the RDM bandwidth constraints model.</td>
</tr>
</tbody>
</table>
bandwidth rdm (RSVP)

To configure RSVP bandwidth on an interface using the Russian Doll Model (RDM) bandwidth constraints model, use the `bandwidth rdm` command in RSVP interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
bandwidth rdm {total-reservable-bw | bc0 total-reservable-bw | global-pool total-reservable-bw} [largest-reservable-flow] [bc1 reservable-bw] [sub-pool reservable-bw]
```

Syntax Description

- `total-reservable-bw`: Total reservable bandwidth (in Kbps, Mbps or Gbps). The default value is expressed in Kbps.
- `bc0 total-reservable-bw`: Reserves bandwidth in the bc0 pool (in Kbps, Mbps or Gbps).
- `global-pool`: Reserves bandwidth in the global pool.
- `largest-reservable-flow`: (Optional) Largest reservable flow (in Kbps, Mbps or Gbps). The default value is expressed in Kbps.
- `bc1`: (Optional) Reserves bandwidth in the bc1 pool (in Kbps, Mbps or Gbps).
- `sub-pool`: (Optional) Reserves bandwidth in the sub-pool.
- `reservable-bandwidth`: Reservable bandwidth in the sub- and bc1 pools (in Kbps, Mbps or Gbps). The default value is expressed in Kbps.

Command Default

No default behavior or values.

Command Modes

RSVP interface configuration

Command History

- **Release 5.0.0**: This command was introduced.

Usage Guidelines

Both the MAM and RDM bandwidth constraint models support up two bandwidth pools.

Cisco IOS XR software provides global configuration when switching between bandwidth constraint models. Both models are configured on a single interface to allow switching between models.

Note

Non-stop forwarding (NSF) is not guaranteed when the bandwidth constraint model is changed.

The `global pool` and `sub-pool` keywords are included in this command for backward compatibility with prestandard DS-TE. The `global pool` keyword is equivalent to the `bc0` keyword. The `sub-pool` keyword is equivalent to the `bc1` keyword.

RDM is the default bandwidth constraint model used in both pre-standard and IETF mode.
The following example shows how to limit the total of all RSVP reservations on POS interface 0/3/0/0 to 7500 kbps, and allows each single flow to reserve no more than 1000 kbps:

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

To eliminate RSVP security association (SA) before the lifetime expires, use the `clear rsvp authentication` command in EXEC mode.

`clear rsvp authentication [type interface-path-id] [destination IP address] [source IP address]`

## Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>type</strong></td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><em>interface-path-id</em></td>
<td>Physical interface or a virtual interface.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Use the <code>show interfaces</code> command to see a list of all possible interfaces currently configured on the router.</td>
</tr>
</tbody>
</table>

For more information about the syntax for the router, use the question mark (?) online help function.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>destination IP address</strong></td>
<td>(Optional) Eliminates the RSVP security associations (SA) before their lifetimes expire. All SAs with this destination IP address are cleared.</td>
</tr>
<tr>
<td><strong>source IP address</strong></td>
<td>(Optional) Eliminates the RSVP security associations (SA) before their lifetimes expire. All SAs with this source IP address are cleared.</td>
</tr>
</tbody>
</table>

## Command Default
No default behavior or values

## Command Modes
EXEC

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

Use the `clear rsvp authentication` command for the following reasons:

- To eliminate security associations before their lifetimes expire
- To free up memory
- To resolve a problem with a security association being in an indeterminate state

You can delete all RSVP security associations if you do not enter an optional filter (interface, source, or destination IP address).

If you delete a security association, it is recreated as needed.

## Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>execute</td>
</tr>
</tbody>
</table>

## Examples

The following example shows how to clear each SA:
clear rsvp authentication

The following example shows how to clear each SA with the destination address 1.1.1.1:

RP/0/RP0/CPU0:router# clear rsvp authentication destination 1.1.1.1

The following example shows how to clear each SA with the source address 2.2.2.2:

RP/0/RP0/CPU0:router# clear rsvp authentication source 2.2.2.2

The following example shows how to clear each SA with the POS interface 0/2/1/0:

RP/0/RP0/CPU0:router# clear rsvp authentication POS 0/2/1/0

The following example shows how to clear each SA on the POS interface 0/2/1/0, destination address 1.1.1.1, and source address 2.2.2.2:

RP/0/RP0/CPU0:router# clear rsvp authentication POS 0/2/1/0 destination 1.1.1.1 source 2.2.2.2

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>life-time (RSVP), on page 408</td>
<td>Controls how long RSVP maintains idle security associations with other trusted RSVP neighbors.</td>
</tr>
</tbody>
</table>
clear rsvp counters authentication

To eliminate RSVP counters for each security association (SA), use the `clear rsvp counters authentication` command in EXEC mode.

```
clear rsvp counters authentication [type interface-path-id] [destination IP address ] [source IP address ]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>type</code></td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or a virtual interface. <strong>Note</strong> Use the <code>show interfaces</code> command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>destination IP address</code></td>
<td>(Optional) Eliminates authentication-related statistics for each security association (SA) with this destination IP address.</td>
</tr>
<tr>
<td><code>source IP address</code></td>
<td>(Optional) Eliminates authentication-related statistics for each security association (SA) with this source IP address.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

- **Task Operations ID**: mpls execute

**Examples**

The following example shows how to clear authentication counters for each SA:

```
RP/0/RP0/CPU0:router# clear rsvp counters authentication
```

The following example shows how to clear authentication counters for each SA with the destination address 1.1.1.1:

```
RP/0/RP0/CPU0:router# clear rsvp counters authentication destination 1.1.1.1
```
The following example shows how to clear authentication counters for each SA with the source address 2.2.2.2:

```
RP/0/RP0/CPU0:router# clear rsvp counters authentication source 2.2.2.2
```

The following example shows how to clear authentication counters for each SA with the POS interface 0/2/1/0:

```
RP/0/RP0/CPU0:router# clear rsvp counters authentication POS 0/2/1/0
```

The following example shows how to clear authentication counters for each SA on the POS interface 0/2/1/0, destination address 1.1.1.1, and source address 2.2.2.2:

```
RP/0/RP0/CPU0:router# clear rsvp counters authentication POS 0/2/1/0 destination 1.1.1.1 source 2.2.2.2
```
# clear rsvp counters all

To clear (set to zero) all RSVP message and event counters that are being maintained by the router, use the `clear rsvp counters all` command in EXEC mode.

## Syntax Description

- **type** *(Optional) Interface type.* For more information, use the question mark (?) online help function.

- **interface-path-id** Physical interface or a virtual interface.

## Note

Use the `show interfaces` command to see a list of all possible interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

## Command Modes

**EXEC**

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Task ID

- mpls-te: read, write

## Examples

The following example shows how to clear all message and event counters:

```
RP/0/RP0/CPU0:router# clear rsvp counters all
```

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear rsvp counters events, on page 401</td>
<td>Clears all RSVP event counters that are being maintained by the router.</td>
</tr>
<tr>
<td>clear rsvp counters messages, on page 402</td>
<td>Clears all RSVP message counters that are being maintained by the router.</td>
</tr>
<tr>
<td>show rsvp counters, on page 420</td>
<td>Shows all RSVP message/event counters that are being maintained by the router.</td>
</tr>
</tbody>
</table>
clear rsvp counters chkpt

To clear RSVP checkpoint counters, use the clear rsvp counters chkpt command in EXEC mode.

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

**Command Default**
No default behavior or values

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to clear all message and event counters:

```
RP/0/RP0/CPU0:router# clear rsvp counters chkpt
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear rsvp counters events, on page 401</td>
<td>Clears all RSVP event counters that are being maintained by the router.</td>
</tr>
<tr>
<td>clear rsvp counters messages, on page 402</td>
<td>Clears all RSVP message counters that are being maintained by the router.</td>
</tr>
<tr>
<td>show rsvp counters, on page 420</td>
<td>Shows all RSVP message/event counters that are being maintained by the router.</td>
</tr>
</tbody>
</table>
clear rsvp counters events

To clear (set to zero) all RSVP event counters that are being maintained by the router, use the **clear rsvp counters events** command in EXEC mode.

**clear rsvp counters events [type interface-path-id]**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or a virtual interface.</td>
</tr>
</tbody>
</table>

**Note**

Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear all event counters:

```
RP/0/RP0/CPU0:router# clear rsvp counters events
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear rsvp counters messages, on page 402</td>
<td>Clears all RSVP message counters that are being maintained by the router.</td>
</tr>
<tr>
<td>show rsvp counters, on page 420</td>
<td>Shows RSVP event counters that are being maintained by the router when the <strong>events</strong> option is specified.</td>
</tr>
</tbody>
</table>
clear rsvp counters messages

To clear (set to zero) all RSVP message counters that are being maintained by the router, use the **clear rsvp counters messages** command in EXEC mode.

**clear rsvp counters messages** [type  interface-path-id]

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or a virtual interface.</td>
</tr>
</tbody>
</table>

**Note** Use the **show interfaces** command to see a list of all possible interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

The following example shows how to set all RSVP message counters for POS interface 0/3/0/2 to zero:

```plaintext
RP/0/RP0/CPU0:router# clear rsvp counters messages pos0/3/0/2
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show rsvp counters, on page 420</td>
<td>Displays the number of RSVP messages sent and received.</td>
</tr>
</tbody>
</table>
clear rsvp counters oor

To clear internal RSVP counters on out of resources (OOR) events, use the clear rsvp counters oor command in EXEC mode.

**clear rsvp counters oor [type interface-path-id]**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or a virtual interface.</td>
</tr>
</tbody>
</table>

**Note**
Use the show interfaces command to see a list of all possible interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**
No default behavior or values

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the clear rsvp counters oor command to set RSVP OOR counters to zero.

**Examples**
The following example show how to clear all RSVP message counters for POS interface 0/3/0/2 to zero:

```
RP/0/RP0/CPU0:router# clear rsvp counters oor pos0/3/0/2
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show rsvp counters oor, on page 424</td>
<td>Displays the internal RSVP counters on OOR events.</td>
</tr>
</tbody>
</table>
clear rsvp counters prefix-filtering

To clear internal prefix-filtering related RSVP counters, use the `clear rsvp counters prefix-filtering` command in EXEC mode.

`clear rsvp counters prefix-filtering {interface [type interface-path-id] | access-list [aclname]}`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Clears RSVP prefix-filtering counters for all interfaces.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or a virtual interface.</td>
</tr>
<tr>
<td>aclname</td>
<td>(Optional) Name of the access list.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `clear rsvp counters prefix-filtering` command to set RSVP prefix-filtering related RSVP counters to zero.

**Examples**

The following example shows how to set all RSVP message counters for POS interface 0/3/0/2 to zero:

```
RP/0/RP0/CPU0:router# clear rsvp counters prefix-filtering interface pos0/3/0/2
```
The following example shows how to set all RSVP prefix-filtering counters for access-list banks to zero:

```
RP/0/RP0/CPU0:router# clear rsvp counters prefix-filtering access-list banks
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show rsvp counters prefix-filtering, on page 426</td>
<td>Displays the internal prefix-filtering related RSVP counters.</td>
</tr>
</tbody>
</table>
key-source key-chain (RSVP)

To specify the source of the key information to authenticate RSVP messages, use the `key-source key-chain` command in the appropriate RSVP authentication configuration mode. To remove the key source from the appropriate RSVP authentication configuration mode, use the `no` form of this command.

```
key-source key-chain  key-chain-name
no  key-source key-chain  key-chain-name
```

**Syntax Description**

- `key-chain-name` Name of the keychain. The maximum number of characters is 32.

**Command Default**

The default value is none, which means that the key source is not specified.

**Command Modes**

- RSVP authentication configuration
- RSVP interface authentication configuration
- RSVP neighbor authentication configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- RSVP authentication is enabled regardless of whether or not the specified keychain exists or has no available keys to use. If the specified keychain does not exist or there are no available keys in the keychain, RSVP authentication processing fails.
- The `key-source key-chain` command does not create a keychain but just specifies which keychain to use. You must configure a keychain first. For an example of how a key chain is configured, see .

- The `no key-source key-chain` command does not necessarily disable the authentication.
- RSVP authentication supports only keyed-hash message authentication code (HMAC)-type algorithms. For inheritance procedures, see .

**Examples**

The following example shows that the source of the key information is specified for the keychain mpls-keys in RSVP authentication configuration mode:
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp authentication
RP/0/RP0/CPU0:router(config-rsvp-auth)# key-source key-chain mpls-keys

The following example shows that the source of the key information is specified for the keychain mpls-keys for a POS interface in RSVP authentication configuration mode:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface POS 0/2/1/0
RP/0/RP0/CPU0:router(config-rsvp-if)# authentication
RP/0/RP0/CPU0:router(config-rsvp-if-auth)# key-source key-chain mpls-keys

The following example shows that the source of the key information is specified for the keychain mpls-keys in RSVP neighbor authentication configuration mode:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp neighbor 1.1.1.1 authentication
RP/0/RP0/CPU0:router(config-rsvp-nbor-auth)# key-source key-chain mpls-keys

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>life-time (RSVP), on page 408</td>
<td>Controls how long RSVP maintains idle security associations with other trusted RSVP neighbors.</td>
</tr>
<tr>
<td></td>
<td>window-size (RSVP), on page 477</td>
<td>Specifies the tolerance to accept out-of-sequence messages.</td>
</tr>
</tbody>
</table>
**life-time (RSVP)**

To control how long RSVP maintains idle security associations with other trusted RSVP neighbors, use the `life-time` command in the appropriate RSVP authentication configuration mode. To disable the lifetime setting, use the `no` form of this command.

```
life-time  seconds
no life-time  seconds
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>seconds</th>
<th>Length of time, in seconds, that RSVP maintains security associations with other trusted RSVP neighbors. Range is 30 to 86400.</th>
</tr>
</thead>
</table>

**Command Default**

```
seconds: 1800 (30 minutes)
```

**Command Modes**

- RSVP authentication configuration
- RSVP interface authentication configuration
- RSVP neighbor authentication configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For inheritance procedures, see.

Use the `life-time (RSVP)` command to indicate when to end idle security associations with RSVP trusted neighbors.

By setting a larger lifetime, the router remembers the state for a long period time which provides better protection against a replay attack.

Use the `clear rsvp authentication` command to free security associations before their lifetimes expire.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a lifetime of 2000 seconds for each SA in RSVP authentication configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp authentication
RP/0/RP0/CPU0:router(config-rsvp-auth)# life-time 2000
```
The following example shows how to configure a lifetime of 2000 seconds for each SA in RSVP neighbor authentication configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp neighbor 1.1.1.1 authentication
RP/0/RP0/CPU0:router(config-rsvp-nbor-auth)# life-time 2000
```

The following example shows how to configure a lifetime of 2000 seconds for each SA in RSVP interface authentication configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface POS 0/2/1/0
RP/0/RP0/CPU0:router(config-rsvp-if)# authentication
RP/0/RP0/CPU0:router(config-rsvp-if-auth)# life-time 2000
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear rsvp authentication, on page 395</td>
<td>Clears out RSVP security associations.</td>
</tr>
<tr>
<td>key-source key-chain (RSVP), on page 406</td>
<td>Specifies the source of the key information to authenticate RSVP signaling messages.</td>
</tr>
<tr>
<td>window-size (RSVP), on page 477</td>
<td>Specifies the tolerance to accept out-of-sequence messages.</td>
</tr>
</tbody>
</table>
**rsvp**

To enable functionality for Resource Reservation Protocol (RSVP) and enter RSVP configuration commands, use the `rsvp` command in global configuration mode. To return to the default behavior, use the `no` form of this command.

```
rsvp
no rsvp
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

No default behavior or values

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable RSVP functionality and enter the sub-mode for RSVP configuration commands:

```
RP/0/RP0/CPU0:router(config)# rsvp
RP/0/RP0/CPU0:router(config-rsvp)#
```
rsvp interface

To configure RSVP on an interface, use the `rsvp interface` command in global configuration mode. To disable RSVP on that interface, use the `no` form of this command.

```
rsvp interface type interface-path-id
no rsvp interface type interface-path-id
```

**Syntax Description**

- `type` Interface type. For more information, use the question mark (?) online help function.
- `interface-path-id` Physical interface or a virtual interface.

**Note** Use the `show interfaces` command to see a list of all possible interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

RSVP is enabled by default on an interface under the following conditions. (Enabling RSVP on an interface means that interface can be used by RSVP to send and receive RSVP messages).

- RSVP is configured on that interface using the `rsvp interface` command.
- MPLS is configured on that interface.
- Automatically enabled as in the case of out-of-band signaling for the Optical User Network Interface (O-UNI) application, where an RSVP message could be received on an interface which is not configured under RSVP or MPLS.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When RSVP is enabled on an interface by any of the three methods mentioned in the above section, the default bandwidth is 0. Use the bandwidth command in RSVP interface configuration mode to configure the bandwidth on an interface.

If the interface bandwidth is 0, RSVP can be used only to signal flows that do not require bandwidth on this interface.

The `rsvp interface` command enables the RSVP interface configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>
Examples

The following example shows how to enable the RSVP interface configuration mode and to enable RSVP on this interface with 0 bandwidth:

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth (RSVP), on page 389</td>
<td>Configures RSVP bandwidth on an interface using prestandard DS-TE mode.</td>
</tr>
<tr>
<td>signalling dscp (RSVP), on page 452</td>
<td>Gives all RSVP packets sent out on a specific interface higher priority in the network by marking them with a particular DSCP.</td>
</tr>
</tbody>
</table>
rsvp neighbor

To specify an RSVP neighbor, use the **rsvp neighbor** command in global configuration mode. To deactivate authentication for a neighbor, use the **no** form of this command.

```
rsvp neighbor  IP-address  authentication
no  rsvp neighbor  IP-address  authentication
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-address</td>
<td>IP address of the neighbor. A single IP address of a specific neighbor; usually one of the neighbor's physical or logical (loopback) interfaces.</td>
</tr>
<tr>
<td>authentication</td>
<td>Configures RSVP authentication parameters.</td>
</tr>
</tbody>
</table>

**Command Default**

No default values or behaviors

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- **Note**
  - RSVP neighbor configuration mode can be used only if you want to configure authentication for a particular neighbor.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enter RSVP neighbor authentication configuration mode for IP address 1.1.1.1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp neighbor 1.1.1.1 authentication
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key-source key-chain (RSVP), on page 406</td>
<td>Specifies the source of the key information to authenticate RSVP signaling messages.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>life-time (RSVP), on page 408</td>
<td>Controls how long RSVP maintains idle security associations with other trusted RSVP neighbors.</td>
</tr>
<tr>
<td>window-size (RSVP), on page 477</td>
<td>Specifies the tolerance to accept out-of-sequence messages.</td>
</tr>
</tbody>
</table>
show rsvp authentication

To display the database for the security association that RSVP has established with other RSVP neighbors, use the **show rsvp authentication** command in EXEC mode.

```
show rsvp authentication [type interface-path-id] [destination IP-address] [detail] [mode {receive | send}] [neighbor IP-address] [source IP-address]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or a virtual interface.</td>
</tr>
<tr>
<td>Note</td>
<td>Use the <strong>show interfaces</strong> command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>destination IP-address</td>
<td>(Optional) Displays the database for the security association (SA) for the destination IP address. The IP address argument is the IP address of the destination address.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays additional information about RSVP security SAs.</td>
</tr>
<tr>
<td>mode</td>
<td>(Optional) Specifies the SA type. An SA is used to authenticate either incoming (receive) or outgoing (send) messages.</td>
</tr>
<tr>
<td>receive</td>
<td>Displays SAs for incoming messages.</td>
</tr>
<tr>
<td>send</td>
<td>Displays SAs for outgoing messages.</td>
</tr>
<tr>
<td>neighbor IP-address</td>
<td>(Optional) Displays the RSVP authentication information for the neighbor IP address. The IP-address argument is the IP address of the neighbor. For the send SA, the neighbor address is the destination address. For receive, the neighbor address is the source address.</td>
</tr>
<tr>
<td>source IP-address</td>
<td>(Optional) Displays the database for the SA for the source IP address. The IP-address argument is the IP address of the source address.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
The following sample output displays information for RSVP authentication:

RP/0/RP0/CPU0:router# show rsvp authentication

Codes: S - static, G - global, N - neighbor, I - interface, C - chain

<table>
<thead>
<tr>
<th>Source Address</th>
<th>Dest Address</th>
<th>Interface</th>
<th>Mode</th>
<th>Key-Source</th>
<th>Key-ID</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0.0.1</td>
<td>3.0.0.2</td>
<td>PO0/7/0/2</td>
<td>Send mpls-keys</td>
<td>1</td>
<td>SGC</td>
<td></td>
</tr>
<tr>
<td>3.0.0.2</td>
<td>3.0.0.1</td>
<td>PO0/7/0/2</td>
<td>Recv mpls-keys</td>
<td>1</td>
<td>SGC</td>
<td></td>
</tr>
</tbody>
</table>

This table describes the significant fields shown in the display.

**Table 56: show rsvp authentication Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>IP address of the sender. For Send mode, this is the local address (either the address of the Interface field or the local router ID). For Recv mode, this is the address of the RSVP neighbor.</td>
</tr>
<tr>
<td>Dest Address</td>
<td>IP address of the receiver. For Send mode, this is the address of the RSVP neighbor. For Recv mode, this is the local address (either the address of the Interface field or the local router ID).</td>
</tr>
<tr>
<td>Interface</td>
<td>Name of the interface over which the security association is being maintained.</td>
</tr>
<tr>
<td>Mode</td>
<td>Direction of the association for the following mode types:</td>
</tr>
<tr>
<td></td>
<td><strong>Send</strong></td>
</tr>
<tr>
<td></td>
<td>Authenticates messages that you forward.</td>
</tr>
<tr>
<td></td>
<td><strong>Recv</strong></td>
</tr>
<tr>
<td></td>
<td>Authenticates messages that you receive.</td>
</tr>
<tr>
<td>Key-Source</td>
<td>Key source identification string that is currently set to the configured keychain name.</td>
</tr>
<tr>
<td>Key-ID</td>
<td>The last successful key ID that is used for authentication and maps to the keychain ID configuration. If the value is too large to fit into the column, it is truncated and a (...) suffix is appended. Use the detail mode to see the non-truncated key ID.</td>
</tr>
</tbody>
</table>
**Field** | **Description**
---|---
**Code** | Code field has the following terms:
**Static** | Key is static and configured.
**Global** | Key is global-based.
**Neighbor** | Key is neighbor-based.
**Interface** | Key is interface-based.
**Chain** | Key is part of a keychain.

The following sample output shows detailed information about a Send mode SA that is followed by a Receive mode SA:

