CONTENTS

PREFACE

Preface xi
Changes to This Document xi
Communications, Services, and Additional Information xii

CHAPTER 1

MPLS Label Distribution Protocol Commands 1
backoff 3
clear mpls ldp forwarding 4
clear mpls ldp msg-counters neighbor 5
clear mpls ldp neighbor 6
default-route 7
discovery hello 8
discovery instance-tlv disable 9
discovery targeted-hello 10
discovery transport-address 12
downstream-on-demand 14
explicit-null 15
graceful-restart (MPLS LDP) 17
session holdtime (MPLS LDP) 19
igp auto-config disable 20
igp sync delay 21
igp sync delay on-proc-restart 22
implicit-null-overide 24
interface (MPLS LDP) 26
label accept 28
label advertise 30
label allocate 33
MPLS Static Commands

address family ipv4 unicast (mpls-static) 99

clear mpls static local-label discrepancy 100
interface (mpls-static) 101
show mpls static local-label 103
show mpls static summary 105
CHAPTER 3  MPLS Forwarding Commands  107

- clear mpls forwarding counters  108
- mpls label range  109
- show mpls ea interfaces  111
- show mpls forwarding  112
- show mpls forwarding exact-route  117
- show mpls forwarding labels  121
- show mpls forwarding summary  122
- show mpls interfaces  125
- show mpls label range  128
- show mpls label table  129
- show mpls lsd applications  131
- show mpls lsd clients  133
- show mpls lsd forwarding labels  135
- show mpls lsd forwarding summary  136

CHAPTER 4  RSVP Infrastructure Commands  139

- authentication (RSVP)  141
- clear rsvp authentication  143
- clear rsvp counters all  145
- clear rsvp counters authentication  146
- clear rsvp counters chkpt  148
- clear rsvp counters events  149
- clear rsvp counters messages  150
- clear rsvp counters oor  151
- clear rsvp counters prefix-filtering  152
- key-source key-chain (RSVP)  154
- life-time (RSVP)  156
- rsvp  158
- rsvp interface  159
- rsvp neighbor  161
- show rsvp request  162
- show rsvp authentication  164
show rsvp counters 169
show rsvp counters oor 172
show rsvp counters prefix-filtering 174
show rsvp fast-reroute 177
show rsvp graceful-restart 179
show rsvp hello instance 182
show rsvp hello instance interface-based 184
show rsvp interface 186
show rsvp neighbor 187
show rsvp reservation 188
show rsvp sender 191
show rsvp session 194
signalling dscp (RSVP) 197
signalling graceful-restart 199
signalling hello graceful-restart interface-based 201
signalling hello graceful-restart refresh interval 202
signalling prefix-filtering access-list 204
signalling prefix-filtering default-deny-action 205
signalling rate-limit 206
signalling refresh interval 208
signalling refresh missed 210
window-size (RSVP) 211
signalling refresh reduction summary 213
signalling refresh reduction reliable 214
signalling refresh reduction disable 217
signalling refresh reduction bundle-max-size 218

CHAPTER 5

MPLS Traffic Engineering Commands 219
adjustment-threshold (MPLS-TE) 223
admin-weight 224
affinity 225
affinity-map 229
application (MPLS-TE) 231
attribute-flags 232
attribute-names 233
attribute-set 234
auto-bw (MPLS-TE) 238
auto-bw collect frequency (MPLS-TE) 240
autoroute announce 241
autoroute destination 243
autoroute metric 244
auto-tunnel backup (MPLS-TE) 245
backup-path tunnel-te 246
bidirectional 248
bw-limit (MPLS-TE) 249
clear mpls traffic-eng auto-bw (MPLS-TE EXEC) 251
clear mpls traffic-eng auto-tunnel backup unused 253
clear mpls traffic-eng auto-tunnel mesh 254
clear mpls traffic-eng auto-tunnel mesh 255
clear mpls traffic-eng counters auto-tunnel backup 256
clear mpls traffic-eng counters global 257
clear mpls traffic-eng counters signaling 258
clear mpls traffic-eng counters soft-preemption 259
clear mpls traffic-eng fast-reroute log 260
clear mpls traffic-eng link-management statistics 261
collect-bw-only (MPLS-TE) 262
destination (MPLS-TE) 263
disable (explicit-path) 264
exclude srlg (auto-tunnel backup) 265
fast-reroute 266
fast-reroute protect 267
fast-reroute timers promotion 268
flooding thresholds 269
forward-class 270
forwarding-adjacency 271
index exclude-address 273
index exclude-srlg 275
index next-address 276
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface (MPLS-TE)</td>
<td>278</td>
</tr>
<tr>
<td>interface (SRLG)</td>
<td>280</td>
</tr>
<tr>
<td>interface tunnel-te</td>
<td>281</td>
</tr>
<tr>
<td>ipv4 unnumbered (MPLS)</td>
<td>283</td>
</tr>
<tr>
<td>ipv4 unnumbered mpls traffic-eng</td>
<td>284</td>
</tr>
<tr>
<td>link-management timers bandwidth-hold</td>
<td>285</td>
</tr>
<tr>
<td>link-management timers periodic-flooding</td>
<td>286</td>
</tr>
<tr>
<td>link-management timers preemption-delay</td>
<td>287</td>
</tr>
<tr>
<td>load-share</td>
<td>288</td>
</tr>
<tr>
<td>load-share unequal</td>
<td>289</td>
</tr>
<tr>
<td>match mpls disposition</td>
<td>290</td>
</tr>
<tr>
<td>maxabs (MPLS-TE)</td>
<td>291</td>
</tr>
<tr>
<td>mpls traffic-eng</td>
<td>292</td>
</tr>
<tr>
<td>mpls traffic-eng auto-bw apply (MPLS-TE)</td>
<td>293</td>
</tr>
<tr>
<td>mpls traffic-eng fast-reroute promote</td>
<td>295</td>
</tr>
<tr>
<td>mpls traffic-eng level</td>
<td>296</td>
</tr>
<tr>
<td>mpls traffic-eng link-management flood</td>
<td>297</td>
</tr>
<tr>
<td>mpls traffic-eng path-protection switchover tunnel-te</td>
<td>298</td>
</tr>
<tr>
<td>mpls traffic-eng reoptimize (EXEC)</td>
<td>299</td>
</tr>
<tr>
<td>mpls traffic-eng reoptimize events link-up</td>
<td>300</td>
</tr>
<tr>
<td>mpls traffic-eng router-id (MPLS-TE router)</td>
<td>301</td>
</tr>
<tr>
<td>mpls traffic-eng repotimize mesh group</td>
<td>303</td>
</tr>
<tr>
<td>mpls traffic-eng srlg</td>
<td>304</td>
</tr>
<tr>
<td>nhop-only (auto-tunnel backup)</td>
<td>306</td>
</tr>
<tr>
<td>overflow threshold (MPLS-TE)</td>
<td>307</td>
</tr>
<tr>
<td>path-option (MPLS-TE)</td>
<td>309</td>
</tr>
<tr>
<td>path-protection (MPLS-TE)</td>
<td>312</td>
</tr>
<tr>
<td>path-protection timers reopt-after-switchover</td>
<td>313</td>
</tr>
<tr>
<td>path-selection cost-limit</td>
<td>314</td>
</tr>
<tr>
<td>path-selection ignore overload (MPLS-TE)</td>
<td>315</td>
</tr>
<tr>
<td>path-selection loose-expansion affinity (MPLS-TE)</td>
<td>317</td>
</tr>
<tr>
<td>path-selection loose-expansion metric (MPLS-TE)</td>
<td>318</td>
</tr>
<tr>
<td>path-selection metric (MPLS-TE)</td>
<td>319</td>
</tr>
<tr>
<td>path-selection metric (interface)</td>
<td>320</td>
</tr>
</tbody>
</table>
policy-class 321
priority (MPLS-TE) 323
record-route 324
redirect default-route nexthop 325
redirect nexthop 326
reoptimize (MPLS-TE) 327
reoptimize timers delay (MPLS-TE) 328
route-priority 330
router-id secondary (MPLS-TE) 332
set destination-address 333
set ipv4 df 334
set source-address 335
show explicit-paths 336
show interfaces tunnel-te accounting 338
show mpls traffic-eng affinity-map 339
show mpls traffic-eng attribute-set 341
show mpls traffic-eng autoroute 343
show mpls traffic-eng auto-tunnel backup 345
show mpls traffic-eng auto-tunnel mesh 348
show mpls traffic-eng collaborator-timers 351
show mpls traffic-eng counters signaling 353
show mpls traffic-eng forwarding 357
show mpls traffic-eng forwarding-adjacency 359
show mpls traffic-eng igp-areas 360
show mpls traffic-eng link-management admission-control 363
show mpls traffic-eng link-management advertisements 367
show mpls traffic-eng link-management bandwidth-allocation 370
show mpls traffic-eng link-management igp-neighbors 373
show mpls traffic-eng link-management interfaces 375
show mpls traffic-eng link-management statistics 378
show mpls traffic-eng link-management summary 380
show mpls traffic-eng maximum tunnels 382
show mpls traffic-eng preemption log 385
show mpls traffic-eng topology 387
show mpls traffic-eng tunnels 391
show mpls traffic-eng tunnels auto-bw brief 420
show mpls traffic-eng link-management soft-preemption 422
show srlg 424
signalled-name 427
signalling advertise explicit-null (MPLS-TE) 428
snmp traps mpls traffic-eng 429
soft-preemption 431
soft-preemption frr-rewrite 432
srlg 433
timers loose-path (MPLS-TE) 434
timers removal unused (auto-tunnel backup) 435
timeout (soft-preemption) 436
topology holddown sigerr (MPLS-TE) 437
tunnel-id (auto-tunnel backup) 438

CHAPTER 6

MPLS OAM Commands 441

clear mpls oam counters 442
echo disable-vendor-extension 443
mpls oam 444
ping mpls ipv4 445
show mpls oam 450
show mpls oam database 452
traceroute mpls ipv4 453
traceroute mpls multipath 457
Preface

The preface contains these sections:

- Changes to This Document, on page xi
- Communications, Services, and Additional Information, on page xii

Changes to This Document

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 2015</td>
<td>Initial release of this document.</td>
</tr>
<tr>
<td>November 2016</td>
<td>Republished with release 6.1.2 command reference updates.</td>
</tr>
<tr>
<td>March 2017</td>
<td>Republished with release 6.2.1 command reference updates.</td>
</tr>
<tr>
<td>July 2017</td>
<td>Republished for Release 6.2.2</td>
</tr>
<tr>
<td>September 2017</td>
<td>Republished for Release 6.3.1</td>
</tr>
<tr>
<td>March 2018</td>
<td>Republished for Release 6.4.1</td>
</tr>
<tr>
<td>August 2018</td>
<td>Republished for Release 6.5.1</td>
</tr>
<tr>
<td>January 2019</td>
<td>Republished for Release 6.5.2</td>
</tr>
<tr>
<td>March 2019</td>
<td>Republished for Release 6.5.3</td>
</tr>
<tr>
<td>May 2019</td>
<td>Republished for Release 6.6.25</td>
</tr>
<tr>
<td>August 2019</td>
<td>Published for the Release 7.0.1</td>
</tr>
<tr>
<td>January 2020</td>
<td>Published for the Release 7.1.1</td>
</tr>
</tbody>
</table>
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 the.

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

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

For detailed information about MPLS concepts, configuration tasks, and examples, see *MPLS Configuration Guide for Cisco NCS 5000 Series Routers*.

- backoff, on page 3
- clear mpls ldp forwarding, on page 4
- clear mpls ldp msg-counters neighbor, on page 5
- clear mpls ldp neighbor, on page 6
- default-route, on page 7
- discovery hello, on page 8
- discovery instance-tlv disable, on page 9
- discovery targeted-hello, on page 10
- discovery transport-address, on page 12
- downstream-on-demand, on page 14
- explicit-null, on page 15
- graceful-restart (MPLS LDP), on page 17
- session holdtime (MPLS LDP), 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
- implicit-null-override, on page 24
- interface (MPLS LDP), on page 26
- label accept, on page 28
- label advertise, on page 30
- label allocate, on page 33
- log graceful-restart, on page 35
• log neighbor, on page 36
• log session-protection, on page 37
• mpls ldp, on page 38
• neighbor password, on page 39
• neighbor targeted, on page 41
• router-id (MPLS LDP), on page 42
• router ospf, on page 43
• session protection, on page 45
• show mpls ldp backoff, on page 46
• show mpls ldp bindings, on page 48
• show mpls ldp capabilities, on page 54
• show mpls ldp discovery, on page 55
• show mpls ldp forwarding, on page 59
• show mpls ldp graceful-restart, on page 63
• show mpls ldp igp sync, on page 65
• show mpls ldp interface, on page 68
• show mpls ldp neighbor, on page 71
• show mpls ldp parameters, on page 79
• show mpls ldp statistics fwd-setup, on page 81
• show mpls ldp statistics msg-counters, on page 83
• show mpls ldp summary, on page 85
• show mpls ldp trace, on page 87
• show igp, on page 91
• signalling dscp (LDP), on page 93
• snmp-server traps mpls ldp, on page 94
• address-family ipv4 label, on page 95
backoff

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

```
backoff initial maximum
no backoff
```

**Syntax Description**

- `initial` Initial backoff delay, in seconds. Range is 5 to 2147483 50331.
- `maximum` Maximum backoff delay, in seconds. Range is 5 to 2147483 50331.

**Command Default**

- `initial`: 15
- `maximum`: 120

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</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.

**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
```
clear mpls ldp forwarding

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

```
clear mpls ldp [ipv4] forwarding [prefix/length]
```

**Syntax Description**
- **ipv4** (Optional) Specifies IP version 4 address family.
- **prefix** (Optional) Destination prefix, written in A.B.C.D format.
- **length** (Optional) Network mask length, in bits. Range is 0 to 32.

**Command Default**
No default behavior or values

**Command Modes**
XR EXEC mode

**Command History**
- **Release** 6.0  This command was introduced.

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

**Task ID**
- **mpls-ldp**  read, write

**Example**
This example shows how to clear (or reset) the MPLS LDP forwarding rewrites using the `clear mpls ldp forwarding` command:

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

**Syntax Description**
- `lsr-id`  
  LSR ID of neighbor in A.B.C.D format.
- `ldp-id`  
  LDP ID of neighbor in A.B.C.D: format.

**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>Release 6.0</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
```
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>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>(Optional) Neighbor IP address.</td>
</tr>
<tr>
<td><code>ldp-id</code></td>
<td>(Optional) Neighbor LDP ID in A.B.C.D: format.</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>6.0</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).

**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 force an unconditional LDP session restart:

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

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

```
default-route
no default-route
```

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

MPLS LDP configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</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
```
**discovery hello**

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

```
discovery hello {holdtime seconds | interval seconds}
no discovery hello {holdtime | interval}
```

### Syntax Description

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

### Command Default

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

### Command Modes

MPLS LDP configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</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
```
**discovery instance-tlv disable**

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

```
discovery instance-tlv disable
no discovery instance-tlv disable
```

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

**Command Default**
No default behavior or values

**Command Modes**
MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</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-lwp</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
```
discovery targeted-hello

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

```
discovery targeted-hello {holdtime seconds | interval seconds} {address-family ipv4 discovery targeted-hello} {accept | [from acl]}
no discovery targeted-hello {accept | holdtime | interval}
```

### Syntax Description

- **accept** Accepts targeted hellos from any source.
- **ipv4** Specifies IP version 4 address family.
- **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>Release 6.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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 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
```
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)# address-family ipv4
RP/0/RP0/CPU0:router(config-ldp-af)# 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-ipv4-acl)# mpls ldp
RP/0/RP0/CPU0:router(config-ldp)# address-family ipv4
RP/0/RP0/CPU0:router(config-ldp-af)# discovery targeted-hello accept from peer_acl_10
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.

```
[interface type interface-path-id] address-family
ipv4
discovery transport-address {ip-address}
no [interface type interface-path-id address-family] {ipv4} discovery transport-address {ip-address}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Command Default</th>
<th>Command Modes</th>
<th>Command History</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface type</code></td>
<td>LDP advertises its LDP router ID as the transport address in LDP discovery hello messages.</td>
<td>MPLS LDP interface configuration</td>
<td>Release 6.0</td>
<td>Establishing an LDP session between two routers requires a TCP session connection. To establish the TCP session 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.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
<td></td>
<td>Modification</td>
<td></td>
</tr>
</tbody>
</table>
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>

### Examples

The following example shows how to specify an exiting address (10.10.3.1) as the transport address on an interface tenGigE 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:
  tenGigE 0/0/0/1
Addresses bound to this peer:
  10.10.3.2 10.44.44.44
downstream-on-demand

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

```
session downstream-on-demand with access-list
no session downstream-on-demand with access-list
```

**Syntax Description**

- `session` (Optional) Configures session parameters.
- `with` Displays access list of LDP peers.
- `access-list` IPv4 access-list name.

**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>Release 6.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Examples**

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

```
RP/0/RP0/CPU0:router(config-ldp)# downstream-on-demand with acl1
```
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.

```
address-family {ipv4} label local advertise explicit-null [{to peer-acl | for prefix-acl [to peer-acl]}]
no address-family {ipv4} label local advertise explicit-null [{to peer-acl | for prefix-acl [to peer-acl]}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4</td>
<td>Specifies IP version 4 address family.</td>
</tr>
<tr>
<td>label</td>
<td>Configures label control and policies.</td>
</tr>
<tr>
<td>local</td>
<td>Configures local label control and policies.</td>
</tr>
<tr>
<td>advertise</td>
<td>Configures outbound label advertisement control.</td>
</tr>
<tr>
<td>to peer-acl</td>
<td>(Optional) Specifies LDP peers for which explicit-null is advertised instead of implicit-null. Range is 1 to 99.</td>
</tr>
<tr>
<td>for prefix-acl</td>
<td>(Optional) Specifies prefixes for which explicit-null is advertised instead of implicit-null. Range is 1 to 99.</td>
</tr>
</tbody>
</table>

**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>Release 6.0</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.
<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 command shows how to advertise explicit null for all directly connected routes to all LDP peers:

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

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

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

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

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list peer_acl_10
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 10.1.1.1
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 10.2.2.2
RP/0/RP0/CPU0:router(config-ldp-af-lbl-lcl-advt)# 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-af-lbl-lcl-advt)# 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}]
no graceful-restart [{reconnect-timeout | forwarding-state-holdtime}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reconnect-timeout seconds</td>
<td>(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.</td>
</tr>
<tr>
<td>forwarding-state-holdtime seconds</td>
<td>(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.</td>
</tr>
</tbody>
</table>

**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>Release 6.0</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 (MPLS LDP) between two peers, enable LDP graceful restart on both label switch routers (LSRs).

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

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

**Note**

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

### Task ID

**Task ID Operations**

```plaintext
| mpls-ldp | read, write |
```

### Examples

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

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

```
RP/0/RP0/CPU0:router:Apr 3 10:56:05.392 : mpls_ldp[336]: %ROUTING-LDP-5-NBR_CHANGE : Nbr 2.2.2.2:0, DOWN
RP/0/RP0/CPU0:router:Apr 3 10:56:05.392 : mpls_ldp[336]: %ROUTING-LDP-5-NBRCHANGE : 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 8</td>
</tr>
<tr>
<td>2.2.2.2:0</td>
<td>N</td>
<td>00:01:02</td>
<td>2 5</td>
</tr>
</tbody>
</table>
```

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

Forwarding State Hold timer : Not Running
GR Neighbors : 1

<table>
<thead>
<tr>
<th>Neighbor ID</th>
<th>Up</th>
<th>Connect Count</th>
<th>Liveness Timer</th>
<th>Recovery Timer</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.3.3</td>
<td>Y</td>
<td>1</td>
<td>-</td>
<td>-</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
no session holdtime
```

**Syntax Description**

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

**Command Default**

`seconds`: 180

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

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

**Examples**

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

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

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

```
igp auto-config disable
no igp auto-config disable
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

MPLS LDP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</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 *Routing Configuration Guide for Cisco NCS 5000 Series Routers*.

**Task ID**

```
Task ID   Operations
mpls-ldp  read, write
```
i gp 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.

```plaintext
igp sync delay seconds
no igp sync delay
```

**Syntax Description**

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

**Command Default**

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

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</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:

```plaintext
RP/0/RP0/CP00:router# configure
RP/0/RP0/CP00:router(config)# mpls ldp
RP/0/RP0/CP00:router(config-ldp)# igp sync delay 30
```
igp sync delay on-proc-restart

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

`igp sync delay on-proc restart seconds`

`no igp sync delay on-proc restart seconds`

**Syntax Description**

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

**Command Default**

This command is disabled by default.

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</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, Global 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
**implicit-null-override**

To configure a router to advertise implicit null labels to a set of prefixes, for which a non-null label is to be advertised by default, use the `implicit-null-override` command in MPLS LDP label configuration mode. To return to the default behavior, use the `no` form of this command.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>address-family {ipv4 } label local implicit-null-override {for prefix-acl}</code></td>
<td>Specifies IP version 4 address family.</td>
</tr>
<tr>
<td><code>for prefix-acl</code></td>
<td>Specifies the usage of implicit-null label to a set of prefixes. Range is 1 to 99.</td>
</tr>
</tbody>
</table>

**Command Default**

Implicit null is advertised as default null label for routes, such as directly connected routes, whereas a non-null label is advertised for IGP, BGP, and static prefixes.

**Command Modes**

MPLS LDP label configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</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>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

The following command shows how to advertise implicit-null label to a specific LDP peer:

```
RP/0/RP0/CPU0:router(config)#mpls ldp
```
RP/0/RP0/CPU0:router(config-ldp)#address-family ipv4
RP/0/RP0/CPU0:router(config-ldp-af)#label
RP/0/RP0/CPU0:router(config-ldp-af-lbl)#locl
RP/0/RP0/CPU0:router(config-ldp-af-lbl-lcl)#implicit-null-override for 80
interface (MPLS LDP)

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

```
interface type interface-path-id
no interface type interface-path-id
```

**Syntax Description**

<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 a virtual interface.</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>Release 6.0</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.

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.

**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>
This example shows how to configure MPLS LDP over tenGigE interfaces:

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

```
address-family ipv4 label {local | remote} {accept from ip-address} {for prefix-acl}
no label accept for prefix-acl from ip-address
```

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

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

**Command Modes**
MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</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**
- 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)# mpls ldp
RP/0/RP0/CPU0:router(config-ldp)# address-family ipv4
RP/0/RP0/CPU0:router(config-ldp-af)# label
RP/0/RP0/CPU0:router(config-ldp-af-lbl)# remote
```
label accept

RP/0/RP0/CPU0:router(config-ldp-af-lbl-rmt)# accept from 13.13.13.0 for acl1
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.

```plaintext
address-family ipv4 label local advertise [disable | explicit-null | for prefix-acl [to prefix-acl]] interface type interface-path-id
no label advertise [{disable | for prefix-acl [to peer-acl]] interface type interface-path-id}]
```

### Syntax Description

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

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

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

### Command Default

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

### Command Modes

MPLS LDP configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</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 is 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 any peer.
  - 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.

<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 advertisement of all locally assigned labels to all peers:

```
RP/0/RP0/CPU0:router(config)# mpls ldp
RP/0/RP0/CPU0:router(config-ldp)# address-family ipv4
RP/0/RP0/CPU0:router(config-ldp-af)# label
RP/0/RP0/CPU0:router(config-ldp-af-lbl)# local
RP/0/RP0/CPU0:router(config-ldp-af-lbl-lcl)# advertise
RP/0/RP0/CPU0:router(config-ldp-af-lbl-lcl-advt)# disable
```

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

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

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

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.

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

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

```plaintext
RP/0/RP0/CPU0:router(config-ldp-af)# label local advertise
RP/0/RP0/CPU0:router(config-ldp-af-lbl-lcl-advt)# interface tenGigE 0/0/0/1
```
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.

```
address-family ipv4 label allocate for {prefix-acl | host-routes}
no label allocate
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>for</td>
<td>Specifies set of prefixes for which local label needs to be allocated.</td>
</tr>
<tr>
<td>prefix-acl</td>
<td>IP access-list name or number. Range is from 1 to 99.</td>
</tr>
<tr>
<td>host-routes</td>
<td>Allocates the label for host routes only.</td>
</tr>
</tbody>
</table>

**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>Release 6.0</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)# address-family ipv4
RP/0/RP0/CPU0:router(config-ldp-af)# label
RP/0/RP0/CPU0:router(config-ldp-af-lbl)# local
```
RP/O/RP0/CPU0:router(config-ldp0-af-lbl-lcl)# allocate for pfx_acl_1
The `log graceful-restart` command is used to set up notification describing graceful-restart (GR) session events. To enable this functionality, use the `log graceful-restart` command in MPLS LDP configuration mode. To return to the default behavior, use the `no log graceful-restart` command. This command has no arguments or keywords.

**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>Release 6.0</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.

A logging message is issued upon graceful restart session events.

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

```
log neighbor
no log neighbor
```

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

**Command Default**
No default behavior or values

**Command Modes**
MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</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.

**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
```
log session-protection

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

```
log session-protection
no log session-protection
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

MPLS LDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</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
```
**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>Release 6.0</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-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

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

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

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

```
neighbor ldp-id password {clear | disable | encrypted password }
no neighbor ldp-id password
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ldp-id</code></td>
<td>LDP ID of neighbor in A.B.C.D:0 format.</td>
</tr>
<tr>
<td><code>clear</code></td>
<td>Clears the password for the encryption parameter to specify that an unencrypted password will follow.</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>Disables the global password from the specified neighbor.</td>
</tr>
<tr>
<td><code>encrypted</code></td>
<td>Specifies that an encrypted password will follow.</td>
</tr>
<tr>
<td><code>password</code></td>
<td>(Clear text) Encrypted or unencrypted password string.</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>Release 6.0</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**

- `mpls-ldp` read, write
Examples

The following example shows how to configure the password `abc` for neighbor 10.20.20.20 and how to clear it:

```
RP/0/RP0/CPU0:router(config-ldp)#neighbor 10.20.20.20:0 password encrypted abc
RP/0/RP0/CPU0:router(config-ldp)#neighbor 10.20.20.20:0 password clear abc
```
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 {ipv4} neighbor Ip-address targeted
no address-family {ipv4} neighbor ip-address targeted
```

**Syntax Description**

- `ip-address`: Neighbor IP address.
- `ipv4`: Specifies IP version 4 address family.

**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>Release 6.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

Task ID: Operations

- mpls-ldp: read, write

**Examples**

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

```
RP/0/RP0/CPU0:router (config-ldp)# clear mpls ldp forwarding
RP/0/RP0/CPU0:router (config-ldp-af)# neighbor 200.1.1.1 targeted
```
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.