```
RP/0/RP0/CPU0:router# show rsvp authentication detail

RSVP Authentication Information:
Source Address: 3.0.0.1
Destination Address: 3.0.0.2
Neighbour Address: 3.0.0.2
Interface: POS0/7/0/2
Direction: Send
LifeTime: 1800 (sec)
LifeTime left: 1305 (sec)
KeyType: Static Global KeyChain
Key Source: name1
Key Status: No error
KeyID: 1
Challenge: Not supported
Digest: HMAC MD5 (16)
TX Sequence: 5023969459702858020 (0x45b8b99b00000124)
Messages successfully authenticated: 245
Messages failed authentication: 0

Receive Errors:
Incomplete security association: 0
Missing INTEGRITY object: 0
Incorrect digest: 0
Digest type mismatch: 0
Duplicate sequence number: 0
Out-of-range sequence number: 0
Invalid message format: 0
```
This table describes the significant fields shown in the display.

**Table 57: show rsvp authentication detail Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>IP address of the sender. For Send mode, this is the local address (either the address of the Interface field or the local router ID). For Recv mode, this is the address of the RSVP neighbor.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>IP address of the receiver. For Send mode, this is the address of the RSVP neighbor. For Recv mode, this is the local address (either the address of the Interface field or the local router ID).</td>
</tr>
<tr>
<td>Neighbor Address</td>
<td>IP address of the RSVP neighbor with which the security association is being maintained.</td>
</tr>
<tr>
<td>Interface</td>
<td>Name of the interface over which the security association is being maintained.</td>
</tr>
</tbody>
</table>
| Direction | Direction of the association for the following mode types:  
  Send  
  Authenticates messages that you forward.  
  Recv  
  Authenticates messages that you receive. |
| LifeTime | Configured expiration timer value.                                                                                                          |
| LifeTime left | Number of seconds until the expiration timer expires.                                                                                      |
| KeyType | Keys that are used:  
  Static  
  Key is static and configured.  
  Global  
  Key is global-based.  
  Neighbor  
  Key is neighbor-based.  
  Interface  
  Key is interface-based.  
  Chain  
  Key is part of a keychain. |
<p>| Key-Source | Key source identification string that is currently set to the configured keychain name.                                                |
| Key Status | Last status reported from the key source.                                                                                                 |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key-ID</td>
<td>Last successful key ID that is used for authentication and that maps to the keychain ID configuration. If the value is too large to fit into the column, it is truncated and a (...) suffix is appended. (Use the detail mode to see the non-truncated key ID.)</td>
</tr>
<tr>
<td>Digest</td>
<td>Digest algorithm that is used. The algorithms are either HMAC-MD5 or HMAC-SHA1.</td>
</tr>
<tr>
<td>Challenge</td>
<td>Current challenge status (always not supported) reported.</td>
</tr>
<tr>
<td>Tx Sequence</td>
<td>Last sequence number that was sent.</td>
</tr>
<tr>
<td>Messages successfully authenticated</td>
<td>Number of messages authenticated by using this SA.</td>
</tr>
<tr>
<td>Messages failed authentication</td>
<td>Number of messages that failed authentication using this SA.</td>
</tr>
<tr>
<td>Sequence Window Size</td>
<td>Maximum configured RX sequence number window.</td>
</tr>
<tr>
<td>Sequence Window Count</td>
<td>Currently used size of the RX sequence number window.</td>
</tr>
<tr>
<td>Incomplete security association</td>
<td>Number of messages that are dropped due to a key failure.</td>
</tr>
<tr>
<td>Incorrect digest</td>
<td>Number of messages that are dropped due to an incorrect digest.</td>
</tr>
<tr>
<td>Digest type mismatch</td>
<td>Number of messages that are dropped due to an incorrect digest length, which implies an algorithm mismatch.</td>
</tr>
<tr>
<td>Duplicate sequence number</td>
<td>Number of messages that are dropped due to a duplicate sequence number.</td>
</tr>
<tr>
<td>Out-of-range sequence number</td>
<td>Number of messages that are dropped due to a sequence number range (window-size) checking.</td>
</tr>
<tr>
<td>Invalid message format</td>
<td>Number of messages that are dropped due to formatting errors, such as incorrect objects.</td>
</tr>
</tbody>
</table>
show rsvp counters

To display internal RSVP counters, use the show rsvp counters command in EXEC mode.

```
show rsvp counters  {messages  [{type  interface-path-id | summary }] | events | database}
```

**Syntax Description**

- **messages**
  - Displays a historical count of the number of messages RSVP has received and sent on each interface along with a summation.

- **type**
  - (Optional) Interface type. For more information, use the question mark (?) online help function.

- **interface-path-id**
  - Physical interface or a virtual interface.

  **Note**
  - Use the show interfaces command to see a list of all possible interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

- **summary**
  - (Optional) Displays the aggregate counts of all interfaces.

- **events**
  - Displays the number of states expired for lack of refresh and a count of received No Acknowledgements (NACKs).

- **database**
  - Displays counters on RSVP database, including number of paths, session, and so on.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

In message counters, bundle messages are counted as single bundle messages. The component messages are not counted separately.

The **messages** keyword shows the counters for all the interfaces. In addition, the aggregate summary is shown by using both the **messages** and **summary** keywords.

**Task ID**

- **mpls-te**
  - read,
  - write

**Examples**

The following is sample output from the **show rsvp counters messages** command for POS0/3/0/0:
This table describes the significant fields shown in the display.

**Table 58: show rsvp counters messages Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>Number of Path messages sent downstream or received from an upstream node.</td>
</tr>
<tr>
<td>PathError</td>
<td>Number of PathError messages received from a downstream neighbor or sent to an upstream neighbor.</td>
</tr>
<tr>
<td>PathTear</td>
<td>Number of PathTear messages sent downstream, or messages received, from upstream neighbors.</td>
</tr>
<tr>
<td>ResvConfirm</td>
<td>Number of ResvConfirm messages received from an upstream neighbor or sent to a downstream neighbor.</td>
</tr>
<tr>
<td>Bundle</td>
<td>Number of Bundle messages containing RSVP messages sent and received by the neighbor.</td>
</tr>
<tr>
<td>SRefresh</td>
<td>Number of Summary Refresh messages sent to and received by a neighbor to refresh the path and reservation states.</td>
</tr>
<tr>
<td>Retransmit</td>
<td>Number of messages retransmitted to ensure reliable messaging (related to refresh reduction).</td>
</tr>
<tr>
<td>Resv</td>
<td>Number of Reservation messages received from a downstream neighbor or sent to an upstream neighbor to reserve resources.</td>
</tr>
<tr>
<td>ResvError</td>
<td>Number of Reservation Error messages received from a upstream neighbor or sent to a downstream neighbor.</td>
</tr>
<tr>
<td>ResvTear</td>
<td>Number of Reservation Tear messages received from a downstream neighbor or sent to an upstream neighbor to tear down RSVP flows.</td>
</tr>
<tr>
<td>Ack</td>
<td>Number of Acknowledgement messages sent and received by a neighbor acknowledging receipt of a message.</td>
</tr>
<tr>
<td>Hello</td>
<td>Number of Hello messages sent to and received by a neighbor.</td>
</tr>
<tr>
<td>OutOfOrder</td>
<td>Number of messages received that are out of order.</td>
</tr>
<tr>
<td>RateLimited</td>
<td>Number of RSVP packets affected by rate limiting.</td>
</tr>
</tbody>
</table>

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
  Expired Path states 0 Expired Path states 0
  Expired Resv states 0 Expired Resv states 0
  NACKs received 0 NACKs received 0

POS0/3/0/3 All RSVP Interfaces
  Expired Path states 0 Expired Path states 0
  Expired Resv states 0 Expired Resv states 0
  NACKs received 0 NACKs received 0

This table describes the significant fields shown in the display.

Table 59: show rsvp counters events Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expired Path states</td>
<td>Number of Path states expired for lack of refresh.</td>
</tr>
<tr>
<td>Expired Reserve states</td>
<td>Number of Resv states expired for lack of refresh.</td>
</tr>
<tr>
<td>NACKs received</td>
<td>Number of NACKS received.</td>
</tr>
</tbody>
</table>

The following is sample output from the show rsvp counters database command:

RP/0/RP0/CPU0:router# show rsvp counters database

Sessions: 0
Locally created and incoming paths: 0
Outgoing paths: 0
Locally created and incoming Reservations: 0
Outgoing Reservations: 0
Interfaces: 4

This table describes the significant fields shown in the display.

Table 60: show rsvp counters database Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions</td>
<td>RSVP sessions.</td>
</tr>
<tr>
<td>Locally created and incoming paths</td>
<td>Path states created by a:</td>
</tr>
<tr>
<td></td>
<td>• Local application on the node.</td>
</tr>
<tr>
<td></td>
<td>• Path message received from the network.</td>
</tr>
<tr>
<td>Outgoing paths</td>
<td>Outgoing path states.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Locally created and incoming Reservations</td>
<td>Reservations created by a:</td>
</tr>
<tr>
<td></td>
<td>• Local application on the node.</td>
</tr>
<tr>
<td></td>
<td>• Path message received from the network.</td>
</tr>
<tr>
<td>Outgoing Reservations</td>
<td>Outgoing reservation (request) states.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Known RSVP interfaces.</td>
</tr>
</tbody>
</table>
show rsvp counters oor

To display internal RSVP counters on out of resources (OOR) events, use the `show rsvp counters oor` command in EXEC mode.

```
show rsvp counters oor [type interface-path-id | summary]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>type</code></td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or a virtual interface. Note: Use the <code>show interfaces</code> command to see a list of all possible interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>summary</code></td>
<td>(Optional) Displays a summary of OOR events.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>No default behavior or values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>EXEC</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `show rsvp counters oor` command:

```
RP/0/RP0/CPU0:router# show rsvp counters oor

POS 0/3/0/0 Rejected Path 24
POS 0/3/0/2 Rejected Path 31
All RSVP Interfaces Rejected Path 55
```
This table describes the significant fields shown in the display.

Table 61: `show rsvp counters oor` Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>Number of Path messages received on the interface that were rejected due to oor conditions.</td>
</tr>
</tbody>
</table>
# show rsvp counters prefix-filtering

To display internal prefix-filtering related RSVP counters, use the `show rsvp counters prefix-filtering` command in EXEC mode.

`show rsvp counters prefix-filtering interface [{type interface-path-id|summary}] access-list [aclname]`

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface</code></td>
<td>Displays RSVP prefix-filtering counters for all interfaces.</td>
</tr>
<tr>
<td><code>type</code></td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or a virtual interface.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Use the <code>show interfaces</code> command to see a list of all possible interfaces currently configured on the router.</td>
</tr>
<tr>
<td><code>summary</code></td>
<td>(Optional) Displays a summary of RSVP prefix-filtering counters on all interfaces.</td>
</tr>
<tr>
<td><code>access-list</code></td>
<td>Displays RSVP prefix-filtering counters for the access control list.</td>
</tr>
<tr>
<td><code>aclname</code></td>
<td>(Optional) Name of the access control list.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Counters do not increment if you have not configured an access control list for prefix-filtering.

**Task ID**

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

**Examples**

The following is sample output from the `show rsvp counters prefix-filtering` command:
RP/0/RP0/CPU0:router#  show rsvp counters prefix-filtering interface

<table>
<thead>
<tr>
<th>Route</th>
<th>Fwd</th>
<th>Local</th>
<th>Drop</th>
<th>Def-Drop</th>
<th>Def-Proc</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ResvConfirm</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Fwd</th>
<th>Local</th>
<th>Drop</th>
<th>Def-Drop</th>
<th>Def-Proc</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>1</td>
<td>0</td>
<td>219</td>
<td>0</td>
<td>0</td>
<td>222</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
<td>0</td>
<td>31</td>
<td>0</td>
<td>0</td>
<td>31</td>
</tr>
<tr>
<td>ResvConfirm</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>1</td>
<td>0</td>
<td>219</td>
<td>0</td>
<td>0</td>
<td>253</td>
</tr>
</tbody>
</table>

The following is sample output from the show rsvp counters prefix-filtering interface type command:

RP/0/RP0/CPU0:router#  show rsvp counters prefix-filtering interface POS 0/5/0/1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Fwd</th>
<th>Local</th>
<th>Drop</th>
<th>Def-Drop</th>
<th>Def-Proc</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ResvConfirm</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

The following is sample output from the show rsvp counters prefix-filtering interface summary command:

RP/0/RP0/CPU0:router#  show rsvp counters prefix-filtering interface summary

<table>
<thead>
<tr>
<th>Route</th>
<th>Fwd</th>
<th>Local</th>
<th>Drop</th>
<th>Def-Drop</th>
<th>Def-Proc</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>219</td>
<td>0</td>
<td>227</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
<td>0</td>
<td>31</td>
<td>0</td>
<td>0</td>
<td>31</td>
</tr>
<tr>
<td>ResvConfirm</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>250</td>
<td>0</td>
<td>258</td>
</tr>
</tbody>
</table>

The following is sample output from the show rsvp counters prefix-filtering access-list banks command:

RP/0/RP0/CPU0:router#  show rsvp counters prefix-filtering access-list banks

<table>
<thead>
<tr>
<th>ACL: banks</th>
<th>Forward</th>
<th>Local</th>
<th>Drop</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PathTear</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

MPLS Command Reference for Cisco NCS 6000 Series Routers
This table describes the significant fields shown in the display.

**Table 62: show rsvp counters prefix-filtering interface and summary CommandField Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fwd</td>
<td>Number of messages forwarded to the next router.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The messages are counted against the <em>routed</em> interface only because RSVP has no record of what interface the messages will be forwarded to.</td>
</tr>
<tr>
<td>Local</td>
<td>Number of messages not forwarded (because they are locally destined).</td>
</tr>
<tr>
<td>Drop</td>
<td>Number of messages dropped.</td>
</tr>
<tr>
<td>Def-Drop</td>
<td>Number of messages dropped when an access control list match returns an implicit deny. (Results when RSVP is configured to drop implicit deny messages.)</td>
</tr>
<tr>
<td>Def-Proc</td>
<td>Number of messages processed by RSVP when an access control list match returns an implicit deny.</td>
</tr>
<tr>
<td>Path</td>
<td>Number of Path messages.</td>
</tr>
<tr>
<td>PathTear</td>
<td>Number of Path Tear messages.</td>
</tr>
<tr>
<td>ResvConfirm</td>
<td>Number of ResvConfirm messages.</td>
</tr>
</tbody>
</table>
**show rsvp fast-reroute**

To display RSVP Fast-Reroute (FRR) information, use the `show rsvp fast-reroute` command in EXEC mode.

```
show rsvp fast-reroute [destination IP-address] [dst-port port] [source IP-address] [src-port source-port] [summary]
```

**Syntax Description**

- **destination IP-address** (Optional) Displays the entries that match the specified address.
- **dst-port port** (Optional) Displays the port address of the destination router.
- **source IP-address** (Optional) Displays the IP address of the source network.
- **src-port source-port** (Optional) Displays the port number of the source router.
- **summary** (Optional) Displays summarized information about the FRR database.

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

- **mpls-te**
  - read, write

**Examples**

This is sample output from the `show rsvp fast-reroute` command:

```
RP/0/RP0/CPU0:router# show rsvp fast-reroute

Type  Destination   TunID  Source   PSBs  RSBs
-------  -----------  ------  --------  ------  ------
LSP4  70.70.70.70    1      50.50.50.50  Ready  Ready
```

This table describes the significant fields shown in the display.

**Table 63: show rsvp fast-reroute Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of session.</td>
</tr>
</tbody>
</table>
This is sample output from the `show rsvp fast-reroute summary` command:

```
RP/0/RP0/CPU0# show rsvp fast-reroute summary

States          Total    Ready  Act-Wait  Active
PSBs            1         1      0         0
RSBs            1         1      0         0
```

This table describes the significant fields shown in the display.

**Table 64: show rsvp fast-reroute summary Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>States</td>
<td>FRR&lt;sup&gt;28&lt;/sup&gt; state.</td>
</tr>
<tr>
<td>Total</td>
<td>Total number of path and reservation states.</td>
</tr>
<tr>
<td>Ready</td>
<td>Number of states in FRR ready state. No FRR processing has been done on these states.</td>
</tr>
<tr>
<td>Act-Wait</td>
<td>Number of states in “Active Wait” FRR state.</td>
</tr>
<tr>
<td></td>
<td>• For PSBs, this indicates that after FRR the path message has not yet been sent.</td>
</tr>
<tr>
<td></td>
<td>• For RSBs, this indicates that after FRR, the reservation message has not yet been received.</td>
</tr>
<tr>
<td>Active</td>
<td>Number of states in “Active” FRR state.</td>
</tr>
<tr>
<td></td>
<td>• For PSBs, this indicates that after FRR the path message has been sent.</td>
</tr>
<tr>
<td></td>
<td>• For RSBs, this indicates that after FRR, the reservation message has been received.</td>
</tr>
</tbody>
</table>

<sup>28</sup> Fast reroute.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mrrib mpls traffic-eng fast-reroute</code></td>
<td>Configures the multicast routing information base MPLS traffic engineering fast reroute information.</td>
</tr>
</tbody>
</table>
**show rsvp graceful-restart**

To display the local graceful-restart information for RSVP, use the `show rsvp graceful-restart` command in EXEC mode.

```
show rsvp graceful-restart [neighbors] [IP-address] [detail]
```

**Syntax Description**

- **neighbors** (Optional) Displays single-line status for each neighbor. If this keyword is not specified, only a multiline table entry is displayed showing local graceful-restart information.

- **IP-address** (Optional) Address of the neighbor you are displaying. Displays a specific neighbor with that destination address only. If this keyword is not specified, all neighbors are displayed.

- **detail** (Optional) Displays multiline status for each neighbor. If this keyword is not specified, only a single-line table entry is displayed.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Graceful-restart neighbors are displayed in ascending order of neighbor IP address.

**Task ID**

<table>
<thead>
<tr>
<th>Task</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show rsvp graceful-restart` command:

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

Graceful restart: enabled  Number of global neighbors: 1
Local MPLS router id: 192.168.55.55
Restart time: 60 seconds  Recovery time: 120 seconds
Recovery timer: Not running
Hello interval: 5000 milliseconds  Maximum Hello miss-count: 4
```
This table describes the significant fields shown in the display.

Table 65: show rsvp graceful-restart Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graceful restart</td>
<td>Indicates whether graceful restart is configured locally.</td>
</tr>
<tr>
<td>Number of global neighbors</td>
<td>Number of neighbors identified by a unique router ID.</td>
</tr>
<tr>
<td>Local MPLS router id</td>
<td>Local router ID used for the MPLS applications.</td>
</tr>
<tr>
<td>Restart time</td>
<td>Amount of time after a loss in hello messages within which RSVP hello session</td>
</tr>
<tr>
<td></td>
<td>is reestablished. This setting is manually configurable.</td>
</tr>
<tr>
<td>Recovery time</td>
<td>Local recovery time advertised to neighbors. This is dynamically computed</td>
</tr>
<tr>
<td></td>
<td>based on the number of LSPs established and is the time used by neighbors to</td>
</tr>
<tr>
<td></td>
<td>refresh states in the event of a failure.</td>
</tr>
<tr>
<td>Recovery timer</td>
<td>Countdown timer which, upon expiry, causes un-refreshed data forwarding states</td>
</tr>
<tr>
<td></td>
<td>to be deleted (usually beginning with a value that is equivalent to the sum</td>
</tr>
<tr>
<td></td>
<td>of the restart and recovery times).</td>
</tr>
<tr>
<td>Hello interval</td>
<td>Interval at which hello messages are sent to neighbors.</td>
</tr>
<tr>
<td>Maximum hello miss-count</td>
<td>Number of hellos from a neighbor that can be missed before declaring hellos</td>
</tr>
<tr>
<td></td>
<td>down.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show rsvp graceful-restart neighbors` command, which displays information about graceful restart neighbors in the router:

```
RP/0/RP0/CPU0:router# show rsvp graceful-restart neighbors

Neighbor        App     State  Recovery  Reason     Since             LostCnt
--------------- ----- ------ ------- -------- ------------ -------------------- --------
192.168.77.77   MPLS    UP     DONE    N/A       19/12/2002 17:02:25 0
```

This table describes the significant fields shown in the display.

Table 66: show rsvp graceful-restart neighbors Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>Router ID of a global neighbor.</td>
</tr>
<tr>
<td>App</td>
<td>Application type of a global neighbor ( ).</td>
</tr>
<tr>
<td>State</td>
<td>State of the hello session to a global neighbor (up, down, INIT).</td>
</tr>
<tr>
<td>Recovery</td>
<td>State at which the local node is recovering a global neighbor.</td>
</tr>
<tr>
<td>Reason</td>
<td>Last reason for which communication has been lost for a global neighbor. If</td>
</tr>
<tr>
<td></td>
<td>none has occurred, this field is marked as N/A.</td>
</tr>
</tbody>
</table>
The following is sample output from the `show rsvp graceful-restart neighbors detail` command, which displays detailed information about all graceful restart neighbors:

```
RP/0/RP0/CPU0:router# show rsvp graceful-restart neighbors detail

Neighbor: 192.168.77.77 Source: 192.168.55.55 (MPLS)
Hello instance for application MPLS
    Hello State: UP (for 00:20:52)
    Number of times communications with neighbor lost: 0
    Reason: N/A
    Recovery State: DONE
    Number of Interface neighbors: 1
      address: 192.168.55.0
    Restart time: 120 seconds Recovery time: 120 seconds
    Restart timer: Not running
    Recovery timer: Not running
    Hello interval: 5000 milliseconds Maximum allowed missed Hello messages: 4
```

This table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>Router ID of a global neighbor.</td>
</tr>
<tr>
<td>Source</td>
<td>Local router ID and application type.</td>
</tr>
<tr>
<td>Hello State</td>
<td>State of the hello instance for the global neighbor (up, down, or init) and duration of the current state.</td>
</tr>
<tr>
<td>Number of times communications with neighbor lost</td>
<td>Number of times hello communication has been lost with a global neighbor.</td>
</tr>
<tr>
<td>Reason</td>
<td>Last reason indicating why communication was lost for a global neighbor. If none has occurred, this field is marked as N/A.</td>
</tr>
<tr>
<td>Recovery State</td>
<td>State at which the local node is recovering a global neighbor.</td>
</tr>
<tr>
<td>Number of Interface neighbors</td>
<td>Number of interfaces belonging to a global neighbor.</td>
</tr>
<tr>
<td>Address</td>
<td>IP address of the interface neighbor.</td>
</tr>
<tr>
<td>Recovery timer</td>
<td>Remote recovery time for a global neighbor.</td>
</tr>
<tr>
<td>Hello interval</td>
<td>Interval at which hello messages are sent by the remote global neighbor.</td>
</tr>
<tr>
<td>Maximum allowed missed Hello messages</td>
<td>Number of hellos that can be missed by the remote global neighbor before declaring hellos down.</td>
</tr>
</tbody>
</table>
show rsvp hello instance

To display the RSVP hello instances, use the show rsvp hello instance command in EXEC mode.