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>lsr-id</code></td>
<td>LSR ID in A.B.C.D format.</td>
</tr>
</tbody>
</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>Release 6.0</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.

**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 specify an LSR ID as the router ID:

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

To enable Open Shortest Path First (OSPF) LDP IGP synchronization for area interface, use the `router ospf` command in XR Config mode.

```
router ospf  process-id  [area  {area-id ip-address}]  [interface  type  interface-path-id]  mpls  ldp  sync
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process.</td>
</tr>
<tr>
<td>area</td>
<td>(Optional) Enters the OSPF area configuration submode.</td>
</tr>
<tr>
<td>area-id</td>
<td>Specifies the OSPF area ID as a decimal value.</td>
</tr>
<tr>
<td>ip-address</td>
<td>Specifies the OSPF area ID as an IP address in A.B.C.D format.</td>
</tr>
<tr>
<td>interface</td>
<td>(Optional) Enters the OSPF interface configuration submode.</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>
<tr>
<td>sync</td>
<td>Enables LDP IGP synchronization on the specified interface.</td>
</tr>
</tbody>
</table>

### 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>Release 6.0</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>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Example

The following example shows how to enable OSPF LDP IGP synchronization:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)#router ospf 109
RP/0/RP0/CPU0:router(config-ospf)# mpls ldp sync
```
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] [for peer-acl]
no session protection
```

**Syntax Description**

- **duration seconds** (Optional) Specifies the protection duration, that is, the number of seconds that targeted discovery should continue following the loss of link discovery to a neighbor. Range is 30 to 2147483.
- **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>Release 6.0</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**

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

**Examples**

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

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

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

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

**Syntax Description**

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

**Command Default**

No default behavior or values

**Command Modes**

XR EXEC mode

**Command History**

**Release** | **Modification**
---|---
Release 6.0 | This command was introduced.

**Usage Guidelines**

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

**Task ID**

- mpls-ldp read

**Examples**

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

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

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

Backoff Table: (2 entries)

<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>
The backoff table incorporates the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backoff Table</td>
<td>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:</td>
</tr>
<tr>
<td>LDP Id</td>
<td>Identifies the LDP neighbors.</td>
</tr>
<tr>
<td>Backoff (sec)</td>
<td>Specifies the time that the session setup is delayed.</td>
</tr>
<tr>
<td>Waiting (sec)</td>
<td>Specifies an approximate time the session setup has been delayed.</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 XR EXEC mode command.

```
show mpls ldp [afi-all] [ipv4] 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}] [all]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>afi-all</td>
<td>(Optional) Displays all address families.</td>
</tr>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IP version 4 address family.</td>
</tr>
<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>
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**

### Usage Guidelines

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

### 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 150.150.150.150/32:

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
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>
<tr>
<td>(rewrite)</td>
<td>Binding has been written into MPLS forwarding and is in use.</td>
</tr>
<tr>
<td>(no route)</td>
<td>Route is not valid. LDP times it out before the local binding is deleted.</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>
<tr>
<td>Revision No</td>
<td>Current revision number of LIB entries as well as the minimum revision number that has been advertised to all peers.</td>
</tr>
<tr>
<td>Local Bindings</td>
<td>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.</td>
</tr>
<tr>
<td>Remote Bindings</td>
<td>Number of remote bindings.</td>
</tr>
</tbody>
</table>

The following sample output shows the access-list advertisement:

```
RP/0/RP0/CPU0:router# show mpls ldp bindings advertisement-acls
Advertisement Spec:
  Prefix ACL = 'pfx_11'
  Prefix ACL = 'pfx_22'
  Prefix ACL = 'pfx_40_1'; Peer ACL = 'peer_11'
  5.41.0.0/16 , rev 82
  11.11.11.11/32 , rev 69
  Advert ACL(s): Prefix ACL 'pfx_11'
  20.20.20.20/32 , rev 83
  22.22.22.22/32 , rev 78
  Advert ACL(s): Prefix ACL 'pfx_22'
  40.1.1.0/24 , rev 79
  Advert ACL(s): Prefix ACL 'pfx_40_1'; Peer ACL 'peer_11'
```

This table describes the significant fields shown in the display.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertisement Spec</td>
<td>Lists all prefix and peer access-lists used as outbound label advertisement control.</td>
</tr>
<tr>
<td>Advert ACL(s)</td>
<td>Lists the first matching rule (if any) for the prefix entry for outbound label advertisement control (for prefix-acl).</td>
</tr>
</tbody>
</table>

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

```
RP/0/RP0/CPU0:router# show mpls ldp bindings brief
Prefix         | Local Advertised | Remote Bindings |
---------------|------------------|-----------------|
               | Label (peers)    | (peers)         |
---------------|------------------|-----------------|
1.1.2.2/32     | -                | 0               |
1.2.3.4/32     | 16010            | 396             |
4.4.4.4/32     | 16004            | 396             |
```
The following sample output shows that the binding matches with a local label:

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

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

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

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

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

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

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

To display the database capability information for an LDP session, use the `show mpls ldp capabilities` command in XR EXEC mode.

```
show mpls ldp capabilities [detail] location node-id
```

**Syntax Description**

- `detail`  
  (Optional) Displays detailed database capability information for an LDP session.

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

**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>Release 6.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

```
Task ID Operation
mpls-ldp read
```

**Example**

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

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

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x50b</td>
<td>Typed Wildcard FEC</td>
<td>LDP</td>
</tr>
<tr>
<td>0x3eff</td>
<td>Cisco IOS-XR</td>
<td>LDP</td>
</tr>
<tr>
<td>0x508</td>
<td>MP: Point-to-Multipoint (P2MP)</td>
<td>mLDP</td>
</tr>
<tr>
<td>0x509</td>
<td>MP: Multipoint-to-Multipoint (MP2MP)</td>
<td>mLDP</td>
</tr>
</tbody>
</table>
<pre><code>  |                        |       |
</code></pre>
```
## show mpls ldp discovery

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

```plaintext
show mpls ldp [afi-all] [{ipv4 }] discovery [{lsr-id ldp-id}] [{type interface-path-id | brief | link | targeted | summary [all]]} [detail] [{location node-id }]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>afi-all</code></td>
<td>(Optional) Displays all address families.</td>
</tr>
<tr>
<td><code>ipv4</code></td>
<td>(Optional) Specifies IP version 4 address family.</td>
</tr>
<tr>
<td><code>lsr-id</code></td>
<td>(Optional) Neighbor LSR ID in A.B.C.D format.</td>
</tr>
<tr>
<td><code>ldp-id</code></td>
<td>(Optional) Neighbor LDP ID in A.B.C.D: format.</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><code>brief</code></td>
<td>(Optional) Displays concise information about a specified LDP-enabled interface.</td>
</tr>
<tr>
<td><code>link</code></td>
<td>(Optional) Displays link information for LDP discovery.</td>
</tr>
<tr>
<td><code>targeted</code></td>
<td>(Optional) Displays targeted information for LDP discovery.</td>
</tr>
<tr>
<td><code>summary</code></td>
<td>(Optional) Displays summarized information for LDP discovery.</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.
**show mpls ldp discovery**

| all | (Optional) Displays the aggregate summary across LDP processes and all VRFs. |
| detail | (Optional) Displays detailed information (including, inbound label filtering, session KAs, and session protection state) for an LDP session. |
| location node-id | (Optional) Displays location information for the specified node ID. |

**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>Release 6.0</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.

**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:
    tenGigE 0/0/0/1 : 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>
</tbody>
</table>
Interfaces engaged in LDP discovery activity, as follows:

- **xmit field**
  - Indicates that the interface is transmitting LDP discovery hello packets.

- **recv field**
  - Indicates that the interface is receiving LDP discovery hello packets.

The LDP identifiers indicate the LDP neighbors discovered on the interface.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>Interfaces engaged in LDP discovery activity, as follows:</td>
</tr>
<tr>
<td>LDP Identifier</td>
<td>LDP identifier of the LDP peer.</td>
</tr>
<tr>
<td>Hold time</td>
<td>State of the forwarding hold timer and its current value.</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>
<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>
</tbody>
</table>
Summary of LDP discovery process.

**Hello xmit**
Number of local LDP discovery sources (including link and targeted hellos) emitting LDP hellos.

**Hello recv**
Number of discovered hello sources via link or targeted hello mechanics.

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

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

Local LDP Identifier: 1.2.34:0

<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>Te0/0/0/0</td>
<td>default</td>
<td>13.13.13.13:0</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: 1.2.3.4:0

<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>Te0/0/0/0</td>
<td>IPV4</td>
<td>default</td>
<td>13.13.13.13:0</td>
<td>15</td>
<td>Y</td>
</tr>
<tr>
<td>Te0/0/0/0.1</td>
<td>IPV4</td>
<td>default</td>
<td>13.13.13.13:0</td>
<td>15</td>
<td>Y</td>
</tr>
<tr>
<td>Te0/0/0/4</td>
<td>IPV4</td>
<td>default</td>
<td>8.8.8.8:0</td>
<td>15</td>
<td>Y</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 XR EXEC mode mode.

```
show mpls ldp [afi-all] [ipv4] 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]] [all]
```

**Syntax Description**

- `afi-all` (Optional) Displays all address families.
- `ipv4` (Optional) Specifies IP version 4 address family.
- `prefix` (Optional) Destination prefix, written in A.B.C.D format.
- `length` (Optional) Network mask length, in bits. Range is 0 to 32.
- `detail` (Optional) Displays detailed information on for the LDP timestamp that is used for the routing and forwarding update.
- `fast-reroute` (Optional) Displays the prefix that is LFA FRR protected in nature.
- `next-hop` Matches prefixes by next-hop IP address.
- `local-label label-value` (Optional) Displays the prefix with the specified local label. Range is from 0 to 1048575.
- `neighbor` Matches prefixes with a path through specified LDP neighbor.
- `unlabelled` Matches prefixes containing unlabelled paths.
- `location node-id` (Optional) Displays location information for the specified node ID.
- `summary` (Optional) Displays the summary information for the LDP forwarding information base (LFIB).
- `standby` (Optional) Displays standby-node specific information.
- `all` (Optional) Displays the aggregate summary across LDP processes and all VRFs.

**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>Release 6.0</td>
<td>This command was introduced.</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.
show mpls ldp forwarding

Examples

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

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

Codes:
- = GR label recovering, (!) = LFA FRR pure backup path
{} = Label stack with multi-line output for a routing path
G = GR, S = Stale, R = Remote LFA FRR backup

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Label</th>
<th>Label</th>
<th>Outgoing</th>
<th>Next Hop</th>
<th>GR</th>
<th>Stale</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>In</td>
<td>Out</td>
<td>Interface</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0.0.2/32</td>
<td>24001</td>
<td>ExpNull</td>
<td>Te0/0/0/2</td>
<td>5.0.0.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2.3.4/32</td>
<td>24000</td>
<td>ImpNull</td>
<td>Te0/0/0/1</td>
<td>12.1.1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.4.4.0/24</td>
<td>24052</td>
<td>24040</td>
<td>Te0/0/0/1</td>
<td>12.1.1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.5.5.5/32</td>
<td>24011</td>
<td>ImpNull</td>
<td>Te0/0/0/0</td>
<td>22.1.1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1.2.0/24</td>
<td>24010</td>
<td>24039</td>
<td>Te0/0/0/4</td>
<td>12.2.2.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>24038</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>24037</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>24036</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

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

Note

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 12.12.12.32 detail

Codes:
- = GR label recovering, (!) = LFA FRR pure backup path
{} = Label stack with multi-line output for a routing path
G = GR, S = Stale, R = Remote LFA FRR backup

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Label</th>
<th>Label</th>
<th>Outgoing</th>
<th>Next Hop</th>
<th>GR</th>
<th>Stale</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>In</td>
<td>Out</td>
<td>Interface</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0.0.2/32</td>
<td>24001</td>
<td>ExpNull</td>
<td>Te0/0/0/2</td>
<td>5.0.0.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2.3.4/32</td>
<td>24000</td>
<td>ImpNull</td>
<td>Te0/0/0/1</td>
<td>12.1.1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.4.4.0/24</td>
<td>24052</td>
<td>24040</td>
<td>Te0/0/0/1</td>
<td>12.1.1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.5.5.5/32</td>
<td>24011</td>
<td>ImpNull</td>
<td>Te0/0/0/0</td>
<td>22.1.1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1.2.0/24</td>
<td>24010</td>
<td>24039</td>
<td>Te0/0/0/4</td>
<td>12.2.2.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>24038</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>24037</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>24036</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
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 (8 backup, 8 FRR protected)
      Labelled: 16 (8 backup)
```

This table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix/mask</td>
<td>Prefix on the FEC(^2) for an MPLS forwarding entry.</td>
</tr>
</tbody>
</table>
### show mpls ldp forwarding

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<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 along with 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>Note</td>
<td>backup path and FRR are not supported in 6.0</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>
<tr>
<td>Note</td>
<td>backup path and FRR are not supported in 6.0</td>
</tr>
</tbody>
</table>

2 Forwarding Equivalence Class.
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 XR EXEC mode.

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>location node-id</td>
<td>(Optional) Displays location information for the specified node ID.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays detailed information about the specified VRF.</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>Release 6.0</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.

**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>
<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>
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 XR EXEC mode.

```
show mpls ldp [afi-all] [ipv4] igp sync [interface type interface-path-id] [brief] [location node-id]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>afi-all</td>
<td>(Optional) Displays all address families.</td>
</tr>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IP version 4 address family.</td>
</tr>
<tr>
<td>brief</td>
<td>(Optional) Displays brief information about a specified LDP-enabled interface.</td>
</tr>
<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>
</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
XR EXEC mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</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).

**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

TenGigE0/0/0/0:  VRF: 'default' (0x60000000)
     Sync delay: Disabled
     Sync status: Ready
```

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-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>
Graceful Restart.
show mpls ldp interface

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

```
show mpls ldp [afi-all] [{ipv4}] interface [{type interface-path-id | summary}] [brief] [{location node-id}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>afi-all</td>
<td>(Optional) Displays all address families.</td>
</tr>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IP version 4 address family.</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 <code>show interfaces</code> command to see a list of all possible interfaces currently configured on the router.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays summary information about a specified LDP-enabled interface.</td>
</tr>
<tr>
<td>brief</td>
<td>(Optional) Displays concise information about a specified LDP-enabled interface.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays detailed information about a specified LDP-enabled interface.</td>
</tr>
<tr>
<td>location node-id</td>
<td>(Optional) Displays location information for the specified node ID.</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>Release 6.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

No specific guidelines impact the use of this command.

### Task ID

```plaintext
Task ID Operations
mpls-ldp read
```
The following shows a sample output from the `show mpls ldp interface` command:

```
RP/0/RP0/CPU0:router# show mpls ldp interface
Interface TenGigE0/0/0/1 (0x8000040)
  VRF: 'default' (0x60000000)
  Enabled via config: LDP interface
Interface TenGigE0/0/0/1.10 (0x80009b8)
  VRF: 'default' (0x60000000)
  Enabled via config: LDP interface
Interface TenGigE0/0/0/1.11 (0x80009c0)
  VRF: 'default' (0x60000000)
  Enabled via config: LDP interface
Interface TenGigE0/0/0/1.12 (0x80009c8)
  VRF: 'default' (0x60000000)
RP/0/RP0/CPU0:router# show mpls ldp interface
Interface TenGigE0/0/0/0 (0x8000038)
  VRF: 'default' (0x60000000)
  Enabled via config: LDP interface
Interface TenGigE0/0/0/0.1 (0x80001c8)
  VRF: 'default' (0x60000000)
  Enabled via config: LDP interface
Interface TenGigE0/0/0/4 (0x8000058)
  VRF: 'default' (0x60000000)
  Enabled via config: LDP interface
```

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</td>
<td>Lists IGPs that specify an interface for MPLS LDP auto-configuration:</td>
</tr>
<tr>
<td>items</td>
<td>OSPF</td>
</tr>
<tr>
<td></td>
<td><code>ospf instance area</code></td>
</tr>
<tr>
<td></td>
<td>ISIS</td>
</tr>
<tr>
<td></td>
<td><code>isis instance</code></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 TenGigE0/0/0/1 (0x8000040)
  VRF: 'default' (0x60000000)
  Enabled via config: LDP interface
Interface TenGigE0/0/0/1.10 (0x80009b8)
  VRF: 'default' (0x60000000)
  Enabled via config: LDP interface
Interface TenGigE0/0/0/1.11 (0x80009c0)
  VRF: 'default' (0x60000000)
  Enabled via config: LDP interface
```

MPLS Command Reference for Cisco NCS 5000 Series Routers
show mpls ldp interface

Interface TenGigE0/0/0/1.12 (0x80009c8)
VRF: 'default' (0x60000000)
Enabled via config: LDP interface
show mpls ldp neighbor

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

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>(Optional) Neighbor IP address.</td>
</tr>
<tr>
<td><code>ldp-id</code></td>
<td>(Optional) Neighbor LDP ID in A.B.C.D: format.</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><code>brief</code></td>
<td>(Optional) Displays the existing LDP sessions in brief format.</td>
</tr>
<tr>
<td><code>capabilities</code></td>
<td>(Optional) Displays the neighbor capabilities information.</td>
</tr>
<tr>
<td><code>detail</code></td>
<td>(Optional) Displays detailed information (including, inbound label filtering, session KAs, and session protection state) for an LDP session.</td>
</tr>
<tr>
<td><code>gr</code></td>
<td>(Optional) Displays graceful restartable neighbors.</td>
</tr>
<tr>
<td><code>location node-id</code></td>
<td>(Optional) Displays location information for the specified node ID.</td>
</tr>
<tr>
<td><code>non-gr</code></td>
<td>(Optional) Displays non-graceful restartable neighbors.</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.

MPLS Command Reference for Cisco NCS 5000 Series Routers
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

Here is a sample output from the `show mpls ldp neighbor` command using an IP address:

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

Peer LDP Identifier: 12.12.12.12:0
TCP connection: 12.12.12.12:33432 - 5.5.5.5:646
Graceful Restart: No
Session Holdtime: 180 sec
State: Oper; Mags sent/rcvd: 1464/1479; Downstream-UNSolicited
Up time: 14:08:40
LDP Discovery Sources:
IPv4: (16)
  TenGigE0/0/0/1.15
  TenGigE0/0/0/1.11
  TenGigE0/0/0/1
  TenGigE0/0/0/1.13
  TenGigE0/0/0/1.3
  TenGigE0/0/0/1.7
  TenGigE0/0/0/1.14
  TenGigE0/0/0/1.6
  TenGigE0/0/0/1.2
  TenGigE0/0/0/1.10
  TenGigE0/0/0/1.4
  TenGigE0/0/0/1.5
  TenGigE0/0/0/1.16
  TenGigE0/0/0/1.8
  TenGigE0/0/0/1.9
  TenGigE0/0/0/1.12
IPv6: (0)
```
Addresses bound to this peer:

IPv4: (73)
4.4.4.1 10.64.98.26 12.12.12.12 20.20.20.1
21.21.21.2 27.27.27.27 43.43.43.1 53.53.53.1
55.55.55.1 59.1.0.2 63.63.63.1 66.66.66.1
69.1.0.2 73.73.73.1 77.77.77.77 79.1.0.2
81.81.81.1 83.83.83.1 89.1.0.2 90.1.0.2
91.1.0.2 92.1.0.2 93.1.0.2 93.93.93.1
94.1.0.2 95.1.0.2 96.1.0.2 97.1.0.2
98.1.0.2 99.1.0.2 100.1.0.2 101.1.0.2
102.1.0.2 103.1.0.2 103.103.103.1 104.1.0.2
105.1.0.2 106.1.0.2 107.1.0.2 108.1.0.2
109.1.0.2 110.1.0.2 111.1.0.2 112.1.0.2
113.1.0.2 113.113.113.1 114.1.0.2 115.1.0.2
116.1.0.2 117.123.123.1 117.133.133.1 117.143.143.1
153.153.153.1 163.163.163.1 173.173.173.1 181.181.181.1
183.183.183.1 184.184.184.1 185.185.185.1 186.186.186.1
187.187.187.1 188.188.188.1 189.189.189.1 190.190.190.1
191.191.191.1 193.193.193.1 194.194.194.1 195.195.195.1
196.196.196.1 197.197.197.1 198.198.198.1 199.199.199.1
203.203.203.1

IPv6: (0)

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

Peer LDP Identifier: 12.12.12.12:0
TCP connection: 12.12.12.12:33432 - 5.5.5.5:646
Graceful Restart: No
Session Holdtime: 180 sec
State: Oper; Msgs sent/rcvd: 1464/1479; Downstream-Unsolicited
Up time: 14:08:49
LDP Discovery Sources:
IPv4: (16)
TenGigE0/0/0/1.15
TenGigE0/0/0/0/1.11
TenGigE0/0/0/0/1.13
TenGigE0/0/0/0/1.3
TenGigE0/0/0/0/1.7
TenGigE0/0/0/0/1.14
TenGigE0/0/0/0/1.6
TenGigE0/0/0/0/1.2
TenGigE0/0/0/0/1.10
TenGigE0/0/0/0/1.4
TenGigE0/0/0/0/1.5
TenGigE0/0/0/0/1.16
TenGigE0/0/0/0/1.8
TenGigE0/0/0/0/1.9
TenGigE0/0/0/0/1.12
IPv6: (0)
Addresses bound to this peer:
IPv4: (73)
4.4.4.1 10.64.98.26 12.12.12.12 20.20.20.1
21.21.21.2 27.27.27.27 43.43.43.1 53.53.53.1
55.55.55.1 59.1.0.2 63.63.63.1 66.66.66.1
69.1.0.2 73.73.73.1 77.77.77.77 79.1.0.2
81.81.81.1 83.83.83.1 89.1.0.2 90.1.0.2
91.1.0.2 92.1.0.2 93.1.0.2 93.93.93.1
94.1.0.2 95.1.0.2 96.1.0.2 97.1.0.2
98.1.0.2 99.1.0.2 100.1.0.2 101.1.0.2
102.1.0.2 103.1.0.2 103.103.103.1 104.1.0.2
105.1.0.2 106.1.0.2 107.1.0.2 108.1.0.2
109.1.0.2 110.1.0.2 111.1.0.2 112.1.0.2
113.1.0.2 113.113.113.1 114.1.0.2 115.1.0.2
116.1.0.2 117.123.123.1 117.133.133.1 117.143.143.1
153.153.153.1 163.163.163.1 173.173.173.1 181.181.181.1
183.183.183.1 184.184.184.1 185.185.185.1 186.186.186.1
187.187.187.1 188.188.188.1 189.189.189.1 190.190.190.1
191.191.191.1 193.193.193.1 194.194.194.1 195.195.195.1
196.196.196.1 197.197.197.1 198.198.198.1 199.199.199.1
203.203.203.1

IPv6: (0)
show mpls ldp neighbor

Peer LDP Identifier: 8.8.8.8:0
TCP connection: 8.8.8.8:42784 - 1.2.3.4:646
Graceful Restart: No
Session Holdtime: 180 sec
State: Oper; Msgs sent/rcvd: 1276/1250; Downstream-Unsolicited
Up time: 15:37:39
LDP Discovery Sources:
IPv4: (1)
TenGigE0/0/0/4
IPv6: (0)
Addresses bound to this peer:
IPv4: (9)
5.0.0.2 8.8.8.8 10.1.0.1 10.64.98.28
12.1.1.2 41.41.41.41 77.77.77.77 167.167.167.167
IPv6: (0)

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

show mpls ldp neighbor non-gr

Peer LDP Identifier: 13.13.13.13:0
TCP connection: 13.13.13.13:63262 - 1.2.3.4:646
Graceful Restart: No
Session Holdtime: 180 sec
State: Oper; Msgs sent/rcvd: 1322/1361; Downstream-Unsolicited
Up time: 15:38:02
LDP Discovery Sources:
IPv4: (1)
TenGigE0/0/0/0
IPv6: (0)
Addresses bound to this peer:
IPv4: (24)
1.1.1.1 4.4.4.4 10.1.0.2 10.1.1.2
10.1.2.2 10.1.3.2 10.1.4.2 10.1.5.2
10.1.6.2 10.1.7.2 10.64.98.27 11.10.9.8
13.13.13.13 18.0.0.1 33.33.33.33 79.0.0.2
79.1.0.2 79.2.0.2 79.3.0.2 79.4.0.2
79.5.0.2 100.100.100.100 178.0.0.2 201.201.201.201
IPv6: (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>Peer LDP Identifier</td>
<td>LDP identifier of the neighbor (peer) for this session.</td>
</tr>
</tbody>
</table>
TCP connection used to support the LDP session, shown in the following format:

- neighbor IP address
- peer port
- local IP address
- local port

Graceful-restart status (Y or N). Graceful Restart State of the LDP session. Generally this is Oper (operational), but transient is another possible state.

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.

The length of time that this session has been up for (in hh:mm:ss format).

The source(s) of LDP discovery activity leading to the establishment of the LDP session.

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.