```
show rsvp hello instance [Hostname \(\) or \(\) IP-address] [detail]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname or IP-address</td>
<td>(Optional) Address of the neighbor you are displaying. If this argument is not specified, all neighbors are displayed.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays multiline status for each hello instance. If this keyword is not specified, only a single-line table entry is displayed.</td>
</tr>
</tbody>
</table>

| Command Default | No default behavior or values |
| Command Modes | EXEC |
| Command History | Release 5.0.0 This command was introduced. |

Hello instances are displayed in ascending order of neighbor IP address.

### Task ID

-mplste read, write

### Examples

The following is sample output from the show rsvp hello instance command, which displays brief information about all hello instances in the router:

```
RP/0/RP0/CPU0:router# show rsvp hello instance

Neighbor Type State Interface LostCnt
---------------- ------ -------- ------------ --------
192.168.77.77 ACTIVE UP None 0
```

This table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>Router ID of a global neighbor hosting the hello instance.</td>
</tr>
<tr>
<td>Type</td>
<td>Hello instance type (active or passive). Active type indicates that a node is sending hello requests and passive indicates that a node is sending hello acknowledgements.</td>
</tr>
</tbody>
</table>
State of the hello session to a global neighbor (up, down, or init).

Interface for interface bound hello's used for FRR. Hello instances bound to a global neighbor show Interface as None. Hellos used for FRR are currently not supported.

Number of times hello communication has been lost with a global neighbor.

30 Fast reroute.

The following is sample output from the `show rsvp hello instance` command, which displays detailed information about all hello instances in the router:

```
RP/0/RP0/CPU0:router# show rsvp hello instance detail

Neighbor: 192.168.77.77 Source: 192.168.55.55 (MPLS)
State: UP (for 00:07:14)
Type: ACTIVE (sending requests)
I/F: None
Hello interval (msec) (used when ACTIVE) Configured: 5000
Src_instance 0x484b01, Dst_instance 0x4d4247
Counters:
Communication with neighbor lost:
  Num of times: 0 Reasons:
    Missed acks: 0
    New Src_Inst received: 0
    New Dst_Inst received: 0
    I/f went down: 0
    Neighbor disabled Hello: 0
  Msgs Received: 93
  Sent: 92
  Suppressed: 87
```

This table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>Router ID of a global neighbor.</td>
</tr>
<tr>
<td>Source</td>
<td>Local router ID and application type.</td>
</tr>
<tr>
<td>State</td>
<td>State of the hello instance for the global neighbor (up, down or init) and duration of the current state.</td>
</tr>
<tr>
<td>Type</td>
<td>Hello instance type (active or passive). Active type indicates that a node is sending hello requests and passive indicates that a node is sending hello acks.</td>
</tr>
<tr>
<td>I/F</td>
<td>Interface for interface bound hellos. Hello instances for Graceful restart show interface as None.</td>
</tr>
</tbody>
</table>
show rsvp hello instance interface-based

To display the RSVP hello instances on a specific interface, use the `show rsvp hello instance interface-based` command in EXEC mode.

```
show rsvp hello instance interface-based  [IP-address] [detail]
```

**Syntax Description**

- **IP-address** (Optional) Address of the neighboring interface you are displaying. If this argument is not specified, all neighbors are displayed.
- **detail** (Optional) Displays detailed information for the specified interface.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Hello instances are displayed in ascending order of neighbor IP address.

**Examples**

The following is sample output from the `show rsvp hello instance interface-based` command, which displays detailed information about hello instances on a specific interface:

```
RP/0/RP0/CPU0:router# show rsvp hello instance interface-based 10.10.10.10

Neighbor     Type     State     Interface     LostCnt
------------- -------- -------- -------------- --------
10.10.10.10   ACTIVE    UP       None          0
```

This table describes the significant fields shown in the display.

**Table 70: show rsvp hello instance interface-based Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>Router ID of a global neighbor hosting the hello instance.</td>
</tr>
<tr>
<td>Type</td>
<td>Hello instance type (active or passive). Active type indicates that a node is sending hello requests and passive indicates that a node is sending hello acknowledgements.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
State | State of the hello session to a global neighbor (up, down, or init).
Interface | Interface for interface bound hello's used for FRR\(^{31}\). Hello instances bound to a global neighbor show interface as none. Hellos used for FRR are currently not supported.
LostCnt | Number of times hello communication has been lost with a global neighbor.

\(^{31}\) Fast reroute.
show rsvp interface

To display information about all interfaces with RSVP enabled, use the `show rsvp interface` command in EXEC mode.

```
show rsvp interface  [type  interface-path-id]  [detail]
```

**Syntax Description**

- **type** (Optional) Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id** Physical interface or a virtual interface.

**Note** Use the `show interfaces` command to see a list of all possible interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

- **detail** (Optional) Displays multiline status for each interface. If this keyword is not specified, only a single-line table entry is displayed.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

- **Release 3.9.0** Sample output was modified.
- **Release 5.0.0** This command was introduced.

**Usage Guidelines**

Use the `show rsvp interface` 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 the RSVP-configured interfaces running in prestandard DS-TE mode:

```
RP/0/RP0/CPU0:router# show rsvp interface gigabitEthernet 0/3/0/0
Thu Oct 22 20:35:07.737 UTC
INTERFACE: GigabitEthernet0/3/0/0 (ifh=0x4000300).
  BW (bits/sec): Max=750M. MaxFlow=750M.
  Allocated=0 (0%).
```
BC0=750M. BC1=0.

The following is sample output from the `show rsvp interface` command, which displays brief information about the RSVP-configured interfaces for the GigabitEthernet interface type:

```
RP/0/RP0/CPU0:router# show rsvp interface gigabitEthernet 0/3/0/0
Thu Oct 22 20:35:42.323 UTC
Interface MaxBW (bps) MaxFlow (bps) Allocated (bps) MaxSub (bps)
----------- ----------- ------------- -------------------- ------------
Gi0/3/0/0 750M 750M 0 ( 0%) 0
```

This following is sample output from the `show rsvp interfaces detail` command running in standard DS-TE mode:

```
RP/0/RP0/CPU0:router# show rsvp interface gigabitEthernet 0/3/0/0 detail
Thu Oct 22 20:35:11.638 UTC
INTERFACE: GigabitEthernet0/3/0/0 (ifh=0x4000300).
VRF ID: 0x60000000 (Default).
BW (bits/sec): Max=750M. MaxFlow=750M.
  Allocated=0 (0%).
  BC0=750M. BC1=0.
Signalling: No DSCP marking. No rate limiting.
States in: 0. Max missed msgs: 4.
  Expiry timer: Not running. Refresh interval: 45s.
  Ack hold: 400 ms, Ack max size: 1500 bytes. Retransmit: 900ms.
Neighbor information:
  Neighbor-IP  Nbor-MsgIds States-out Refresh-Reduction Expiry(min::sec)
  ------------------ ------------- ------------------------ ------------------
  9.0.0.1 0 6 Enabled 14::56
  10.10.10.10 0 0 Enabled 14::33
```

This table describes the significant fields shown in the display.

### Table 71: `show rsvp interface detail` Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth</td>
<td>Configured values on the interface and currently allocated bandwidth.</td>
</tr>
<tr>
<td>Ack hold</td>
<td>Time, in milliseconds, before RSVP responds with an acknowledgment.</td>
</tr>
<tr>
<td>Neighbor-IP</td>
<td>Address of peer that RSVP is exchanging messages on that interface.</td>
</tr>
<tr>
<td>Nbor-msglds</td>
<td>Message IDs received from the neighbor (corresponding to the number of LSPs with reliable messaging).</td>
</tr>
<tr>
<td>States-out</td>
<td>States (including paths or reservations) sent on this interface to the neighbor.</td>
</tr>
<tr>
<td>Refresh Reduction</td>
<td>Neighbor Refresh Reduction capability.</td>
</tr>
</tbody>
</table>
### Expiry

Time a neighbor entry in the interface database expires if there is no activity on this interface with the corresponding neighbor.

### Related Commands

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show rsvp counters, on page 420</td>
<td>Displays internal RSVP counters.</td>
</tr>
</tbody>
</table>
show rsvp request

To list all the requests that RSVP knows about on a router, use the **show rsvp request** command in EXEC mode.

```
show rsvp request  [destination  IP-address]  [detail]  [dst-port  port-num]  [source  IP-address]  [src-port  port-num]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>(Optional) Displays multiline status for each path. If this keyword is not specified, only a single-line table entry is displayed.</td>
</tr>
<tr>
<td>destination IP-address</td>
<td>(Optional) Displays the entries that match the specified address.</td>
</tr>
<tr>
<td>dst-port port-num</td>
<td>(Optional) Displays destination port and tunnel information.</td>
</tr>
<tr>
<td>source IP-address</td>
<td>(Optional) Displays source address information.</td>
</tr>
<tr>
<td>src-port port-num</td>
<td>(Optional) Displays port and LSP ID information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>No default behavior or values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>EXEC</td>
</tr>
<tr>
<td>Command History</td>
<td></td>
</tr>
<tr>
<td>Release   Modification</td>
<td></td>
</tr>
<tr>
<td>Release 5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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 is sample output from the **show rsvp request** command:

```
RP/0/RP0/CPU0:router# show rsvp request

Dest Addr DPort Source Addr SPort Pro OutputIF Sty Serv Rate Burst
---------------- ----- ---------------- ----- --- ---------- --- ---- ---- ----
192.168.40.40 2001 192.168.67.68 2 0 PO0/7/0/1 SE LOAD 0 1K
```
The following is sample output from the `show rsvp request detail` command, which displays detailed information about all requests in the router. Requests are reservation states for the reservation messages sent upstream:

```
RP/0/RP0/CPU0:router# show rsvp request detail

    Output interface: POS0/7/0/1. Next hop: 192.168.67.68 (lih: 0x19700001).
    Flags: Local Receiver.
    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 Addr DPort  Source Addr SPort Pro Input IF Rate Burst Prot
    192.168.40.40    2001  192.168.67.68    2 0 POS0/7/0/1    0 1K Off
    Number of supporting RSBs: 1
    Destination Addr DPort  Source Addr SPort Pro Input IF Sty Serv Rate Burst
    192.168.40.40    2001  65.66.67.68    2 0 None SE LOAD 0 1K
```

This table describes the significant fields shown in the display.

**Table 72: show rsvp request detail Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of supporting PSBs</td>
<td>Number of senders for this session (typically, 1).</td>
</tr>
<tr>
<td>Number of supporting RSBs</td>
<td>Number of reservations per session (typically, 1).</td>
</tr>
<tr>
<td>Policy</td>
<td>Admission control status.</td>
</tr>
<tr>
<td>Policy source</td>
<td>Entity performing the admission control (MPLS-TE or COPS).</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show rsvp reservation, on page 443</td>
<td>Displays internal RSVP reservation counters.</td>
</tr>
</tbody>
</table>
show rsvp reservation

To display all reservations that RSVP knows about on a router, use the `show rsvp reservation` command in EXEC mode.

```
show rsvp reservation [destination IP address] [detail] [dst-port port-num] [source IP-address] [src-port port-num]
```

**Syntax Description**

- `detail` (Optional) Displays multiline status for each reservation. If the `detail` keyword is not specified, only a single-line table entry is displayed.
- `destination IP-address` (Optional) Displays the entries that match the specified address.
- `dst-port port-num` (Optional) Displays destination port and tunnel ID information.
- `source IP-address` (Optional) Displays source address information.
- `src-port port-num` (Optional) Displays source port and LSP ID information.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show rsvp reservation` command displays information about downstream reservations only (that is, reservations received on this device or created by application program interface (API) calls). Upstream reservations or requests are displayed using the `show rsvp request` command.

**Examples**

The following is sample output from the `show rsvp reservation` command:

```
RP/0/RP0/CPU0:router# show rsvp reservation

Dest Addr DPort Source Addr SPort Pro Input IF Sty Serv Rate Burst
------------------------------ ------ ---------------- ----- ------ ---------- --- ---- ---- ----
192.168.40.40 2001 192.168.67.68 2 0 None SE LOAD 0 1K
192.168.67.68 2000 10.40.40.40 15 0 POO/7/0/1 SE LOAD 0 1K
```

The following example displays detailed information about all reservations in the router:
show rsvp reservation detail


This table describes the significant fields shown in the display.

Table 73: show rsvp reservation detail Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input adjusted interface</td>
<td>Interface to reflect the path’s outgoing interface.</td>
</tr>
<tr>
<td>Input physical interface</td>
<td>Interface where the reservation was received.</td>
</tr>
<tr>
<td>Next hop</td>
<td>Address of the downstream node that sent the reservation to this node.</td>
</tr>
<tr>
<td>Lih</td>
<td>Logical interface handle sent in the hop object of path returned to us in the reservation to figure out what interface the path was sent on.</td>
</tr>
<tr>
<td>Flags</td>
<td>Indicates path state, including as Local Repair, Local Sender (LSP ingress node), and others.</td>
</tr>
<tr>
<td>Policy</td>
<td>Admission control status.</td>
</tr>
<tr>
<td>Policy source</td>
<td>Entity performing the admission control on the LSP.</td>
</tr>
<tr>
<td>Header info</td>
<td>RSVP header information as described in RFC 2205.</td>
</tr>
</tbody>
</table>

32 Link-state packet
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show rsvp request, on page 441</code></td>
<td>Lists all the requests that RSVP knows about on a router.</td>
</tr>
</tbody>
</table>
show rsvp sender

To display all path states that RSVP knows about on this router, use the show rsvp sender command in EXEC mode.

```
show rsvp sender [destination IP-address] [detail] [dst-port port-num] [source IP-address] [src-port port-num]
```

**Syntax Description**

- **detail** (Optional) Displays multiline status for each path. If the `detail` keyword is not specified, only a single-line table entry is displayed.
- **destination IP-address** (Optional) Displays the entries that match the specified address.
- **dst-port port-num** (Optional) Displays destination port and tunnel ID information.
- **source IP-address** (Optional) Displays source address information.
- **src-port port-num** (Optional) Displays source port and LSP ID information.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show rsvp sender` command displays information about path states.

**Task ID**

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

**Examples**

The following is sample output from the `show rsvp sender` command:

```
RP/0/RP0/CPU0:router# show rsvp sender

Dest Addr    DPort    Source Addr    SPort    Pro    Input IF    Rate  Burst  Prot
------------- -------- -------------- -------- ------ ---------- ------ ----- -----
10.40.40.40   2001    10.66.67.68   2        0      P00/7/0/1   0      1K   Off
10.66.67.68   2000    10.40.40.40   15       0      None      0      1K   Off
```
This table describes the significant fields shown in the display.

**Table 74: show rsvp sender Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DProt</td>
<td>Destination port number and tunnel-id.</td>
</tr>
<tr>
<td>Dest Addr</td>
<td>Destination and session address of LSP</td>
</tr>
<tr>
<td>SPort</td>
<td>Source port and LSP ID</td>
</tr>
<tr>
<td>Source Addr</td>
<td>Address of the ingress node of the LSP.</td>
</tr>
<tr>
<td>Input IF</td>
<td>Interface on which the Path message was received</td>
</tr>
</tbody>
</table>

Link-state packet

The following example displays detailed information about all paths in the system:

```
RP/0/RP0/CPU0:router# show rsvp sender detail
    Prot: Off. Backup tunnel: None.
    Setup Priority: 7, Reservation Priority: 0
    Rate: 0 bits/sec. Burst: 1K bytes. Peak: 0 bits/sec.
    Min unit: 40 bytes, Max unit: 500 bytes
    Flags: Bidirectional.
    State expires in 370.154 sec.
    Policy: Accepted. Policy source(s): Default.
    Header info: RSVP TTL=254. IP TTL=254. Flags: 0x1. TOS=0xc0.
    Input interface: PO0/3/0/0. Previous hop: 40.40.40.40 (lih: 0x40600001).
    Resource:
        Labels: Outgoing upstream: 3.
        Class-Type: None.
        Explicit Route (Incoming):
            Strict, 65.66.67.68(interface-path-id 5)
            Strict, 65.66.67.68/32
```

This table describes the significant fields shown in the display.

**Table 75: show rsvp sender detail Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prot</td>
<td>LSP configured as a protected tunnel.</td>
</tr>
<tr>
<td>Backup tunnel</td>
<td>Name of the backup tunnel assigned to protect this LSP</td>
</tr>
<tr>
<td>Flags</td>
<td>Path state, including as local repair, local sender (LSP ingress node), and others.</td>
</tr>
<tr>
<td>Policy</td>
<td>Admission control status for Path message in the incoming direction.</td>
</tr>
<tr>
<td>Policy source</td>
<td>Entity doing the admission control, such as COPS or MPLS-TE</td>
</tr>
</tbody>
</table>

---

33 Link-state packet

34 Name of the backup tunnel assigned to protect this LSP

35 Entity doing the admission control, such as COPS or MPLS-TE
### Field | Description
--- | ---
Header info | RSVP header information as described in RFC 2205.
Input interface | Interface on which the path was received. At ingress mode, it is None.
Previous hop | Address of the upstream peer who sent us the Path message. May be the interface address or node-id depending on LSP (packet or optical).
Lih | Logical interface handle received in the hop object of the path.
Output interface | Interface on which the path was forwarded to the downstream neighbor.
Policy | Admission control status for the path in the outgoing direction.
Explicit route | Explicit route specified in the explicit-route object of the Path message.

34 Link-state packet
35 MPLS-Traffic Engineering
show rsvp session

To list all sessions that RSVP knows about on this router, use the show rsvp session command in EXEC mode.

```
show rsvp session [destination IP-address] [detail] [dst-port port-num] [tunnel-name tunnel-name]
```

**Syntax Description**

- **detail** (Optional) Displays multiline status for each path. If the detail keyword is not specified, only a single-line table entry is displayed.
- **destination IP-address** (Optional) Displays the entries that match the specified address.
- **dst-port port-num** (Optional) Displays destination port and tunnel ID information.
- **tunnel-name tunnel-name** (Optional) Displays status for the session matching the specified tunnel-name.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Sessions are displayed in ascending order of destination IP address, destination port, and source IP address.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the show rsvp session command:

```
RP/0/RP0/CPU0:router# show rsvp session

Type  Session Addr Port Proto/ExtTunID PSBs RSBs Reqs
-----  --------------- ----- --------------- ----- ----- -----
LSP4   10.40.40.40   2001  10.66.67.68   1     1   1
LSP4   10.66.67.68   2000  10.40.40.40   1     1   0
```

This table describes the significant fields shown in the display.

**Table 76: show rsvp session Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of data flow (Traffic-Engineering LSP (LSP4 or IPV4 session)).</td>
</tr>
<tr>
<td>Session Addr</td>
<td>Destination address of the data packets and also tail of the LSP.</td>
</tr>
</tbody>
</table>
The following is sample output for the `show rsvp session detail` command:

```
RP/0/RP0/CPU0:router# show rsvp session detail

SESSION: IPv4-LSP Addr: 65.66.67.68, TunID: 1, ExtID: 40.40.40.40
PSBs: 1, RSBs: 1, Requests: 0
LSPID: 1
Tunnel Name: newhead_t1
  RSVP Path Info:
    InLabel: No intf, No label
    Incoming Address: Unknown
    Explicit Route:
      Strict, 65.66.67.68(interface-path-id 5)
      Strict, 65.66.67.68/32
    Record Route: None
    Tspec: avg rate=0, burst=1K, peak rate=0
  RSVP Resv Info:
    OutLabel: POS0/7/0/1, 5
    FRR OutLabel: No intf, No label
    Record Route:
      Node-id 65.66.67.68, interface index 5
    Fspec: avg rate=0, burst=1K, peak rate=0
```

This table describes the significant fields shown in the display.

**Table 77: show rsvp session detail Command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TunID</td>
<td>Tunnel identifier and the destination port of the LSP.</td>
</tr>
<tr>
<td>ExtID</td>
<td>Ingress node address of LSP.</td>
</tr>
<tr>
<td>Tunnel Instance</td>
<td>Source port of the LSP (with the ExtId forming the source parameters).</td>
</tr>
<tr>
<td>Tunnel Name</td>
<td>Name of the tunnel and LSP.</td>
</tr>
<tr>
<td>InLabel</td>
<td>Incoming interface and label info for the LSP in the upstream direction.</td>
</tr>
<tr>
<td></td>
<td>At the egress node, using penultimate hop popping at the egress node, (implicit-null) appears as No Label.</td>
</tr>
<tr>
<td>Incoming Address</td>
<td>Address of the ingress interface.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Explicit Route</td>
<td>Explicit route specified in the explicit-route object of the Path message.</td>
</tr>
<tr>
<td>Record Route</td>
<td>Record route object in either the path or reservation message.</td>
</tr>
<tr>
<td>Tspec</td>
<td>Traffic parameters.</td>
</tr>
<tr>
<td>OutLabel</td>
<td>Outgoing interface and label sent downstream.</td>
</tr>
<tr>
<td>FRR OutLabel</td>
<td>For FRR\textsuperscript{37}, displays the backup tunnel and Merge-point label.</td>
</tr>
<tr>
<td>Fspec</td>
<td>Flow spec parameters for specified QoS.</td>
</tr>
</tbody>
</table>

\textsuperscript{36} Link-state packet.
\textsuperscript{37} Fast reroute.
signalling dscp (RSVP)

To give all RSVP signaling packets sent out on a specific interface higher priority in the network by marking them with a particular Differentiated Service Code Point (DSCP), use the `signalling dscp` command in RSVP interface configuration submode. To return to the default behavior, use the `no` form of this command.