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 ipv4  Discovery ipv6  Addresses ipv4  Addresses ipv6  Labels ipv4  Labels ipv6
------- --- -- ------- -------- -------- -------- ------ ------ ------- ------ ------- ------
4.4.4.4:0  Y  N     1d00h    1      0      0      0      1      0      5      0
46.46.46.2:0  N  N     1d00h    1      1      3      3      5      5
46.46.46.46:0  Y  N     1d00h    2      2      4      4      5      5
6.6.6.1:0    Y  N   23:25:50    0      1      0      2      0      5
```

This table describes the significant fields shown in the display.

Table 12: show mpls ldp neighbor brief Command Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer</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>
</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

eer LDP Identifier: 12.12.12:0
TCP connection: 12.12.12.12:33432 - 5.5.5.5:646
Graceful Restart: No
Session Holdtime: 180 sec
State: Oper; Msgs sent/rcvd: 1465/1481; Downstream-Unsolicited
Up time: 14:10:17
LDP Discovery Sources:
IPv4: (16)
  TenGigE0/0/0/1.15
  TenGigE0/0/0/1.11
  TenGigE0/0/0/1.13
  TenGigE0/0/0/1.1
  TenGigE0/0/0/1.3
  TenGigE0/0/0/1.7
  TenGigE0/0/0/1.14
  TenGigE0/0/0/1.6
  TenGigE0/0/0/1.12
  TenGigE0/0/0/1.10
  TenGigE0/0/0/1.4
  TenGigE0/0/0/1.5
  TenGigE0/0/0/1.16
  TenGigE0/0/0/1.8
  TenGigE0/0/0/1.9
  TenGigE0/0/0/1.12
IPv4: (0)
Addresses bound to this peer:
IPv4: (73)
  4.4.4.1 10.64.98.26 12.12.12.12 20.20.20.1
  21.21.21.2 27.27.27.27 43.43.43.1 53.53.53.1
  55.55.55.1 59.1.0.2 63.63.63.1 66.66.66.1
  69.1.0.2 73.73.73.1 77.77.77.77 79.1.0.2
  81.81.81.1 83.83.83.1 89.1.0.2 90.1.0.2
  91.1.0.2 92.1.0.2 93.1.0.2 93.93.93.1
  94.1.0.2 95.1.0.2 96.1.0.2 97.1.0.2
  98.1.0.2 99.1.0.2 100.1.0.2 101.1.0.2
  102.1.0.2 103.1.0.2 103.103.103.1 104.1.0.2
  105.1.0.2 106.1.0.2 107.1.0.2 108.1.0.2
  109.1.0.2 110.1.0.2 111.1.0.2 112.1.0.2
  113.1.0.2 113.113.113.1 114.1.0.2 115.1.0.2
  116.1.0.2 123.123.123.1 133.133.133.1 143.143.143.1
  153.153.153.1 163.163.163.1 173.173.173.1 181.181.181.1
  183.183.183.1 184.184.184.1 185.185.185.1 186.186.186.1
  187.187.187.1 188.188.188.1 189.189.189.1 190.190.190.1
  191.191.191.1 193.193.193.1 194.194.194.1 195.195.195.1
  196.196.196.1 197.197.197.1 198.198.198.1 199.199.199.1
IPV6: (0)
Addresses bound to this peer:
IPv4: (73)
```

### Field | Description
---|---
Discovery | Number of LDP discovery sources corresponding to the neighbor.
Address | Number of addresses bound to this peer.
show mpls ldp neighbor
detail

Peer LDP Identifier: 8.8.8.8:0
TCP connection: 8.8.8.8:42784 - 1.2.3.4:646
Graceful Restart: No
Session Holdtime: 180 sec
State: Oper; Mags sent/rcvd: 1280/1254; Downstream-Unsolicited
Up time: 15:41:06
LDP Discovery Sources:
IPv4: (1)
TenGigE0/0/0/4
IPv6: (0)
Addresses bound to this peer:
IPv4: (9)
5.0.0.2 8.8.8.8 10.1.0.1 10.64.98.28
12.1.1.2 41.41.41.41 77.77.77.77 167.167.167.167
IPv6: (0)
Peer holdtime: 180 sec; KA interval: 60 sec; Peer state: Estab
NSR: Disabled
Capabilities:
Sent:
0x508 (MP: Point-to-Multipoint (P2MP))
0x509 (MP: Multipoint-to-Multipoint (MP2MP))
0x50b (Typed Wildcard FEC)
Received:
0x508 (MP: Point-to-Multipoint (P2MP))
0x509 (MP: Multipoint-to-Multipoint (MP2MP))
0x50b (Typed Wildcard FEC)

This table describes the significant fields shown in the display.

Table 13: show mpls ldp neighbor detail 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>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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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 \textit{hh:mm:ss} 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:</td>
</tr>
<tr>
<td></td>
<td>\textbf{Incomplete} \hspace{1cm} Targeted discovery requested but not yet up.</td>
</tr>
<tr>
<td></td>
<td>\textbf{Ready} \hspace{1cm} Targeted discovery and at least one link hello adjacency to the peer are up.</td>
</tr>
<tr>
<td></td>
<td>\textbf{Protecting} \hspace{1cm} 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 &quot;protecting&quot; state, time to keep LDP peer session up without receipt of LDP protocol message from a peer.</td>
</tr>
</tbody>
</table>
show mpls ldp parameters

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>location node-id</td>
<td>(Optional) Displays location information for the specified node ID.</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>Release 6.0</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**

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

**Examples**

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

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

LDP Parameters:
  Protocol Version: 1
  Router ID: 10.11.11.11
  Null Label: Implicit
  Session:
    Hold time: 180 sec
    Keepalive interval: 60 sec
    Backoff: Initial:15 sec, Maximum:120 sec
  Discovery:
    Link Hellos: Holdtime:15 sec, Interval:5 sec
    Targeted Hellos: Holdtime:90 sec, Interval:10 sec
    (Accepting peer ACL 'peer_acl_10')
  Graceful Restart:
    Enabled (Configured)
    Reconnect Timeout:120 sec, Forwarding State Holdtime:180 sec
  Timeouts:
    Binding with no-route: 300 sec
    LDP application recovery (with LSD): 360 sec
  OOR state
    Memory: Normal
```
This table describes the significant fields shown in the display.

**Table 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>
</tbody>
</table>
| Discovery Targeted Hellos | Indicates the time:  
  • To remember that a neighbor platform wants an LDP session when the neighbor platform is not directly connected to the router or the neighbor platform has not sent an LDP hello message. This intervening interval is known as hold time.  
  • Interval between the transmission of consecutive hello messages to a neighbor not directly connected to the router and if targeted hellos are being accepted, displaying peer-acl (if any). |
| Graceful Restart       | Status of graceful-restart status (Y or N).                                |
| Timeouts               | Various timeouts (of interest) that the LDP is using. One timeout is binding no route, which indicates how long the LDP waits for an invalid route before deleting it. It also shows restart recovery time for LSD and LDP. |
| OOR state              | Out of resource memory state: Normal, Major, or Critical.                  |
show mpls ldp statistics fwd-setup

To display the statistics of the forwarding setup counters related to RIB/LSD, use the `show mpls ldp statistics fwd-setup` command in XR EXEC mode.

```
show mpls ldp statistics fwd-setup [{location node-id}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>node-id</td>
<td>(Optional) Displays location information for the specified node ID.</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>Release 6.0</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>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read</td>
</tr>
</tbody>
</table>

**Example**

The following shows a sample output from the `show mpls ldp statistics fwd-setup` command:

```
RP/0/RP0/CPU0:router# show mpls ldp statistics fwd-setup
RIB
---
Thread counters:
  Events In : 10
  Events Out : 39
  RIB fetch throttled : 0 (0 during last throttle)
TC Thread counters:
  Events In : 39 (3 skipped)
  Events Out : 12 (0 failed, 2 skipped)
Address Family: IPv4
  RIB server connects: 1
  RIB converged: Yes
Op counters:
  Fetch : 4 (2 buffers per fetch)
    no-data: 0
    callbacks: 33 routes, 3 convg, 0 rcmd
  Route Up : 33 (0 protected; Paths: 29/0/0 total/backups/protected)
```
Route Down : 0
Route Filtered : 5 (0 intern, 5 misc, 0 alloc, 0 admin,
0 unsupp-intf 0, unsupp-protection,
0 bgp, 0 bgp-unlabelled, 0 ibgp-no-lbl-ucast)

MFI

Thread counters:
Events In : 9
Events Out : 8
LSD Rsrc-Complete : 1
LSD server connects : 1

Op counters:

<table>
<thead>
<tr>
<th></th>
<th>Successful</th>
<th>Failed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>RCMMD Markers</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>State cleanup</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Interface Enable</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>Interface Disable</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Label alloc</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>Label alloc - mldp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Label free</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Label free - mldp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rewrite create</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>Rewrite delete</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Label/Rewrite create</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Label/Rewrite delete</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Label OOR cleared</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Total LSD Reqs/Msgs</td>
<td>7</td>
<td>0</td>
</tr>
</tbody>
</table>

LSD flow control status:
Flow control : 0
Flow control cnt : 0
Evt queue cnt : 0
Last flow control : N/A
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 XR EXEC mode.

```
show mpls ldp statistics msg-counters [{lsr-id ldp-id}] [{location node-id}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>lsr-id</code></td>
<td>(Optional) LSR ID of neighbor in A.B.C.D format.</td>
</tr>
<tr>
<td><code>ldp-id</code></td>
<td>(Optional) LDP ID of neighbor in A.B.C.D: format.</td>
</tr>
<tr>
<td><code>location node-id</code></td>
<td>(Optional) Displays location information for the specified node ID.</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>Release 6.0</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.

**Task ID**
```
Task ID Operations
mpls-ldp read
```

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

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

Peer LDP Identifier: 13.13.13.13:0

Sent Rcvd
------- -------
Initialization 1 1
Address 15 46
Address-Withdraw 14 25
Label-Mapping 28 498
Label-Withdraw 14 439
Label-Release 439 14
Label-Request 0 0
Label-Abort-Request 0 0
Notification 0 0
```
The below table describes the significant fields shown in the display.

*Table 15: show mpls ldp statistics msg-counters 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).</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>
show mpls ldp summary

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

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

**Syntax Description**
- `location node-id`: (Optional) Displays location information for the specified node ID.
- `all`: (Optional) Displays the aggregate summary across LDP processes and all VRFs.

**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>Release 6.0</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
Addresses : 3
Interfaces : 4 (1 forward reference, 2 LDP configured)
Collaborators:

<table>
<thead>
<tr>
<th>Connected</th>
<th>Registered</th>
</tr>
</thead>
<tbody>
<tr>
<td>SysDB</td>
<td>Y</td>
</tr>
<tr>
<td>IM</td>
<td>Y</td>
</tr>
<tr>
<td>RSI</td>
<td>-</td>
</tr>
<tr>
<td>IP-ARM</td>
<td>-</td>
</tr>
<tr>
<td>IPv4-RIB</td>
<td>Y</td>
</tr>
<tr>
<td>LSD</td>
<td>Y</td>
</tr>
<tr>
<td>LDP-NSR-Partner</td>
<td>Y</td>
</tr>
<tr>
<td>L2VPN-ATOM</td>
<td>-</td>
</tr>
<tr>
<td>mLDP</td>
<td>-</td>
</tr>
</tbody>
</table>

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>
show mpls ldp trace

To display the Label Distribution Protocol (LDP) VRF event traces, use the **show mpls ldp trace** command in XR EXEC mode.

```
show mpls ldp trace
[binding] [capabilities] [config] [dev] [discovery] [error] [file file-name]
[forwarding] [gr] [hexdump] [iccp] [igp-sync] [interface] [last]
[location {node-id name all mgmt-nodes}] [misc] [mldp] [nsr] [peer] [process]
[reverse] [route] [since] [stats] [tailf] [unique] [usec]
[verbose] [wide] [wrapping]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>binding</td>
<td>(Optional) Displays the binding event traces.</td>
</tr>
<tr>
<td>capabilities</td>
<td>(Optional) Displays the capabilities event traces.</td>
</tr>
<tr>
<td>config</td>
<td>(Optional) Displays the configuration event traces.</td>
</tr>
<tr>
<td>dev</td>
<td>(Optional) Displays the development private traces.</td>
</tr>
<tr>
<td>discovery</td>
<td>(Optional) Displays Hello or discovery and adj event traces.</td>
</tr>
<tr>
<td>error</td>
<td>(Optional) Displays error traces.</td>
</tr>
<tr>
<td>file file-name</td>
<td>(Optional) Displays trace of a specific file.</td>
</tr>
<tr>
<td>forwarding</td>
<td>(Optional) Displays forwarding event traces.</td>
</tr>
<tr>
<td>gr</td>
<td>(Optional) Displays graceful-restart event traces.</td>
</tr>
<tr>
<td>hexdump</td>
<td>(Optional) Displays traces in hexadecimal.</td>
</tr>
<tr>
<td>iccp</td>
<td>(Optional) Displays ICCP signaling event traces.</td>
</tr>
<tr>
<td>igp-sync</td>
<td>(Optional) Displays IGP sync event traces.</td>
</tr>
<tr>
<td>interface</td>
<td>(Optional) Displays interface event traces.</td>
</tr>
<tr>
<td>last</td>
<td>(Optional) Displays last number of entries.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>location</code></td>
<td>Identifies the location of the card whose CPU controller trace information you want to display.</td>
</tr>
<tr>
<td><code>node-id</code></td>
<td>The node-id argument is expressed in the <strong>rack/slot/module</strong> notation.</td>
</tr>
<tr>
<td><code>name</code></td>
<td>Specifies the name of the card.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Specifies all locations.</td>
</tr>
<tr>
<td><code>mgmt-nodes</code></td>
<td>Specifies all managements nodes.</td>
</tr>
<tr>
<td><code>misc</code></td>
<td>Displays miscellaneous event traces.</td>
</tr>
<tr>
<td><code>mldp</code></td>
<td>Displays MLDP event traces.</td>
</tr>
<tr>
<td><code>nsr</code></td>
<td>Displays non-stop routing event traces.</td>
</tr>
<tr>
<td><code>peer</code></td>
<td>Displays peer session event traces.</td>
</tr>
<tr>
<td><code>process</code></td>
<td>Displays process-level event traces.</td>
</tr>
<tr>
<td><code>pw</code></td>
<td>Displays L2VPN pseudo-wire event traces.</td>
</tr>
<tr>
<td><code>reverse</code></td>
<td>Displays latest traces first.</td>
</tr>
<tr>
<td><code>route</code></td>
<td>Displays route event traces.</td>
</tr>
<tr>
<td><code>since last-start</code></td>
<td>Displays traces since the last start time.</td>
</tr>
<tr>
<td><code>stats</code></td>
<td>Displays statistics.</td>
</tr>
<tr>
<td><code>tailf</code></td>
<td>Displays new traces as they are added.</td>
</tr>
<tr>
<td><code>unique</code></td>
<td>Displays unique entries with count.</td>
</tr>
<tr>
<td><code>usec</code></td>
<td>Displays timestamp w/usec detail.</td>
</tr>
<tr>
<td><code>verbose</code></td>
<td>Displays internal debugging information.</td>
</tr>
</tbody>
</table>
### Command Default

| Command Default | No default behavior or values |

### Command Modes

| Command Modes | XR EXEC mode |

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

| 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-ldp</td>
<td>read</td>
</tr>
</tbody>
</table>

### Example

The following example shows how to display the LDP event traces:

```
RP/0/RP0/CPU0:router# show mpls ldp trace
Dec 12 17:14:58.193 mpls/ldp/proc 0/RP0/CPU0 t7049 [PROC]:117: **** PROCESS MPLS-LDP STARTED ****
Dec 12 17:14:58.193 mpls/ldp/proc 0/RP0/CPU0 t7049 [PROC]:1061: Thread 'ldp_main' started
Dec 12 17:14:58.194 mpls/ldp/proc 0/RP0/CPU0 t7049 [PROC]:368: Init done for module 'Os'
Dec 12 17:14:58.206 mpls/ldp/proc 0/RP0/CPU0 t7049 [PROC]:368: Init done for module 'Dbg'
Dec 12 17:14:58.212 mpls/ldp/proc 0/RP0/CPU0 t7049 [PROC]:368: Init done for module 'Global'
Dec 12 17:14:58.213 mpls/ldp/proc 0/RP0/CPU0 t7049 [PROC]:368: Init done for module 'TDP'
Dec 12 17:14:58.213 mpls/ldp/misc 0/RP0/CPU0 t7049 [MISC]:293: s_ldp_chkpt_lib_initied=0
Dec 12 17:14:58.213 mpls/ldp/proc 0/RP0/CPU0 t7049 [PROC]:46: Thread 'ldp_hello_tx' started
Dec 12 17:14:58.244 mpls/ldp/proc 0/RP0/CPU0 t7049 [PROC]:368: Init done for module 'Chkpt'
Dec 12 17:14:58.245 mpls/ldp/proc 0/RP0/CPU0 t7049 [PROC]:368: Init done for module 'Gsp'
Dec 12 17:14:58.245 mpls/ldp/proc 0/RP0/CPU0 t7049 [PROC]:368: Init done for module 'IO EVM'
Dec 12 17:14:58.248 mpls/ldp/config 0/RP0/CPU0 t7049 [CFG]:151: sr_cfg_pre_init DONE
Dec 12 17:14:58.248 mpls/ldp/proc 0/RP0/CPU0 t7049 [PROC]:368: Init done for module 'Cfg Pre-Init'
Dec 12 17:14:58.253 mpls/ldp/config 0/RP0/CPU0 t7049 [INTF]:685: im_attr_owner_init: DONE
Dec 12 17:14:58.253 mpls/ldp/proc 0/RP0/CPU0 t7049 [PROC]:368: Init done for module 'IM Attr Pre-Init'
Dec 12 17:14:58.253 mpls/ldp/proc 0/RP0/CPU0 t7049 [PROC]:368: Init done for module 'UDP-xport Pre-Init'
Dec 12 17:14:58.253 mpls/ldp/proc 0/RP0/CPU0 t7271 [PROC]:227: Thread 'ldp_im_attr_nfy' started
Dec 12 17:14:58.254 mpls/ldp/proc 0/RP0/CPU0 t7049 [PROC]:368: Init done for module 'TCP-xport Pre-Init'
Dec 12 17:14:58.256 mpls/ldp/proc 0/RP0/CPU0 t7049 [PROC]:3792: TAGCON started
Dec 12 17:14:58.256 mpls/ldp/proc 0/RP0/CPU0 t7049 [PROC]:368: Init done for module 'TC Init'
```
Dec 12 17:14:58.277 mpls/ldp/proc 0/RP0/CPU0 t7049 [PROC]:368: Init done for module 'LDP mLDP Pre-Init'
**show lcc**

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>Specifies IP version 4 address prefixes.</td>
</tr>
<tr>
<td>unicast</td>
<td>Specifies unicast address prefixes.</td>
</tr>
<tr>
<td>all</td>
<td>Scans all routes.</td>
</tr>
<tr>
<td>label</td>
<td>Scans all labels.</td>
</tr>
<tr>
<td>tunnel-interface</td>
<td>Specifies the interface of a tunnel.</td>
</tr>
<tr>
<td>statistics</td>
<td>Displays route consistency check statistics information.</td>
</tr>
<tr>
<td>scan-id</td>
<td>Specifies the value of scan-id. Range is from 0 to 10000.</td>
</tr>
<tr>
<td>summary</td>
<td>Displays background route consistency check statistics summary information.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

IPv4 address family configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</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>IPv4</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

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

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

Sending scan initiation request to IPv4 LSD ... done
Waiting for scan to complete (max time 600 seconds)........................
Scan Completed
Collecting scan results from FIBs (max time 30 seconds)... done
Number of nodes involved in the scan: 1
Number of nodes replying to the scan: 1
```
Legend:
? - Currently Inactive Node, ! - Non-standard SVD Role
* - Node did not reply

Node Checks Performed Errors
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>Release 6.0</td>
<td>This command was introduced.</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.

**Task ID**

- `mpls-ldp` read, write

**Examples**

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

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

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

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

**Syntax Description**

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

**Command Default**

LDP does not send SNMP traps.

**Command Modes**

XR Config mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</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**

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

**Examples**

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

```bash
RP/0/RP0/CPU0:router(config)# snmp-server traps mpls ldp up
```
**address-family ipv4 label**

To configure label control and policies on a specific IPv4 destination, use the `address-family ipv4 label` command in the MPLS LDP configuration mode.

```
address-family {ipv4 }
label [remote accept from ldp-id for prefix-acl]
local [default-route] [allocate for {prefix-acl | host-routes}]
[ advertise [to ldp-id for prefix-acl]
 [interface type interface-path-id ]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family</td>
<td>Configure address-family and its parameters.</td>
</tr>
<tr>
<td>ipv4</td>
<td>Specifies IP version 4 address family.</td>
</tr>
<tr>
<td>label</td>
<td>(Optional) Configure label control and policies.</td>
</tr>
<tr>
<td>remote</td>
<td>(Optional) Configure remote/peer label control and policies.</td>
</tr>
<tr>
<td>accept</td>
<td>(Optional) Configure inbound label acceptance control.</td>
</tr>
<tr>
<td>from ldp-id</td>
<td>Specifies which LDP neighbors will receive label advertisements. LDP ID is written in A.B.C.D: format.</td>
</tr>
<tr>
<td>for prefix-acl</td>
<td>Specifies prefix destinations for which labels will be advertised.</td>
</tr>
<tr>
<td>local</td>
<td>(Optional) Configure local label control and policies.</td>
</tr>
<tr>
<td>default-route</td>
<td>(Optional) Enable MPLS forwarding for default route.</td>
</tr>
<tr>
<td>allocate</td>
<td>(Optional) Configure label allocation control.</td>
</tr>
<tr>
<td>for prefix-acl</td>
<td>Specifies prefix destinations for which labels will be allocated.</td>
</tr>
<tr>
<td>host-routes</td>
<td>Allocates labels for host routes only.</td>
</tr>
<tr>
<td>advertise</td>
<td>(Optional) Configure outbound label advertisement control.</td>
</tr>
</tbody>
</table>
to ldp-id

(Optional) Specifies which LDP neighbors will receive label advertisements. LDP ID is written in A.B.C.D: format.

for prefix-acl

(Optional) Specifies prefix destinations for which labels will be advertised.

interface

(Optional) Advertise interface host address.

type

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

interface-path-id

Physical interface or a virtual interface.

Note

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

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

Command Default

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>Release 6.0</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>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-ldp</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Example

The following example shows how to configure label control and policies on a specific IPv4 destination:
address-family ipv4 label
address-family ipv4 label
MPLS Static Commands

This module describes the commands used to configure static MPLS labels in a Multiprotocol Label Switching (MPLS) network on the.

For detailed information about MPLS concepts, configuration tasks, and examples, see *MPLS Configuration Guide for Cisco NCS 5000 Series Routers*.

- address family ipv4 unicast (mpls-static), on page 100
- clear mpls static local-label discrepancy, on page 102
- interface (mpls-static), on page 103
- show mpls static local-label, on page 104
- show mpls static summary, on page 105
address family ipv4 unicast (mpls-static)

To enable static MPLS label binding on a specific IPv4 unicast destination address prefix and on the forwarding next-hop address, use the `address-family ipv4 unicast` command in MPLS static configuration mode. To remove MPLS static binding, use the `no` form of this command.

```
address-family ipv4 unicast local-label label_value allocate [per-prefix ipv4_prefix_value] forward path path_value nexthop nexthop_information interface-type interface-path-id out-label {label_value | pop | exp-null}
no address-family ipv4 unicast
```

**Syntax Description**

- `local-label label_value`: Specifies MPLS local-label value for static binding and forwarding. The range is from 16 to 1048575.
- `allocate`: Displays local-label allocation options.
- `per-prefix ipv4_prefix_value`: Specifies IPv4 prefix value to which the specified MPLS label will be statically bound.
- `forward`: Configure forwarding for traffic with static MPLS label.
- `path path_value`: Specifies path-ID for MPLS cross-connect path.
- `nexthop nexthop_information`: Specifies the next-hop information that is either an IP address or interface.
- `interface-type interface-id`: Interface type. For more information, use the question mark (?) online help function.
- `out-label label_value`: Specifies mpls local-label value for static binding on the egress packet.
- `pop`: Removes label from egress packet.
- `exp-null`: Applies explicit null label on the egress packet.

**Command Default**

None

**Command Modes**

MPLS static configuration

**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>

**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-static</td>
<td>read</td>
</tr>
</tbody>
</table>
Example

The following command sequence shows how to specify local label for an ip-prefix and define LSP.

RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#mpls static
RP/0/RP0/CPU0:router(config-mpls-static)#address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-mpls-static-af)#local-label 30500 allocate per-prefix 10.1.1.1/24
  forward path 1 nexthop 12.2.2.2 out-label 30600
clear mpls static local-label discrepancy

To clear any discrepancy between statically allocated and dynamically allocated local labels, use the **clear mpls static local-label discrepancy** command in XR EXEC mode. A label discrepancy is generated when:

- A static label is configured for an IP prefix (per VRF) that already has a binding with a dynamic label.
- A static label is configured for an IP prefix, when the same label value is dynamically allocated to another IP prefix.

### clear mpls static local-label discrepancy {label-value | all}

#### Syntax Description

- **label-value** A value that denotes the label for which the discrepancies need to be cleared.
- **all** Specifies that all discrepancies need to be cleared.

#### Command Default

None

#### Command Modes

XR EXEC mode

#### 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

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-static</td>
<td>read</td>
</tr>
</tbody>
</table>

RP/0/RP0/CPU0:router#clear mpls static local-label discrepancy all
interface (mpls-static)

To enable MPLS encapsulation on specified interfaces, use the `interface` command in MPLS static configuration mode. To disable MPLS encapsulation on specified interfaces, use the `no` form of the command.

```
interface interface-type interface-id
no interface interface-type interface-id
```

### Syntax Description

- `interface-type`: Interface type. For more information, use the question mark (?) online help function.
- `interface-path-id`: Physical interface instance.

### Command Default

None

### Command Modes

MPLS static 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

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-static</td>
<td>read and write</td>
</tr>
</tbody>
</table>

### Example

The following command sequence shows how to enable MPLS encapsulation on a TenGigE port.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls static
RP/0/RP0/CPU0:router(config-mpls-static)# interface TenGigE 0/0/0/1
```
show mpls static local-label

To display information about local labels allocated using mpls static command, use the show mpls static local-label command in XR EXEC mode.

```
show mpls static local-label {label-value | all [detail] | discrepancy [detail] | error [detail]}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>local-label label-value</td>
<td>Specifies local label value to display MPLS static information for only that label.</td>
</tr>
<tr>
<td>all</td>
<td>Displays MPLS static information about all local labels.</td>
</tr>
<tr>
<td>discrepancy</td>
<td>Displays label discrepancy between static labels and dynamic labels.</td>
</tr>
<tr>
<td>error</td>
<td>Displays MPLS static labeling errors.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Detailed information is displayed.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

XR EXEC mode

**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**

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-static</td>
<td>read</td>
</tr>
</tbody>
</table>

The following command sequence shows how to view label discrepancy information:

```
RP/0/RP0/CPU0:router#show mpls static local-label discrepancy detail
Tue Apr 22 18:20:47.183 UTC
Label VRF Type Prefix RW Configured Status
------- --------------- ------------ ---------------- --------------- --------
16003 default Per-Prefix 1.1.1.1/32 No Discrepancy

STATUS : Label has discrepancy
```

The following command sequence shows how to view MPLS static information for all local labels:

```
RP/0/RP0/CPU0:router#show mpls static local-label all
Tue Apr 22 18:21:41.813 UTC
Label VRF Type Prefix RW Configured Status
------- --------------- ------------ ---------------- --------------- --------
200 default Per-Prefix 10.10.10.32 Yes Created
16003 default Per-Prefix 1.1.1.1/32 No Discrepancy
```
To display MPLS static summary information, use the `show mpls static summary` command in XR EXEC mode.

### Syntax Description
- **summary** Displays MPLS static binding information.

### Command Default
None

### Command Modes
XR EXEC mode

### Command History
- **Release** 6.0 This command was introduced.

### Usage Guidelines
No specific guidelines impact the use of this command.

### Task ID
- **Task ID** mpls-static
- **Operation** read

This is the sample output for `show mpls static summary` command:

```
RP/0/RP0/CPU0:router#show mpls static summary
Tue Apr 22 18:22:17.931 UTC
Label : Total 2 Errored 0 Discrepancies 1
VRF : Total 1 Active 1
Interface : Total 7 Enabled 1 Forward-Reference 0
LSD : CONNECTED
IM : CONNECTED
RSI : CONNECTED
```
show mpls static summary
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 5000 Series Routers*.

- clear mpls forwarding counters, on page 108
- mpls label range, on page 109
- show mpls ea interfaces, on page 111
- show mpls forwarding, on page 112
- show mpls forwarding exact-route, on page 117
- show mpls forwarding labels, on page 121
- show mpls forwarding summary, on page 122
- show mpls interfaces, on page 125
- show mpls label range, on page 128
- show mpls label table, on page 129
- show mpls lsd applications, on page 131
- show mpls lsd clients, on page 133
- show mpls lsd forwarding labels, on page 135
- show mpls lsd forwarding summary, on page 136
clear mpls forwarding counters

To clear (set to zero) the MPLS forwarding counters, use the `clear mpls forwarding counters` command in XR EXEC mode.

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

### 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>Release 6.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

### 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-static</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Example:
This a test.

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

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

<table>
<thead>
<tr>
<th>Local</th>
<th>Outgoing</th>
<th>Prefix</th>
<th>Outgoing</th>
<th>Next Hop</th>
<th>Bytes</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Label or ID</td>
<td>Interface</td>
<td>Switched</td>
<td>O</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>-----------</td>
<td>----------</td>
<td>-----</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Exp-Null-v4 33.33.33.33/32</td>
<td>PO0/2/0/0</td>
<td>10.1.2.3</td>
<td>17000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Local</th>
<th>Outgoing</th>
<th>Prefix</th>
<th>Outgoing</th>
<th>Next Hop</th>
<th>Bytes</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Label or ID</td>
<td>Interface</td>
<td>Switched</td>
<td>O</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>-----------</td>
<td>----------</td>
<td>-----</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Exp-Null-v4 33.33.33.33/32</td>
<td>PO0/2/0/0</td>
<td>10.1.2.3</td>
<td>16762</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
mpls label range

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

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

**Syntax Description**

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

**Command Default**

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

**Command Modes**

- XR Config mode

**Command History**

- **Release 6.0**  This command was introduced.

**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.

The maximum allowed label limit is 1000000 when ASR 9000 Enhanced Ethernet Line Card is used.

**Note**

- Labels outside the current range and which are allocated by MPLS applications remain in circulation until released.
- The maximum labels that are available are 144K.
- You must understand the maximum labels that are supported for each platform versus the labels that are supported for the CLI.
Task ID | Task ID | Operations
--------|---------|-------------
mpls-ldp | read, write

Examples

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

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

To display the interface label security information, use the `show mpls ea interfaces` command in XR EXEC mode.

```
show mpls ea interface [location node-id]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>location node-id</code></td>
</tr>
</tbody>
</table>

Displays the interfaces on which MPLS is enabled.

**Command Modes**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The keywords and arguments described allow display of the interface label security 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>
<tr>
<td>mpls-static</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following sample output is from the `show mpls ea interfaces` command and specific interface and location:

```
RP/0/RP0/CPU0:router# show mpls ea interfaces location 0/1/CPU0
Interface IFH MTU Flags Type
------------- --------- ------ ----- ------
Te0/0/0/1    0x08000040 1500   -------  -------  -------
Te0/0/0/1.2  0x08001d90 1500   -------  -------  -------
Te0/0/0/1.3  0x08001d98 1500   -------  -------  -------
Te0/0/0/1.4  0x08001da0 1500   -------  -------  -------
Te0/0/0/1.5  0x08001da8 1500   -------  -------  -------
Te0/0/0/1.6  0x08001db0 1500   -------  -------  -------
Te0/0/0/1.7  0x08001db8 1500   -------  -------  -------
Te0/0/0/1.8  0x08001dc0 1500   -------  -------  -------
Te0/0/0/1.9  0x08001dc8 1500   -------  -------  -------
Te0/0/0/1.10 0x08001dd0 1500   -------  -------  -------
Te0/0/0/1.11 0x08001dd8 1500   -------  -------  -------
Te0/0/0/1.12 0x08001de0 1500   -------  -------  -------
Te0/0/0/1.13 0x08001de8 1500   -------  -------  -------
Te0/0/0/1.14 0x08001df0 1500   -------  -------  -------
Te0/0/0/1.15 0x08001df8 1500   -------  -------  -------
Te0/0/0/1.16 0x08001e00 1500   -------  -------  -------
```
show mpls forwarding

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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>detail</code></td>
<td>(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).</td>
</tr>
<tr>
<td><code>hardware</code></td>
<td>(Optional) Displays the hardware location entry.</td>
</tr>
<tr>
<td><code>ingress</code></td>
<td>(Optional) Reads information from the ingress PSE.</td>
</tr>
<tr>
<td><code>egress</code></td>
<td>(Optional) Reads information from the egress PSE.</td>
</tr>
<tr>
<td><code>interface</code></td>
<td>(Optional) Displays information for 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 a virtual interface.</td>
</tr>
<tr>
<td><code>labels low-value</code></td>
<td>(Optional) Entries with a local labels range. Ranges for both low-value and high-value are 0 to 1048575.</td>
</tr>
<tr>
<td><code>location node-id</code></td>
<td>(Optional) Displays hardware resource counters on the designated node.</td>
</tr>
<tr>
<td><code>p2mp</code></td>
<td>(Optional) Displays only P2MP LSPs.</td>
</tr>
<tr>
<td><code>Note</code></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>Note</code></td>
<td>For more information about the syntax for the router, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>local</code></td>
<td>(Optional) Displays only P2MP LSP MPLS output paths that are local to a line card.</td>
</tr>
<tr>
<td><code>unresolved</code></td>
<td>(Optional) Displays P2MP LSPs that have failures. For example, one or more MPLS output paths are unresolved or have platform failures.</td>
</tr>
<tr>
<td><code>leafs</code></td>
<td>(Optional) Displays P2MP LSPs that have failures on the leaf such as platform failures.</td>
</tr>
<tr>
<td><code>prefix network/mask</code></td>
<td>(Optional) Displays the destination address and mask/prefix length.</td>
</tr>
<tr>
<td><code>Note</code></td>
<td>The forward slash (/) between <code>network</code> and <code>mask</code> is required.</td>
</tr>
<tr>
<td><code>Note</code></td>
<td>This will be supported in a future release of Cisco IOS XR software.</td>
</tr>
</tbody>
</table>
### Command Modes

XR EXEC mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</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.

**Note**
This router does not support label accounting for vrf labels. Instead, it supports accounting for the IGP and LDP labels. As a result, the Bytes Switched counter is 0 for the `show mpls forwarding vrf` command.

**Note**
Even if there are multiple outgoing paths the `show mpls forwarding detail` command shows the stats in the first path only as Cisco NCS 5000 Series Router supports only one stat per local label. The statistics are counted at the ingress when a labeled packet enters.

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-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:

```
RP/0/RP0/CPU0:router# show mpls forwarding
```
The following sample output shows detailed information for the LSP:

```
RP/0/RP0/CPU0:router# show mpls forwarding prefix 3.3.3.1/32 detail

Local Outgoing Prefix Outgoing Next Hop Bytes
Label Label or ID Interface Switched
------- ----------- ------------------ ------------ --------------- ------------
24035 24027 3.3.3.1/32 BE241 191.4.1.2 371356

Updated: Nov 29 12:30:14.671
Version: 42, Priority: 3
Label Stack (Top -> Bottom): { 24027 }
NHID: 0x0, Encap-ID: N/A, Path idx: 0, Backup path idx: 0, Weight: 0
MAC/Encaps: 14/18, MTU: 8986
Packets Switched: 4883

24027 3.3.3.1/32 BE242 191.4.1.26

Updated: Nov 29 12:30:14.671
Version: 42, Priority: 3
Label Stack (Top -> Bottom): { 24027 }
NHID: 0x0, Encap-ID: N/A, Path idx: 1, Backup path idx: 0, Weight: 0
MAC/Encaps: 14/18, MTU: 9086
Packets Switched: 0

24027 3.3.3.1/32 BE243 191.4.1.50

Updated: Nov 29 12:30:14.671
Version: 42, Priority: 3
Label Stack (Top -> Bottom): { 24027 }
NHID: 0x0, Encap-ID: N/A, Path idx: 2, Backup path idx: 0, Weight: 0
MAC/Encaps: 14/18, MTU: 9086
Packets Switched: 0

24027 3.3.3.1/32 BE241.1 191.4.1.6

Updated: Nov 29 12:30:14.671
Version: 42, Priority: 3
Label Stack (Top -> Bottom): { 24027 }
NHID: 0x0, Encap-ID: N/A, Path idx: 3, Backup path idx: 0, Weight: 0
MAC/Encaps: 18/22, MTU: 8986
Packets Switched: 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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Bytes Switched</td>
<td>Number of bytes switched with this incoming label.</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 XR EXEC mode.

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

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>label label-number</td>
<td>Displays the Label Number. Range is 0 to 1048575.</td>
</tr>
</tbody>
</table>
| bottom-label | Displays the bottom label value. Range is 0 to 1048575.  
**Note**  
bottom-label is not required for packets with single label. |
| 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.  
**Note**  
This will be supported in a future release of Cisco IOS XR software. |
| detail | (Optional) Displays detailed information. |
| protocol protocol | (Optional) Displays the specified protocol for the route.  
**Note**  
protocol is not used for load balancing. |
| 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-based tunnel selection (PBTS)**

The `policy-class value` command 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.

**Note**

This will be supported in a future release of Cisco IOS XR software.

**Hardware Location Entry**

The `hardware` command displays the hardware location entry.

**Ingress PSE**

The `ingress` command reads information from the ingress PSE.

**Egress PSE**

The `egress` command reads information from the egress PSE.

---

**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>Release 6.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Note**

**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-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 24001
```
The table below shows the significant fields displayed in the output:

<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 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 ‘*’ 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^5 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 LFIB^6 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>
</tbody>
</table>

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

1. **Label** assigned by this router.
2. **Outgoing Label**: Label assigned by the next hop or downstream peer. Some of the entries in this column are:
   - **Unlabeled**: No label for the destination from the next hop, or label switching is not enabled on the outgoing interface.
   - **Pop Label**: Next hop advertised an implicit-null label for the destination.
3. **Prefix or Tunnel ID**: Address or tunnel to which packets with this label are going.
4. **Outgoing Interface**: Interface through which packets with this label are sent.
5. **Next Hop**: IP address of neighbor that assigned the outgoing label.
6. **Bytes Switched**: Number of bytes switched with this incoming label.
7. **TO**: Timeout: Indicated by an “*” if entry is being timed out in forwarding.
8. **MAC/Encaps**: Length in bytes of Layer 2 header, and length in bytes of packet encapsulation, including Layer 2 header and label header.
9. **MTU**: MTU^5 of labeled packet.
10. **Label Stack**: All the outgoing labels on the forwarded packet.
11. **Packets Switched**: Number of packets switched with this incoming label.
12. **Label switching**: Number of Label switching LFIB^6 forwarding entries.
13. **IPv4 label imposition**: Number of IPv4 label imposition forwarding entries (installed at ingress LSR).
14. **MPLS TE tunnel head**: Number of forwarding entries (installed at ingress LSR) on MPLS TE tunnel head.
15. **MPLS TE fast-reroute**: Number of forwarding entries (installed at PLR) for MPLS-TE fast reroute.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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.
show mpls forwarding labels

To display the contents of the MPLS label information, use the show mpls forwarding labels command in XR EXEC mode.

show mpls forwarding [labels low-value high-value ][detail] [rpf]

Syntax Description

<table>
<thead>
<tr>
<th>labels low-value high-value</th>
<th>(Optional) Entries with a local labels range. Ranges for low-value is 0 and high-value is 0 1048575.</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>(Optional) Displays label RPF information.</td>
</tr>
<tr>
<td>rpf</td>
<td>(Optional)</td>
</tr>
</tbody>
</table>

Note: This will be supported in a future release of Cisco IOS XR software.

Command Modes

XR EXEC mode

Command History

Release 6.0 This command was introduced.

Usage Guidelines

The optional keywords and arguments described allow display of MPLS label security and RPF 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>
<tr>
<td>mpls-static</td>
<td>read</td>
</tr>
</tbody>
</table>

Examples

The following sample output is from the show mpls forwarding labels command using the rpf:

```
RP/0/RP0/CPU0:router# show mpls forwarding labels 24035
Local  Outgoing Prefix  Outgoing Interface  Next Hop   Switched
------- -------- -------- -------- ------------ ---------------
24035  24027  3.3.3.1/32  BE241  191.4.1.2  371896
24027  3.3.3.1/32  BE242  191.4.1.26  0
24027  3.3.3.1/32  BE243  191.4.1.50  0
24027  3.3.3.1/32  BE241.1 191.4.1.6  0
24027  3.3.3.1/32  BE242.1 191.4.1.30  0
24027  3.3.3.1/32  BE243.1 191.4.1.54  0
24027  3.3.3.1/32  Te0/0/0/79  191.4.1.74  0
24027  3.3.3.1/32  Te0/0/0/79.1 191.4.1.78  0
```
show mpls forwarding summary

To display the summary of the MPLS label table, use the `show mpls forwarding summary` command in XR EXEC mode.

`show mpls forwarding summary [debug] [location node-id] no-counters private rpf`

**Syntax Description**

- **debug** (Optional) Displays the information for internal debugging in the command output.
- **location node-id** (Optional) Displays the interfaces on which MPLS is enabled.
- **no-counters** (Optional) Skips displaying counters.
- **private** (Optional) Displays private information.
- **rpf** (Optional) Displays label RPF information.

**Command Modes**

XR EXEC mode

**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**

The optional keywords and arguments described allow display of an MPLS label security information.

**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 sample output is from the `show mpls forwarding summary` command:

```
RP/0/RP0/CPU0:router# show mpls forwarding summary
Forwarding entries:
  Label switching: 1123, protected: 0
  MPLS TE tunnel head: 0, protected: 0
  MPLS TE midpoint: 0, protected: 0
  MPLS TE internal: 0, protected: 0
  MPLS P2MP TE tunnel head: 0
  MPLS P2MP TE tunnel midpoint/tail: 0
  MPLS P2MP MLDP tunnel head: 0
  MPLS P2MP MLDP tunnel midpoint/tail: 0
Forwarding updates:
  messages: 22
  p2p updates: 50
Labels in use:
  Reserved: 4
```
The following sample output is from the `show mpls forwarding summary` command using the **debug** keyword:

```
RP/0/RP0/CPU0:router# show mpls forwarding summary debug
Forwarding entries:
  Label switching: 0, protected: 0
  MPLS TE tunnel head: 0, protected: 0
  MPLS TE midpoint: 0, protected: 0
  MPLS TE internal: 0, protected: 0
  MPLS P2MP TE tunnel head: 0
  MPLS P2MP TE tunnel midpoint/tail: 0
  MPLS P2MP MLDP tunnel head: 0
  MPLS P2MP MLDP tunnel midpoint/tail: 0
Forwarding updates:
  messages: 2
    p2p updates: 4
Labels in use:
  Reserved: 4
  Lowest: 0
  Highest: 13
  Deleted stale label entries: 0
Pkts dropped: 0
Pkts fragmented: 0
Failed lookups: 0
```

The following sample output is from the `show mpls forwarding summary` command using the **no-counters**:

```
RP/0/RP0/CPU0:router# show mpls forwarding summary no-counters
Forwarding entries:
  Label switching: 0, protected: 0
  MPLS TE tunnel head: 0, protected: 0
  MPLS TE midpoint: 0, protected: 0
  MPLS TE internal: 0, protected: 0
  MPLS P2MP TE tunnel head: 0
  MPLS P2MP TE tunnel midpoint/tail: 0
  MPLS P2MP MLDP tunnel head: 0
  MPLS P2MP MLDP tunnel midpoint/tail: 0
Forwarding updates:
  messages: 2
    p2p updates: 4
Labels in use:
  Reserved: 4
  Lowest: 0
  Highest: 13
  Deleted stale label entries: 0
```

The following sample output is from the `show mpls forwarding summary` command using the **private**:
show mpls forwarding summary

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

Forwarding entries:
  Label switching: 0, protected: 0
  MPLS TE tunnel head: 0, protected: 0
  MPLS TE midpoint: 0, protected: 0
  MPLS TE internal: 0, protected: 0
  MPLS P2MP TE tunnel head: 0
  MPLS P2MP TE tunnel midpoint/tail: 0
  MPLS P2MP MLDP tunnel head: 0
  MPLS P2MP MLDP tunnel midpoint/tail: 0

Forwarding updates:
  messages: 2
  p2p updates: 4

Labels in use:
  Reserved: 4
  Lowest: 0
  Highest: 13
  Deleted stale label entries: 0

Path count:
  Unicast: 0

Pkts dropped: 0
Pkts fragmented: 0
Failed lookups: 0
fwd-flags: 0x5, ttl-expire-pop-cnt: 0

This table describes the significant fields shown in the display.

Table 19: show mpls forwarding summary Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label switching</td>
<td>Number of Label switching Label Forwarding Information Base (LFIB) forwarding entries.</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>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>
show mpls interfaces

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

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

**Syntax Description**

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

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

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

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

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

- **detail** (Optional) Displays detailed information for the designated node.

**Command Default**

No default behavior or values

**Command Modes**

XR EXEC mode

**Command History**

- **Release** Modification

  Release 6.0  This command was introduced.

**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-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

<table>
<thead>
<tr>
<th>Interface</th>
<th>LDP</th>
<th>Tunnel</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bundle-Ether241</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```
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 Bundle-Ether241:
  LDP labelling enabled
  LSP labelling not enabled
  MPLS enabled

Interface Bundle-Ether242:
  LDP labelling enabled
  LSP labelling not enabled
  MPLS enabled

Interface Bundle-Ether243:
  LDP labelling enabled
  LSP labelling not enabled
  MPLS enabled

Interface TenGigE0/0/0/4:
  LDP labelling enabled
  LSP labelling not enabled
  MPLS enabled

Interface Bundle-Ether341:
  LDP labelling enabled
  LSP labelling not enabled
  MPLS enabled

Interface Bundle-Ether344:
  LDP labelling enabled
  LSP labelling not enabled
  MPLS enabled

Interface Bundle-Ether345:
  LDP labelling not enabled
  LSP labelling not enabled
  MPLS ISIS enabled
  MPLS enabled

Interface Bundle-Ether451:
  LDP labelling enabled
  LSP labelling not enabled
  MPLS enabled

Interface Bundle-Ether452:
  LDP labelling enabled
  LSP labelling not enabled
  MPLS enabled

Interface Bundle-Ether461:
  LDP labelling enabled
  LSP labelling not enabled
  MPLS enabled

Interface Bundle-Ether462:
  LDP labelling enabled
  LSP labelling not enabled
  MPLS enabled

Interface Bundle-Ether463:
  LDP labelling enabled
  LSP labelling not enabled
  MPLS enabled

Interface TenGigE0/0/0/27:
  LDP labelling enabled
  LSP labelling not enabled
  MPLS enabled
```
This table describes the significant fields in the sample display.

**Table 20: 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>MTU</td>
<td>MTU² of labeled packet.</td>
</tr>
<tr>
<td>Caps</td>
<td>Capsulation switching chains installed on an interface.</td>
</tr>
<tr>
<td>M</td>
<td>MPLS switching encapsulation/switching chains are installed on the interface and are ready to switch MPLS traffic.</td>
</tr>
<tr>
<td>Static</td>
<td>MTU = Maximum Transmission Unit.</td>
</tr>
</tbody>
</table>

² 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 XR EXEC mode.

**show mpls label range**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>This command has no arguments or keywords.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Default</td>
<td>No default behavior or values</td>
</tr>
<tr>
<td>Command Modes</td>
<td>XR EXEC mode</td>
</tr>
<tr>
<td>Command History</td>
<td><strong>Release</strong></td>
</tr>
<tr>
<td></td>
<td>6.0</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.

<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 21: 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 table**

To display the local labels contained in the MPLS label table, use the `show mpls label table` command in XR 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**

XR EXEC mode

**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**

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

**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-static</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

 Table   Label  Owner  State  Rewrite
------- ------ ------ -------- -------
   0      0    LSD(A) InUse Yes
   0      1    LSD(A) InUse Yes
```
This table describes the significant fields shown in the display.

Table 22: 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>
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 XR EXEC mode.

```
show mpls lsd applications [application application]
```

**Syntax Description**

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

**Command Default**
No default behavior or values

**Command Modes**
XR EXEC mode

**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**

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 133 command), but not all clients are applications.

**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-static</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

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

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

Application     State Recovery Time Location
---------------- ----------- ----------------- -----------
LSD(A)           Active 0/0 (0)  0/RP0/CPU0
OSPF(A):ospf-george Active 0/0 (30) 0/RP0/CPU0
OSPF(A):ospf-1     Active 0/0 (30) 0/RP0/CPU0
Static(A)         Active 0/0 (120) 0/RP0/CPU0
LDP(A)            Active 0/0 (15)  0/RP0/CPU0
PIM(A):pim        Active 0/0 (300) 0/RP0/CPU0
PIM6(A):pim6      Active 0/0 (300) 0/RP0/CPU0
L2VPN(A)          Active 0/0 (1800) 0/RP0/CPU0
```
This table describes the significant fields shown in the display.

**Table 23: 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 re-registered 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>
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 XR EXEC mode.

Syntax Description
This command has no arguments or keywords.

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>6.0</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

ID Services Location
-------------- ------------
0  LSD(A) 0/RP0/CPU0
1  OSPF:ospf-ospf-sr(A) 0/RP0/CPU0
2  OSPF:ospf-ospf-v4(A) 0/RP0/CPU0
3  OSPF:ospf-core(A) 0/RP0/CPU0
4  ISIS:isis-v4(A) 0/RP0/CPU0
5  ISIS:core(A) 0/RP0/CPU0
6  ISIS:isis-sr(A) 0/RP0/CPU0
7  Static(A) 0/RP0/CPU0
8  LDP(A) 0/RP0/CPU0
9  LDPV4(A) 0/RP0/CPU0
10 BGP-VPNv4:bgp-default(A) 0/RP0/CPU0
```
The following table describes the significant fields shown in the display.

*Table 24: 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>Location</td>
<td></td>
</tr>
</tbody>
</table>
show mpls lsd forwarding labels

To display the LSD label RPF information, use the **show mpls lsd forwarding labels** command in XR EXEC mode.

```
show mpls lsd forwarding [labels low-value high-value ] [location node-id]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>labels low-value high-value</th>
<th>(Optional) Entries with a local labels range. Ranges for both low-value and high-value are 0 to 1048575.</th>
</tr>
</thead>
<tbody>
<tr>
<td>location node-id</td>
<td>Displays hardware resource counters on the designated node.</td>
</tr>
</tbody>
</table>

**Command Modes**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The optional keywords and arguments described allow display of an MPLS label security 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>
<tr>
<td>mpls-static</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following sample output is from the **show mpls lsd forwarding labels** command using a specific location:

```
RP/0/RP0/CPU0:router# show mpls lsd forwarding labels 24035
In Label, (ID), Path Info: <Type>
24035, (IPv4, 'default':4U, 3.3.3.1/32), 8 Paths
  1/8: IPv4, 'default':4U, BE241, nh=191.4.1.2, lbl=24027, flags=0x0, ext_flags=0x0
  2/8: IPv4, 'default':4U, BE242, nh=191.4.1.16, lbl=24027, flags=0x0, ext_flags=0x0
  3/8: IPv4, 'default':4U, BE243, nh=191.4.1.50, lbl=24027, flags=0x0, ext_flags=0x0
  4/8: IPv4, 'default':4U, BE241.1, nh=191.4.1.6, lbl=24027, flags=0x0, ext_flags=0x0
  5/8: IPv4, 'default':4U, BE242.1, nh=191.4.1.30, lbl=24027, flags=0x0, ext_flags=0x0
  6/8: IPv4, 'default':4U, BE243.1, nh=191.4.1.54, lbl=24027, flags=0x0, ext_flags=0x0
  7/8: IPv4, 'default':4U, Te0/0/0/79, nh=191.4.1.74, lbl=24027, flags=0x0, ext_flags=0x0
  8/8: IPv4, 'default':4U, Te0/0/0/79.1, nh=191.4.1.78, lbl=24027, flags=0x0, ext_flags=0x0
```
show mpls lsd forwarding summary

To display the LSD label information, use the **show mpls lsd forwarding summary** command in XR EXEC mode.

```
show mpls lsd forwarding summary  [location  node-id]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Location node-id</th>
<th>Displays hardware resource counters on the designated node.</th>
</tr>
</thead>
</table>

**Command Modes**

XR EXEC mode

**Command History**

**Release 6.0** This command was introduced.

**Usage Guidelines**

The optional keywords and arguments described allow display of the interface label security information.

**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 sample output is from the **show mpls lsd forwarding summary** command:

```
RP/0/RP0/CPU0:router# show mpls lsd forwarding summary
Messages: 813
Forwarding updates: 17889
Rewrites: 322
FPFs:
  Label: 322
  IPv4: 284
  IPv6: 0
  TE: 0
  PW List: 0
  DMTC Ext_intf: 0
MOIs: 1644
  IPv4 paths: 1640 (0 backup, 0 protected)
  IPv6 paths: 0 (0 backup, 0 protected)
  Pop-and_lookup IPv4 paths: 3
  Pop-and_lookup IPv6 paths: 1
  TEv4: 0
  Pseudo-wire: 0
  IP subscriber: 0
  DMTC Ext_intf: 0
RPF Nbrs:
  IPv4 Neighbors: 0
  IPv6 Neighbors: 0
  Total RWs with RPF Neighbors: 0
```
show mpls lsd forwarding summary
show mpls lsd forwarding summary
RSVP Infrastructure Commands

This module describes the commands used 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 5000 Series Routers.