```
signalling dscp  dscp
no signalling  dscp
```

**Syntax Description**

- `dscp` DSCP priority number. Range is 0 to 63.

**Command Default**

No default behavior or values

**Command Modes**

RSVP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

DSCP marking improves signaling setup and teardown times.

Ordinarily, when a router receives Path messages for a particular state marked with a DSCP value, it sends out Path messages for that state marked with the same DSCP value. This command overrides that DSCP persistence and ensures that all messages sent out a particular interface are marked with a specified DSCP.

Though this command controls RSVP signaling packets, it has no effect on ordinary IP or MPLS data packets traveling along the path created or reserved by this RSVP session.

DSCP persistence operates on a per-state basis, but this command operates on a per-interface basis. So, if some incoming message (for example, multicast Path) with DSCP 10 causes two outgoing messages on interfaces A and B, ordinarily both are sent with DSCP 10. If `signalling dscp 5` is configured for RSVP on interface A, the Path messages being sent out interface A is marked with DSCP 5, but the Path messages being sent out interface B are marked with DSCP 10.

There is a difference between the `signalling dscp 0` and `no signalling dscp` commands. The first command instructs RSVP to explicitly set to 0 the DSCP on all packets sent out this interface. The second command removes any override on the packets being sent out this interface, and allows the DSCP of received packets that created this state to persist on packets forwarded out this interface.

The RFC specifies a standard mapping from the eight IP precedence values to eight values in the 64-value DSCP space. You can use those special DSCP values to specify IP precedence bits only.
The following example shows how to mark all RSVP packets going out on POS interface 0/1/0/1 as DSCP 20:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/1/0/1
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling dscp 20
```

The following example shows how to disable DSCP marking of signaling packets going out POS interface 0/1/0/1:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/1/0/1
RP/0/RP0/CPU0:router(config-rsvp-if)# interface pos 0/1/0/1
RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling dscp
```
signalling graceful-restart

To enable or disable RSVP signalling graceful restart, use the signalling graceful-restart command in RSVP configuration mode. To return to the default behavior, use the no form of this command.

```
signalling graceful-restart [recovery-time time | restart-time time]
no signalling graceful-restart
```

**Syntax Description**

- **recovery-time** (Optional) Configures the recovery time that is advertised in the Restart Cap object in the Hello messages.
  - `time` Time, in seconds, for the neighbor to wait for the node to recover (replay) existing states after the Hello session is reestablished before initiating TEARs. Range is 0 to 3600.

- **restart-time** (Optional) Configures the restart time that is advertised in the Restart Cap object in hello messages.
  - `time` Time, in seconds, after a control-plane restart that RSVP can start exchanging hello messages. Range is 60 to 3600. Default is 120.

**Command Default**

RSVP signaling graceful restart is disabled.

**Command Modes**

RSVP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The signalling graceful-restart command provides a mechanism that helps minimize the negative effects on MPLS traffic for the following types of faults. This is an implementation of the fault handling section of the IETF standard RFC 3473:

- **Control-channel-failure**
  
  Disruption of communication channels between 2 nodes when the communication channels are separated from the data channels.

- **Node-failure**
  
  Control plane of a node fails, but the node preserves its data forwarding states.

The signalling graceful-restart command instigates the exchange of RSVP hello messages between the router and its neighbor nodes. After the hello messages are established with a given neighbor, RSVP can detect these types of faults when they occur.

If no hello messages are received from a neighbor within a certain number of hello intervals, a node assumes that communication with the neighbor has been lost. The node waits the amount of time advertised by the last restart time communicated by the neighbor, before invoking procedures for recovery from communication loss.

The configured restart time is important in case of recovery from failure. The configured value should accurately reflect the amount of time within which, after a control-plane restart, RSVP can start exchanging hello messages.
The following example shows how to enable RSVP signalling graceful restart:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp
RP/0/RP0/CPU0:router(config-rsvp)# signalling graceful-restart
```

The following example shows how to set the restart time:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp
RP/0/RP0/CPU0:router(config-rsvp)# signalling graceful-restart restart-time 200
```

The following example shows how to reset the restart time to the default of 120 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp
RP/0/RP0/CPU0:router(config-rsvp)# no signalling graceful-restart restart-time
```
**signalling hello graceful-restart interface-based**

To enable RSVP to accept interface-based hello requests from the neighbor on an interface and send a Hello Acknowledgment to it, use the `signalling hello graceful-restart interface-based` command in RSVP configuration mode. To return to the default behavior, use the `no` form of this command.

```
signalling hello graceful-restart interface-based
no signalling hello graceful-restart interface-based
```

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

**Command Default**
No default behavior or values

**Command Modes**
RSVP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to enable interface-based graceful restart:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface Bundle-Ether2
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling hello graceful-restart interface-based
```
**signalling hello graceful-restart refresh interval**

To configure the interval at which RSVP graceful-restart hello messages are sent to each neighbor, use the `signalling hello graceful-restart refresh interval` command in RSVP configuration mode. To return to the default behavior, use the `no` form of this command.

```
signalling hello graceful-restart refresh interval refresh-interval
no signalling hello graceful-restart refresh interval
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th><code>refresh-interval</code> Interval, in milliseconds, at which RSVP graceful-restart hello messages are sent to each neighbor. Range is 3000 to 30000.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th><code>refresh interval</code>: 5000</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>RSVP configuration</th>
</tr>
</thead>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `signalling hello graceful-restart refresh interval` command determines how often hello messages are sent to each neighbor. If the interval is made short, the hello messages are sent more frequently. Although a short interval may help detect failures quickly, it also results in increased network traffic. Optimizations in the RSVP hello mechanism exist to reduce the number of hello messages traveling over the network.

When an RSVP hello message is received, the receiving node acknowledges the hello and restarts its hello timer to the neighbor. By doing this, a hello is transmitted to the neighbor only if a hello is not received before the hello refresh interval has expired.

If two neighboring nodes do not have the same hello interval, the node with the larger hello interval has to acknowledge its neighbor’s (more frequent) hellos. For instance, if node A has a hello interval of 5 seconds, and node B has a hello interval of 10 seconds, node B still has to send hello messages every 5 seconds.

The hello backoff mechanism is an optimization that is tailored to minimize the number of hello messages from a neighbor that either does not have graceful restart enabled, or that fails to come back up during the restart interval. The restart interval is provided by the neighbor in the restart cap object.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example sets the hello graceful-restart refresh interval to 4000 msecs:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp
```
RP/0/RP0/CPU0:router(config-rsvp)# signalling hello graceful-restart refresh interval 4000

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>signalling hello graceful-restart refresh misses, on page 459</td>
<td>Configures the number of consecutive missed RSVP hello messages before a neighbor is declared down or unreachable.</td>
</tr>
</tbody>
</table>
signalling hello graceful-restart refresh misses

To configure the number of consecutive missed RSVP hello messages before a neighbor is declared down or unreachable, use the `signalling hello graceful-restart refresh misses` command in RSVP configuration mode. To return to the default behavior, use the `no` form of this command.

**Syntax Description**

```
refresh-misses
```

Number of misses for hello messages before a neighbor is declared down or unreachable. Range is 1 to 10. Default is 3.

**Command Default**

```
refresh-misses: 3
```

**Command Modes**

RSVP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If no hello messages (request or ACK) are received from a neighbor within the configured number of refresh misses, the node assumes that communication with the neighbor has been lost.

**Task ID**

```
mpls-te read, write
```

**Examples**

The following example shows how to set hello graceful-restart refresh misses to 4:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp
RP/0/RP0/CPU0:router(config-rsvp)# signalling hello graceful-restart refresh misses 4
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>signalling hello graceful-restart refresh interval, on page 457</td>
<td>Configures the interval at which RSVP graceful restart hello messages are sent per neighbor.</td>
</tr>
</tbody>
</table>
signalling prefix-filtering access-list

To specify the extended access control list to use for prefix filtering of RSVP Router Alert messages, use the `signalling prefix-filtering access-list` command in RSVP configuration mode. To return to the default behavior, use the `no` form of this command.

```
signalling prefix-filtering access-list access list name
no signalling prefix-filtering access-list access list name
```

**Syntax Description**

- `access list name`: Extended access-list name as a string (maximum 32 characters).

**Command Default**

No default behavior or values

**Command Modes**

RSVP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The extended access control list containing the source and destination prefixes used for packet filtering is configured separately.

**Examples**

The following example shows how to configure the access control list name banks for prefix-filtering of RSVP Router Alert messages:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp
RP/0/RP0/CPU0:router(config-rsvp)# signalling prefix-filtering access-list banks
```

The following example shows how to disable RSVP prefix-filtering of RSVP Router Alert messages:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp
RP/0/RP0/CPU0:router(config-rsvp)# no signalling prefix-filtering access-list banks
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>signalling prefix-filtering default-deny-action, on page 462</td>
<td>Configures RSVP to drop messages when an access control list match yields an implicit deny.</td>
</tr>
</tbody>
</table>
signalling prefix-filtering default-deny-action

To configure RSVP to drop RSVP Router Alert messages when an access control list match returns an implicit deny, use the `signalling prefix-filtering default-deny-action` command in RSVP configuration mode. To return to the default behavior, use the `no` form of this command.

```
signalling prefix-filtering default-deny-action drop
no signalling prefix-filtering default-deny-action drop
```

**Syntax Description**
- **drop**: Specifies when RSVP router alert messages are dropped.

**Command Default**
Performs normal RSVP processing of Path, Path Tear, and ResvConfirm message packets.

**Command Modes**
- RSVP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**
- `mplste` read, write

**Examples**
The following example shows how to configure RSVP Router Alert messages when an access control list match returns an implicit deny:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp
RP/0/RP0/CPU0:router(config-rsvp)# signalling prefix-filtering default-deny-action drop
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>signalling prefix-filtering access-list, on page 460</td>
<td>Configures extended access control lists for prefix-filtering of an RSVP Router Alert messages.</td>
</tr>
</tbody>
</table>
signalling rate-limit

To limit the rate of RSVP signaling messages being sent out a particular interface, use the `signalling rate-limit` command in RSVP interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
signalling rate-limit [rate messages] [interval interval-length]
o no signalling rate-limit [rate messages] [interval interval-length]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>rate messages</code></td>
<td>(Optional) Configures the number of messages sent per scheduling interval. Range is 1 to 500 messages.</td>
</tr>
<tr>
<td><code>interval interval-length</code></td>
<td>(Optional) Specifies the length, in milliseconds, between scheduling intervals. Range is 250 to 2000.</td>
</tr>
</tbody>
</table>

**Command Default**

- `messages`: 100
- `interval-length`: 1,000 (1 second)

**Command Modes**

RSVP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the rate-limiting feature with caution. Limiting the rate of RSVP signaling has the advantage of avoiding an overload of the next hop router's input queue, because such overloads would cause the next hop router to drop RSVP messages. However, reliable messaging and rapid retransmit usually enable the router to recover very rapidly from message drops; so rate limiting might not be necessary.

If the rate is set too low, it causes slower convergence times. This command limits all RSVP messages except acknowledgments (ACK) and SRefresh messages. The command does not let you make a router generate messages faster than its inherent limit. (That limit differs among router models.)

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable rate-limiting:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface POS0/3/0/0
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling rate-limit
```

The following example shows how to limit the rate to 50 messages per second:
The following example shows how to set a limit at 40 messages for every 250 milliseconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/3/0/0
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling rate-limit rate 50
```

The following example shows how to restore the rate to the default of 100 messages per second:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/3/0/0
RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling rate-limit rate
```

The following example shows how to disable rate-limiting:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/3/0/0
RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling rate-limit
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>signalling refresh reduction bundle-max-size, on page 469</td>
<td>Specifies the maximum bundle size of maximum size of single RSVP bundle message.</td>
</tr>
</tbody>
</table>
**signalling refresh interval**

To change the frequency with which a router updates the network about the RSVP state of a particular interface, use the `signalling refresh interval` command in RSVP interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
signalling refresh interval  seconds
no  signalling refresh interval
```

### Syntax Description

- **seconds**: Number of seconds the router waits to update the network about the RSVP state of an interface, in seconds. Range is 10 to 180. Default is 45.

### Command Default

- **seconds**: 45

### Command Modes

- RSVP interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

RSVP relies on a soft-state mechanism to maintain state consistency in the face of network losses. That mechanism is based on continuous refresh messages to keep a state current. Each RSVP router is responsible for sending periodic refresh messages to its neighbors.

The router attempts to randomize network traffic and reduce metronomic burstiness by jittering the actual interval between refreshes by as much as 50 percent. As a result, refreshes may not be sent at exactly the interval specified. However, the average rate of refreshes are within the specified refresh interval.

Lengthening the interval reduces the refresh load of RSVP on the network but causes downstream nodes to hold state longer. This reduces the responsiveness of the network to failure scenarios. Shortening the interval improves network responsiveness but expands the messaging load on the network.

The reliable messaging extension, implemented through the `signalling refresh reduction reliable` command, may cause new or changed messages to be temporarily refreshed at a more rapid rate than specified to improve network responsiveness.

The use of reliable messaging with rapid retransmit substantially improves network responsiveness in case of transient message loss; if the refresh interval is changed when using the reliable messaging feature, it is more useful to lengthen the interval than to shorten it.

The summary refresh extension, implemented through the `signalling refresh reduction summary` command, provides a lower-cost mechanism to refresh RSVP state. The router uses the same refresh interval between successive refreshes of a single state when using summary refresh and when using ordinary message-based refresh.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mplste</td>
<td>read, write</td>
</tr>
</tbody>
</table>
Examples

The following example shows how to specify a refresh interval of 30 seconds:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface tunnel-te 2
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling refresh interval 30

The following example shows how to restore the refresh interval to the default value of 45 seconds:

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface tunnel-te 2
RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling refresh interval

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>signalling refresh missed, on page 467</td>
<td>Specifies the number of successive missed refresh messages before RSVP deems the state expired and tears it down.</td>
</tr>
<tr>
<td>signalling refresh reduction reliable, on page 472</td>
<td>Customizes acknowledgment message size and hold interval, and the RSVP message retransmit interval.</td>
</tr>
<tr>
<td>signalling refresh reduction summary, on page 475</td>
<td>Enables and configures the maximum size of the SRefresh message.</td>
</tr>
</tbody>
</table>
signalling refresh missed

To specify the number of successive refresh messages that can be missed before the RSVP deems a state to be expired (resulting in the state to be torn down), use the `signalling refresh missed` command in RSVP interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
signalling refresh missed number
no signalling refresh missed
```

**Syntax Description**

| `number` | Number of successive missed refresh messages. Range is 1 to 8. Default is 4. |

**Command Default**

`number: 4`

**Command Modes**

RSVP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Decreasing the missed-message number improves RSVP responsiveness to major failures like router failure or link faults, but decreases the resilience of RSVP resulting in packet drops or temporary network congestion. The latter condition makes RSVP too sensitive.

Increasing the missed-message number increases the resilience of RSVP to such transient packet loss, but decreases the RSVP responsiveness to more intransient network failures such as router failure or link fault.

The default value of 4 provides a balance of resilience and responsiveness factors.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to specify a missed refresh limit of six (6) messages:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface tunnel-te 2
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling refresh missed 6
```

The following example shows how to return the missed refresh limit to the default value of four (4):

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface tunnel-te 2
RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling refresh missed
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>signalling refresh interval, on page 465</td>
<td>Changes the frequency with which a router updates the network about the RSVP state of an interface.</td>
</tr>
<tr>
<td></td>
<td>signalling refresh reduction reliable, on page 472</td>
<td></td>
</tr>
<tr>
<td></td>
<td>signalling refresh reduction summary, on page 475</td>
<td>Enables and configures the maximum size of the SRefresh message.</td>
</tr>
</tbody>
</table>
signalling refresh reduction bundle-max-size

To configure the maximum size of a single RSVP bundle message, use the signalling refresh reduction bundle-max-size command in RSVP interface configuration mode.

```plaintext
signalling refresh reduction bundle-max-size size
```

**Syntax Description**

- `size` Maximum size, in bytes, of a single RSVP bundle message. Range is 512 to 65000.

**Command Default**

- `size`: 4096

**Command Modes**

- RSVP interface configuration

**Command History**

- **Release** 5.0.0
  - This command was introduced.

**Task ID**

- `mpls-te` read, write

**Examples**

The following example shows how to set the maximum bundle size of a single RSVP bundle message to 4000:

```plaintext
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface tunnel-te 2
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling refresh reduction bundle-max-size 4000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show rsvp interface, on page 438</td>
<td>Displays information about all interfaces with RSVP enabled.</td>
</tr>
</tbody>
</table>
signalling refresh reduction disable

To disable RSVP refresh reduction on an interface, use the signalling refresh reduction disable command in RSVP interface configuration mode. To return to the default behavior, use the no form of this command.

```
signalling refresh reduction disable
no signalling refresh reduction disable
```

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

**Command Default**
No default behavior or values

**Command Modes**
RSVP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The following features of the IETF refresh reduction standard RFC 2961 are enabled with this command:

- Setting the refresh-reduction-capable bit in message headers
- Message-ID usage
- Reliable messaging with rapid retransmit, acknowledgment (ACK), and NACK messages
- Summary refresh extension

Because refresh reduction relies on cooperation of the neighbor, the neighbor must also support the standard. If the router detects that a neighbor is not supporting the refresh reduction standard (either through observing the refresh-reduction-enabled bit in messages received from the next hop, or by sending a Message-ID object to the next hop and receiving an error), refresh reduction is not used on this link. That information is obtained through use of the `show rsvp interface detail` command.

**Examples**
The following example shows how to disable RSVP refresh reduction on an interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface tunnel-te 2
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling refresh reduction disable
```

The following example shows how to enable RSVP refresh reduction on the interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface tunnel-te 2
```
RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling refresh reduction disable

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show rsvp interface, on page 438</td>
<td>Displays information about all interfaces with RSVP enabled.</td>
</tr>
<tr>
<td>signalling refresh interval, on page 465</td>
<td>Changes the frequency with which a router updates the network about the RSVP state of an interface.</td>
</tr>
<tr>
<td>signalling refresh reduction reliable, on page 472</td>
<td>Customizes acknowledgment message size and hold interval, and the RSVP message retransmit interval.</td>
</tr>
<tr>
<td>signalling refresh reduction summary, on page 475</td>
<td>Enables and configures the maximum size of the signalling refresh message.</td>
</tr>
</tbody>
</table>
signalling refresh reduction reliable

To configure the parameters of reliable messaging, use the `signalling refresh reduction reliable` command in RSVP interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
signalling refresh reduction reliable {ack-max-size \bytes\ | ack-hold-time \milliseconds\ | retransmit-time \milliseconds\ | summary-refresh}
no signalling refresh reduction reliable {ack-max-size \bytes\ | ack-hold-time \milliseconds\ | retransmit-time \milliseconds\ | summary-refresh}
```

**Syntax Description**

- **ack-max-size**
  - Specifies the maximum size of the RSVP component within a single acknowledgment message.
  - \bytes\ Number of bytes that define the maximum size of an RSVP component. Range is 20 to 65000.

- **ack-hold-time**
  - Specifies the maximum amount of time a router holds an acknowledgment before sending it, in an attempt to bundle several acknowledgments into a single acknowledgment message.
  - \milliseconds\ Number of milliseconds that define the acknowledgment hold time. Range is 100 to 5000.

- **retransmit-time**
  - Specifies the amount of time the router initially waits for an acknowledgment message before resending the RSVP message.
  - \milliseconds\ Number of milliseconds that define the retransmit time. Range is 100 to 10000.

- **summary-refresh**
  - Enables the use of reliable transmission for RSVP summary refresh messages.

**Command Default**

- **ack-max-size \bytes\:** 4096
- **ack-hold-time \milliseconds\:** 400 (0.4 seconds)
- **retransmit-time \milliseconds\:** 900 (0.9 seconds)

**Command Modes**

- RSVP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For reliable messaging to work properly, configure the retransmit time on the send router (A) and acknowledgment hold time on the peer router (B). (Vice versa for messages in reverse direction.)

The retransmit time must be greater than the acknowledgment hold time, so that the acknowledgment message has time to get back to the sender before the message retransmits. We recommend that the retransmit-time interval be at least twice the acknowledgment hold-time interval. If the retransmit-time value is smaller than the acknowledgment hold-time value, then router A retransmits the message even though router B may have received the message and is waiting for an acknowledgment hold time to time out to send the acknowledgment. This causes unnecessary network traffic.
Reducing the value of **ack-max-size** causes more acknowledgment messages to be issued, with fewer acknowledgments contained within each acknowledgment message. However, reducing the acknowledgment-max-size does not speed up the rate at which acknowledgment messages are issued because their frequency is still controlled by the time values (acknowledgment hold time and retransmit time).