Disable or Enable RSVP Message Checksum

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:

```bash
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.

- authentication (RSVP), on page 141
- clear rsvp authentication, on page 143
- clear rsvp counters all, on page 145
- clear rsvp counters authentication, on page 146
- clear rsvp counters chkpt, on page 148
- clear rsvp counters events, on page 149
- clear rsvp counters messages, on page 150
• clear rsvp counters oor, on page 151
• clear rsvp counters prefix-filtering, on page 152
• key-source key-chain (RSVP), on page 154
• life-time (RSVP), on page 156
• rsvp, on page 158
• rsvp interface, on page 159
• rsvp neighbor, on page 161
• show rsvp request, on page 162
• show rsvp authentication, on page 164
• show rsvp counters, on page 169
• show rsvp counters oor, on page 172
• show rsvp counters prefix-filtering, on page 174
• show rsvp fast-reroute, on page 177
• show rsvp graceful-restart, on page 179
• show rsvp hello instance, on page 182
• show rsvp hello instance interface-based, on page 184
• show rsvp interface, on page 186
• show rsvp neighbor, on page 187
• show rsvp reservation, on page 188
• show rsvp sender, on page 191
• show rsvp session, on page 194
• signalling dscp (RSVP), on page 197
• signalling graceful-restart, on page 199
• signalling hello graceful-restart interface-based, on page 201
• signalling hello graceful-restart refresh interval, on page 202
• signalling prefix-filtering access-list, on page 204
• signalling prefix-filtering default-deny-action, on page 205
• signalling rate-limit, on page 206
• signalling refresh interval, on page 208
• signalling refresh missed, on page 210
• window-size (RSVP), on page 211
• signalling refresh reduction summary, on page 213
• signalling refresh reduction reliable, on page 214
• signalling refresh reduction disable, on page 217
• signalling refresh reduction bundle-max-size, on page 218
authentication (RSVP)

To enter RSVP authentication mode, use the `authentication` command in global configuration mode, RSVP interface configuration mode, or RSVP neighbor XR Config 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**

- XR Config mode
- RSVP interface configuration
- RSVP neighbor configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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 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 authentication configuration mode from global configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp authentication
RP/0/RP0/CPU0:router(config-rsvp-auth)#
```

The following example shows how to activate the RSVP on an interface and enter RSVP authentication configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface HundredGigE 0/0/0/3
RP/0/RP0/CPU0:router(config-rsvp-if)# authentication
RP/0/RP0/CPU0:router(config-rsvp-if-auth)#
```

The following example shows how to configure the RSVP neighbor with IP address 1.1.1.1 and enter neighbor authentication configuration mode:
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp neighbor 1.1.1.1 authentication
RP/0/RP0/CPU0:router(config-rsvp-nbor-auth)#
clear rsvp authentication

To eliminate RSVP security association (SA) before the lifetime expires, use the **clear rsvp authentication** command in XR EXEC mode.

**clear rsvp authentication**  [**type**  *interface-path-id*]  [**destination**  *IP address* ]  [**source**  *IP address*]

**Syntax Description**

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

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

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

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

**destination IP address**  
(Optional) Eliminates the RSVP security associations (SA) before their lifetimes expire. All SAs with this destination IP address are cleared.

**source IP address**  
(Optional) Eliminates the RSVP security associations (SA) before their lifetimes expire. All SAs with this source IP address are cleared.

**Command Default**
No default behavior or values

**Command Modes**
XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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>Operations 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 interface:

RP/0/RP0/CPU0:router# clear rsvp authentication HundredGigE 0/0/0/3

The following example shows how to clear each SA on the interface, destination address 1.1.1.1, and source address 2.2.2.2:

RP/0/RP0/CPU0:router# clear rsvp authentication HundredGigE 0/0/0/3 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 XR EXEC mode.

Syntax Description

clear rsvp counters all [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>
<tr>
<td>Note</td>
<td>Use the show interfaces 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.

Command Modes

XR EXEC mode

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.2.1</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 clear all message and event counters:

```
RP/0/RP0/CPU0:router# clear rsvp counters all
```
To eliminate RSVP counters for each security association (SA), use the `clear rsvp counters authentication` command in XR EXEC mode.

```plaintext
clear rsvp counters authentication [type interface-path-id] [destination IP address ] [source IP address ]
```

**Syntax Description**

- **type** (Optional) Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id** Physical interface or a virtual interface.
- **destination IP address** (Optional) Eliminates authentication-related statistics for each security association (SA) with this destination IP address.
- **source IP address** (Optional) Eliminates authentication-related statistics for each security association (SA) with this source IP address.

**Command Default**
No default behavior or values

**Command Modes**
XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Examples**
The following example shows how to clear authentication counters for each SA:

```
RP/0/RP0/CP00: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/CP00:router# clear rsvp counters authentication destination 1.1.1.1
```
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:

clear rsvp counters authentication source 2.2.2.2

The following example shows how to clear authentication counters for each SA with an interface.

clear rsvp counters authentication HundredGigE 0/0/0/3

The following example shows how to clear authentication counters for each SA on an interface, destination address 1.1.1.1, and source address 2.2.2.2:

clear rsvp counters authentication HundredGigE 0/0/0/3 destination 1.1.1.1 source 2.2.2.2
clear rsvp counters chkpt

To clear RSVP checkpoint counters, use the `clear rsvp counters chkpt` command in XR EXEC mode.

**clear rsvp counters chkpt**

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

**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>6.2.1</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 ID</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
```
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 XR EXEC mode.

**clear rsvp counters events [type interface-path-id]**

**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>
</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**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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 ID</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
```
To clear (set to zero) all RSVP message counters that are being maintained by the router, use the `clear rsvp counters messages` command in XR EXEC mode.

```
clear rsvp counters messages [type interface-path-id]
```

### Syntax Description

- **type** *(Optional) Interface type. For more information, use the question mark (?) online help function.*
- **interface-path-id** Physical interface or a virtual interface.

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

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

### Command Default

No default behavior or values

### Command Modes

XR EXEC mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.2.1</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.

### 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 all RSVP message counters for an interface to zero:

```
RP/0/RP0/CPU0:router# clear rsvp counters messages HundredGigE0/0/0/3
```
clear rsvp counters oor

To clear internal RSVP counters on out of resources (OOR) events, use the clear rsvp counters oor command in XR EXEC mode.

clear rsvp counters oor [type interface-path-id]

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>
</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

XR EXEC mode

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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.

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 show how to clear all RSVP message counters for HundredGigE interface 0/0/0/3 to zero:

RP/0/RP0/CPU0:router# clear rsvp counters oor HundredGigE0/0/0/3
clear rsvp counters prefix-filtering

To clear internal prefix-filtering related RSVP counters, use the `clear rsvp counters prefix-filtering` command in XR 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>Note</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>access-list</td>
<td>Clears RSVP prefix-filtering counters for access control list.</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**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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 HundredGigE interface 0/0/0/3 to zero:

```
RP/0/RP0/CPU0:router# clear rsvp counters prefix-filtering interface HundredGigE0/0/0/3
```
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
```
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>6.2.1</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.
- 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.

**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 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 HundredGigE interface in RSVP authentication configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface HundredGigE 0/0/0/3
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
```
To control how long RSVP maintains idle security associations with other trusted RSVP neighbors, use the `life-time` command in the appropriate RSVP authentication configuration mode. To disable the lifetime setting, use the `no` form of this command.

```
life-time  seconds
no  life-time  seconds
```

**Syntax Description**
- `seconds` Length of time, in seconds, that RSVP maintains security associations with other trusted RSVP neighbors. Range is 30 to 86400.

**Command Default**
- `seconds`: 1800 (30 minutes)

**Command Modes**
- RSVP authentication configuration
- RSVP interface authentication configuration
- RSVP neighbor authentication configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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.

**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: 

```
```
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 neighbor 1.1.1.1 authentication
RP/0/RP0/CPU0:router(config-rsvp-nbor-auth)# life-time 2000
```

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface HundredGigE 0/0/0/3
RP/0/RP0/CPU0:router(config-rsvp-if)# authentication
RP/0/RP0/CPU0:router(config-rsvp-if-auth)# life-time 2000
```
To enable functionality for Resource Reservation Protocol (RSVP) and enter RSVP configuration commands, use the `rsvp` command in XR Config 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**
XR Config mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**

| mpls-te | read, write |

**Examples**
The following example shows how to enable RSVP functionality and enter the sub-mode for RSVP configuration commands:

```
RP/0/RP0/CPU0:router(config)# rsvp
RP/0/RP0/CPU0:router(config-rsvp)#
```
rsvp interface

To configure RSVP on an interface, use the `rsvp interface` command in XR Config 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**

<table>
<thead>
<tr>
<th>Field</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 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**

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.

**Command Modes**

XR Config mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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 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 the RSVP interface configuration mode and to enable RSVP on this interface with 0 bandwidth:
rp0/rp0/cpu0:router# configure
rp0/rp0/cpu0:router(config)# rsvp interface HundredGigE 0/0/0/3
**rsvp neighbor**

To specify an RSVP neighbor, use the `rsvp neighbor` command in XR Config 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**

XR Config mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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</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
RP/0/RP0/CPU0:router(config-rsvp-nbor-auth)#
```
show rsvp request

To list all the requests that RSVP knows about on a router, use the `show rsvp request` command in XR EXEC mode.

```
show rsvp request  [destination  IP-address]  [detail]  [dst-port  port-num]  [session-type  { lsp-p2p }]
[source  IP-address]  [src-port  port-num]
```

**Syntax Description**

- **detail**  (Optional) Displays multiline status for each path. If this keyword is not specified, only a single-line table entry is displayed.
- **destination  IP-address**  (Optional) Displays the entries that match the specified address.
- **dst-port  port-num**  (Optional) Displays destination port and tunnel information.
- **session-type**  (Optional) Displays the entries that match the specified session type.
- **lsp-p2p**  Displays the entries that are used for P2P sessions.
- **source  IP-address**  (Optional) Displays source address information.
- **src-port  port-num**  (Optional) Displays port and LSP ID information.

**Command Default**

No default behavior or values

**Command Modes**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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.

**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 request` command:

```
RP/0/RP0/CPU0:router# show rsvp request
```
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: HundredGigE 0/0/0/3. 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
Number of supporting RSBs: 1

This table describes the significant fields shown in the display.

**Table 25: 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.</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 XR EXEC mode.

```plaintext
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>Syntax</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 show interfaces command to see a list of all possible interfaces currently configured on the router.</td>
</tr>
<tr>
<td></td>
<td>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**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.
The following sample output displays information for RSVP authentication:

```plaintext
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>10.0.0.1</td>
<td>10.0.0.2</td>
<td>HundredGigE 0/0/0/3</td>
<td>Send</td>
<td>mpls-keys</td>
<td>1</td>
<td>SGC</td>
</tr>
<tr>
<td>10.0.0.2</td>
<td>10.0.0.1</td>
<td>HundredGigE 0/0/0/3</td>
<td>Recv</td>
<td>mpls-keys</td>
<td>1</td>
<td>SGC</td>
</tr>
</tbody>
</table>
```

This table describes the significant fields shown in the display.

**Table 26: 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>Send</td>
<td>Authenticated messages that you forward.</td>
</tr>
<tr>
<td>Recv</td>
<td>Authenticated 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: 10.0.0.1
  - Destination Address: 10.0.0.2
  - Neighbour Address: 10.0.0.2
  - Interface: HundredGigE 0/0/0/3
  - Direction: Send
  - LifeTime: 1800 (sec)
  - LifeTime left: 1305 (sec)
  - KeyType: Static Global KeyChain
  - Key Source: name1
  - Key Status: No error
  - KeyID: 1
  - Digest: HMAC MD5 (16)
  - Challenge: Not supported
  - TX Sequence: 5023960459702858020 (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 27: 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</td>
</tr>
<tr>
<td></td>
<td>the address of the Interface field or the local router ID). For Recv mode,</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>neighbor. For Recv mode, this is the local address (either the address of</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>being maintained.</td>
</tr>
<tr>
<td>Interface</td>
<td>Name of the interface over which the security association is being</td>
</tr>
<tr>
<td></td>
<td>maintained.</td>
</tr>
<tr>
<td>Direction</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>LifeTime</td>
<td>Configured expiration timer value.</td>
</tr>
<tr>
<td>LifeTime left</td>
<td>Number of seconds until the expiration timer expires.</td>
</tr>
<tr>
<td>KeyType</td>
<td>Keys that are used:</td>
</tr>
<tr>
<td></td>
<td><strong>Static</strong></td>
</tr>
<tr>
<td></td>
<td>- Key is static and configured.</td>
</tr>
<tr>
<td></td>
<td><strong>Global</strong></td>
</tr>
<tr>
<td></td>
<td>- Key is global-based.</td>
</tr>
<tr>
<td></td>
<td><strong>Neighbor</strong></td>
</tr>
<tr>
<td></td>
<td>- Key is neighbor-based.</td>
</tr>
<tr>
<td></td>
<td><strong>Interface</strong></td>
</tr>
<tr>
<td></td>
<td>- Key is interface-based.</td>
</tr>
<tr>
<td></td>
<td><strong>Chain</strong></td>
</tr>
<tr>
<td></td>
<td>- Key is part of a keychain.</td>
</tr>
<tr>
<td>Key-Source</td>
<td>Key source identification string that is currently set to the configured</td>
</tr>
<tr>
<td></td>
<td>keychain name.</td>
</tr>
<tr>
<td>Key Status</td>
<td>Last status reported from the key source.</td>
</tr>
</tbody>
</table>
### show rsvp authentication

<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 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 XR EXEC mode mode.

```
show rsvp counters {messages [{type interface-path-id | summary }] | events | database}
```

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>messages</td>
<td>Displays a historical count of the number of messages RSVP has received and sent on each interface along with a summation.</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 <code>show interfaces</code> command to see a list of all possible interfaces currently configured on the router.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays the aggregate counts of all interfaces.</td>
</tr>
<tr>
<td>events</td>
<td>Displays the number of states expired for lack of refresh and a count of received No Acknowledgements (NACKs).</td>
</tr>
<tr>
<td>database</td>
<td>Displays counters on RSVP database, including number of paths, session, and so on.</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>6.2.1</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

<table>
<thead>
<tr>
<th>Task</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mplste</td>
<td>read, write</td>
</tr>
</tbody>
</table>
The following is sample output from the **show rsvp counters messages** command for HundredGigE 0/0/0/3:

```
RP/0/RP0/CPU0:router# show rsvp counters messages HundredGigE 0/0/0/3

<table>
<thead>
<tr>
<th>HundredGigE0/0/0/3</th>
<th>Recv</th>
<th>Xmit</th>
<th>Recv</th>
<th>Xmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>24</td>
<td>1</td>
<td>Resv</td>
<td>0</td>
</tr>
<tr>
<td>PathError</td>
<td>0</td>
<td>0</td>
<td>ResvError</td>
<td>0</td>
</tr>
<tr>
<td>PathTear</td>
<td>5</td>
<td>1</td>
<td>ResvTear</td>
<td>0</td>
</tr>
<tr>
<td>ResvConfirm</td>
<td>0</td>
<td>0</td>
<td>Ack</td>
<td>34</td>
</tr>
<tr>
<td>Bundle</td>
<td>0</td>
<td>Hello</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>SRefresh</td>
<td>10118</td>
<td>0</td>
<td>OutOfOrder</td>
<td>0</td>
</tr>
<tr>
<td>Retransmit</td>
<td>0</td>
<td>Rate Limited</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
```

This table describes the significant fields shown in the display.

**Table 28: 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>Rate Limited</td>
<td>Number of RSVP packets affected by rate limiting.</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 29: 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:</td>
</tr>
<tr>
<td></td>
<td>• A 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>Locally created and incoming Reservations</td>
<td>Reservations created by:</td>
</tr>
<tr>
<td></td>
<td>• A 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 XR EXEC mode.

show rsvp counters oor  [\{type  interface-path-id | summary\}]

**Syntax Description**

- **type** (Optional) Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id** Physical interface or a virtual interface.
- **summary** (Optional) Displays a summary of OOR events.

**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>6.2.1</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 is sample output from the show rsvp counters oor command:

RP/0/RP0/CPU0:router# show rsvp counters oor

    HundredGigE 0/0/0/3 Rejected 24
    HundredGigE 0/0/0/4 Rejected 31
    All RSVP Interfaces Rejected 55
This table describes the significant fields shown in the display.

*Table 30: 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 XR EXEC mode.

```
show rsvp counters prefix-filtering interface [{type interface-path-id | summary}] access-list [aclname]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Displays 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>Note</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>summary</td>
<td>(Optional) Displays a summary of RSVP prefix-filtering counters on all interfaces.</td>
</tr>
<tr>
<td>access-list</td>
<td>Displays RSVP prefix-filtering counters for the access control list.</td>
</tr>
<tr>
<td>aclname</td>
<td>(Optional) Name of the access control list.</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>6.2.1</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.

**Examples**

The following is sample output from the `show rsvp counters prefix-filtering` command:

```
RP/0/RP0/CPU0:router# show rsvp counters prefix-filtering interface
Routed Fwd Local Drop Def-Drop Def-Proc Total
Path 4 4
```

**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>

**MPLS Command Reference for Cisco NCS 5000 Series Routers**

174
The following is sample output from the `show rsvp counters prefix-filtering interface` command:

```
RP/0/RP0/CPU0:router# show rsvp counters prefix-filtering interface HundredGigE 0/0/0/3

HundredGigE0/0/0/3 Fwd Local Drop Def-Drop Def-Proc Total
Path 1 0 219 2 222
PathTear 0 0 31 0 31
ResvConfirm 0 0 0 0 0
Total 1 0 219 2 253
```

The following is sample output from the `show rsvp counters prefix-filtering interface summary` command:

```
RP/0/RP0/CPU0:router# show rsvp counters prefix-filtering interface summary

ALL RSVP
Interfaces Fwd Local Drop Def-Drop Def-Proc Total
Path 4 1 0 219 3 227
PathTear 0 0 31 0 31
ResvConfirm 0 0 0 0 0
Total 4 1 0 250 3 258
```

The following is sample output from the `show rsvp counters prefix-filtering access-list banks` command:

```
RP/0/RP0/CPU0:router# show rsvp counters prefix-filtering access-list banks

ACL: banks Forward Local Drop Total
Path 0 0 0 0
```
This table describes the significant fields shown in the display.

### Table 31: 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] [session-type { lsp-p2p }] [source IP-address] [src-port source-port] [summary]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>destination IP-address</strong></td>
<td>(Optional) Displays the entries that match the specified address.</td>
</tr>
<tr>
<td><strong>dst-port port</strong></td>
<td>(Optional) Displays the port address of the destination router.</td>
</tr>
<tr>
<td><strong>session-type</strong></td>
<td>(Optional) Displays the entries that match the specified session type.</td>
</tr>
<tr>
<td><strong>lsp-p2p</strong></td>
<td>Displays the entries that are used for P2P sessions.</td>
</tr>
<tr>
<td><strong>source IP-address</strong></td>
<td>(Optional) Displays the IP address of the source network.</td>
</tr>
<tr>
<td><strong>src-port source-port</strong></td>
<td>(Optional) Displays the port number of the source router.</td>
</tr>
<tr>
<td><strong>summary</strong></td>
<td>(Optional) Displays summarized information about the FRR database.</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 6.2.1</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**

This is sample output from the `show rsvp fast-reroute` command:

```
RP/0/RP0/CPU0:router# show rsvp fast-reroute

<table>
<thead>
<tr>
<th>Type</th>
<th>Destination</th>
<th>TunID</th>
<th>Source</th>
<th>PSBs</th>
<th>RSBs</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP4</td>
<td>10.10.10.10</td>
<td>1</td>
<td>10.20.20.20</td>
<td>Ready</td>
<td>Ready</td>
</tr>
</tbody>
</table>
```
This table describes the significant fields shown in the display.

**Table 32: 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>
<tr>
<td>Destination</td>
<td>Destination address of session.</td>
</tr>
<tr>
<td>TunID</td>
<td>Tunnel ID number.</td>
</tr>
<tr>
<td>Source</td>
<td>Source address of session.</td>
</tr>
<tr>
<td>PSBs</td>
<td>PSB FRR(^8) state.</td>
</tr>
<tr>
<td>RSBs</td>
<td>RSB FRR state.</td>
</tr>
</tbody>
</table>

\(^8\) Fast reroute.

This is sample output from the `show rsvp fast-reroute summary` command:

```
RP/0/RP0/CPU0:router# show rsvp fast-reroute summary

<table>
<thead>
<tr>
<th>States</th>
<th>Total</th>
<th>Ready</th>
<th>Act-Wait</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSBs</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RSBs</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

This table describes the significant fields shown in the display.

**Table 33: 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(^9) 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>

\(^9\) Fast reroute.
show rsvp graceful-restart

To display the local graceful-restart information for RSVP, use the `show rsvp graceful-restart` command in XR 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**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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**

- **Task ID**
  - mpls-te read, write

**Examples**

The following is sample output from the `show rsvp graceful-restart` command:

```
RP/0/RP0/CPU0:router# show rsvp graceful-restart
Graceful restart: enabled Number of global neighbors: 1
Local MPLS router id: 192.168.55.55
Restart time: 60 seconds Recovery time: 120 seconds
Recovery timer: Not running
Hello interval: 5000 milliseconds Maximum Hello miss-count: 4
```
This table describes the significant fields shown in the display.

**Table 34: 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 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 based on the number of LSPs established and is the time used by neighbors to 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 to be deleted (usually beginning with a value that is equivalent to the sum 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 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 19/12/2016 17:02:25 0
```

This table describes the significant fields shown in the display.

**Table 35: 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 (MPLS).</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 none has occurred, this field is marked as N/A.</td>
</tr>
<tr>
<td>Since</td>
<td>Time at which the current hello state for a global neighbor has been established.</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 XR EXEC mode.

`show rsvp hello instance [Hostname or IP-address] [detail]`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</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**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Hello instances are displayed in ascending order of neighbor 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 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 37: show rsvp hello instance 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 hellos used for FRR. 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.

10 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 38: show rsvp hello instance detail 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>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 XR 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**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Hello instances are displayed in ascending order of neighbor 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 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 39: 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>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>State</td>
<td>State of the hello session to a global neighbor (up, down, or init).</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface for interface bound hellos used for FRR\textsuperscript{11}. For hello instances bound to a global neighbor, interface will be displayed as none.</td>
</tr>
<tr>
<td>LostCnt</td>
<td>Number of times hello communication has been lost with a global neighbor.</td>
</tr>
</tbody>
</table>

\textsuperscript{11} Fast reroute.
show rsvp interface

To display information about all interfaces with RSVP enabled, use the show rsvp interface command in System Admin EXEC mode.

```
show rsvp interface  [type  interface-path-id]  [detail]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</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 show interfaces command to see a list of all possible interfaces currently configured on the router.</td>
</tr>
<tr>
<td>Detail</td>
<td>(Optional) Displays multiline status for each interface. 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**

XR EXEC mode

**Usage Guidelines**

Use the show rsvp interface command to display various configuration settings such as the list of neighbors and their refresh reduction capabilities.

**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 interface command, which displays brief information about the RSVP-configured interfaces for the GigabitEthernet interface type:

```
RP/0/RP0/CPU0:router# show rsvp interface HundredGigE 0/0/0/3
Thu Oct 22 20:35:42.323 UTC
Interface   MaxBW (bps) MaxFlow (bps) Allocated (bps) MaxSub (bps)
------------ ----------- ------------- ------------------ -------------
HundredGigE 0/0/0/3   750M     750M       0 ( 0%)       0
```
show rsvp neighbor

To display information about RSVP neighbors, use the `show rsvp neighbor` command in XR EXEC mode.

```
show rsvp neighbor [detail]
```

**Syntax Description**
- `detail` (Optional) Displays detailed information about RSVP neighbors.

**Command Default**
No default behavior or values

**Command Modes**
XR EXEC mode

**Command History**
- **Release** 6.2.1
  - 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.

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

**Examples**
The following is sample output from the `show rsvp neighbor` command using the `detail` keyword:

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

Global Neighbor: 10.10.10.10
Interface Neighbor: 1.1.1.1
Interface: HundredGigE0/0/0/3
Refresh Reduction: "Enabled" or "Disabled".
Remote epoch: 0xXXXXXXX
Out of order messages: 0
Retransmitted messages: 0
Interface Neighbor: 2.2.2.2
Interface: HundredGigE0/0/0/3
Refresh Reduction: "Enabled" or "Disabled".
Remote epoch: 0xXXXXXXX
Out of order messages: 0
Retransmitted messages: 0
```
show rsvp reservation

To display all reservations that RSVP knows about on a router, use the `show rsvp reservation` command in XR EXEC mode.

```
show rsvp reservation [destination IP address] [detail] [dst-port port-num] [session-type { lsp-p2p }] [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.
- **session-type** (Optional) Displays the entries that match the specified session type.
- **lsp-p2p** Displays the entries that are used for P2P sessions.
- **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**

XR EXEC mode

**Command History**

- **Release**
  - 6.2.1
- **Modification**
  - This command was introduced.

**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.

**Task ID**

- **mpls-te** read, write

**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
```
The following example displays detailed information about all reservations in the router:

```
RP/0/RP0/CPU0:router# show rsvp reservation detail
```

Input adjusted interface: None. Input physical interface: None.
Next hop: 0.0.0.0 (lih: 0x0).
Rate: 0 bits/sec. Burst: 1K bytes. Peak: 0 bits/sec.
MTU min: 40, max: 500 bytes.
Flags: Local Receiver.
State expires in 0.000 sec.
Policy: Accepted. Policy source(s): MPLS/TE.
Header info: RSVP TTL=255. IP TTL=255. Flags: 0x0. TOS=0xff.
Resource:
Labels: Local downstream: 3.

Input adjusted interface: HundredGigE 0/0/0/3. Input physical interface: HundredGigE
0/0/0/3.
Next hop: 10.66.67.68 (lih: 0x8DE00002).
Rate: 0 bits/sec. Burst: 1K bytes. Peak: 0 bits/sec.
MTU min: 0, max: 500 bytes.
Flags: None.
State expires in 361.184 sec.
Policy: Accepted. Policy source(s): MPLS/TE.
Header info: RSVP TTL=254. IP TTL=254. Flags: 0x1. TOS=0xff.
Resource:
Labels: Outgoing downstream: 3.

This table describes the significant fields shown in the display.

**Table 40: 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>
show rsvp reservation

12 Link-state packet
show rsvp sender

To display all path states that RSVP knows about on this router, use the **show rsvp sender** command in XR EXEC mode mode.