To use reliable messaging for summary refresh messages, use the `rsvp interface interface-name` and `signalling refresh reduction summary` commands.

### Examples

The following example shows how to set the maximum acknowledgment message size to 4096 bytes on POS interface 0/4/0/1:

```bash
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:

```bash
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:

```bash
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:

```bash
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:

```bash
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:

```bash
RP/0/RP0/CPU0:router(config)# rsvp interface pos 0/4/0/1
```
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>signalling refresh reduction disable, on page 470</td>
<td>Disables RSVP refresh reduction on an interface.</td>
</tr>
</tbody>
</table>
signalling refresh reduction summary

To configure RSVP summary refresh message size on an interface, use the `signalling refresh reduction summary` command in RSVP interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
signalling refresh reduction summary max-size bytes
no signalling refresh reduction summary max-size bytes
```

Syntax Description

- `max-size bytes`: Specifies the maximum size, in bytes, of a single RSVP summary refresh message. Range is 20 to 65000.

Command Default

- `bytes`: 4096

Command Modes

- RSVP interface configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the `signalling refresh reduction summary` command to specify the maximum size of the summary refresh messages sent. Message size is verified using the `show rsvp interface detail` command.

Task ID

- `mpls-te`: read, write

Examples

The following example shows how to change the summary message maximum size on an interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface tunnel-te 2
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling refresh reduction summary max-size 6000
```

The following example shows how to return the summary message maximum size to the default value on an interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface tunnel-te 2
RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling refresh reduction summary max-size 6000
```
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show rsvp interface, on page 438</code></td>
<td>Displays information about all interfaces with RSVP enabled.</td>
</tr>
<tr>
<td><code>signalling refresh interval, on page 465</code></td>
<td>Changes the frequency with which a router updates the network about the RSVP state of an interface.</td>
</tr>
</tbody>
</table>
**window-size (RSVP)**

To specify the maximum number of RSVP authenticated messages that can be received out of sequence, use the `window-size` command in RSVP authentication configuration mode, RSVP interface authentication configuration mode, or RSVP neighbor authentication configuration mode. To disable the window size, use the `no` form of this command.

```
window-size N
no window-size
```

**Syntax Description**

- **N**: Size of the window to restrict out-of-sequence messages. Range is 1 to 64. Default is 1. All out-of-sequence messages are dropped.

**Command Default**

- **N**: 1

**Command Modes**

- RSVP authentication configuration
- RSVP interface authentication configuration
- RSVP neighbor authentication configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

Use the `window-size` command to specify the maximum number of authenticated messages that are received out of sequence. All RSVP authenticated messages include a sequence number that is used to prevent replays of RSVP messages.

With a default window size of one message, RSVP rejects any out-of-order or out-of-sequence authenticated messages because they are assumed to be replay attacks. However, sometimes bursts of RSVP messages become reordered between RSVP neighbors. If this occurs on a regular basis, and you can verify that the node sending the burst of messages is trusted, you can use the window-size option to adjust the burst size such that RSVP does not discard such reordered bursts. RSVP checks for duplicate messages within these bursts.

**Examples**

The following example shows how to configure the size of the window to 33 in RSVP neighbor authentication configuration mode:
 RP/0/RP0/CPU0:router# configure
 RP/0/RP0/CPU0:router(config)# rsvp neighbor 1.1.1.1 authentication
 RP/0/RP0/CPU0:router(config-rsvp-nbor-auth)# window-size 33

The following example shows how to configure the size of the window to 33 in RSVP authentication configuration mode:

 RP/0/RP0/CPU0:router# configure
 RP/0/RP0/CPU0:router(config)# rsvp authentication
 RP/0/RP0/CPU0:router(config-rsvp-auth)# window-size 33

The following example shows how to configure the size of the window to 33 in RSVP interface authentication configuration mode by using the `rsvp interface` command:

 RP/0/RP0/CPU0:router# configure
 RP/0/RP0/CPU0:router(config)# rsvp interface POS 0/2/1/0
 RP/0/RP0/CPU0:router(config-rsvp-if)# authentication
 RP/0/RP0/CPU0:router(config-rsvp-if-auth)# window-size 33

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key-source key-chain (RSVP), on page 406</td>
<td>Specifies the source of the key information to authenticate RSVP signaling messages.</td>
</tr>
<tr>
<td>life-time (RSVP), on page 408</td>
<td>Controls how long RSVP maintains idle security associations with other trusted RSVP neighbors.</td>
</tr>
</tbody>
</table>
MPLS OAM Commands

This module describes Multiprotocol Label Switching (MPLS) label switched path (LSP) verification commands. These commands provide a means to detect and diagnose data plane failures and are the first set of commands in the MPLS Operations, Administration, and Maintenance (OAM) solution.

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

- clear mpls oam counters, on page 480
- echo disable-vendor-extension, on page 481
- echo revision, on page 482
- mpls oam, on page 483
- ping mpls ipv4, on page 484
- ping pseudowire (AToM), on page 489
- ping mpls traffic-eng tunnel-te (P2P), on page 493
- ping mpls traffic-eng tunnel-mte (P2MP), on page 496
- ping mpls mldp (P2MP), on page 502
- ping mpls mldp (MP2MP), on page 508
- show mpls oam, on page 514
- show mpls oam database, on page 516
- traceroute mpls ipv4, on page 517
- traceroute mpls multipath, on page 520
- traceroute mpls traffic-eng tunnel-te (P2P), on page 524
- traceroute mpls traffic-eng tunnel-mte (P2MP), on page 527
- traceroute mpls mldp (P2MP), on page 531
- traceroute mpls mldp (MP2MP), on page 536
clear mpls oam counters

To clear MPLS OAM counters, use the `clear mpls oam counters` command in EXEC mode.

```
clear mpls oam counters  {global | interface  [{type  interface-path-id}] | packet}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>global</td>
<td>Clears global counters.</td>
</tr>
<tr>
<td>interface</td>
<td>Clears counters on a specified interface.</td>
</tr>
<tr>
<td>type</td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note**

Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

| packet | Clears global packet counters.                   |

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>execute</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>execute</td>
</tr>
<tr>
<td>mpls-static</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear all global MPLS OAM counters:

```
RP/0/RP0/CPU0:router# clear mpls oam counters global
```
**echo disable-vendor-extension**

To disable sending the vendor extension type length and value (TLV) in the echo request, use the `echo disable-vendor-extension` command in MPLS OAM configuration mode. To return to the default behavior, use the `no` form of this command.

```
no echo disable-vendor-extension
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The default value is 4.

**Command Modes**

MPLS OAM configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

- **mpls-te**
  - read, write
- **mpls-ldp**
  - read, write
- **mpls-static**
  - read, write

**Examples**

The following example shows how to disable inclusion of the vendor extensions TLV in the echo requests:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls oam
RP/0/RP0/CPU0:router(config-oam)# echo disable-vendor-extension
```
**echo revision**

To set the echo packet revision, use the `echo revision` command in MPLS OAM configuration mode. To return to the default behavior, use the `no` form of this command.

```plaintext
echo revision  {1 | 2 | 3 | 4}
no echo revision
```

**Syntax Description**

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

Draft revision number:

- 1: draft-ietf-mpls-lsp-ping-03 (initial)
- 2: draft-ietf-mpls-lsp-ping-03 (rev 1)
- 3: draft-ietf-mpls-lsp-ping-03 (rev 2)
- 4: draft-ietf-mpls-lsp-ping-09 (initial)

**Command Default**

The default echo revision is 4 (in draft 9).

**Command Modes**

- MPLS OAM configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-static</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the echo packet default revision:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls oam
RP/0/RP0/CPU0:router(config-oam)# echo revision 1
```
mpls oam

To enable MPLS OAM LSP verification, use the `mpls oam` command in global configuration mode. To return to the default behavior, use the `no` form of this command.

```
mpls oam
no mpls oam
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

By default, MPLS OAM functionality is disabled.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `mpls oam` command and OAM functionality is described in the IETF LSP ping draft.

**Task ID**

```
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-static</td>
<td>read, write</td>
</tr>
</tbody>
</table>
```

**Examples**

The following example shows how to enable MPLS OAM:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls oam
RP/0/RP0/CPU0:router(config-oam)#
```
ping mpls ipv4

To check MPLS host reachability and network connectivity by specifying the destination type as a Label Distribution Protocol (LDP) IPv4 address, use the **ping mpls ipv4** command in EXEC mode.

**ping mpls ipv4**  *address/mask*  *[destination start-address end-address increment]*  *[dmap]*  *[exp exp-bits]*  *[force-explicit-null]*  *[interval min-send-delay]*  *[output interface type interface-path-id]*  *[next-hop nexthop-address]*  *[pad pattern]*  *[repeat count]*  *[reply dscp dscp-value]*  *[reply mode ipv4]*  *[no-reply router-alert]*  *[reply pad-tlv]*  *[revision version]*  *[size packet-size]*  *[source source-address]*  *[sweep min value max value increment]*  *[timeout timeout]*  *[ttl value]*  *[verbose]*  *[fec-type ldp]*  

**Syntax Description**

- **address/mask**: Address prefix of the target and number of bits in the target address network mask.
- **destination start address end address address increment**: Specifies a network 127/8 address to be used as the destination address in the echo request packet.
  - **start address**: Start of the network address.
  - **end address**: Start of the ending network address.
  - **address increment**: Incremental value of the network address, which is expressed as a decimal number value or IP address.
- **dmap**: (Optional) Indicates that a downstream mapping (DSMAP) type length and value should be included in the LSP echo request.
- **exp exp-bits**: (Optional) Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.
- **force-explicit-null**: (Optional) Forces an unsolicited explicit null label to be added to the MPLS label stack and allows LSP ping to be used to detect LSP breakages at the penultimate hop.
- **interval min-send-delay**: (Optional) Specifies a send interval, in milliseconds, between requests. Range is 0 to 3600000. Default is 0.
- **output interface**: (Optional) Specifies the output interface where echo request packets are sent.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Use the <code>show interfaces</code> command to see a list of all interfaces currently configured on the router. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>next-hop</td>
<td>(Optional) Specifies the next hop as an IP address.</td>
</tr>
<tr>
<td>nexthop-i-address</td>
<td>(Optional) IP address for the next hop.</td>
</tr>
<tr>
<td>pad pattern</td>
<td>(Optional) Specifies the pad pattern for an echo request.</td>
</tr>
<tr>
<td>repeat count</td>
<td>(Optional) Specifies the number of times to resend a packet. Range is 1 to 2147483647. Default is 5.</td>
</tr>
<tr>
<td>reply dscp dscp-value</td>
<td>Specifies the differentiated service codepoint value for an MPLS echo reply.</td>
</tr>
<tr>
<td>reply mode [ ipv4</td>
<td>router-alert</td>
</tr>
<tr>
<td></td>
<td><strong>no-reply</strong> Do not reply</td>
</tr>
<tr>
<td></td>
<td><strong>ipv4</strong> Reply with an IPv4 UDP packet (this is the default)</td>
</tr>
<tr>
<td></td>
<td><strong>router-alert</strong> Reply with an IPv4 UDP packet with the IP router alert set</td>
</tr>
<tr>
<td>reply pad-tlv</td>
<td>Indicates that a pad TLV should be included.</td>
</tr>
<tr>
<td>revision version</td>
<td>(Optional) Specifies the Cisco extension TLV versioning field:</td>
</tr>
<tr>
<td></td>
<td>• 1 draft-ietf-mpls-lsp-ping-03 (initial)</td>
</tr>
<tr>
<td></td>
<td>• 2 draft-ietf-mpls-lsp-ping-03 (rev 1)</td>
</tr>
<tr>
<td></td>
<td>• 3 draft-ietf-mpls-lsp-ping-03 (rev 2)</td>
</tr>
<tr>
<td></td>
<td>• 4 draft-ietf-mpls-lsp-ping-09 (initial)</td>
</tr>
<tr>
<td>size packet size</td>
<td>(Optional) Specifies the packet size or number of bytes in each MPLS echo request packet. Range is 100 to 17986. Default is 100.</td>
</tr>
<tr>
<td>Command Default</td>
<td>exp exp bits: 0</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>interval min-send-delay: 0</td>
<td></td>
</tr>
<tr>
<td>repeat count : 5</td>
<td></td>
</tr>
<tr>
<td>reply-mode: IPv4</td>
<td></td>
</tr>
<tr>
<td>timeout timeout : 2</td>
<td></td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **output interface** keyword specifies the output interface on which the MPLS echo request packets are sent. If the specified output interface is not part of the LSP, the packets are not transmitted.

In cases where the **sweep** keyword is used, values larger than the outgoing interface’s MTU are not transmitted.

The **ping** command sends an echo request packet to an address, and then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

<table>
<thead>
<tr>
<th>source source-address</th>
<th>(Optional) Specifies the source address used in the echo request packet.</th>
</tr>
</thead>
<tbody>
<tr>
<td>sweep min value max value interval</td>
<td>(Optional) Specifies a range of sizes for the echo packets sent.</td>
</tr>
<tr>
<td>min value</td>
<td>Minimum or start size for an echo packet (range is 100 to 17986)</td>
</tr>
<tr>
<td>max value</td>
<td>Maximum or end size for an echo packet (range is 100 to 17986)</td>
</tr>
<tr>
<td>interval</td>
<td>Number used to increment an echo packet size (range is 1 to 8993)</td>
</tr>
<tr>
<td>timeout timeout</td>
<td>(Optional) Specifies the timeout interval, in seconds. Range is 0 to 3600. Default is 2.</td>
</tr>
<tr>
<td>ttl value</td>
<td>(Optional) Specifies the TTL value to be used in the MPLS labels (range is 1 to 255).</td>
</tr>
<tr>
<td>verbose</td>
<td>(Optional) Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.</td>
</tr>
</tbody>
</table>
The **ping mpls** command is not supported on optical LSPs. If an optical LSP is encountered along the LSP's path, it is treated as a physical interface.

For detailed configuration information about the MPLS **ping** command, see *System Monitoring Configuration Guide*.

### Examples

The following example shows the destination type as a label distribution protocol (LDP) prefix and specifies a range of sizes for the echo packets sent:

```
RP/0/R0/CP0:router# ping mpls ipv4 140.140.140/32 verbose sweep 100 200 15 repeat 1
```

```
Sending 1, [100..200]-byte MPLS Echos to 140.140.140.140/32, timeout is 2 seconds, send interval is 0 msec:


Type escape sequence to abort.

! size 100, reply addr 196.100.1.26, return code 3
! size 115, reply addr 196.100.1.26, return code 3
! size 130, reply addr 196.100.1.26, return code 3
! size 145, reply addr 196.100.1.26, return code 3
! size 160, reply addr 196.100.1.26, return code 3
! size 175, reply addr 196.100.1.26, return code 3
!

Success rate is 100 percent (7/7), round-trip min/avg/max = 5/6/8 ms
```

The following example shows the destination type as a label distribution protocol (LDP) prefix and specifies FEC type as generic and verbose option:

```
RP/0/R0/CP0:router# ping mpls ipv4 11.11.11.11/32 fec-type generic output interface gigabitEthernet 0/0/0/3 nexthop 172.40.103.2 verbose
```

```
Sending 5, 100-byte MPLS Echos to 11.11.11.11/32, timeout is 2 seconds, send interval is 0 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout, 'L' - labeled output interface, 'B' - unlabeled output interface, 'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
```

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

! size 100, reply addr 11.101.11.11, return code 3
! size 100, reply addr 11.101.11.11, return code 3
! size 100, reply addr 11.101.11.11, return code 3
! size 100, reply addr 11.101.11.11, return code 3
! size 100, reply addr 11.101.11.11, return code 3

Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/6 ms
**ping pseudowire (AToM)**

To verify connectivity between provider edge (PE) LSRs in an Any Transport over MPLS (AToM) setup, use the *ping pseudowire* command in EXEC mode.

```
ping [mpls] pseudowire {remote-PE-address pw-id} [exp exp-bits] [interval min-send-delay] [pad pattern] [repeat count] [reply {dscp dscp-value | reply mode {ipv4 | no-reply | router-alert | control-channel | reply pad-tlv}}] [size packet-size] [source source-address] [sweep min-value max-value increment] [timeout timeout] [ttl value] [verbose]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls</td>
<td>(Optional) Verifies the Labeled Switch Path (LSP).</td>
</tr>
<tr>
<td>remote-PE address</td>
<td>IP address of the remote PE LSR.</td>
</tr>
<tr>
<td>pw-id</td>
<td>Pseudowire ID that identifies the pseudowire in which MPLS connectivity is being verified. The pseudowire is used to send the echo request packets. The range is from 1 to 4294967295.</td>
</tr>
<tr>
<td>exp exp-bits</td>
<td>(Optional) Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.</td>
</tr>
<tr>
<td>interval min-send-delay</td>
<td>(Optional) Specifies a send interval, in milliseconds, between requests. Range is 0 to 3600000. Default is 0.</td>
</tr>
<tr>
<td>pad pattern</td>
<td>(Optional) Specifies the pad pattern for an echo request.</td>
</tr>
<tr>
<td>repeat count</td>
<td>(Optional) Specifies the number of times to resend a packet. Range is 1 to 2147483647. Default is 5.</td>
</tr>
<tr>
<td>reply dscp dscp-value</td>
<td>(Optional) Specifies the differentiated service codepoint value for an MPLS echo reply.</td>
</tr>
</tbody>
</table>
**reply mode** \{ipv4 | router-alert | no-reply | control-channel\}  
(Optional) Specifies the reply mode for the echo request packet.

- **no-reply**  
  Do not reply

- **ipv4**  
  Reply with an IPv4 UDP packet (the default)

- **router-alert**  
  Reply with an IPv4 UDP packet with the IP router alert set

- **control-channel**  
  Force the use of a VCCV control channel.  
  Reply using an application for a defined control channel. This applies only to pseudowires in which VCCV is used in the reply path. This is the default choice for pseudowire ping.

**reply pad-tlv**  
(Optional) Indicates that a reply pad TLV should be included.

**size** \{packet-size\}  
(Optional) Specifies the packet size or number of bytes in each MPLS echo request packet. Range is 100 to 17986. Default is 100.

**source** \{source-address\}  
(Optional) Specifies the source address used in the echo request packet.

**sweep** \{min-value max-value interval\}  
Specifies a range of sizes for the echo packets sent.

  **min-value**  
  Minimum or start size for an echo packet (range is 100 to 17986)

  **max-value**  
  Maximum or end size for an echo packet (range is 100 to 17986)

  **interval**  
  Number used to increment an echo packet size (range is 1 to 8993)

**timeout** \{timeout\}  
(Optional) Specifies the timeout interval in seconds. Range is 0 to 3600. Default is 2 seconds.

**ttl** \{value\}  
(Optional) Specifies the TTL value to be used in the MPLS labels (range is 1 to 255).

**verbose**  
(Optional) Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.
**Command Default**

- exp *exp* bits: 0
- interval *min-send-delay*: 0
- repeat *count*: 5
- reply-mode: IPv4
- timeout timeout : 2

**Command Modes**

EXEC

**Command History**

Release | Modification
---|---
5.2.1 | This command was introduced.

**Usage Guidelines**

In cases in which the **sweep** keyword is used, values larger than the outgoing interface’s MTU are not transmitted.

The **ping** command sends an echo request packet to an address, and then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

**Note**

The **ping mpls** command is not supported on optical LSPs. If an optical LSP is encountered along the LSP's path, it is treated as a physical interface.

AToM VCCV allows the sending of control packets inband of an AToM pseudowire (PW) from the originating provider edge (PE) router. The transmission is intercepted at the destination PE router, instead of being forwarded to the customer edge (CE) router. This lets you use MPLS LSP ping to test the pseudowire section of AToM virtual circuits (VCs).

The no interactive version of the **ping pseudowire (AToM)** command is supported.

The control word setting is either enabled along the entire path between the Terminating-Provider Edge (T-PE) or it is completely disabled. If the control word configuration is enabled on one segment and disabled on another segment, the multisegment pseudowire does not come up.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how the **ping mpls pseudowire** command is used to verify PE to PE connectivity in which the remote PE address is 150.150.150.150. Only one echo request packet is sent and the remote PE is to answer using IPv4 instead of the control channel.

```
RP/0/RP0/CPU0:router# ping mpls pseudowire 150.150.150.150 21 repeat 1 reply mode ipv4
Sending 1, 100-byte MPLS Echos to 150.150.150.150 VC: 21,
```
timeout is 2 seconds, send interval is 0 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

Success rate is 100 percent (1/1), round-trip min/avg/max = 23/23/23 ms
### ping mpls traffic-eng tunnel-te (P2P)

To specify the destination type as an MPLS-TE tunnel and tunnel interface, use the `ping mpls traffic-eng tunnel-te` command in EXEC mode.

```
ping mpls traffic-eng tunnel-te tunnel-ID [destination start-address end-address increment] [dsmap] [exp exp-bits] [force-explicit-null] [interval min-send-delay] [pad pattern] [repeat count] [reply {dscp dscp-value | mode {ipv4 | no-reply | router-alert} | pad-tlv}] [revision version] [size packet-size] [source source-address] [sweep min-value max-value increment] [timeout timeout] [ttl value] [verbose]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>tunnel-te tunnel-ID</code></td>
<td>Specifies the destination type as an MPLS traffic engineering (TE) tunnel and the tunnel interface number. The range for the tunnel interface number is 0 to 65535.</td>
</tr>
<tr>
<td><code>destination start-address end-address increment</code></td>
<td>Specifies a network 127/8 address to be used as the destination address in the echo request packet.</td>
</tr>
<tr>
<td><code>start address</code></td>
<td>Start of the network address.</td>
</tr>
<tr>
<td><code>end address</code></td>
<td>Start of the ending network address.</td>
</tr>
<tr>
<td><code>address increment</code></td>
<td>Incremental value of the network address, which is expressed as a decimal number value or IP address.</td>
</tr>
<tr>
<td><code>dsmap</code></td>
<td>(Optional) Indicates that a downstream mapping (DSMAP) type length and value should be included in the LSP echo request.</td>
</tr>
<tr>
<td><code>exp exp-bits</code></td>
<td>(Optional) Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.</td>
</tr>
<tr>
<td><code>force-explicit-null</code></td>
<td>(Optional) Forces an unsolicited explicit null label to be added to the MPLS label stack and allows LSP ping to be used to detect LSP breakages at the penultimate hop.</td>
</tr>
<tr>
<td><code>interval min-send-delay</code></td>
<td>(Optional) Specifies a send interval, in milliseconds, between requests. Range is 0 to 3600000. Default is 0.</td>
</tr>
<tr>
<td><code>pad pattern</code></td>
<td>(Optional) Specifies the pad pattern for an echo request.</td>
</tr>
<tr>
<td><code>repeat count</code></td>
<td>(Optional) Specifies the number of times to resend a packet. Range is 1 to 2147483647. Default is 5.</td>
</tr>
<tr>
<td><code>reply dscp dscp-value</code></td>
<td>(Optional) Specifies the differentiated service codepoint value for an MPLS echo reply.</td>
</tr>
</tbody>
</table>
**mode [ipv4 | router-alert | no-reply]**  
(Optional) Specifies the reply mode for the echo request packet.

**no-reply**  
Do not reply

**ipv4**  
Reply with an IPv4 UDP packet (this is the default)

**router-alert**  
Reply with an IPv4 UDP packet with the IP router alert set

**reply pad-tlv**  
(Optional) Indicates that a pad TLV should be included.

**revision version**  
(Optional) Specifies the Cisco extension TLV versioning field:
- 1 draft-ietf-mpls-lsp-ping-03 (initial)
- 2 draft-ietf-mpls-lsp-ping-03 (rev 1)
- 3 draft-ietf-mpls-lsp-ping-03 (rev 2)
- 4 draft-ietf-mpls-lsp-ping-09 (initial)

**size packet-size**  
(Optional) Specifies the packet size or number of bytes in each MPLS echo request packet. Range is 100 to 17986. Default is 100.

**source source-address**  
(Optional) Specifies the source address used in the echo request packet.

**sweep min-value max-value interval**  
(Optional) Specifies a range of sizes for the echo packets sent.

**min-value**  
Minimum or start size for an echo packet (range is 100 to 17986)

**max-value**  
Maximum or end size for an echo packet (range is 100 to 17986)

**interval**  
Number used to increment an echo packet size (range is 1 to 8993)

**timeout timeout**  
(Optional) Specifies the timeout interval, in seconds. Range is 0 to 3600. Default is 2.

**ttl value**  
(Optional) Specifies the TTL value to be used in the MPLS labels (range is 1 to 255).
verbose

(Optional) Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.

**Command Default**

- `exp exp-bits: 0`
- `interval min-send-delay: 0`
- `repeat count: 5`
- `reply-mode: IPv4`
- `timeout timeout : 2`

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `output interface` keyword specifies the output interface on which the MPLS echo request packets are sent. If the specified output interface is not part of the LSP, the packets are not transmitted.

In cases where the `sweep` keyword is used, values larger than the outgoing interface's MTU are not transmitted.

The `ping` command sends an echo request packet to an address, and then waits for a reply. Ping output helps you evaluate path-to-host reliability, delays over the path. It also helps you determine whether the host is reachable or is functioning.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mpls traffic-eng tunnels</code></td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
<tr>
<td></td>
<td>Verifies the connectivity of the LSP path for the MPLS-TE P2MP tunnels.</td>
</tr>
</tbody>
</table>
ping mpls traffic-eng tunnel-mte (P2MP)

To specify the destination type as a Point-to-Multipoint (P2MP) for MPLS-TE tunnel and tunnel interface, use the `ping mpls traffic-eng tunnel-mte` command in EXEC mode.

```plaintext
ping mpls traffic-eng tunnel-mte tunnel-ID [ddmap {destination start-address end-address increment}] [responder-id ipv4-address] [exp exp-bits] [interval min-send-delay] [jitter jitter-value] [lsp {active | reopt}] [pad pattern] [repeat count] [reply {dscp dscp-value | mode {ipv4 | no-reply | router-alert} | pad-tlv}] [size packet-size] [source source-address] [sweep min-value max-value increment] [timeout timeout] [ttl value] [verbose]
```

**Syntax Description**

- **tunnel-mte tunnel-ID**
  - Specifies the destination type as an MPLS traffic engineering (TE) P2MP tunnel and the tunnel interface number. The range for the tunnel interface number is 0 to 65535.

- **ddmap**
  - (Optional) Indicates that a downstream detailed mapping TLV should be included in the LSP echo request.

- **destination start-address end-address increment**
  - Specifies a network 127/8 address to be used as the destination address in the echo request packet.

  - **start-address**
    - Start of the network address.

  - **end-address**
    - End of the network address.

  - **address increment**
    - Incremental value of the network address, which is expressed as a decimal number value or IP address.

- **responder-id ipv4-address**
  - (Optional) Specifies the responder IPv4 address.

- **exp exp-bits**
  - (Optional) Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.

- **interval min-send-delay**
  - (Optional) Specifies a send interval, in milliseconds, between requests. Range is 0 to 3600000. Default is 0.

- **jitter jitter-value**
  - (Optional) Specifies a jitter value, in milliseconds. Range is 0 to 2147483647. Default is 200.
**pad pattern**  
(Optional) Specifies the pad pattern for an echo request.

**repeat count**  
(Optional) Specifies the number of times to resend a packet. Range is 1 to 2147483647. Default is 5.

**reply dscp dscp-value**  
(Optional) Specifies the differentiated service codepoint value for an MPLS echo reply.

**mode [ipv4 | router-alert | no-reply]**  
(Optional) Specifies the reply mode for the echo request packet.

- **no-reply**  
  Do not reply

- **ipv4**  
  Reply with an IPv4 UDP packet (this is the default)

- **router-alert**  
  Reply with an IPv4 UDP packet with the IP router alert set

**reply pad-tlv**  
(Optional) Indicates that a pad TLV should be included.

**size packet-size**  
(Optional) Specifies the packet size or number of bytes in each MPLS echo request packet. Range is 100 to 17986. Default is 100.

**source source-address**  
(Optional) Specifies the source address used in the echo request packet.

**sweep min-value max-value interval**  
(Optional) Specifies a range of sizes for the echo packets sent.

- **min-value**  
  Minimum or start size for an echo packet (range is 100 to 17986)

- **max-value**  
  Maximum or end size for an echo packet (range is 100 to 17986)

- **interval**  
  Number used to increment an echo packet size (range is 1 to 8993)
**timeout**

(Optional) Specifies the timeout interval, in seconds. Range is 0 to 3600. Default is 2.

**ttl**

(Optional) Specifies the TTL value to be used in the MPLS labels (range is 1 to 255). Default is 255.

**verbose**

(Optional) Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.

---

**Command Default**

- **exp** exp-bits: 0
- **interval** min-send-delay: 0
- **repeat** count: 5
- **reply-mode**: IPv4
- **timeout** timeout: 2
- **lsp**: active

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To ping for LSP reoptimization, ensure that the reoptimization timer for the tunnel is running by using the `show mpls traffic-eng tunnels reoptimized within-last` command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>basic-services</td>
<td>execute</td>
</tr>
<tr>
<td>mpls-te or mpls-ldp</td>
<td>read</td>
</tr>
</tbody>
</table>

**Example**

The following example shows how to check connectivity by using the `ping mpls traffic-eng tunnel-mte` command with the `jitter` keyword:

```
RP/0/RP0/CPU0:router# ping mpls traffic-eng tunnel-mte 10 jitter 300

Mon Apr 12 12:13:00.630 EST

Sending 1, 100-byte MPLS Echos to tunnel-mte10, timeout is 2.3 seconds, send interval is 0 msec, jitter value is 300 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout, 'L' - labeled output interface, 'U' - unlabeled output interface,
```
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0, 'd' - DDMAP

Type escape sequence to abort.

Request #1
! reply addr 192.168.222.2
! reply addr 192.168.140.2
! reply addr 192.168.170.1

Success rate is 100 percent (3 received replies/3 expected replies),
round-trip min/avg/max = 148/191/256 ms

The following example shows how to check connectivity by using the ping mpls traffic-eng
* tunnel-mte * command with the ddmap keyword:

RP/0/RP0/CPU0:router# ping traffic-eng tunnel-mte 10 ddmap

Mon Apr 12 12:13:34.365 EST
Sending 1, 100-byte MPLS Echos to tunnel-mte10,
timeout is 2.2 seconds, send interval is 0 msec, jitter value is 200 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0, 'd' - DDMAP

Type escape sequence to abort.

Request #1
! reply addr 192.168.222.2
! reply addr 192.168.140.2
! reply addr 192.168.170.1

Success rate is 100 percent (3 received replies/3 expected replies),
round-trip min/avg/max = 105/178/237 ms

The following example shows how to identify the LSP ID tunnel information by using the show
mpls traffic-eng tunnels p2mp command, and then using the lsp id keyword with the ping mpls
traffic-eng tunnel-mte command.

RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels p2mp 10

Mon Apr 12 12:13:55.075 EST
Signalling Summary:
LSP Tunnels Process: running
RSVP Process: running
Forwarding: enabled
Periodic reoptimization: every 3600 seconds, next in 654 seconds
Periodic FRR Promotion: every 300 seconds, next in 70 seconds
Auto-bw enabled tunnels: 0 (disabled)

Name: tunnel-mte10
Status:
   Admin: up  Oper: up (Up for 12w4d)
Config Parameters:
Bandwidth: 0 kbps (CT0) Priority: 7 7 Affinity: 0x0/0xffff
Metric Type: TE (default)
Fast Reroute: Not Enabled, Protection Desired: None
Record Route: Not Enabled

Destination summary: (3 up, 0 down, 0 disabled) Affinity: 0x0/0xffff
Auto-bw: disabled
Destination: 11.0.0.1
State: Up for 12w4d
Path options:
  path-option 1 dynamic [active]
Destination: 12.0.0.1
State: Up for 12w4d
Path options:
  path-option 1 dynamic [active]
Destination: 13.0.0.1
State: Up for 12w4d
Path options:
  path-option 1 dynamic [active]

History:
Reopt. LSP:
  Last Failure:
    LSP not signalled, identical to the [CURRENT] LSP
    Date/Time: Thu Jan 14 02:49:22 EST 2010 [12w4d ago]

Current LSP:
lsp-id: 10002 p2mp-id: 10 tun-id: 10 src: 10.0.0.1 extid: 10.0.0.1
LSP up for: 12w4d
Reroute Pending: No
Inuse Bandwidth: 0 kbps (CT0)
Number of S2Ls: 3 connected, 0 signaling proceeding, 0 down

S2L Sub LSP: Destination 11.0.0.1 Signaling Status: connected
  S2L up for: 12w4d
  Sub Group ID: 1 Sub Group Originator ID: 10.0.0.1
  Path option path-option 1 dynamic (path weight 1)
  Path info (OSPF 1 area 0)
    192.168.222.2
    11.0.0.1

S2L Sub LSP: Destination 12.0.0.1 Signaling Status: connected
  S2L up for: 12w4d
  Sub Group ID: 2 Sub Group Originator ID: 10.0.0.1
  Path option path-option 1 dynamic (path weight 2)
  Path info (OSPF 1 area 0)
    192.168.222.2
    192.168.140.3
    192.168.140.2
    12.0.0.1

S2L Sub LSP: Destination 13.0.0.1 Signaling Status: connected
  S2L up for: 12w4d
  Sub Group ID: 3 Sub Group Originator ID: 10.0.0.1
  Path option path-option 1 dynamic (path weight 2)
  Path info (OSPF 1 area 0)
    192.168.222.2
    192.168.170.3
    192.168.170.1
    13.0.0.1

Reoptimized LSP (Install Timer Remaining 0 Seconds):
None
Cleaned LSP (Cleanup Timer Remaining 0 Seconds):
None
Displayed 1 (of 16) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads

RP/0/RP0/CPU0:router# ping mpls traffic-eng tunnel-mte 10 lsp id 10002

Mon Apr 12 12:14:04.532 EST
Sending 1, 100-byte MPLS Echos to tunnel-mte10,
timeout is 2.2 seconds, send interval is 0 msec, jitter value is 200 msec:

Codes: '! - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0, 'd' - DDMAP

Type escape sequence to abort.
Request #1
! reply addr 192.168.222.2
! reply addr 192.168.170.1
! reply addr 192.168.140.2
Success rate is 100 percent (3 received replies/3 expected replies),
round-trip min/avg/max = 128/153/167 ms

The following example shows how to use the ping mpls traffic-eng tunnel-mte command to check connectivity with a router's host address 13.0.0.1:

RP/0/RP0/CPU0:router# ping mpls traffic-eng tunnel-mte 10 egress 13.0.0.1

Mon Apr 12 12:15:34.205 EST
Sending 1, 100-byte MPLS Echos to tunnel-mte10,
timeout is 2.2 seconds, send interval is 0 msec, jitter value is 200 msec:

Codes: '! - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0, 'd' - DDMAP

Type escape sequence to abort.
Request #1
! reply addr 192.168.170.1
Success rate is 100 percent (1 received reply/1 expected reply),
round-trip min/avg/max = 179/179/179 ms

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls traffic-eng tunnels</td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
</tbody>
</table>
ping mpls mldp (P2MP)

To check data plane and control plane of MPLS for the Point-to-Multipoint (P2MP) label switch path, use the **ping mpls mldp p2mp** command in EXEC mode.

```
ping mpls mldp p2mp root-address {IPv4 source-ipv4-address group-ipv4-address | IPv6 source-ipv6-address group-ipv6-address | vpnv4 AS-number [source-ipv4-address group-ipv4-address] | vpnv6 AS-number [source-ipv6-address group-ipv6-address] | mdt oui:vpn-index mdt-number | global-id lsp-id} [options]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>mldp</strong></td>
<td>Verifies the ping capability for multicast label distribution protocol (mldp).</td>
</tr>
<tr>
<td><strong>p2mp</strong></td>
<td>Indicates the Point-to-Multipoint (P2MP) label switch path.</td>
</tr>
<tr>
<td><strong>root-address</strong></td>
<td>Specifies the root address.</td>
</tr>
<tr>
<td><strong>IPv4 ipv4-address</strong></td>
<td>Defines IPv4 opaque encoding.</td>
</tr>
<tr>
<td><strong>IPv6 ipv6-address</strong></td>
<td>Defines IPv6 opaque encoding.</td>
</tr>
<tr>
<td><strong>vpnv4 AS-number [source-ipv4-address group-ipv4-address]</strong></td>
<td>Defines VPNv4 opaque encoding.</td>
</tr>
<tr>
<td><strong>vpnv6 AS-number [source-ipv6-address group-ipv6-address]</strong></td>
<td>Defines VPNv6 opaque encoding.</td>
</tr>
<tr>
<td><strong>mdt oui:vpn-index mdt number</strong></td>
<td>Defines VPN ID opaque encoding. Range of 3-byte OUI is 0 to 16777215. Range of <strong>mdt-number</strong> is 0 to 4294967295.</td>
</tr>
<tr>
<td><strong>global-id lsp-id</strong></td>
<td>Defines 4 byte global LSP ID opaque encoding.</td>
</tr>
<tr>
<td><strong>source-address</strong></td>
<td>Specifies the source address of target multicast address.</td>
</tr>
<tr>
<td><strong>group-address</strong></td>
<td>Specifies the target address of target multicast address.</td>
</tr>
<tr>
<td><strong>AS-number</strong></td>
<td>Specifies the Autonomous system number as follows:</td>
</tr>
<tr>
<td></td>
<td>• 4-byte AS-number with asdot (X.Y) : aa:bb:cc format (for example, 11.22:33)</td>
</tr>
<tr>
<td></td>
<td>• 2-byte AS-number or 4-byte AS-number: aa:bb format (for example, 11:22)</td>
</tr>
<tr>
<td></td>
<td>• IPv4 address and index:aa.bb.cc.dd:ee format (for example, 11.22.33.44:55)</td>
</tr>
</tbody>
</table>
ping mpls mldp (P2MP)

options
Specifies a set of various options:

**ddmap**
(Optional) Indicates that a downstream detailed mapping TLV (ddmap) should be included in the LSP echo request.

**destination**
(Optional) Specifies a network 127/8 address to be used as the destination address in the echo request packet.

- **start-address**: Start of the network address.
- **end-address**: End of the network address.
- **address increment**: Incremental value of the network address, which is expressed as a decimal number value or IP address.

**exp-exp-bits**
(Optional) Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.

**flags**

- **fec**: (Optional) Specifies that forwarding equivalent class (FEC) stack checking is to be performed at transit routers.
- **no-ttl**: (Optional) Specifies not to add TTL expired flag in echo request.

**force-explicit-null**
(Optional) Forces an unsolicited explicit null label to be added to the MPLS label stack and allows LSP ping to be used to detect LSP breakages at the penultimate hop.

**interval min-send-delay**
(Optional) Specifies a send interval, in milliseconds, between requests. Range is 0 to 3600000. Default is 0.

**jitter**
(Optional) Specifies a jitter value for a corresponding echo request, in milliseconds. Range is 0 to 2147483647. Default is 200.

**pad pattern**
(Optional) Specifies the pad pattern for an echo request.

**repeat count**
(Optional) Specifies the number of times to resend a packet. Range is 1 to 2147483647. Default is 5.

**reply dscp dscp-value**

(Optional) Specifies the differentiated service codepoint value for an MPLS echo reply.

**mode [ipv4 | router-alert ]**

(Optional) Specifies the reply mode for the echo request packet.

**ipv4**

Reply with an IPv4 UDP packet (this is the default)

**router-alert**

Reply with an IPv4 UDP packet with the IP router alert set

**responder-id ipv4-address**

(Optional) Adds responder identifier into corresponding echo request.

**size packet size**

(Optional) Specifies the packet size or number of bytes in each MPLS echo request packet. Range is 100 to 17986. Default is 100.

**source ipv4-address**

(Optional) Specifies the source address used in the echo request packet.

**sweep**

(Optional)

**timeout timeout**

(Optional) Specifies the timeout interval, in seconds. Range is 0 to 3600. Default is 2.

**ttl**

(Optional) Specifies the TTL value to be used in the MPLS labels (range is 1 to 255). Default is 255.

**verbose**

(Optional) Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.

---

**Command Default**

No default behavior or values
command was introduced.

Release 5.2.1

Task ID Description
---
execute basic-services
read mpls-te
read mpls-ldp

The following examples show how to check connectivity for P2MP by using the **ping mpls mldp p2mp** command.

```
RP/0/RP0/CPU0:router# ping mpls mldp p2mp 192.168.0.1 ipv4 2.2.2.2 232.1.1.1
```

Sending 1, 100-byte MPLS Echos to mldp p2mp 192.168.0.1 ipv4 (2.2.2.2, 232.1.1.1),
timeout is 2.2 seconds, send interval is 0 msec, jitter value is 200 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0, 'd' - DDMAP

Type escape sequence to abort.

Request #1
! reply addr 11.11.11.3
! reply addr 12.12.12.4

Round-trip min/avg/max = 17/27/38 ms

```
RP/0/RP0/CPU0:router# ping mpls mldp p2mp 192.168.0.1 ipv4 2.2.2.2 232.1.1.1 dmap ttl 1
```

Sending 1, 100-byte MPLS Echos to mldp p2mp 192.168.0.1 ipv4 (2.2.2.2, 232.1.1.1),
timeout is 2.2 seconds, send interval is 0 msec, jitter value is 200 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0, 'd' - DDMAP

Type escape sequence to abort.

Request #1
d reply addr 10.10.10.2
[L] DDMAP 0: 11.11.11.3 11.11.11.3 MRU 1500 [Labels: 16016 Exp: 0]
This table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Opaque Type</th>
<th>Opaque Value</th>
<th>Supported Multicast Application</th>
<th>Signaling</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>S, G</td>
<td>PIM-SSM transit of IPv4</td>
<td>In-Band</td>
</tr>
<tr>
<td>IPv6</td>
<td>S, G</td>
<td>PIM-SSM transit of IPv6</td>
<td>In-Band</td>
</tr>
<tr>
<td>MDT</td>
<td>VPN-ID, MDT#</td>
<td>mVPN Default-MDT (MDT# = 0)</td>
<td>In-Band</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mVPN Data-MDT (MDT# &gt; 0)</td>
<td></td>
</tr>
<tr>
<td>Global ID</td>
<td>4 byte value</td>
<td>BGP Assigned LSPs</td>
<td>Out-of-Band</td>
</tr>
<tr>
<td>VPNv4</td>
<td>(S,G), VPN-ID</td>
<td>VPNv4</td>
<td>In-Band</td>
</tr>
<tr>
<td>VPNv6</td>
<td>(S,G), VPN-ID</td>
<td>VPNv6</td>
<td>In-Band</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping mpls mldp (MP2MP), on page 508</td>
<td>Verifies data plane and control plane for the Multipoint-to-Multipoint (MP2MP) label switch path.</td>
</tr>
<tr>
<td>traceroute mpls mldp (P2MP), on page 531</td>
<td>Verifies hop-by-hop fault localization and path tracing for the point-to-multipoint path.</td>
</tr>
<tr>
<td>traceroute mpls mldp (MP2MP), on page 536</td>
<td>Verifies hop-by-hop fault localization and path tracing for the multipoint-to-multipoint path.</td>
</tr>
</tbody>
</table>
**ping mpls mldp (MP2MP)**

To check data plane and control plane of MPLS for the Multipoint-to-Multipoint (MP2MP) label switch path, use the `ping mpls mldp mp2mp` command in exec mode.