`show rsvp sender [destination IP-address] [detail] [dst-port port-num] [session-type { lsp-p2p }] [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.
- `session-type` (Optional) Displays the entries that match the specified session type.
- `lsp-p2p` Displays the entries that are used for P2P sessions.
- `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**
XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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: 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   HundredGigE0/0/0/3 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 41: 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 Address</td>
<td>Destination and session address of LSP&lt;sup&gt;13&lt;/sup&gt;.</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>

<sup>13</sup> Link-state packet

The following example displays detailed information about all paths in the system:

```
RP/0/RP0/CPU0:router# show rsvp sender detail
PATH: IPv4-LSP Session addr: 10.66.67.68. TunID: 1. LSPId: 25.
    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=0x0.
    Input interface: HundredGigE 0/0/0/3. Previous hop: 10.40.40.40 (lih: 0x40600001).
    Resource:
        Labels: Outgoing upstream: 3.
        Class-Type: None.
        Explicit Route (Incoming):
            Strict, 10.66.67.68(interface-path-id 5)
            Strict, 10.66.67.68/32
```

This table describes the significant fields shown in the display.

**Table 42: 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&lt;sup&gt;14&lt;/sup&gt;.</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&lt;sup&gt;15&lt;/sup&gt;.</td>
</tr>
<tr>
<td>Header info</td>
<td>RSVP header information as described in RFC 2205.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Input interface</td>
<td>Interface on which the path was received. At ingress mode, it is None.</td>
</tr>
<tr>
<td>Previous hop</td>
<td>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).</td>
</tr>
<tr>
<td>Lih</td>
<td>Logical interface handle received in the hop object of the path.</td>
</tr>
<tr>
<td>Output interface</td>
<td>Interface on which the path was forwarded to the downstream neighbor</td>
</tr>
<tr>
<td>Policy</td>
<td>Admission control status for the path in the outgoing direction.</td>
</tr>
<tr>
<td>Explicit route</td>
<td>Explicit route specified in the explicit-route object of the Path message.</td>
</tr>
</tbody>
</table>

14 Link-state packet
15 MPLS-Traffic Engineering
**show rsvp session**

To list all sessions that RSVP knows about on this router, use the `show rsvp session` command in XR EXEC mode.

```
show rsvp session [destination IP-address] [detail] [dst-port port-num] [session-type { lsp-p2p }]
[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.
- `session-type` (Optional) Displays the entries that match the specified session type.
- `lsp-p2p` Displays the entries that are used for P2P sessions.
- `tunnel-name tunnel-name` (Optional) Displays status for the session matching the specified tunnel-name.

**Command Modes**

- XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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**

- Task ID: `mpls-te`
- Operations: `read, write`

**Examples**

The following is sample output from the `show rsvp session` command:

```
RP/0/RP0/CPU0:router# show rsvp session

<table>
<thead>
<tr>
<th>Type</th>
<th>Session Addr</th>
<th>Port</th>
<th>Proto/ExtTunID</th>
<th>PSSB</th>
<th>RSSB</th>
<th>Reqs</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP4</td>
<td>10.40.40.40</td>
<td>2001</td>
<td>10.66.67.68</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>LSP4</td>
<td>10.66.67.68</td>
<td>2000</td>
<td>10.40.40.40</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
```
This table describes the significant fields shown in the display.

Table 43: 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>
<tr>
<td>Port</td>
<td>Destination port or tunnel ID in case of TE tunnels.</td>
</tr>
<tr>
<td>Proto/ExtTunID</td>
<td>Source address of TE tunnels or protocol as in the case of IPV4 sessions.</td>
</tr>
<tr>
<td>PSBs</td>
<td>Number of path state blocks for this session.</td>
</tr>
<tr>
<td>RSBs</td>
<td>Number of reservation state blocks pertaining to incoming or local reservations for this session.</td>
</tr>
<tr>
<td>Reqs</td>
<td>Number of requests. State data structure representing reservations sent up-stream.</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: 10.66.67.68, TunID: 1, ExtID: 10.40.40.40
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, 10.66.67.68(interface-path-id 5)
    Strict, 10.66.67.68/32
Record Route: None
Tspec: avg rate=0, burst=1K, peak rate=0
RSVP Resv Info:
  OutLabel: HundredGigE0/0/0/3, 5
  FRR OutLabel: No intf, No label
  Record Route:
    Node-id 10.66.67.68, interface index 5
    Fspec: avg rate=0, burst=1K, peak rate=0
```

This table describes the significant fields shown in the display.

Table 44: 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&lt;sup&gt;16&lt;/sup&gt;.</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>
</tbody>
</table>
### Field | Description
--- | ---
InLabel | Incoming interface and label info for the LSP in the upstream direction. At the egress node, using penultimate hop popping at the egress node, (implicit-null) appears as No Label.
Incoming Address | Address of the ingress interface.
Explicit Route | Explicit route specified in the explicit-route object of the Path message.
Record Route | Record route object in either the path or reservation message.
Tspec | Traffic parameters.
OutLabel | Outgoing interface and label sent downstream.
FRR OutLabel | For FRR\(^\text{17}\), displays the backup tunnel and Merge-point label.
Fspec | Flow spec parameters for specified QoS.

\(^{16}\) Link-state packet.
\(^{17}\) 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>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

DSCP marking improves signaling setup and teardown times.

Usually, 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, usually 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 of interface B are marked with DSCP 10.

There is a difference between `signalling dscp 0` and `no signalling dscp` commands. The first command instructs RSVP to explicitly set the DSCP value to 0 on all packets sent out of this interface. The second command removes any override on the packets being sent out of this interface, and allows the DSCP of received packets that created this state to persist on packets forwarded out of 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 examples show how to mark all RSVP packets going out on a HundredGigE interface with DSCP value 20.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface HundredGigE 0/0/0/3
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 on a HundredGigE interface.

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface HundredGigE 0/0/0/3
RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling dscp
```
**signalling graceful-restart**

To enable or disable RSVP signaling graceful restart, use the `signalling graceful-restart` command in RSVP configuration mode. To return to the default behavior, use the `no` form of this command.

```
signalling graceful-restart [{recovery-time time | restart-time time}]
no signalling graceful-restart
```

**Syntax Description**

- **recovery-time** (Optional) Configures the recovery time that is advertised in the Restart Cap object in the Hello messages.
- **time** Time, in seconds, for the neighbor to wait for the node to recover (replay) existing states after the Hello session is reestablished before initiating TEARs. Range is 0 to 3600.
- **restart-time** (Optional) Configures the restart time that is advertised in the Restart Cap object in hello messages.
- **time** Time, in seconds, after a control-plane restart that RSVP can start exchanging hello messages. Range is 60 to 3600. Default is 120.

**Command Default**

RSVP signaling graceful restart is disabled.

**Command Modes**

RSVP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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 and Optical User Network Interface (O-UNI) traffic for the following types of faults. This is an implementation of the fault handling section of the IETF standard RFC 3473:

- **Control-channel-failure**
  
  Disruption of communication channels between 2 nodes when the communication channels are separated from the data channels.

- **Node-failure**
  
  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.
signalling graceful-restart

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>6.2.1</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 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 interface-based graceful restart:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface tunnel-te 66
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 signalling hello graceful-restart refresh interval` command.

```
signalling hello graceful-restart refresh interval  refresh-interval
no signalling hello graceful-restart refresh interval
```

**Syntax Description**

- `refresh-interval`: Interval, in milliseconds, at which RSVP graceful-restart hello messages are sent to each neighbor. Range is 3000 to 30000.

**Command Default**

- `refresh interval: 5000`

**Command Modes**

- RSVP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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
```
signalling hello graceful-restart refresh interval 4000
signalling prefix-filtering access-list

To specify the extended access control list to use for prefix filtering of RSVP Router Alert messages, use the **signalling prefix-filtering access-list** command in RSVP configuration mode. To return to the default behavior, use the **no** form of this command.

**signalling prefix-filtering access-list  access list name**

**no  signalling prefix-filtering access-list  access list name**

**Syntax Description**

- **access list name**
  - Extended access-list name as a string (maximum 32 characters).

**Command Default**

No default behavior or values

**Command Modes**

RSVP configuration

**Command History**

- **Release 6.2.1**
  - This command was introduced.

**Usage Guidelines**

The extended access control list containing the source and destination prefixes used for packet filtering is configured separately.

**Task ID**

- **mpls-te**
  - **read,** **write**

**Examples**

The following example shows how to configure the access control list name banks for prefix-filtering of RSVP Router Alert messages:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp
RP/0/RP0/CPU0:router(config-rsvp)# signalling prefix-filtering access-list banks
```

The following example shows how to disable RSVP prefix-filtering of RSVP Router Alert messages:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp
RP/0/RP0/CPU0:router(config-rsvp)# no signalling prefix-filtering access-list banks
```
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>6.2.1</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 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
```
signalling rate-limit

To limit the rate of RSVP signaling messages being sent out a particular interface, use the `signalling rate-limit` command in RSVP interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
signalling rate-limit [rate messages] [interval interval-length]
no signalling rate-limit [rate messages] [interval interval-length]
```

**Syntax Description**

- `rate messages` (Optional) Configures the number of messages sent per scheduling interval. Range is 1 to 500 messages.
- `interval interval-length` (Optional) Specifies the length, in milliseconds, between scheduling intervals. Range is 250 to 2000.

**Command Default**

- `messages`: 100
- `interval-length`: 1,000 (1 second)

**Command Modes**

RSVP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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,</td>
</tr>
<tr>
<td></td>
<td>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 HundredGigE 0/0/0/3
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 HundredGigE 0/0/0/3
RP/0/RP0/CPU0:router(config-rsvp-if)# signalling rate-limit rate 40 interval 250
```

The following example shows how to restore the rate to the default of 100 messages per second:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# rsvp interface HundredGigE 0/0/0/3
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 HundredGigE 0/0/0/3
RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling rate-limit
```
**signalling refresh interval**

To change the frequency with which a router updates the network about the 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>6.2.1</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>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>
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
```
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>Release 6.2.1</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</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
```
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>Release 6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `window-size` command to specify the maximum number of authenticated messages that are received out of sequence. All RSVP authenticated messages include a sequence number that is used to prevent replays of RSVP messages.

With a default window size of one message, RSVP rejects any out-of-order or out-of-sequence authenticated messages because they are assumed to be replay attacks. However, sometimes bursts of RSVP messages become reordered between RSVP neighbors. If this occurs on a regular basis, and you can verify that the node sending the burst of messages is trusted, you can use the window-size option to adjust the burst size such that RSVP does not discard such reordered bursts. RSVP checks for duplicate messages within these bursts.

**Task ID**

<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 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 HundredGigE 0/0/0/3
RP/0/RP0/CPU0:router(config-rsvp-if)# authentication
RP/0/RP0/CPU0:router(config-rsvp-if-auth)# window-size 33
```
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>Release 6.2.1</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.

**Examples**

The following example shows how to change the summary message maximum size on an interface:

```
RP/0/RP0/CPF00:router# configure
RP/0/RP0/CPF00:router(config)# rsvp interface tunnel-te 2
RP/0/RP0/CPF00: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/CPF00:router# configure
RP/0/RP0/CPF00:router(config)# rsvp interface tunnel-te 2
RP/0/RP0/CPF00:router(config-rsvp-if)# no signalling refresh reduction summary max-size 6000
```
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>Release 6.2.1</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 a HundredGigE interface.

```plaintext
RP/0/RP0/CPU0:router(config)# rsvp interface HundredGigE 0/0/0/3
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 a HundredGigE interface.

```plaintext
RP/0/RP0/CPU0:router(config)# rsvp interface HundredGigE 0/0/0/3
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.

```plaintext
RP/0/RP0/CPU0:router(config)# rsvp interface HundredGigE 0/0/0/3
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.

```plaintext
RP/0/RP0/CPU0:router(config)# rsvp interface HundredGigE 0/0/0/3
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.

```plaintext
RP/0/RP0/CPU0:router(config)# rsvp interface HundredGigE 0/0/0/3
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.

```plaintext
RP/0/RP0/CPU0:router(config)# rsvp interface HundredGigE 0/0/0/3
```
signalling refresh reduction reliable

RP/0/RP0/CPU0:router(config-rsvp-if)# no signalling refresh reduction reliable

The following example shows how to enable the use of reliable transmission for RSVP summary refresh messages.

RP/0/RP0/CPU0:router(config-rsvp-if)# signalling refresh reduction reliable summary-refresh
**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.

```
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>Release 6.2.1</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.

**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 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
```
signalling refresh reduction bundle-max-size

To configure the maximum size of a single RSVP bundle message, use the `signalling refresh reduction bundle-max-size` command in RSVP interface configuration mode.

`signalling refresh reduction bundle-max-size` `size`

**Syntax Description**

- `size` Maximum size, in bytes, of a single RSVP bundle message. Range is 512 to 65000.

**Command Default**

- `size`: 4096

**Command Modes**

- RSVP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**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:

```
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
```
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 *MPLS Configuration Guide for Cisco NCS 5000 Series Routers*.

- adjustment-threshold (MPLS-TE), on page 223
- admin-weight, on page 224
- affinity, on page 225
- affinity-map, on page 229
- application (MPLS-TE), on page 231
- attribute-flags, on page 232
- attribute-names, on page 233
- attribute-set, on page 234
- auto-bw (MPLS-TE), on page 238
- auto-bw collect frequency (MPLS-TE), on page 240
- autoroute announce, on page 241
- autoroute destination, on page 243
- autoroute metric, on page 244
- auto-tunnel backup (MPLS-TE), on page 245
- backup-path tunnel-te, on page 246
- bidirectional, on page 248
- bw-limit (MPLS-TE), on page 249
- clear mpls traffic-eng auto-bw (MPLS-TE EXEC), on page 251
- clear mpls traffic-eng auto-tunnel backup unused, on page 253
• clear mpls traffic-eng auto-tunnel mesh, on page 254
• clear mpls traffic-eng counters auto-tunnel mesh, on page 255
• clear mpls traffic-eng counters auto-tunnel backup, on page 256
• clear mpls traffic-eng counters global, on page 257
• clear mpls traffic-eng counters signaling, on page 258
• clear mpls traffic-eng counters soft-preemption, on page 259
• clear mpls traffic-eng fast-reroute log, on page 260
• clear mpls traffic-eng link-management statistics, on page 261
• collect-bw-only (MPLS-TE), on page 262
• destination (MPLS-TE), on page 263
• disable (explicit-path), on page 264
• exclude srlg (auto-tunnel backup), on page 265
• fast-reroute, on page 266
• fast-reroute protect, on page 267
• fast-reroute timers promotion, on page 268
• flooding thresholds, on page 269
• forward-class, on page 270
• forwarding-adjacency, on page 271
• index exclude-address, on page 273
• index exclude-srlg, on page 275
• index next-address, on page 276
• interface (MPLS-TE), on page 278
• interface (SRLG), on page 280
• interface tunnel-te, on page 281
• ipv4 unnumbered (MPLS), on page 283
• ipv4 unnumbered mpls traffic-eng, on page 284
• link-management timers bandwidth-hold, on page 285
• link-management timers periodic-flooding, on page 286
• link-management timers preemption-delay, on page 287
• load-share, on page 288
• load-share unequal, on page 289
• match mpls disposition, on page 290
• maxabs (MPLS-TE), on page 291
• mpls traffic-eng, on page 292
• mpls traffic-eng auto-bw apply (MPLS-TE), on page 293
• mpls traffic-eng fast-reroute promote, on page 295
• mpls traffic-eng level, on page 296
• mpls traffic-eng link-management flood, on page 297
• mpls traffic-eng path-protection switchover tunnel-te, on page 298
• mpls traffic-eng reoptimize (EXEC), on page 299
• mpls traffic-eng reoptimize events link-up, on page 300
• mpls traffic-eng router-id (MPLS-TE router), on page 301
• mpls traffic-eng repotimize mesh group, on page 303
• mpls traffic-eng srlg, on page 304
• nhop-only (auto-tunnel backup), on page 306
• overflow threshold (MPLS-TE), on page 307
• path-option (MPLS-TE), on page 309
• path-protection (MPLS-TE), on page 312
• path-protection timers reopt-after-swatchover, on page 313
• path-selection cost-limit, on page 314
• path-selection ignore overload (MPLS-TE), on page 315
• path-selection loose-expansion affinity (MPLS-TE), on page 317
• path-selection loose-expansion metric (MPLS-TE), on page 318
• path-selection metric (MPLS-TE), on page 319
• path-selection metric (interface), on page 320
• policy-class, on page 321
• priority (MPLS-TE), on page 323
• record-route, on page 324
• redirect default-route nexthop, on page 325
• redirect nexthop, on page 326
• reoptimize (MPLS-TE), on page 327
• reoptimize timers delay (MPLS-TE), on page 328
• route-priority, on page 330
• router-id secondary (MPLS-TE), on page 332
• set destination-address, on page 333
• set ipv4 df, on page 334
• set source-address, on page 335
• show explicit-paths, on page 336
• show interfaces tunnel-te accounting, on page 338
• show mpls traffic-eng affinity-map, on page 339
• show mpls traffic-eng attribute-set, on page 341
• show mpls traffic-eng autoroute, on page 343
• show mpls traffic-eng auto-tunnel backup, on page 345
• show mpls traffic-eng auto-tunnel mesh, on page 348
• show mpls traffic-eng collaborator-timers, on page 351
• show mpls traffic-eng counters signaling, on page 353
• show mpls traffic-eng forwarding, on page 357
• show mpls traffic-eng forwarding-adjacency, on page 359
• show mpls traffic-eng igp-areas, on page 360
• show mpls traffic-eng link-management admission-control, on page 363
• show mpls traffic-eng link-management advertisements, on page 367
• show mpls traffic-eng link-management bandwidth-allocation, on page 370
• show mpls traffic-eng link-management igp-neighbors, on page 373
• show mpls traffic-eng link-management interfaces, on page 375
• show mpls traffic-eng link-management statistics, on page 378
• show mpls traffic-eng link-management summary, on page 380
• show mpls traffic-eng maximum tunnels, on page 382
• show mpls traffic-eng preemption log, on page 385
• show mpls traffic-eng topology, on page 387
• show mpls traffic-eng tunnels, on page 391
• show mpls traffic-eng tunnels auto-bw brief, on page 420
• show mpls traffic-eng link-management soft-preemption, on page 422
• show srlg, on page 424
• signalled-name, on page 427
• signalling advertise explicit-null (MPLS-TE), on page 428
• snmp traps mpls traffic-eng, on page 429
• soft-preemption, on page 431
• soft-preemption frr-rewrite, on page 432
• srlg, on page 433
• timers loose-path (MPLS-TE), on page 434
• timers removal unused (auto-tunnel backup), on page 435
• timeout (soft-preemption), on page 436
• topology holddown sigerr (MPLS-TE), on page 437
• tunnel-id (auto-tunnel backup), on page 438
adjustment-threshold (MPLS-TE)

To configure the tunnel bandwidth 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` Configures the bandwidth 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

**MPLS-TE automatic bandwidth interface configuration**

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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 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
```
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, IS-IS 10)

**Command Modes**

MPLS-TE interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use 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</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to override the IGP cost of the link and sets 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 HundredGigE 0/0/0/3
RP/0/RP0/CPU0:router(config-mpls-te-if)# admin-weight 20
```
affinity

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

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

**Syntax Description**

- **affinity-value**
  - Attribute values that are required for links to carry this tunnel. A 32-bit decimal number. Range is from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.

- **mask mask-value**
  - Checks the link attribute. A 32-bit decimal number. Range is 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute mask is 0 or 1.

- **exclude name**
  - Configures a particular affinity to exclude.

- **exclude-all**
  - Excludes all affinities.

- **include name**
  - Configures the affinity to include in the loose sense.

- **include-strict name**
  - Configures the affinity to include in the strict sense.

**Command Default**

- `affinity-value`: 0X00000000
- `mask-value`: 0x0000FFFF

**Command Modes**

- Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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.

If there is an affinity failure, a 5-minute timer is started at the LSP headend. If the tunnel is not able to reoptimize within the timeframe, it is torn down. However, if you execute the `mpls traffic-eng reoptimize disable affinity-failure` command, no timer is started and the tunnel is not torn down. At a subsequent time, other triggers for reoptimization may start the timer for the LSPs with affinity failure.

Any properties set to 1 in the affinity should be 1 in the mask. The affinity and mask should be set as follows:
You can configure up to 16 affinity constraints under a given tunnel. These constraints are used to configure affinity constraints for the tunnel:

**Include constraint**

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

**Include-strict constraint**

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

**Exclude constraint**

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

**Exclude-all constraint**

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

You set 1 bit for each color; however, the sample output shows multiple bits at the same time. For example, you can configure red and black colors on HundredGigabitEthernet 0/0/0/3 from the `interface` command. The sample output from the `show mpls traffic-eng link-management interfaces`, on page 375 command shows that the Attributes field is set to 0x21, which means that there are 0x20 and 0x1 bits on the link.

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

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

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

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

This example shows that a link is eligible for CSPF if it has at least red and black colors. The link can have any additional colors.
This sample output shows that the include constraint from the `show mpls traffic-eng tunnels` command is 0x20 and 0x1:

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

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

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

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

Reason for the tunnel being down: No destination is configured

History:

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

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

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

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

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

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

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

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

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>affinity name</code></td>
<td>Affinity map name-to-value designator (in hexadecimal, (0xffffffff)).</td>
</tr>
<tr>
<td><code>affinity value</code></td>
<td>Affinity map value designator. Range is from 1 to 80000000.</td>
</tr>
<tr>
<td><code>bit-position value</code></td>
<td>Configures the value of an affinity map for the bit position of the 32-bit number.</td>
</tr>
<tr>
<td><code>value</code></td>
<td>Bit position value. Range is from 0 to 31. Range is from 0 to 255.</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>6.2.1</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.

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

The following example shows how to configure the value of 15 for an affinity map by bit position:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
```
RP/0/RP0/CPU0:router(config-mpls-te)# affinity-map red2 bit-position 15
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you configure and modify the application frequency, the application period can reset and restart for that tunnel. The next bandwidth application for the tunnel happens within the specified minutes.

**Task ID**

- Task ID: `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
```
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>6.2.1</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**

- `Task ID`: mpls-te
- `Operations`: read, write

**Examples**

The following example shows how to set attribute flags to 0x0101:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# interface HundredGigE 0/0/0/3
RP/0/RP0/CPU0:router(config-mpls-te-if)# attribute-flags 0x0101
```
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. Up to 32 attribute-names can be assigned.

`index` Specifies an entry index for attribute names.

`index-number` Specifies the index number. Range is from 1 to 8.

**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>6.2.1</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 256-bit value.

**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 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 HundredGigabitEthernet 0/0/0/3
RP/0/RP0/CPU0:router(config-mpls-te-if)# attribute-name red
```
attribute-set

To configure attribute-set for auto-backup tunnels, use the `attribute-set` command in MPLS-TE configuration mode.

```
attribute-set auto-backup attribute-set-name {affinity affinity-value mask mask-value | exclude name | exclude-all | include name | include-strict name | logging events lsp-status {reoptimize | state} | policy-class {range | default} | priority setup-range hold-range | record-route}
```

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} | policy-class {range | default} | 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><code>auto-backup</code></td>
<td>Specifies the values of an attribute set for the auto-backup group.</td>
</tr>
<tr>
<td><code>auto-mesh</code></td>
<td>Specifies the values of an attribute set for the auto-mesh group.</td>
</tr>
<tr>
<td><code>path-option</code></td>
<td>Specifies the values of an attribute set for the path option.</td>
</tr>
<tr>
<td><code>xro</code></td>
<td>Specifies that the attribute-set is used to define an XRO.</td>
</tr>
<tr>
<td><code>attribute-set-name</code></td>
<td>A 32-bit character string, specifies the name of the attribute-set template.</td>
</tr>
<tr>
<td><code>affinity-value</code></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><code>mask mask-value</code></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>
</tbody>
</table>
exclude name

Configures a specific affinity that is to be excluded.

exclude-all

Excludes all affinities.

include name

Configures the affinity to include in the loose sense.

include-strict name

Configures the affinity to include in the strict sense.

logging

Per-interface logging configuration.

events

Per-interface logging events.

lsp-status

Enables interface LSP state change alarms.

reoptimize

Enables interface LSP REOPT change alarms.

state

Enables interface LSP UP/DOWN change alarms.

policy-class

Specifies class for policy-based tunnel selection.

range

Tunnel policy class range 1 to 7.

default

Default class for policy-based tunnel selection.

priority

Specifies the tunnel priority.

setup-range

Specifies setup priority. Range is 0 to 7.

hold-range

Specifies hold priority. Range is 0 to 7.

record-route

Records the route used by the tunnel.

signalled-bandwidth

Specifies the tunnel bandwidth requirement to be signaled.

bandwidth

Bandwidth required for an MPLS-TE tunnel, specified in kilobits per second. By default, bandwidth is reserved in the global pool. Range is from 0 to 4294967295.

class-type ct

(Optional) Configures the class type of the tunnel bandwidth request. Range is 0 to 1. Class-type 0 is equivalent to global-pool. Class-type 1 is equivalent to subpool.

soft-preemption

Enables the soft-preemption feature on this tunnel.

Command Default

affinity-value: 0x0

mask-value: 0xFFFF

Command Modes

MPLS TE configuration
This command was introduced in Release 6.2.1.

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.

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 configure an attribute-set to a TE interface for an auto-backup tunnel:

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# interface HundredGigabitEthernet 0/0/0/3
RP/0/RP0/CPU0:router(config-mpls-te)# auto-tunnel backup
RP/0/RP0/CPU0:router(config-mpls-te-if-auto-backup)# attribute-set ab
```

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-mpls-te)# 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 attribute-set for auto-backup tunnels:

```
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 auto-backup ab
RP/0/RP0/CPU0:router(config-te-attribute-set)# affinity 0x1 mask 0x1
RP/0/RP0/CPU0:router(config-te-attribute-set)# priority 3 3
RP/0/RP0/CPU0:router(config-te-attribute-set)# policy-class 6
RP/0/RP0/CPU0:router(config-te-attribute-set)# logging events lsp-status reoptimize
RP/0/RP0/CPU0:router(config-te-attribute-set)# logging events lsp-status state
RP/0/RP0/CPU0:router(config-te-attribute-set)# policy-class default
RP/0/RP0/CPU0:router(config-te-attribute-set)# record-route
```

This example shows how to configure the attribute-set for auto-mesh tunnels:

```
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 auto-mesh mesh1
RP/0/RP0/CPU0:router(config-te-attribute-set)# affinity include red blue
```
RP/0/RP0/CPU0:router(config-te-attribute-set)# **affinity include-strict yellow green**
RP/0/RP0/CPU0:router(config-te-attribute-set)# **affinity exclude black**
RP/0/RP0/CPU0:router(config-te-attribute-set)# **affinity exclude-all**
RP/0/RP0/CPU0:router(config-te-attribute-set)# **policy-class default**

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**

The following example shows how to configure attribute set attr01:

RP/0/RP0/CPU0:router(config)# **mpls traffic-eng**
RP/0/RP0/CPU0:router(config-mpls-te)# **attribute-set xro attr01**
RP/0/RP0/CPU0:router(config-te-attribute-set)#
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>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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, it is recommended 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 when the automatic bandwidth is enabled on one tunnel. If automatic bandwidth is disabled from all tunnels, the operation stops.
- If the output rate collection is already active when the automatic bandwidth is configured on a tunnel, the statistics collection for that tunnel starts at the next collection configuration.