```plaintext
ping mpls mldp mp2mp root-address [(IPv4 source-ipv4-address group-ipv4-address) | IPv6 source-ipv6-address group-ipv6-address | vpnv4 AS-number [source-ipv4-address group-ipv4-address] | vpnv6 AS-number [source-ipv6-address group-ipv6-address] | mdt oui:vpn-index mdt-number [global-id lsp-id] | [options]]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mldp</td>
<td>Verifies the ping capability for multicast label distribution protocol (mldp).</td>
</tr>
<tr>
<td>mp2mp</td>
<td>Indicates the Multipoint-to-Multipoint (MP2MP) label switch path.</td>
</tr>
<tr>
<td>root-address</td>
<td>Specifies the root address.</td>
</tr>
<tr>
<td>IPv4 ipv4-address</td>
<td>Defines IPv4 opaque encoding.</td>
</tr>
<tr>
<td>IPv6 ipv6-address</td>
<td>Defines IPv6 opaque encoding.</td>
</tr>
<tr>
<td>vpnv4 AS-number</td>
<td>Defines VPNv4 opaque encoding.</td>
</tr>
<tr>
<td>vpnv6 AS-number</td>
<td>Defines VPNv6 opaque encoding.</td>
</tr>
<tr>
<td>mdt oui:vpn-index</td>
<td>Defines VPN ID opaque encoding. Range of 3-byte OUI is 0 to 16777215. Range of mdt-number is 0 to 4294967295.</td>
</tr>
<tr>
<td>global-id lsp-id</td>
<td>Defines 4 byte global LSP ID opaque encoding.</td>
</tr>
<tr>
<td>source-address</td>
<td>Specifies the source address of target multicast address.</td>
</tr>
<tr>
<td>group-address</td>
<td>Specifies the target address of target multicast address.</td>
</tr>
<tr>
<td>AS-number</td>
<td>Specifies the Autonomous system number as follows:</td>
</tr>
<tr>
<td></td>
<td>• 4-byte AS-number with asdot (X.Y): aa:bb:cc format (for example, 11.22:33)</td>
</tr>
<tr>
<td></td>
<td>• 2-byte AS-number or 4-byte AS-number: aa:bb format (for example, 11:22)</td>
</tr>
<tr>
<td></td>
<td>• IPv4 address and index:aa.bb.cc.dd:ee format (for example, 11.22.33.44:55)</td>
</tr>
</tbody>
</table>

**MPLS Command Reference for Cisco NCS 6000 Series Routers**
ping mpls mldp (MP2MP)

options
Specifies a set of various options:

**ddmap**

(Optional) Indicates that a downstream detailed mapping TLV (ddmap) should be included in the LSP echo request.

**destination**

(Optional) Specifies a network 127/8 address to be used as the destination address in the echo request packet.

- **start-address**: Start of the network address.
- **end-address**: End of the network address.
- **address increment**: Incremental value of the network address, which is expressed as a decimal number value or IP address.

**exp bits**

(Optional) Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.

**flags**

- **fec**: (Optional) Specifies that forwarding equivalent class (FEC) stack checking is to be performed at transit routers.
- **no-ttl**: (Optional) Specifies not to add TTL expired flag in echo request.

**force-explicit-null**

(Optional) Forces an unsolicited explicit null label to be added to the MPLS label stack and allows LSP ping to be used to detect LSP breakages at the penultimate hop.

**interval min-send-delay**

(Optional) Specifies a send interval, in milliseconds, between requests. Range is 0 to 3600000. Default is 0.

**jitter**

(Optional) Specifies a jitter value for a corresponding echo request, in milliseconds. Range is 0 to 2147483647. Default is 200.

**pad pattern**

(Optional) Specifies the pad pattern for an echo request.
(Optional) Specifies the number of times to resend a packet. Range is 1 to 2147483647. Default is 5.

**reply dscp dscp-value**

(Optional) Specifies the differentiated service codepoint value for an MPLS echo reply.

**mode [ipv4 | router-alert]**

(Optional) Specifies the reply mode for the echo request packet.

**ipv4**

Reply with an IPv4 UDP packet (this is the default)

**router-alert**

Reply with an IPv4 UDP packet with the IP router alert set

**responder-id ipv4-address**

(Optional) Adds responder identifier into corresponding echo request.

**size packet size**

(Optional) Specifies the packet size or number of bytes in each MPLS echo request packet. Range is 100 to 17986. Default is 100.

**source ipv4-address**

(Optional) Specifies the source address used in the echo request packet.

**sweep**

(Optional)

**timeout timeout**

(Optional) Specifies the timeout interval, in seconds. Range is 0 to 3600. Default is 2.

**ttl**

(Optional) Specifies the TTL value to be used in the MPLS labels (range is 1 to 255). Default is 255.

**verbose**

(Optional) Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.

---

**Command Default**

No default behavior or values
The following example shows how to check connectivity by using the `ping mpls mldp` command when a root address is present.

```
RP/0/RP0/CPU0:router# ping mpls mldp mp2mp 192.168.0.1 global-id 1
Mon Jul 11 15:35:50.294 JST
Sending 1, 100-byte MPLS Echos to mldp mp2mp 192.168.0.1 global-id 1,
timeout is 2.2 seconds, send interval is 0 msec, jitter value is 200 msec:
Codes: '! - success, 'Q' - request not sent, '. - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0, 'd' - DDMAP
Type escape sequence to abort.
Request #1
! reply addr 10.10.10.2
! reply addr 12.12.12.4
! reply addr 11.11.11.3
Round-trip min/avg/max = 72/112/135 ms
```

```
RP/0/RP0/CPU0:router# ping mpls mldp mp2mp 192.168.0.1 global-id 1 responder-id 11.11.11.3
Mon Jul 11 15:36:16.038 JST
Sending 1, 100-byte MPLS Echos to mldp mp2mp 192.168.0.1 global-id 1,
timeout is 2.2 seconds, send interval is 0 msec, jitter value is 200 msec:
Codes: '! - success, 'Q' - request not sent, '. - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0, 'd' - DDMAP
Type escape sequence to abort.
Request #1
```

- Command Modes
  - EXEC

- Command History
  - Release 5.2.1 This command was introduced.

- Task ID
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>basic-services</td>
<td>execute</td>
</tr>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>read</td>
</tr>
</tbody>
</table>
! reply addr 11.11.11.3

Round-trip min/avg/max = 163/163/163 ms

This table describes the significant fields shown in the display:

<table>
<thead>
<tr>
<th>Opaque Type</th>
<th>Opaque Value</th>
<th>Supported Multicast Application</th>
<th>Signaling</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>S, G</td>
<td>PIM-SSM transit of IPv4</td>
<td>In-Band</td>
</tr>
<tr>
<td>IPv6</td>
<td>S, G</td>
<td>PIM-SSM transit of IPv6</td>
<td>In-Band</td>
</tr>
<tr>
<td>MDT</td>
<td>VPN-ID, MDT#</td>
<td>mVPN Default-MDT (MDT# = 0)</td>
<td>In-Band</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mVPN Data-MDT (MDT# &gt; 0)</td>
<td></td>
</tr>
<tr>
<td>Global ID</td>
<td>4 byte value</td>
<td>BGP Assigned LSPs</td>
<td>Out-of-Band</td>
</tr>
<tr>
<td>VPNv4</td>
<td>(S,G), VPN-ID</td>
<td>VPNv4</td>
<td>In-Band</td>
</tr>
<tr>
<td>VPNv6</td>
<td>(S,G), VPN-ID</td>
<td>VPNv6</td>
<td>In-Band</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping mpls mldp (P2MP), on page 502</td>
<td>Verifies data plane and control plane for the point-to-multipoint (P2MP) label switch path.</td>
</tr>
<tr>
<td>traceroute mpls mldp (P2MP), on page 531</td>
<td>Verifies hop-by-hop fault localization and path tracing for the point-to-multipoint path.</td>
</tr>
<tr>
<td>traceroute mpls mldp (MP2MP), on page 536</td>
<td>Verifies hop-by-hop fault localization and path tracing for the multipoint-to-multipoint path.</td>
</tr>
</tbody>
</table>
show mpls oam

To display MPLS OAM information, use the `show mpls oam` command in EXEC mode.

```
show mpls oam  {client | counters  {global | packet} | interface  type  interface-path-id}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>client</code></td>
<td>Displays clients registered with LSPV server.</td>
</tr>
<tr>
<td><code>counters global</code></td>
<td>Displays LSP verification global counters.</td>
</tr>
<tr>
<td><code>counters packet</code></td>
<td>Displays LSP verification packet counters.</td>
</tr>
<tr>
<td><code>counters interface</code></td>
<td>Displays LSP verification information for a specific interface.</td>
</tr>
<tr>
<td><code>type</code></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values

### Command Modes

EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>read</td>
</tr>
<tr>
<td>mpls-static</td>
<td>read</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to display MPLS OAM client information:

```
RP/0/RP0/CPU0:router# show mpls oam client

Client Process: l2vpn_mgr Node: 0/0/SP Pid: 418014
Client Process: te_control Node: 0/0/SP Pid: 639227
```
This table describes the significant fields shown in the display.

Table 78: show mpls oam client Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
show mpls oam database

To display MPLS OAM database information, use the `show mpls oam database` command in EXEC mode.

```
show mpls oam database  {replies | requests | tt-requests} [detail] [handle handle-value ]
```

**Syntax Description**

- `replies`   Displays replies database.
- `requests`  Displays request database
- `tt-requests` Displays trace trace request database
- `detail`    (Optional) Displays detailed information.
- `handle`    (Optional) Displays handle information.
- `handle-value` Generic handle value. Range is from 0 to 4294967295.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>read</td>
</tr>
<tr>
<td>mpls-static</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to display detailed MPLS OAM database information:

```
RP/0/RP0/CPU0:router# show mpls oam database request detail
```
traceroute mpls ipv4

To learn the routes that packets follow when traveling to their Label Distribution Protocol (LDP) IPv4 destination, use the `traceroute mpls` command in EXEC mode.

```
traceroute mpls ipv4 address/mask [destination start-address end-address address-increment] [exp exp-bits] [flags fec] [force-explicit-null] [output interface type interface-path-id] [nexthop nexthop-address] [reply {dscp dscp-value | reply mode {ipv4 | router-alert}}] [revision version] [source source-address] [timeout timeout] [ttl value] [verbose] [fec-type {bgp | generic | ldp}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address/mask</td>
<td>Specifies the destination type as a label distribution protocol (LDP) prefix. Address prefix of the target and number of bits in the target address network mask.</td>
</tr>
<tr>
<td>destination</td>
<td>Specifies a network 127 address to be used as the destination address in the echo request packet.</td>
</tr>
<tr>
<td>start address</td>
<td>Start of the network address.</td>
</tr>
<tr>
<td>end address</td>
<td>End of the network address.</td>
</tr>
<tr>
<td>address increment</td>
<td>Incremental value of the network address.</td>
</tr>
<tr>
<td>exp exp-bits</td>
<td>(Optional) Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.</td>
</tr>
<tr>
<td>flags fec</td>
<td>(Optional) Specifies that forwarding equivalent class (FEC) stack checking is to be performed at transit routers.</td>
</tr>
<tr>
<td>force-explicit-null</td>
<td>(Optional) Forces an unsolicited explicit null label to be added to the MPLS label stack and allows LSP ping to be used to detect LSP breakages at the penultimate hop.</td>
</tr>
<tr>
<td>output interface</td>
<td>(Optional) Specifies the output interface in which echo request packets are sent.</td>
</tr>
<tr>
<td>type</td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td>nexthop</td>
<td>(Optional) Specifies the IP address for the next hop.</td>
</tr>
<tr>
<td>nexthop-address</td>
<td>(Optional) IP address for the next hop.</td>
</tr>
</tbody>
</table>

**Note**

Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information, use the question mark (?) online help function.
### traceroute mpls ipv4

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default Configuration</th>
<th>Command Modes</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>reply dscp</strong></td>
<td>Specifies the differentiated service codepoint value for an MPLS echo reply.</td>
<td></td>
<td>EXEC</td>
<td></td>
</tr>
<tr>
<td><strong>reply mode</strong></td>
<td>Specifies the reply mode for the echo request packet.</td>
<td>IPv4</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>router-alert</strong></td>
<td>Reply with IPv4 UDP packet with router alert.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>revision</strong></td>
<td>Specifies the Cisco extension TLV versioning field.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>source</strong></td>
<td>Specifies the source address used in the echo request packet.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>timeout</strong></td>
<td>Specifies the timeout interval, in seconds. Range is from 0 to 3600. Default is 2.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ttl</strong></td>
<td>Specifies the maximum number of hops (range is 1 to 255).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>verbose</strong></td>
<td>Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**
- `exp exp-bits: 0`
- `reply mode: IPv4`
- `timeout timeout: 2`

**Command Modes**
- EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Note**

The `traceroute mpls` command is not supported on optical LSPs. If an optical LSP is encountered along the LSPs path, it is treated as a physical interface.

For detailed configuration information about MPLS LSP trace operations, see .

---

**Optional**

- Specific the different service codepoint value for an MPLS echo reply.
- Specifies the reply mode for the echo request packet.
- Specifies the Cisco extension TLV versioning field:
  - 1 draft-ietf-mpls-lsp-ping-03 (initial)
  - 2 draft-ietf-mpls-lsp-ping-03 (rev 1)
  - 3 draft-ietf-mpls-lsp-ping-03 (rev 2)
  - 4 draft-ietf-mpls-lsp-ping-09 (initial)
- Specifies the source address used in the echo request packet.
- Specifies the timeout interval, in seconds. Range is from 0 to 3600. Default is 2.
- Specifies the maximum number of hops (range is 1 to 255).
- Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.

**Example**

```plaintext
traceroute mpls ipv4
```
### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to trace a destination:

```plaintext
RP/0/RP0/CPU0:router# traceroute mpls ipv4 140.140.140.140/32 destination 127.0.0.10 127.0.0.15.1
```

Tracing MPLS Label Switched Path to 140.140.140.140/32, timeout is 2 seconds


Type escape sequence to abort.

Destination address 127.0.0.10

0 196.100.1.41 MRU 4470 [Labels: 19 Exp: 0]
L 1 196.100.1.42 MRU 4470 [Labels: 86 Exp: 0] 360 ms
2 196.100.1.50 MRU 4470 [Labels: implicit-null Exp: 0] 8 ms
! 3 196.100.1.18 9 ms

The following example shows how to trace a destination with FEC type specified as generic and verbose option:

```plaintext
RP/0/RP0/CPU0:router# traceroute mpls ipv4 11.11.11.11/32 fec-type generic output interface gigabitEthernet 0/0/0/3 nexthop 172.40.103.2 verbose
```

Tracing MPLS Label Switched Path to 11.11.11.11/32, timeout is 2 seconds


Type escape sequence to abort.

0 172.40.103.1 172.40.103.2 MRU 1500 [Labels: 16038 Exp: 0]
L 1 172.40.103.2 173.101.103.1 MRU 1500 [Labels: 16037 Exp: 0] 6 ms, ret code 8
L 2 173.101.103.1 11.101.11.11 MRU 1500 [Labels: implicit-null Exp: 0] 4 ms, ret code 8
! 3 11.101.11.11 6 ms, ret code 3
**traceroute mpls multipath**

To discover all possible paths of an LSP between the ingress and egress routers, use the `traceroute mpls multipath` command in EXEC mode.

```
traceroute mpls multipath ipv4 address/mask [destination start-address end-address address-increment] [exp exp-bits] [flags fec] [force-explicit-null] [hashkey ipv4 bitmap bit-size] [interval min-send-delay] [output interface type interface-path-id [nexthop nexthop-address]] [reply {dscp dscp-value | reply mode{ipv4 | router-alert};}] [retry-count count] [revision version] [source source-address] [timeout timeout] [ttl value] [verbose] [fec-type {bgp | generic | ldp}]
```

**Syntax Description**

- **ipv4**
  - Specifies the destination type as a Label Distribution Protocol (LDP) IPv4 address.

- **address/mask**
  - Address prefix of the target and number of bits in the target address network mask.

- **destination start-address end-address address-increment**
  - (Optional) Specifies a network 127 address to be used as the destination address in the echo request packet.

  - **start-address**
    - Start of the network address.

  - **end-address**
    - End of the network address.

  - **address-increment**
    - Incremental value of the network address.

- **exp exp-bits**
  - (Optional) Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.

- **flags fec**
  - (Optional) Specifies that forwarding equivalent class (FEC) stack checking is to be performed at transit routers.

- **force-explicit-null**
  - (Optional) Forces an unsolicited explicit null label to be added to the MPLS label stack and allows LSP ping to be used to detect LSP breakages at the penultimate hop.

- **hashkey ipv4 bitmap bit-size**
  - (Optional) Allows user control of the hash key/multipath settings. Range is 0 to 256. The default is 32.

- **interval min-send-delay**
  - (Optional) Specifies a send interval, in milliseconds, between requests. Range is 0 to 3600000. Default is 0.

- **output interface type**
  - (Optional) Specifies the output interface where echo request packets are sent.

  - **type**
    - Interface type. For more information, use the question mark (?) online help function.
### traceroute mpls multipath

<table>
<thead>
<tr>
<th><strong>interface-path-id</strong></th>
<th>Physical interface or virtual interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>Use the <code>show interfaces</code> command to see a list of all interfaces currently configured on the router.</td>
</tr>
<tr>
<td><strong>For more information, use the question mark (?) online help function.</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>nexthop</strong></th>
<th>(Optional) Specifies the IP address for the next hop.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>nexthop-address</strong></td>
<td>(Optional) IP address for the next hop.</td>
</tr>
<tr>
<td><strong>reply dscp dscp-value</strong></td>
<td>(Optional) Specifies the differentiated service codepoint value for an MPLS echo reply.</td>
</tr>
<tr>
<td>**reply mode [ ipv4</td>
<td>router-alert]**</td>
</tr>
<tr>
<td><strong>ipv4</strong></td>
<td>Reply with IPv4 UDP packet (this is the default)</td>
</tr>
<tr>
<td><strong>router-alert</strong></td>
<td>Reply with IPv4 UDP packet with router alert</td>
</tr>
<tr>
<td><strong>retry-count count</strong></td>
<td>(Optional) Specifies the number of retry attempts during multipath LSP traceroute. A retry is attempted if an outstanding echo request</td>
</tr>
<tr>
<td></td>
<td>• times out waiting for the corresponding echo reply.</td>
</tr>
<tr>
<td></td>
<td>• fails to find a valid destination address set to exercise a specific outgoing path. Range is 0 to 10. Default is 3.</td>
</tr>
<tr>
<td><strong>revision version</strong></td>
<td>(Optional) Specifies the Cisco extension TLV versioning field:</td>
</tr>
<tr>
<td></td>
<td>• 1 draft-ietf-mpls-lsp-ping-03 (initial)</td>
</tr>
<tr>
<td></td>
<td>• 2 draft-ietf-mpls-lsp-ping-03 (rev 1)</td>
</tr>
<tr>
<td></td>
<td>• 3 draft-ietf-mpls-lsp-ping-03 (rev 2)</td>
</tr>
<tr>
<td></td>
<td>• 4 draft-ietf-mpls-lsp-ping-09 (initial)</td>
</tr>
<tr>
<td><strong>source source-address</strong></td>
<td>(Optional) Specifies the source address used in the echo request packet.</td>
</tr>
<tr>
<td><strong>timeout timeout</strong></td>
<td>(Optional) Specifies the timeout interval, in seconds. Range is from 0 to 3600. Default is 2.</td>
</tr>
<tr>
<td><strong>ttl value</strong></td>
<td>(Optional) Specifies the maximum number of hops (range is 1 to 255).</td>
</tr>
<tr>
<td><strong>verbose</strong></td>
<td>(Optional) Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.</td>
</tr>
</tbody>
</table>

**Command Default**

- **exp exp-bits**: 0
- **hashkey ipv4 bitmap bit-size**: 4
- **interval min-send-delay**: 0
- **reply mode**: IPv4
- **retry-count**: 3
timeout timeout : 2

Command Modes
EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines
The hashkey ipv4 bitmap keyword and bit-size value control how many addresses are encoded in the DSMAP multipath field. Larger values allow more coverage of equal cost multiple paths throughout the network, but with more processing at the head, mid, and tail routers.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples
The following example shows how to specify the destination type as an LDP IPv4 prefix:

```
RP/0/RP0/CPU0:router# traceroute mpls multi ipv4 140.140.140.140/32 verbose force-explicit-null

Starting LSP Path Discovery for 140.140.140.140/32

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'P' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

LL!
Path 0 found,
output interface POS0/2/0/3 source 196.100.1.61 destination 127.0.0.1
0 196.100.1.61 196.100.1.62 MRU 4470 [Labels: 18/explicit-null Exp: 0/0] multipaths 0
L 1 196.100.1.62 196.100.1.10 MRU 4470 [Labels: 17/explicit-null Exp: 0/0] ret code 8 multipaths 1
L 2 196.100.1.10 196.100.1.18 MRU 4470 [Labels: implicit-null/explicit-null Exp: 0/0] ret code 8 multipaths 1
! 3 196.100.1.1018, ret code 3 multipaths 0
LL!
Path 1 found,
output interface GigabitEthernet0/3/0/0 source 196.100.1.5 destination 127.0.0.1
0 196.100.1.5 196.100.1.37 6 MRU 1500 [Labels: 18/explicit-null Exp: 0/0] multipaths 0
L 1 196.100.1.6 196.100.1.10 MRU 4470 [Labels: 17/explicit-null Exp: 0/0] ret code 8 multipaths 1
L 2 10196.0100.21.10 18 MRU 4470 [Labels: implicit-null/explicit-null Exp: 0/0] ret code 8 multipaths 1
! 3 10196.0100.21.1018, ret code 3 multipaths 0
```
The following example shows how to specify the FEC type as LDP with verbose option:

```
RP/0/RP0/CPU0:router#  traceroute mpls multipath ipv4 11.11.11.11/32 fec-type ldp output
interface gigabitEthernet 0/0/0/3
nexthop 172.40.103.2 verbose
```

Starting LSP Path Discovery for 11.11.11.11/32

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

LL!

Path 0 found,

output interface GigabitEthernet0/0/0/3 nexthop 172.40.103.2
source 172.40.103.1 destination 127.0.0.0
0 172.40.103.1 172.40.103.2 MRU 1500 [Labels: 16038 Exp: 0] multipaths 0
L 1 172.40.103.2 173.101.103.1 MRU 1500 [Labels: 16037 Exp: 0] ret code 8 multipaths 1
L 2 173.101.103.1 11.101.11.11 MRU 1500 [Labels: implicit-null Exp: 0] ret code 8 multipaths 1
! 3 11.101.11.11, ret code 3 multipaths 0

Paths (found/broken/unexplored) (1/0/0)
Echo Request (sent/fail) (3/0)
Echo Reply (received/timeout) (3/0)
Total Time Elapsed 21 ms
**traceroute mpls traffic-eng tunnel-te (P2P)**

To specify the destination type as an MPLS traffic engineering (TE) tunnel for a point-to-point connection, use the **traceroute mpls traffic-eng tunnel-te (P2P)** command in EXEC mode.

```
traceroute mpls traffic-eng tunnel-te [destination start-address end-address address-increment increment-mask] [exp exp-bits] [flags fec] [force-explicit-null] [reply {dscp dscp-value | mode {ipv4 | router-alert}}] [revision version] [source source-address] [timeout timeout] [ttl value] [verbose]
```

### Syntax Description

- **tunnel-te**: Specifies the MPLS-TE tunnel type.
- **tunnel-ID**: Tunnel interface.
- **destination start-address end-address address-increment increment-mask** (Optional) Specifies a network 127 address to be used as the destination address in the echo request packet.
  - **start-address**: Start of the network address.
  - **end-address**: End of the network address.
  - **address-increment**: Incremental value of the network address.
  - **increment-mask**: Incremental mask of the network address.
- **exp exp-bits** (Optional) Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.
- **flags fec** (Optional) Specifies that forwarding equivalent class (FEC) stack checking is to be performed at transit routers.
- **force-explicit-null** (Optional) Forces an unsolicited explicit null label to be added to the MPLS label stack and allows LSP ping to be used to detect LSP breakages at the penultimate hop.
- **reply dscp dscp-value** (Optional) Specifies the differentiated service codepoint value for an MPLS echo reply.
- **reply-mode [ ipv4 | router-alert]** (Optional) Specifies the reply mode for the echo request packet.
  - **ipv4**: Reply with IPv4 UDP packet (this is the default)
  - **router-alert**: Reply with IPv4 UDP packet with router alert
- **revision version**
- **source source-address**
- **timeout timeout**
- **ttl value**
- **verbose**
revision version  (Optional) Specifies the Cisco extension TLV versioning field:
  • 1 draft-ietf-mpls-lsp-ping-03 (initial)
  • 2 draft-ietf-mpls-lsp-ping-03 (rev 1)
  • 3 draft-ietf-mpls-lsp-ping-03 (rev 2)
  • 4 draft-ietf-mpls-lsp-ping-09 (initial)

source source-address  (Optional) Specifies the source address used in the echo request packet.

timeout timeout  (Optional) Specifies the timeout interval, in seconds. Range is from 0 to 3600. Default is 2.

ttl value  (Optional) Specifies the maximum number of hops (range is 1 to 255).

verbose  (Optional) Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.

Command Default
exp exp-bits : 0
reply-mode: IPv4
timeout timeout : 2

Command Modes
EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.1</td>
<td></td>
</tr>
</tbody>
</table>

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>read</td>
</tr>
</tbody>
</table>

The following example shows how to specify the destination as a MPLS-TE tunnel:

```
RP/0/RP0/CPU0:router#  traceroute mpls traffic-eng tunnel-te 13
Tracing MPLS TE Label Switched Path on tunnel-te13, timeout is 2 seconds
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.

0 0.0.0.0 11.0.0.1 MRU 1500 [Labels: 16003 Exp: 0]
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mpls traffic-eng tunnels</code></td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
</tbody>
</table>
**traceroute mpls traffic-eng tunnel-mte (P2MP)**

To specify the destination type as an MPLS traffic engineering (TE) tunnel for point-to-multipoint connection, use the `traceroute mpls traffic-eng tunnel-mte` command in EXEC mode.

```
traceroute mpls traffic-eng tunnel-mte tunnel-ID [destination start-address end-address address-increment increment-mask] [responder-id ipv4-address] [exp exp-bits] [flags fec] [jitter jitter-value] [reply {dscp dscp-value | mode {ipv4 | router-alert}}] [source source-address] [timeout timeout] [ttl value] [verbose]
```

**Syntax Description**

- **tunnel-mte**: Specifies the MPLS-TE P2MP tunnel type.
- **tunnel-ID**: Tunnel interface.
- **destination start-address end-address address-increment increment-mask**: (Optional) Specifies a network 127 address to be used as the destination address in the echo request packet.
  - **start-address**: Start of the network address.
  - **end-address**: End of the network address.
  - **address-increment**: Incremental value of the network address.
  - **increment-mask**: Incremental mask of the network address.
- **responder-id ipv4-address**: (Optional) Specifies the responder-id IPv4 address.
- **exp exp-bits**: (Optional) Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.
- **flags fec**: (Optional) Specifies that forwarding equivalent class (FEC) stack checking is to be performed at transit routers.
- **jitter jitter-value**: (Optional) Specifies the jitter value. Range is 0 to 2147483647.
- **reply dscp dscp-value**: (Optional) Specifies the differentiated service codepoint value for an MPLS echo reply.
### reply-mode

Optional) Specifies the reply mode for the echo request packet.

**ipv4**

Reply with IPv4 UDP packet. (This is the default.)

**router-alert**

Reply with IPv4 UDP packet with router alert

### source source-address

(Optional) Specifies the source address used in the echo request packet.

### timeout timeout

(Optional) Specifies the timeout interval, in seconds. Range is 0 to 3600. Default is 2.

### ttl value

(Optional) Specifies the maximum number of hops. Range is 1 to 255. Default is 30.

### verbose

(Optional) Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.

---

### Command Default

**exp exp-bits : 0**

**reply-mode: IPv4**

**timeout timeout : 2**

**ttl: 30**

### Command Modes

EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read</td>
</tr>
<tr>
<td>mpls-ldp</td>
<td>read</td>
</tr>
</tbody>
</table>

### Example

The following example shows how to specify the maximum number of hops for the trace route to traverse by using the **ttl** keyword:

```
RP/0/RP0/CPU0:router# traceroute mpls traffic-eng tunnel-mte 10 ttl 4
```

Mon Apr 12 12:16:50.095 EST

Tracing MPLS MTE Label Switched Path on tunnel-mte10, timeout is 2.2 seconds
MPLS Command Reference for Cisco NCS 6000 Series Routers

The following examples show how to specify the egress host address by using the egress keyword:

```
RP/0/RP0/CPU0:router# traceroute mpls traffic-eng tunnel-mte 10 egress 13.0.0.1
Mon Apr 12 12:18:01.994 EST
Tracing MPLS MTE Label Switched Path on tunnel-mte10, timeout is 2.2 seconds
```

Codes: '! ' - success, 'Q' - request not sent, '.', timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0, 'd' - DDMAP

Type escape sequence to abort.

```
d 1 192.168.222.2 113 ms [Estimated Role: Branch]
  [L] DDMAP 0: 192.168.140.2 192.168.140.2 MRU 1500 [Labels: 16001 Exp: 0]
```

```
d 2 192.168.222.2 118 ms [Estimated Role: Branch]
  [L] DDMAP 0: 192.168.140.2 192.168.140.2 MRU 1500 [Labels: 16001 Exp: 0]
```

```
d 3 192.168.222.2 141 ms [Estimated Role: Branch]
  [L] DDMAP 0: 192.168.140.2 192.168.140.2 MRU 1500 [Labels: 16001 Exp: 0]
```

```
d 4 192.168.222.2 110 ms [Estimated Role: Branch]
```

MPLS OAM Commands

traceroute mpls traffic-eng tunnel-mte (P2MP)
The following examples show how to specify the egress host address, the maximum number of hops, and jitter in the tunnel:

```
RP/0/RP0/CPU0:router# traceroute mpls traffic-eng tunnel-mte 10 egress 13.0.0.1 ttl 4 jitter 500
```

```
Mon Apr 12 12:19:00.292 EST
Tracing MPLS MTE Label Switched Path on tunnel-mte10, timeout is 2.5 seconds

Type escape sequence to abort.
d 1 192.168.222.2 238 ms [Estimated Role: Branch]
  [L] DDMAP 0: 192.168.140.2 192.168.140.2 MRU 1500 [Labels: 16001 Exp: 0]

! 2 192.168.170.1 290 ms [Estimated Role: Egress]
  [L] DDMAP 0: 192.168.140.2 192.168.140.2 MRU 1500 [Labels: 16001 Exp: 0]

! 3 192.168.170.1 428 ms [Estimated Role: Egress]
  [L] DDMAP 0: 192.168.140.2 192.168.140.2 MRU 1500 [Labels: 16001 Exp: 0]

! 4 192.168.170.1 327 ms [Estimated Role: Egress]
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mpls traffic-eng tunnels</code></td>
<td>Displays information about MPLS-TE tunnels.</td>
</tr>
<tr>
<td><code>ping mpls traffic-eng tunnel-te (P2P)</code></td>
<td>Displays information about MPLS-TE tunnel for a point-to-point connection.</td>
</tr>
</tbody>
</table>
To verify hop-by-hop fault localization and path tracing for the point-to-multipoint path, use the `traceroute mpls mldp p2mp` command in EXEC mode.

```
traceroute mpls mldp p2mp root-address [IPv4 source-ipv4-address group-ipv4-address | IPv6 source-ipv6-address group-ipv6-address | vpnv4 AS-number [source-ipv4-address group-ipv4-address] | vpnv6 AS-number [source-ipv6-address group-ipv6-address] | mdt oui:vpn-index mdt-number | global-id lsp-id] [options]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mldp</td>
<td>Verifies the ping capability for multicast label distribution protocol (mldp).</td>
</tr>
<tr>
<td>p2mp</td>
<td>Indicates the Point-to-Multipoint (P2MP) label switch path.</td>
</tr>
<tr>
<td>root-address</td>
<td>Specifies the root address.</td>
</tr>
<tr>
<td>IPv4 ipv4-address</td>
<td>Defines IPv4 opaque encoding.</td>
</tr>
<tr>
<td>IPv6 ipv6-address</td>
<td>Defines IPv6 opaque encoding.</td>
</tr>
<tr>
<td>vpnv4 AS-number source-ipv4-address group-ipv4-address</td>
<td>Defines VPNv4 opaque encoding.</td>
</tr>
<tr>
<td>vpnv6 AS-number source-ipv6-address group-ipv6-address</td>
<td>Defines VPNv6 opaque encoding.</td>
</tr>
<tr>
<td>mdt oui:vpn-index mdt-number</td>
<td>Defines VPN ID opaque encoding. Range of 3-byte OUI is 0 to 16777215. Range of mdt-number is 0 to 4294967295.</td>
</tr>
<tr>
<td>global-id lsp-id</td>
<td>Defines 4 byte global LSP ID opaque encoding.</td>
</tr>
<tr>
<td>source-address</td>
<td>Specifies the source address of target multicast address.</td>
</tr>
<tr>
<td>group-address</td>
<td>Specifies the target address of target multicast address.</td>
</tr>
<tr>
<td>AS-number</td>
<td>Specifies the Autonomous system number as follows:</td>
</tr>
<tr>
<td></td>
<td>• 4-byte AS-number with asdot (X.Y) : aa.bb:cc format (for example, 11.22:33)</td>
</tr>
<tr>
<td></td>
<td>• 2-byte AS-number or 4-byte AS-number: aa:bb format (for example, 11:22)</td>
</tr>
<tr>
<td></td>
<td>• IPv4 address and index:aa.bb.cc.dd:ee format (for example, 11.22.33.44:55)</td>
</tr>
</tbody>
</table>
traceroute mpls mldp (P2MP)

options
Specifies a set of various options:

**destination**

(Optional) Specifies a network 127/8 address to be used as the destination address in the echo request packet.

**start-address:** Start of the network address.

**end-address:** End of the network address.

**address increment:** Incremental value of the network address, which is expressed as a decimal number value or IP address.

**exp-exp-bits**

(Optional) Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.

**flags**

**fec:** (Optional) Specifies that forwarding equivalent class (FEC) stack checking is to be performed at transit routers.

**no-ttl:** (Optional) Specifies not to add TTL expired flag in echo request.

**force-explicit-null**

(Optional) Forces an unsolicited explicit null label to be added to the MPLS label stack and allows LSP ping to be used to detect LSP breakages at the penultimate hop.

**jitter**

(Optional) Specifies a jitter value for a corresponding echo request, in milliseconds. Range is 0 to 2147483647. Default is 200.

**reply dscp dscp-value**

(Optional) Specifies the differentiated service codepoint value for an MPLS echo reply.

**mode [ipv4 | router-alert ]**

(Optional) Specifies the reply mode for the echo request packet.

**ipv4**

Reply with an IPv4 UDP packet (this is the default)

**router-alert**

Reply with an IPv4 UDP packet with the IP
router alert set

**responder-id ipv4-address**  
(Optional) Adds responder identifier into corresponding echo request.

**source ipv4-address**  
(Optional) Specifies the source address used in the echo request packet.

**timeout timeout**  
(Optional) Specifies the timeout interval, in seconds. Range is 0 to 3600. Default is 2.

**ttl**  
(Optional) Specifies the TTL value to be used in the MPLS labels (range is 1 to 255). Default is 255.

**verbose**  
(Optional) Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.

---

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>basic-services</td>
<td>execute</td>
</tr>
<tr>
<td>mpls-te or mpls-ldp</td>
<td>read</td>
</tr>
</tbody>
</table>

The following examples show how to verify path tracing for P2MP by using the **traceroute mpls mldp p2mp** command.

RP/0/RP0/CPU0:router#traceroute mpls mldp p2mp 192.168.0.1 ipv4 2.2.2.2 232.1.1.1 ttl 4  
Mon Jul 11 15:36:42.299 JST

Tracing MPLS Label Switched Path to mldp p2mp 192.168.0.1 ipv4 {2.2.2.2, 232.1.1.1}, timeout is 2.2 seconds, jitter value is 200 msec

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,  
'L' - labeled output interface, 'B' - unlabeled output interface,  
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,  
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,  
'P' - no rx intf label prot, 'p' - premature termination of LSP,
Type escape sequence to abort.

```
d 1 10.10.10.2 54 ms [Estimated Role: Branch]
  [L] DDMAP 0: 11.11.11.3 11.11.11.3 MRU 1500 [Labels: 16016 Exp: 0]

! 2 11.11.11.3 47 ms [Estimated Role: Egress]
! 2 12.12.12.4 68 ms [Estimated Role: Egress]
 . 3 *
 . 4 *
```

RP/0/RP0/CPU0:router#traceroute mpls mldp p2mp 192.168.0.1 ipv4 2.2.2.2 232.1.1.1 ttl 4 jitter 300
Mon Jul 11 15:37:18.976 JST

Tracing MPLS Label Switched Path to mldp p2mp 192.168.0.1 ipv4 (2.2.2.2, 232.1.1.1),
timeout is 2.3 seconds, jitter value is 300 msec

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0, 'd' - DDMAP

Type escape sequence to abort.

```
d 1 10.10.10.2 77 ms [Estimated Role: Branch]
  [L] DDMAP 0: 11.11.11.3 11.11.11.3 MRU 1500 [Labels: 16016 Exp: 0]

! 2 12.12.12.4 15 ms [Estimated Role: Egress]
! 2 11.11.11.3 114 ms [Estimated Role: Egress]
 . 3 *
 . 4 *
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping mpls mldp (P2MP), on page 502</td>
<td>Verifies data plane and control plane for the point-to-multipoint (P2MP) label switch path.</td>
</tr>
<tr>
<td>traceroute mpls mldp (MP2MP), on page 536</td>
<td>Verifies hop-by-hop fault localization and path tracing for the multipoint-to-multipoint path.</td>
</tr>
</tbody>
</table>
traceroute mpls mldp (MP2MP)

To verify hop-by-hop fault localization and path tracing for the multipoint-to-multipoint path (MP2MP), use the traceroute mpls mldp mp2mp command in EXEC mode.

```
traceroute mpls mldp mp2mp root-address [IPv4 source-ipv4-address group-ipv4-address | IPv6 source-ipv6-address group-ipv6-address | vpnv4 AS-number [source-ipv4-address group-ipv4-address] | vpnv6 AS-number [source-ipv6-address group-ipv6-address] | mdt oui:vpn-index mdt-number | global-id lsp-id] [options]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mldp</td>
<td>Verifies the ping capability for multicast label distribution protocol (mldp).</td>
</tr>
<tr>
<td>mp2mp</td>
<td>Indicates the Multipoint-to-Multipoint (MP2MP) label switch path.</td>
</tr>
<tr>
<td>root-address</td>
<td>Specifies the root address.</td>
</tr>
<tr>
<td>IPv4 ipv4-address</td>
<td>Defines IPv4 opaque encoding.</td>
</tr>
<tr>
<td>IPv6 ipv6-address</td>
<td>Defines IPv6 opaque encoding.</td>
</tr>
<tr>
<td>vpnv4 AS-number</td>
<td>Defines VPNv4 opaque encoding.</td>
</tr>
<tr>
<td>vpnv6 AS-number</td>
<td>Defines VPNv6 opaque encoding.</td>
</tr>
<tr>
<td>mdt oui:vpn-index mdt number</td>
<td>Defines VPN ID opaque encoding. Range of 3-byte OUI is 0 to 16777215. Range of mdt-number is 0 to 4294967295.</td>
</tr>
<tr>
<td>global-id lsp-id</td>
<td>Defines 4 byte global LSP ID opaque encoding.</td>
</tr>
<tr>
<td>source-address</td>
<td>Specifies the source address of target multicast address.</td>
</tr>
<tr>
<td>group-address</td>
<td>Specifies the target address of target multicast address.</td>
</tr>
<tr>
<td>AS-number</td>
<td>Specifies the Autonomous system number as follows:</td>
</tr>
<tr>
<td></td>
<td>• 4-byte AS-number with asdot (X.Y) : aa.bb:cc format (for example, 11.22:33)</td>
</tr>
<tr>
<td></td>
<td>• 2-byte AS-number or 4-byte AS-number: aa:bb format (for example, 11:22)</td>
</tr>
<tr>
<td></td>
<td>• IPv4 address and index:aa.bb.cc.dd:ee format (for example, 11.22.33.44:55)</td>
</tr>
</tbody>
</table>
traceroute mpls mldp (MP2MP)

```
options
```
Specifies a set of various options:

**destination**

(Optional) Specifies a network 127/8 address to be used as the destination address in the echo request packet.

**start-address**: Start of the network address.

**end-address**: End of the network address.

**address increment**: Incremental value of the network address, which is expressed as a decimal number value or IP address.

**exp-exp-bits**

(Optional) Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.

**flags**

**fec**: (Optional) Specifies that forwarding equivalent class (FEC) stack checking is to be performed at transit routers.

**no-ttl**: (Optional) Specifies not to add TTL expired flag in echo request.

**force-explicit-null**

(Optional) Forces an unsolicited explicit null label to be added to the MPLS label stack and allows LSP ping to be used to detect LSP breakages at the penultimate hop.

**jitter**

(Optional) Specifies a jitter value for a corresponding echo request, in milliseconds. Range is 0 to 2147483647. Default is 200.

**reply dscp-value**

(Optional) Specifies the differentiated service codepoint value for an MPLS echo reply.

**mode [ipv4 | router-alert ]**

(Optional) Specifies the reply mode for the echo request packet.

**ipv4**

Reply with an IPv4 UDP packet (this is the default)

**router-alert**

Reply with an IPv4 UDP packet with the IP
router alert set

**responder-id ipv4-address**

(Optional) Adds responder identifier into corresponding echo request.

**source ipv4-address**

(Optional) Specifies the source address used in the echo request packet.

**timeout timeout**

(Optional) Specifies the timeout interval, in seconds. Range is 0 to 3600. Default is 2.

**ttl**

(Optional) Specifies the TTL value to be used in the MPLS labels (range is 1 to 255). Default is 255.

**verbose**

(Optional) Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes.

<table>
<thead>
<tr>
<th>Command Default</th>
<th>ttl255 jitter200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>EXEC</td>
</tr>
<tr>
<td>Command History</td>
<td>Release</td>
</tr>
<tr>
<td></td>
<td>Release 5.2.1</td>
</tr>
<tr>
<td>Task ID</td>
<td>Task ID</td>
</tr>
<tr>
<td></td>
<td>basic-services</td>
</tr>
<tr>
<td></td>
<td>mpls-te or mpls-ldp</td>
</tr>
</tbody>
</table>

The following examples show how to verify path tracing for MP2MP by using the `traceroute mpls mldp mp2mp` command.

```
RP/0/RP0/CPU0:router#traceroute mpls mldp mp2mp 192.168.0.1 global-id 1 ttl 4
```

Tracing MPLS Label Switched Path to mldp mp2mp 192.168.0.1 global-id 1, timeout is 2.2 seconds, jitter value is 200 msec

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping mpls mldp (MP2MP), on page 508</td>
<td>Verifies data plane and control plane for the multipoint-to-multipoint (MP2MP) label switch path.</td>
</tr>
<tr>
<td>traceroute mpls mldp (P2MP), on page 531</td>
<td>Verifies hop-by-hop fault localization and path tracing for the point-to-multipoint path.</td>
</tr>
</tbody>
</table>