```
Note
Because the collection timer is already running, the first collection event for that tunnel happens in less than C minutes (for example, on an average of C/2 minutes).
```

**Task ID**

- mpls-te read, write
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)#
```
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>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `auto-bw collect frequency` command configures the automatic bandwidth collection frequency for all the tunnels.

Modifying the global collection frequency does not restart the tunnel for the current application period. The application period continues with the modified collection frequency.

**Task ID**

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

**Examples**

The following example configures a tunnel for an automatic bandwidth adjustment of 100 minutes:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# auto-bw collect frequency 100
```
**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 [include-ipv6] [metric value]
no  autoroute announce
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>include-ipv6</td>
<td>(Optional) Announces the MPLS-TE tunnel to IS-IS IGP for IPv6 routing.</td>
</tr>
<tr>
<td>metric value</td>
<td>(Optional) Specify the MPLS-TE tunnel metric that the Interior Gateway Protocol (IGP) enhanced Shortest Path First (SPF) calculation uses.</td>
</tr>
</tbody>
</table>

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>6.2.1</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.

The `autoroute announce metric` configuration overrides the `autoroute metric`, on page 244 configuration, if present.

**Note**

IS-IS is the only IGP supporting IPv6 MPLS-TE tunnel announcements.

**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></td>
<td>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
```
This example shows how to make IPv6 announcements for MPLS-TE tunnel to the IGP:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 65534
RP/0/RP0/CPU0:router(config-if)# autoroute announce
RP/0/RP0/CPU0:router(config-if-tunte-aa)# include-ipv6
```
autoroute destination

To install multiple static routes in the routing information base (RIB) per MPLS TE tunnel, use the autoroute destination command in interface TE tunnel configuration mode. To disable autoroute destination, use the no form of this command.

**Syntax**

```
autoroute destination ip-address
no autoroute destination ip-address
```

**Syntax Description**

- `ip-address` Specifies the host address of the route to be installed in the RIB. A maximum of six routes can be specified apart from the default route.

**Command Default**

Autoroute destination is disabled.

**Command Modes**

Interface Tunnel TE

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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>

This example shows how to configure installing four routes in RIB for TE tunnel 10:

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#interface tunnel-te 10
RP/0/RP0/CPU0:router(config-if)# autoroute destination 192.168.1.2
RP/0/RP0/CPU0:router(config-if)# autoroute destination 192.168.2.2
RP/0/RP0/CPU0:router(config-if)# autoroute destination 192.168.3.2
RP/0/RP0/CPU0:router(config-if)# autoroute destination 192.168.4.2
```
**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>6.2.1</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.

**Note**

The **autoroute announce**, on page 241 configuration overrides the **autoroute metric** configuration, if present.

**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
```
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>Release 6.2.1</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 tunnels that are configured using either the **auto-tunnel backup** command or the **nhop-only** 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 automatically builds NHOP and NNHOP backup tunnels:

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# auto-tunnel backup
```
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>6.2.1</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**

<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>
The following example shows how to protect the interface using tunnels:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# interface HundredGigabitEthernet 0/0/0/3
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
```
bidirectional

To configure a bidirectional LSP for a MPLS TE tunnel and define other parameters for the LSP, use the `bidirectional` command in the MPLS-TE interface configuration mode.

```
bidirectional association {id value | source-address IP address | global-id value | type co-routed | fault-oam}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bidirectional</code></td>
<td>Configures a bidirectional LSP.</td>
</tr>
<tr>
<td>association</td>
<td>Specifies association parameters for the bidirectional LSP.</td>
</tr>
<tr>
<td><code>id value</code></td>
<td>Value number that identifies the association. Range is 0 to 65535.</td>
</tr>
<tr>
<td><code>source-address value</code></td>
<td>Specifies the source IP address of the LSP from which a reverse path is required.</td>
</tr>
<tr>
<td><code>global-id value</code></td>
<td>Value number that identifies the global ID. Range is 0 to 4294967295. The default value is 0.</td>
</tr>
<tr>
<td><code>type co-routed</code></td>
<td>Configures co-routed LSPs with bidirectional CSPF.</td>
</tr>
<tr>
<td><code>fault-oam</code></td>
<td>Configures fault OAM for the bidirectional co-routed LSPs.</td>
</tr>
</tbody>
</table>

### Command Default

Tunnel interfaces are disabled.

### Command Modes

Interface configuration mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Example

This example shows you how to configure an associated bidirectional co-routed MPLS-TE tunnel.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RSP0/CPU0:router(config-if)# bidirectional
RP/0/RSP0/CPU0:router(config-if-bidir)# association id 1 source-address 11.0.0.1
RP/0/RSP0/CPU0:router(config-if-bidir)# association type co-routed
```
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>min bandwidth</code></td>
<td>Configures the minimum automatic bandwidth, in kbps, on a tunnel. The range is from 0 to 4294967295. The default is 0.</td>
</tr>
<tr>
<td><code>max bandwidth</code></td>
<td>Configures the maximum automatic bandwidth, in kbps, on a tunnel. The range is from 0 to 4294967295. The default is 4294967295.</td>
</tr>
</tbody>
</table>

**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>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

- `mpls-te` read, write

**Examples**

The following example shows how to configure the minimum and maximum bandwidth for the tunnel:

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

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 XR 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
XR EXEC mode

### Command History
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
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/RPS1/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 Time</th>
<th>Application Left</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel-te0</td>
<td>278</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>150</td>
<td>12m 38s</td>
<td></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 Name</th>
<th>LSP ID</th>
<th>Last appl</th>
<th>Requested</th>
<th>Signalled</th>
<th>Highest</th>
<th>Application 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>
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 XR EXEC mode.

`clear mpls traffic-eng auto-tunnel backup unused {all | tunnel-te tunnel-number}`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</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**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `unused` auto-tunnel backup tunnel is the tunnel that is not assigned to protect any FRR tunnel.

The behavior of this command is the same as the expiration of the `timers removal unused` command in which, when the timeout value is reached, the automatic backup tunnel is removed.

**Task ID**

<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 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
```
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 XR EXEC mode.

```
clear mpls traffic-eng auto-tunnel mesh unused {all | tunnel-te}
```

**Syntax Description**

- **all** clears all applicable unused auto-tunnel destinations.
- **tunnel-te id** clears an unused auto-tunnel destinations identified by a tunnel identifier.

**Command Default**

None

**Command Modes**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- **mpls-te execute**

**Examples**

This is sample output from the **clear mpls traffic-eng auto-tunnel mesh** command:

```
clear mpls traffic-eng auto-tunnel mesh
```
clear mpls traffic-eng counters auto-tunnel mesh

To clear all auto-tunnel mesh counters, use the `clear mpls traffic-eng counters auto-tunnel mesh` command in XR EXEC mode.

`clear mpls traffic-eng counters auto-tunnel mesh`

This command has no arguments or keywords.

**Command Default**
None

**Command Modes**
XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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>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 XR 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**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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 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
```
clear mpls traffic-eng counters global

To clear the internal MPLS-TE tunnel counters, use the **clear mpls traffic-eng counters global** command in XR EXEC mode.

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

### 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>6.2.1</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 ID</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 XR 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**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

<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 counters:

```
RP/0/RP0/CPU0:router# clear mpls traffic-eng counters signaling all
```
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 XR EXEC mode.

```
clear mpls traffic-eng counters {all | soft-preemption}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Clears counters for all MPLS-TE tunnels.</td>
</tr>
<tr>
<td>soft-preemption</td>
<td>Clears the statistics for soft preemption counters.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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
```
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 XR EXEC mode.

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

**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>6.2.1</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 ID</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
-------- --------- ----- -------- ---------------------- --------------
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 XR 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
XR EXEC mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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 ID</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 the MPLS-TE statistics for admission control:

```
RP/0/RP0/CPU0:router# clear mpls traffic-eng link-management statistics
```
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>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you enable the `collect-bw-only` command while the automatic bandwidth is already running on a tunnel, the bandwidth application is disabled from that moment. Before you enable the actual bandwidth application, you can get the status of the automatic bandwidth behavior.

If you disable the `collect-bw-only` command on a tunnel from which the automatic bandwidth is already running, the actual bandwidth application takes place on the tunnel at the next application period.

It is also possible to manually activate a bandwidth application regardless of the collect bandwidth only flag that is being specified on a tunnel. To activate the bandwidth application, use the `mpls traffic-eng auto-bw apply (MPLS-TE)`, on page 293 command in XR 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
```
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>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**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
```
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>6.2.1</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 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
```
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>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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 ID</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)#
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
```
**fast-reroute**

To enable fast-reroute (FRR) protection for an MPLS-TE tunnel, use the `fast-reroute` command in interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
fast-reroute
no fast-reroute
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

FRR is disabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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 RSP RP switchover before triggering FRR on standby RSPs RPs to synchronize with the active RSP RP (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**

```
<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 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
```
fast-reroute protect

To enable node and bandwidth protection for an MPLS-TE tunnel, use the `fast-reroute protect` command in interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
fast-reroute protect {bandwidth | node}
no fast-reroute protect
```

**Syntax Description**
- `bandwidth` Enables bandwidth protection request.
- `node` Enables node protection request.

**Command Default**
FRR is disabled.

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**
- mpls-te read, write

**Examples**
The following example shows how to enable bandwidth protection for a specified TE tunnel:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)#interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# fast-reroute protect bandwidth
```
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>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- 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**

- `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(config) # configure
RP/0/RP0/CPU0:router(config) # mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te) # fast-reroute timers promotion 600
```
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 6.2.1 This command was introduced.

**Usage Guidelines**
You can configure up to 16 flooding threshold values. The first value is mandatory; the next 15 are optional. When a threshold is crossed, MPLS-TE link management advertises updated link information. If no thresholds are crossed, changes can be flooded periodically unless periodic flooding was disabled.

**Task ID**
- **mpls-te** read, write

**Examples**
The following example shows how to set the reserved bandwidth threshold for the link for decreased resource availability (down) and for increased resource availability (up) thresholds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# interface HundredGigabitEthernet 0/0/0/3
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
```
forward-class

To define the forwarding path in the MPLS-TE interface, use the `forward-class` command in MPLS-TE configuration mode. To remove forward-class configuration, use the `no` form of this command.

```
forward-class  
no forward-class
```

<table>
<thead>
<tr>
<th>Command Default</th>
<th>No default behavior or values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>MPLS-TE configuration</td>
</tr>
<tr>
<td>Command History</td>
<td>Release 6.2.1 This command was introduced.</td>
</tr>
<tr>
<td>Task ID</td>
<td>mpls-te read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to define forwarding path in the MPLS-TE interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)#interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)#forward-class 1
```
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][include-ipv6]
no forwarding-adjacency [holdtime time][include-ipv6]
```

**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.
- **include-ipv6** (Optional) Announces the MPLS-TE tunnel as an IPv6 forwarding adjacency.

**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></td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.2.1</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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.

**Examples**

This example shows how to configure forwarding adjacency with a holdtime value of 60 milliseconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 888
RP/0/RP0/CPU0:router(config-if)# forwarding-adjacency holdtime 60
```
This example shows how to announce MPLS-TE tunnel as an IPv6 forwarding adjacency:

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#interface tunnel-te 65534
RP/0/RP0/CPU0:router(config-if)#forwarding-adjacency
RP/0/RP0/CPU0:router(config-if-tunte-fwdadj)#include-ipv6
```
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>6.2.1</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**
```
Task ID Operations ID
mpls-te read, write
```

**Examples**
The following example shows how to exclude address 192.168.3.2 at index 3 of the explicit path 200:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# explicit-path identifier 200
```
RP/0/RP0/CPU0:router(config-expl-path)# index 3 exclude-address ipv4 unicast 192.168.3.2
### 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.

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>index exclude-srlg ipv4 unicast IP address</td>
<td>Index number at which the path entry is inserted or modified. Range is 1 to 65535.</td>
</tr>
<tr>
<td>ipv4 unicast IP address</td>
<td>Specifies an IP address to get SRLG values from for exclusion.</td>
</tr>
<tr>
<td>exclude-srlg</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>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

No specific guidelines impact the use of this command.

#### 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**
- `index-id`: Index number at which the path entry is inserted or modified. Range is 1 to 65535.
- `ipv4 unicast IP-address`: Includes the IPv4 unicast address (strict address).
- `loose ipv4 unicast IP-address`: (Optional) Specifies the next unicast address in the path as a loose hop.
- `strict ipv4 unicast IP-address`: (Optional) Specifies the next unicast address in the path as a strict hop.

**Command Default**
No default behavior or values

**Command Modes**
Explicit path configuration

**Command History**
- Release 6.2.1: 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**
- mpls-te: read, write

**Examples**
The following example shows how to insert the `next-address` 192.168.3.2 at index 3 of the explicit path 200:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# explicit-path identifier 200
```
RP/0/RP0/CPU0:router(config-expl-path)# index 3 next-address ipv4 unicast 192.168.3.2
interface (MPLS-TE)

To enable MPLS-TE on an interface and to enter MPLS-TE interface configuration mode, use the `interface` command in XR Config mode. To return to the default behavior, use the `no` form of this command.

```plaintext
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
XR Config mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.2.1</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 RSP RP.

### 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:

```plaintext
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# interface HundredGigabitEthernet 0/0/0/3
```

The following example shows how to remove an interface from the MPLS-TE domain:

```plaintext
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 HundredGigabitEthernet 0/0/0/3
interface (SRLG)

To enable Shared Risk Link Groups (SRLGs) on an interface and to enter SRLG interface configuration mode, use the `interface` command in SRLG configuration mode. To return to the previous configuration mode, use the `no` form of this command.

```
interface type interface-path-id
no interface type interface-path-id
```

**Syntax Description**

- `type` Interface type. For more information, use the question mark (?) online help function.
- `interface-path-id` Physical interface or virtual interface.

**Note**

- Use the `show interfaces` command to see a list of all possible interfaces currently configured on the router.
- For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No default behavior or values

**Command Modes**

SRLG configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.2.1</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 enter SRLG interface configuration mode:

```
RP/0/RP0/CPU0:router (config)# srlg
RP/0/RP0/CPU0:router (config-srlg)# interface HundredGigabitEthernet 0/0/3
RP/0/RP0/CPU0:router (config-srlg-if)# value 10
RP/0/RP0/CPU0:router (config-srlg-if)# value 50
```
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**

XR Config mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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 RSP RP.

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.

**Examples**

The following example shows how to configure tunnel interface 1:

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

The following example shows how to set the tunnel-class attribute to map the correct traffic class to the tunnel:
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# policy-class 1
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>Parameter</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 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>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Tunnel-te is not signaled until an IP address is configured on the tunnel interface; therefore, the tunnel state stays down without IP address configuration.

Loopback is commonly used as the interface type.

**Task ID**

<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
```
ipv4 unnumbered mpls traffic-eng

To specify the Internet Protocol Version 4 (IPv4) address, use the `ipv4 unnumbered mpls traffic-eng` command in XR Config mode. To remove the IPv4 address, use the `no` form of this command.

**Syntax Description**

```
ipv4 unnumbered mpls traffic-eng  interface-path-id
no  ipv4 unnumbered mpls traffic-eng
```

- **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.

**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>6.2.1</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>network</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to specify unnumbered IPv4 address for a GigabitEthernet interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipv4 unnumbered mpls traffic-eng HundredGigabitEthernet 0/0/0/3
```

The following example shows how to specify unnumbered IPv4 address for an MPLS-TE tunnel with tunnel ID 200:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ipv4 unnumbered mpls traffic-eng tunnel-te 200
```
**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>holdtime</code></td>
<td>Number of seconds that bandwidth can be held. Range is 1 to 300. Default is 15.</td>
</tr>
</tbody>
</table>

**Command Default**

<table>
<thead>
<tr>
<th>Command</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>holdtime</code></td>
<td>15</td>
</tr>
</tbody>
</table>

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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/CP00:router# configure
RP/0/RP0/CP00:router(config)# mpls traffic-eng
RP/0/RP0/CP00:router(config-mpls-te)# link-management timers bandwidth-hold 10
```
**link-management timers periodic-flooding**

To set the length of the interval for periodic flooding, use the `link-management timers periodic-flooding` command in MPLS-TE configuration mode. To return to the default behavior, use the `no` form of this command.

```
link-management timers periodic-flooding interval
no link-management timers periodic-flooding
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></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>

<table>
<thead>
<tr>
<th>Command Default</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interval</code></td>
<td>180</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS-TE configuration</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The <code>link-management timers periodic-flooding</code> 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.</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Examples</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The following example shows how to set the interval length for periodic flooding to 120 seconds:</td>
<td></td>
</tr>
</tbody>
</table>

```
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
```
**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>bundle-capacity sec</td>
<td>Specifies the bundle-capacity preemption timer value in seconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS-TE configuration</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The value 0 as bundle-capacity value in the <code>link-management timers preemption-delay</code> command disables this timer. This means there is no delay before preemption sets in when the bundle capacity goes down.</td>
<td></td>
</tr>
</tbody>
</table>

<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
```
**load-share**

To determine load-sharing balancing parameters for a specified interface, use the `load-share` command in interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
load-share  value
no  load-share
```

**Syntax Description**

- `value` Load-share value, equivalent to the bandwidth in kbps (that is, the same value in configuration). Range is 1 to 4294967295. Default is 0.

**Command Default**

The default load-share for tunnels with no explicit configuration is the configured signalled bandwidth.

- `value`: 0 (if no value is assigned)

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Configuration schemas are supported for load balancing.

To enable the `load-share` command, you must enable unequal load balancing using the `load-share unequal` command.

**Task ID**

- `mpls-te` read, write

**Examples**

The following example shows how to configure load-sharing parameters on a specified interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 100
RP/0/RP0/CPU0:router(config-if)# load-share 100
```
**load-share unequal**

To configure unequal load-sharing for an MPLS-TE tunnel, use the `load-share unequal` command in MPLS-TE configuration mode. To return to the default behavior, use the `no` form of this command.

```markdown
load-share unequal
no load-share unequal
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

By default, unequal load-balancing is disabled and equal load-balancing occurs.

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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.

**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 unequal load-sharing:

```markdown
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# load-share unequal
```
**match mpls disposition**

To match Tag2IP packets while redirecting MPLS labeled packets to a new destination using PBR policy, use the `match mpls disposition` command in class-map configuration mode. To remove redirection of MPLS labeled packets, use the `no` form of this command.

```
match mpls disposition access-group \{ipv4 | ipv6\} access-list
no match mpls disposition access-group \{ipv4 | ipv6\} access-list
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>access-group</td>
<td>Specifies an access-group.</td>
</tr>
<tr>
<td>ipv4</td>
<td>ipv6</td>
</tr>
<tr>
<td>access-list</td>
<td>Specifies an access-list.</td>
</tr>
</tbody>
</table>

**Command Default**

Match is not set.

**Command Modes**

Class-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Only Tag2IP packets can be redirected.

**Task ID**

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

This example shows how to configure match MPLS disposition sequence for an IPv4 address:

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#class-map type traffic class_mpls_src_test
RP/0/RP0/CPU0:router(config-cmap)#match mpls disposition access-group ipv4 ACL_MPLS_SRC
RP/0/RP0/CPU0:router(config-cmap)#end-class-map
```
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>tunnels</code></td>
<td>Configures all tunnels for MPLS-TE.</td>
</tr>
<tr>
<td><code>tunnel-limit</code></td>
<td>Maximum number of tunnel TE interfaces. Range is 1 to 65536.</td>
</tr>
<tr>
<td><code>destinations</code></td>
<td>Configures all destinations for MPLS-TE.</td>
</tr>
<tr>
<td><code>dest-limit</code></td>
<td>Maximum total number of destinations that can be configured. Range is 1 to 65536.</td>
</tr>
</tbody>
</table>

**Command Default**

- `tunnel-limit`: 4096
- `dest-limit`: 4096

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.2.1</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 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
```
**mpls traffic-eng**

To enter MPLS-TE configuration mode, use the `mpls traffic-eng` command in XR Config mode.

**mpls traffic-eng**

**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>6.2.1</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 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 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 XR 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**

XR EXEC mode

**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>6.2.1</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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 command.
2. Trigger a manual bandwidth application by using the `mpls traffic-eng auto-bw apply` command.
3. Revert the minimum and maximum automatic bandwidth value back to their original value.

**Task ID**

<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 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 XR 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**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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 ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to initiate backup tunnel promote and assignment:

```
RP/0/RP0/CPU0:router# mpls traffic-eng fast-reroute promote
```
**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 XR Config mode. To return to the default behavior, use the `no` form of this command.

```
mpls traffic-eng level isis-level
no mpls traffic-eng level isis-level
```

**Syntax Description**

- `isis-level` IS-IS level (1, 2, or both) where MPLS-TE is enabled.

**Command Default**

No default behavior or values

**Command Modes**

XR Config mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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
```
**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 XR 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

XR EXEC mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If there is no change in the LSA since last flooding, IGP may dampen the advertisement.

### 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 initiate flooding of the local MPLS-TE links:

```
RP/0/RP0/CPU0:router#  mpls traffic-eng link-management flood
```
mpls traffic-eng path-protection switchover tunnel-te

To force a manual switchover for path-protected tunnel, use the `mpls traffic-eng path-protection switchover tunnel-te` command in XR EXEC mode. To disable this feature, use the `no` form of this command.

```
mpls traffic-eng path-protection switchover tunnel-te  tunnel ID
no mpls traffic-eng path-protection switchover tunnel-te  tunnel ID
```

**Syntax Description**

| `tunnel ID`     | Tunnel identifier of the P2P tunnel for the path protection switchover. Range is from 0 to 65535. |

**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>6.2.1</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 ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

The following example configures the switchover for path-protection for tunnel-te:

```
RP/0/RP0/CPU0:router# mpls traffic-eng path-protection switchover tunnel-te 8
```
**mpls traffic-eng reoptimize (EXEC)**

To trigger the reoptimization interval of all TE tunnels, use the `mpls traffic-eng reoptimize` command in XR EXEC mode.

```
mpls traffic-eng reoptimize [tunnel-id] [tunnel-name] [all] [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.
- `all` (Optional) Forces an immediate reoptimization for all tunnels.
- `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**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- `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 reoptimize events link-up**

To turn on automatic reoptimization of Multiprotocol Label Switching (MPLS) traffic engineering when certain events occur, such as, when an interface becomes operational, use the `mpls traffic-eng reoptimize events link-up` command in XR Config mode. To disable automatic reoptimization when link-up event occurs, use the `no` form of this command.

```plaintext
mpls traffic-eng reoptimize events link-up
no mpls traffic-eng reoptimize events link-up
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

XR Config mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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 turn on automatic reoptimization when an interface becomes operational:

```plaintext
RP/0/RP0/CP00:router# mpls traffic-eng reoptimize events link-up
```
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>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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.

We suggest that you configure the `mpls traffic-eng router-id` command explicitly under the IGP; otherwise, TE uses the default algorithm to pick up the TE router-id, which can be the highest IP address of the loopback interfaces or physical interfaces.

A TE router-id configuration is highly recommended to ensure that the tunnel head-end picks up the correct source address, and the configured static RPF address at the tail-end matches the tunnel source which avoids unexpected traffic drops.
### 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 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
```
# mpls traffic-eng reoptimize mesh group

To reoptimize all tunnels of a mesh group, use the `mpls traffic-eng reoptimize mesh group` command in XR EXEC mode.

```
mpls traffic-eng reoptimize auto-tunnel mesh group group_id
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>group_id</code></td>
<td>Defines auto-tunnel mesh group ID that is to be reoptimized. Range is 0 to 4294967295.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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 ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls-te</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

This is sample out from the `mpls traffic-eng reoptimize mesh group` command:

```
RP/0/RP0/CPU0:router mpls traffic-eng reoptimize mesh group 10
```
mpls traffic-eng srlg

To enter MPLS-TE SRLG configuration mode, use the `mpls traffic-eng srlg` command in XR Config mode. To delete all the SRLG values and mapping configured under traffic engineering, use the `no` form of this command. To enter MPLS-TE SRLG value configuration submode, use the `mpls traffic-eng srlg value srlg` command in the MPLS TE SRLG configuration mode. To delete all the SRLG values configured, use the `no` form of this command. To specify administrative weight associated with an SRLG value, use the `admin-weight` keyword in the MPLS TE SRLG value configuration submode.

`mpls traffic-eng srlg {admin-weight weight | value srlg value} ipv4 address ip-address next-hop ipv4 address next-hop-ip-address`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>admin-weight weight</code></td>
<td>Value added to link admin-weight during SRLG-aware path computation. Range is 0 to 4294967295.</td>
</tr>
<tr>
<td><code>value srlg-value</code></td>
<td>SRLG value. Range is 0 to 4294967295.</td>
</tr>
<tr>
<td><code>static</code></td>
<td>Assign SRLG to topology link based on IP address.</td>
</tr>
<tr>
<td><code>ipv4 address ip-address next-hop ipv4 address next-hop-ip-address</code></td>
<td>Assign IP address of the local end-point and next-hop address of the link.</td>
</tr>
</tbody>
</table>

**Command Default**
The default value for `admin-weight` keyword is 1.

**Command Modes**
XR Config mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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 enter MPLS-TE SRLG configuration mode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng srlg
RP/0/RP0/CPU0:router(config-mpls-te-srlg)#
```

The following example shows how to enter MPLS-TE SRLG value configuration submode:
The following example shows how to specify admin-weight in the MPLS-TE SRLG value configuration submode:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng srlg value 150
RP/0/RP0/CPU0:router(config-mpls-te-srlg)# admin-weight 10
```
nhop-only (auto-tunnel backup)

To configure only a next-hop automatic backup tunnel with only link protection, use the `nhop-only` command in MPLS-TE auto-tunnel backup interface configuration mode. To return to the default configuration setting for automatic backup tunnels, use the `no` form of this command.

```
nhop-only
no nhop-only
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Both NHOP and NNHOP protection are enabled.

**Command Modes**

Auto-tunnel backup configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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 HundredGigE 0/0/0/3
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
```
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

<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 tunnel overflow detection for tunnel-te 1:

RP/0/RP0/CPU0:router# configure
overflow threshold (MPLS-TE)

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.

```
path-option preference-priority [protecting number] {dynamic | explicit {name path-name | identifier path-number} [protected-by path-option-level]} [attribute-set name] [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.
- `protecting number`: Specifies a path setup option to protect a path. The range is from 1 to 1000.
- `dynamic`: Specifies that label switched paths (LSP) are dynamically calculated.
- `explicit`: Specifies that LSP paths are IP explicit paths.
- `name path-name`: Specifies the path name of the IP explicit path.
- `identifier path-number`: Specifies a path number of the IP explicit path.
- `protected-by path-option-level`: (Optional) Configures path protection for an explicit path that is protected by another 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>6.2.1</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).

The `protecting` keyword specifies that you can configure path-protection for the primary LSP. The `protecting` keyword is available only for tunnel-gte interfaces.

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.

The `dynamic` keyword is required to configure path-protection.

Any primary explicit path on a path protection enabled tunnel can be configured to be protected by an explicit path option level using `protected-by` keyword. Only one explicit protecting path is supported per path option.

Examples

The following example shows how to configure the tunnel to use a named IPv4 explicit path as verbatim and lockdown options for the tunnel. This tunnel cannot reoptimize when the FRR event goes away, unless you manually reoptimize it:

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

The following example shows how to enable path protection on a tunnel to configure an explicit path:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# path-option 1 explicit name po4
RP/0/RP0/CPU0:router(config-if)# path-option protecting 1 explicit name po6
```

The following example shows how to limit CSPF to a single OSPF instance and area:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# path-option 1 explicit name router1 ospf 3 area 7 verbatim
```

The following example shows how to limit CSPF to a single IS-IS instance and area:
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# path-option 1 dynamic isis mtbf level 1 lockdown
path-protection (MPLS-TE)

To enable path protection for a tunnel interface, use the `path-protection` command in interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
path-protection
no path-protection
```

**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>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Although not as fast as a link or node protection, presignaling a secondary Labeled Switch Path (LSP) is faster than configuring a secondary path option or allowing the tunnel's source router to dynamically recalculate a path. The actual recovery time is topology-dependent, and is affected by delay factors such as propagation delay and switch fabric latency.

**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 path protection for the tunnel-te interface type:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# path-protection
```
**path-protection timers reopt-after-switchover**

To configure the time to wait after a switchover occurs on a tunnel before a reoptimization is attempted for the tunnel, use the `path-protection timers reopt-after-switchover` command in MPLS-TE configuration mode. To disable this feature, use the `no` form of this command.

```
path-protection timers reopt-after-switchover  seconds
no    path-protection timers reopt-after-switchover  seconds
```

**Syntax Description**

- `seconds` Time, in seconds, between path-protection event and tunnel reoptimization. Range is from 0 to 604800.

**Command Default**

`seconds`: 180 (3 minutes)

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is used as a triggered reoptimization, which allows a tunnel to reoptimize to a better path than the standby path after the switchover. This option is used as a one time reoptimization.

**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 adjust the number of seconds between when a path-protection switchover is effected on a tunnel head to when reoptimization is performed on the tunnel:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# path-protection timers reopt-after-switchover 180
```
path-selection cost-limit

To set the upper limit on the path aggregate admin-weight when computing paths for MPLS-TE LSPs, use the path-selection cost-limit command in an appropriate configuration mode. To remove the upper limit, use the no form of this command.

```
path-selection cost-limit cost-limit-value
```

**Syntax Description**

| cost-limit-value | Configures the path-selection cost-limit value. The range is from 1 to 4294967295. |

**Command Default**

The cost-limit is ignored.

**Command Modes**

- XR Config mode
  - Interface tunnel TE configuration
  - MPLS TE path-option attribute set configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Path-selection cost-limit configuration works only on MPLS TE tunnels. The cost-limit configured under path-option attribute-set configuration mode takes priority and will be in effect if the cost-limit is configured under global configuration, interface tunnel TE, and path-option attribute-set configuration modes. The cost-limit is ignored by default.

A LSP is created only if its path aggregate admin-weight is less than the specified path cost limit.

**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 cost-limit for under MPLS TE path-option attribute-set `PO3AttrSet`.

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)#attribute-set path-option PO3AttrSet
RP/0/RP0/CPU0:router(config-te-attribute-set)#path-selection cost-limit 50000
```
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**

This command has no arguments or keywords.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>head</td>
<td>The tunnel stays up if <code>set-overload-bit</code> is set by ISIS on the head router. Ignores overload node during CSPF for the head node.</td>
</tr>
<tr>
<td>mid</td>
<td>The tunnel stays up if <code>set-overload-bit</code> is set by ISIS on the mid router. Ignores overload node during CSPF for the mid node.</td>
</tr>
<tr>
<td>tail</td>
<td>The tunnel stays up if <code>set-overload-bit</code> is set by ISIS on the tail router. Ignores overload node during CSPF for the tail node.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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 ID</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/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# path-selection ignore overload
```
path-selection ignore overload (MPLS-TE)

RP/0/RP0/CPU0:router(config-mpls-te)# path-selection ignore overload head
path-selection loose-expansion affinity (MPLS-TE)

To specify the affinity value to be used to expand a path to the next loose hop for a tunnel on an area border router, use the **path-selection loose-expansion affinity** command in MPLS-TE configuration mode. To return to the default behavior, use the **no** form of this command.

```
path-selection loose-expansion affinity affinity-value mask affinity-mask [class-type type]
no path-selection loose-expansion affinity affinity-value mask affinity-mask [class-type type]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>affinity-value</td>
<td>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.</td>
</tr>
<tr>
<td>mask affinity-mask</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>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**

- **affinity-value**: 0X00000000
- **mask-value**: 0XFFFFFFFF

**Command Modes**

MPLS-TE configuration

**Command History**

- **Release**: 6.2.1
- **Modification**: This command was introduced.

**Usage Guidelines**

The new affinity scheme (based on names) is not supported for loose-hop expansion. New configuration does not affect the already up tunnels.

**Examples**

The following example shows how to configure affinity 0x55 with mask 0xFFFFFFFF:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# path-selection loose-expansion affinity 55 mask FFFFFFFF
```
**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]
nopath-selection loose-expansion metric {igp | te} [class-type type]
```

**Syntax Description**
- `igp` Configures an Interior Gateway Protocol (IGP) metric.
- `te` Configures a TE metric. This is the default.
- `class-type type` (Optional) Requests the class type of the tunnel bandwidth. Range is 0 to 1.

**Command Default**
The default is TE metric.

**Command Modes**
MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
New configurations do not affect tunnels that are already up.

**Task ID**
- 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)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# path-selection loose-expansion metric igp
```
**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>6.2.1</td>
<td>This command was introduced.</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 specify a metric type for the tunnel, 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)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# path-selection metric igp
```
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>6.2.1</td>
<td>This command was introduced.</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.

**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
```
policy-class

To configure policy-based tunnel selection (PBTS) to direct traffic into specific TE tunnels, use the **policy-class** command in interface configuration mode. To disable this feature, use the **no** form of this command.

Multiple EXP values can be specified as part of a policy-class, separated by spaces. The EXP values configured to a TE tunnel effectively form a monolithic policy-class, which should not overlap with other policy-classes. Once an EXP value is used in a policy-class configuration, it can only be reused if the subsequent policy-class configurations containing that EXP value are identical. For example, if the configuration **policy-class 1 2 3** is applied to one or more tunnels, configurations such as **policy-class 1, policy-class 2 3, or policy-class 3 4 5** become invalid.

```
policy-class {1 - 7 | default}
no policy-class
```

**Syntax Description**

- **1 - 7**: Policy-class attribute to map the correct traffic class to this policy. Multiple EXP values can be specified, separated by spaces.
- **default**: Default tunnel policy class.

**Command Default**

The lowest class tunnels are assigned to carry default traffic only if no default tunnel is available for forwarding.

**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>6.2.1</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **policy-class** command to enable policy-based tunnel selection (PBTS). See *Cisco IOS XR MPLS Configuration Guide for the Cisco CRS-1 Router* for more information on PBTS.

To display the configured PBTS policy-class value, use the **show mpls traffic-eng tunnels** command.

To display information about PBTS configuration, use the **show cef** and **show cef hardware** commands in *Cisco IOS XR IP Addresses and Services Command Reference for the Cisco XR 12000 Series Router*.

**Examples**

The following example shows how to configure a policy class:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
```
The following example shows how to configure a policy-class that maps to multiple traffic classes:

```
RP/0/RP0/CPU0:router(config-if)# policy-class 7
```

The following example shows how to configure a default policy-class tunnel:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# policy-class default
RP/0/RP0/CPU0:router(config-if)# commit
```
priority (MPLS-TE)

To configure the setup and reservation priority for an MPLS-TE tunnel, use the `priority` command in interface configuration mode. To return to the default behavior, use the `no` form of this command.

```
priority setup-priority hold-priority
no priority setup-priority hold-priority
```

**Syntax Description**

- **setup-priority**: Priority used when signaling a label switched path (LSP) for this tunnel to determine which existing tunnels can be preempted. Range is 0 to 7 (in which a lower number indicates a higher priority). Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non-0 priority.

- **hold-priority**: Priority associated with an LSP for this tunnel to determine if it should be preempted by other LSPs that are being signaled. Range is 0 to 7 (in which a lower number indicates a higher priority).

**Command Default**

```
setup-priority: 7
hold-priority: 7
```

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

**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 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
```
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>Release</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.2.1</td>
<td></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**

```
read, write
```

**Examples**

The following example shows how to enable record-route on the TE tunnel:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# record-route
```
**redirect default-route nexthop**

To configure multi nexthop tracking on default-route on a VRF for IPv4 or IPv6 address family, use the `redirect default-route nexthop` command in policy-map class type configuration mode.

```
redirect {ipv4 | ipv6} default-route nexthop
    [vrf vrf-name] [{v4v6}] nexthop [vrf vrf-name] [{v4v6}] nexthop [vrf vrf-name] [{v4v6}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>ipv6</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>Specifies the VRF name for nexthop.</td>
</tr>
<tr>
<td>v4</td>
<td>Specifies IPv4 nexthop address in A.B.C.D format.</td>
</tr>
<tr>
<td>v6</td>
<td>Specifies IPv6 nexthop address in X:X::X%zone format.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

Policy-map class type configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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>qos</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

The following example shows how to configure multi nexthop tracking on default-route on a VRF for IPv4:

```
RP/0/RSP0/CPU0:Router# config
RP/0/RSP0/CPU0:Router(config)# policy-map type pbr kmd
RP/0/RSP0/CPU0:Router(config-pmap)# class type traffic acl
RP/0/RSP0/CPU0:Router(config-pmap-c)# redirect ipv4 default-route nexthop vrf vpn1 3.2.1.2
    nexthop vrf vpn2 3.2.3.2 nexthop vrf vpn3 3.2.4.2
```
redirect nexthop

To configure multi nexthop tracking on a VRF for IPv4 or IPv6 address family, use the `redirect nexthop` command in policy-map class type configuration mode.

```
redirect {ipv4 | ipv6} nexthop
        [vrf  vrf-name] [{v4 v6}] nexthop [vrf  vrf-name] [{v4 v6}] nexthop [vrf  vrf-name] [{v4 v6}]
```

**Syntax Description**

- `ipv4 | ipv6`: Specifies IPv4 or IPv6 address family.
- `vrf vrf-name`: Specifies the VRF name for nexthop.
- `v4`: Specifies IPv4 nexthop address in A.B.C.D format.
- `v6`: Specifies IPv6 nexthop address in X:X::X%zone format.

**Command Default**

No default behavior or values

**Command Modes**

Policy-map class type configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A maximum number of three nexthops can be configured. The first nexthop configured has the highest priority as compared to the last nexthop, which has the least priority. The nexthops configured must be either IPv4 or IPv6. Either a VRF name or an IPv4/IPv6 address, or both can be configured for a given nexthop. When VRF is not configured, it is presumed to be ingress interface VRF.

**Task ID**

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

**Example**

The following example shows how to configure multi nexthop tracking on a VRF for IPv4:

```
RP/0/RSP0/CPU0:Router# config
RP/0/RSP0/CPU0:Router(config)# policy-map type pbr kmd
RP/0/RSP0/CPU0:Router(config-pmap)# class type traffic acl
RP/0/RSP0/CPU0:Router(config-pmap-c)# redirect ipv4 nexthop vrf vpn1 3.2.1.2 nexthop vrf vpn2 3.2.3.2 nexthop vrf vpn3 3.2.4.2
```
**reoptimize (MPLS-TE)**

To force the reoptimization interval for all TE tunnels, use the `reoptimize` command in MPLS-TE configuration mode. To return to the default behavior, use the `no` form of this command.

```
reoptimize frequency
no reoptimize frequency
```

**Syntax Description**

- `frequency` Timer frequency range, in seconds. Range is from 0 to 604800.

  **Note:**
  - A value of 0 disables periodic reoptimization.
  - Any value in the range from 1 to 60 results in periodic reoptimization that occurs every 60 seconds.

  **Command Default**
  
  `frequency`: 3600

  **Command Modes**
  
  MPLS-TE configuration

  **Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.2.1</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 force the reoptimization interval to 60 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 60
  ```
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>Parameter</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 from 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`
**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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.

**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
```
route-priority

To enable users to adjust the route-priority given to TE labels into the data plane, compared to labels and route updates from other protocols, use the route-priority command in MPLS-TE configuration mode. To return to the default behavior, use the no form of this command.

```
route-priority role {middle | head {primary | backup}} queue queue
no route-priority role {middle | head {primary | backup}}
```

**Syntax Description**

<table>
<thead>
<tr>
<th><strong>role</strong></th>
<th>Defines the role of the tunnel to which the label belongs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>middle</td>
<td>A tunnel mid-point.</td>
</tr>
<tr>
<td>head backup</td>
<td>A tunnel head which is assigned as a FRR backup to an interface.</td>
</tr>
<tr>
<td>head primary</td>
<td>All other tunnel heads.</td>
</tr>
<tr>
<td>queue</td>
<td>Defines the queue number. Range is from 0 to 12 inclusive; lower values represent higher priority queues.</td>
</tr>
</tbody>
</table>

**Command Default**

- head backup: 9
- head primary: 10
- middle: 10

**Command Modes**

MPLS-TE configuration

**Command History**

<table>
<thead>
<tr>
<th><strong>Release</strong></th>
<th><strong>Modification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to change the priority given to TE labels when updates to the forwarding plane are made from the control plane.

The priority values used by other applications are:

- 0 - Unused
- 1 - Unused
- 2 - RIB/LDP (Critical)
- 3 - Unused
- 4 - Unused
- 5 - RIB/LDP (High)
The default prioritization of label updates from the control plane to the forwarding plane has been carefully chosen to avoid traffic loss under both normal operation and high system load, and to balance the needs of the various features that employ label switching. Changing these defaults may cause unpredictable behavior including traffic loss, especially when the router is experiencing high load. Use of this command is not recommended without proper understanding of its effects and possible side-effects.

**Caution**

**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 route-priority:

```
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# route-priority role middle queue 7
```
**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>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the `router-id secondary` command on tail end nodes to terminate verbatim tunnels to secondary TE RIDs as destinations.

You can configure up to 32 IPv4 addresses as TE secondary router IDs.

**Task ID**
- **Task ID**
  - mpls-te read, write

**Examples**
The following example shows how to configure a secondary TE router identifier in MPLS-TE:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# router-id secondary 1.1.1.1
RP/0/RP0/CPU0:router(config-mpls-te)# router-id secondary 2.2.2.2
```
set destination-address

To set destination address while redirecting Tag2IP MPLS labeled packets using PBR policy, use the set destination-address command in policy map class type configuration mode. To remove this configuration, use the no form of this command.

```
set destination-address {ipv4 | ipv6} ip-address
no set destination-address {ipv4 | ipv6} ip-address
```

**Syntax Description**
- `ipv4 | ipv6` Specifies IPv4 or IPv6 address format.
- `ip-address` Specifies the IPv4 or IPv6 address.

**Command Default**
Destination IP address is not set.

**Command Modes**
Policy-map class type Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Only Tag2IP packets redirection is supported.

**Task ID**

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

This example shows how to set an IPv4 address as the redirect destination address:

```
RP/0/0/CPU0:ios#configure
RP/0/0/CPU0:ios(config)#policy-map type pbr pbr_prec_exp
RP/0/0/CPU0:ios(config-pmap)#class type traffic class_prec_exp
RP/0/0/CPU0:ios(config-pmap-c)#set destination-address ipv4 3.3.3.3
```
**set ipv4 df**

To set or clear the do not fragment (df) bit policy before forwarding the packet in IPv4 traffic, use the `set ipv4 df` command in Policy-map configuration mode. To disable setting or clearing the df bit, use the `no` form of this command.

```
set ipv4 df df-value
```

**Syntax Description**

- **df-value**: Specifies the df bit value. Range is from 1 to 7.

**Command Default**

Set df bit policy is disabled.

**Command Modes**

Policy-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.2.1</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>qos</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows how to set the IPv4 df bit policy value as 1:

```
RP/0/RP0/CPU0:router(config-pmap-c)# set ipv4 df 1
```
set source-address

To set source address while redirecting Tag2IP MPLS labeled packets using PBR policy, use the set source-address command in policy map class type configuration mode. To remove this configuration, use the no form of this command.

```
set source-address {ipv4 | ipv6} ip-address
```

**Syntax Description**

- `ipv4 | ipv6`: Specifies IPv4 or IPv6 address format.
- `ip-address`: Specifies the IPv4 or IPv6 address.

**Command Default**

No default behavior or values

**Command Modes**

Policy-map class type Configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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>qos</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to set an IPv4 address as the source address:

```
RP/0/0/CPU0:ios#configure
RP/0/0/CPU0:ios(config)#policy-map type pbr pbr_prec_exp
RP/0/0/CPU0:ios(config-pmap)#class type traffic class_prec_exp
RP/0/0/CPU0:ios(config-pmap-c)#set source-address ipv4 1.1.1.1
```
show explicit-paths

To display the configured IP explicit paths, use the `show explicit-paths` command in XR 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**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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.

**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 45: 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: next-address</td>
<td>First IP address in the path.</td>
</tr>
<tr>
<td>2: next-address</td>
<td>Second IP address in the path.</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
```
show interfaces tunnel-te accounting

To display IPv4 and IPv6 statistics for MPLS traffic engineering (TE) tunnels, use the `show interfaces tunnel-te accounting` command in XR EXEC mode.

`show interfaces tunnel-te tunnel-number accounting [{location location-id | rates}]`

**Syntax Description**

- `tunnel-number`: Specifies TE tunnel number. Range is from 0 to 6553.
- `location location-id`: Specifies fully qualified location of the TE tunnel.
- `rates`: Displays interface accounting rates.

**Command Default**

None

**Command Modes**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

- `mpls-te read`

This example displays accounting information from tunnel-te interface 1:

```
RP/0/RP0/CPU0:router#show interface tunnel-te 1 accounting

<table>
<thead>
<tr>
<th>tunnel-te1</th>
<th>Protocol</th>
<th>Pkts In</th>
<th>Chars In</th>
<th>Pkts Out</th>
<th>Chars Out</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IPV4_UNICAST</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>520</td>
</tr>
<tr>
<td></td>
<td>IPV6_UNICAST</td>
<td>0</td>
<td>0</td>
<td>15</td>
<td>1560</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 XR EXEC mode.

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

**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></td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>6.2.1</td>
<td></td>
</tr>
</tbody>
</table>

**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**

<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 affinity-map command:

```plaintext
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>bcdedefghabcdefghabcdefghabcdefgh</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>cdefghabcdefghabcdefghabcdefghabcdefgh</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>
</tbody>
</table>
```
Table 46: show mpls traffic-eng affinity-map Field Descriptions, on page 340 describes the significant fields shown in the display.

Table 46: show mpls traffic-eng affinity-map Field Descriptions

<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>
show mpls traffic-eng attribute-set

To display the attribute set for MPLS-TE, use the `show mpls traffic-eng attribute-set` command in XR EXEC mode.

```
show mpls traffic-eng attribute-set [{auto-backup | auto-mesh | path-option | xro[attribute-set-name]}]
```

<table>
<thead>
<tr>
<th>Syntax Description</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>xro</td>
<td>Displays information for the XRO 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  | XR EXEC mode |

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

| Usage Guidelines | To use this command, first enable the MPLS-TE application. |

<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: 0x0/0xffffffff (Default)  
  Priority: 7 7 (Default)  
  Record-route: Enabled  
  Policy-class: 0 (Not configured)  
  Logging: None  
  List of protected interfaces (count 0)  
  List of tunnel IDs (count 0)
The following command shows the attribute set for auto-mesh attribute type.

```
RP/0/RP0/CPU0:router# show mpls traffic-eng attribute-set auto-mesh mesh1
```

Attribute Set Name: mesh1 (Type: auto-mesh)
Bandwidth: 0 kbps (CT0) (Default)
Affinity: 0x0/0xffff (Default)
Priority: 7 7 (Default)
Interface Bandwidth: 0 kbps (Default)
AutoRoute Announce: Disabled
Auto-bw: Disabled
Soft Preemption: Disabled
Fast Reroute: Disabled, Protection Desired: None
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)

The following command shows the attribute set for xro.

```
RP/0/RP0/CPU0:router# show mpls traffic-eng attribute-set xro
```

Attribute Set Name: foo (Type: XRO)
Number of XRO constraints : 2
  LSP, best-effort, LSP-id used
    Specified by FEC: tunnel-id 55, LSP-id 88, ext. id 10.10.10.10
    source 10.10.10.10, destination 20.20.20.20
  LSP, strict, LSP-id ignored
    Specified by FEC: tunnel-id 3, LSP-id 0, ext. id 1.1.1.1
    source 1.1.1.1, destination 2.2.2.2
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 XR EXEC mode.

```
show mpls traffic-eng autoroute  [name  tunnel-name][IP-address]
```

**Syntax Description**

- **IP-address**: (Optional) Tunnel leading to this address.
- **name tunnel-name**: Specifies a tunnel by name.

**Command Default**

None

**Command Modes**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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**

- **mpls-te**: read

**Examples**

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

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

Destination 103.0.0.3 has 2 tunnels in OSPF 0 area 0
tunnel-te1 (traffic share 1, nexthop 103.0.0.3)
tunnel-te2 (traffic share 1, nexthop 103.0.0.3)
```

This table describes the significant fields shown in the display.

<table>
<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. 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.</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>

This sample output displays *Signalled-Name* information:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng autoroute
Destination 192.168.0.4 has 1 tunnels in OSPF ring area 0
tunnel-te1 (traffic share 0, nexthop 192.168.0.4)
Signalled-Name: rtrA_t1
```

This sample output displays IS-IS autoroute information:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng autoroute
Destination 192.168.0.1 has 1 tunnels in IS-IS ring level 1
tunnel-te1 (traffic share 0, nexthop 192.168.0.1)
(IS-IS ring level-1, IPV4 Unicast)
(IS-IS ring level-1, IPV6 Unicast)
```
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 XR EXEC mode.

```
show mpls traffic-eng auto-tunnel {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**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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</td>
</tr>
</tbody>
</table>

**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>Removed (in use)</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</th>
<th>State</th>
<th>Protection</th>
<th>Prot. Flows*</th>
<th>Interface</th>
<th>Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel-te2000</td>
<td>up NHOP</td>
<td>------------</td>
<td>--------------</td>
<td>-----------</td>
<td>------</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/CPU0:router#show mpls traffic-eng auto-tunnel mesh

Auto-tunnel Mesh Global Configuration:
  Unused removal timeout: 2h
  Configured tunnel number range: 10000-12000

Auto-tunnel Mesh Groups Summary:
  Mesh Groups count: 5
  Mesh Groups Destinations count: 50

Mesh Group 40 (2 Destinations, 1 Up, 1 Down):
  Destination-list: dl-40
  Attribute-set: ta_name
  Destination: 40.40.40.40, tunnel-id: 10000, State: Up
  Destination: 10.10.10.10, tunnel-id: 10001, State: Down

Mesh Group 41 (3 Destinations, 2 Up, 1 Down):
  Destination-list: dl-40
  Attribute-set: ta_name
  Destination: 4.4.4.4, tunnel-id: 10005, State: Up
  Destination: 3.3.3.3, tunnel-id: 10006, State: Up
  Destination: 1.1.1.1, tunnel-id: 10007, State: Down

Mesh Group 51 (0 Destinations, 0 Up, 0 Down):
  Destination-list: Not configured
  Attribute-set: Not configured

Mesh Group 52 (0 Destinations, 0 Up, 0 Down):
  Destination-list: NAME1 (Not defined)
  Attribute-set: NAME2 (Not defined)

Mesh Group 53 (2 Destinations, 1 Up, 1 Down):
  Destination-list: dl-53
  Attribute-set: Not configured
  Destination: 40.40.40.40, tunnel-id: 10000, State: Up
  Destination: 10.10.10.10, tunnel-id: 10001, State: Down

Cumulative Counters (last cleared 7h ago):

<table>
<thead>
<tr>
<th></th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>100</td>
</tr>
<tr>
<td>Connected</td>
<td>50</td>
</tr>
<tr>
<td>Removed (unused)</td>
<td>50</td>
</tr>
</tbody>
</table>
```
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 XR 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.
- **onehop**: Displays onehop enabled mesh groups.

### Command Default
None

### Command Modes
XR EXEC mode

### Command History

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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</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.

This destination-list configuration is mandatory. If there is no IPv4 prefix-list by this name on the router, this mesh group create tunnels with all routers in the network.

This sample output displays information about one-hop tunnels:

RP/0/RP0/CPU0:router#show mpls traffic-eng auto-tunnel mesh onehop

Auto-tunnel Mesh Onehop Groups Summary:
  Mesh Groups count: 1
  Mesh Groups Destinations count: 2
  Mesh Groups Tunnels count:
    2 created, 2 up, 0 down, 0 FRR enabled

Mesh Group: 25 (2 Destinations) Onehop
Status: Enabled
Attribute-set: Not configured
Destination-list: dest_list (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>10.10.10.2</td>
<td>3500</td>
<td>up</td>
<td>Not running</td>
</tr>
<tr>
<td>11.11.11.2</td>
<td>3501</td>
<td>up</td>
<td>Not running</td>
</tr>
</tbody>
</table>

Displayed 2 tunnels, 2 up, 0 down, 0 FRR enabled

Auto-mesh Onehop Cumulative Counters:
Total
Created:       2
Connected:     2
Removed (unused): 0
Removed (in use): 0
Range exceeded: 0
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 XR 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**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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 ID</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
  Last start time: 26/08/2009 18:59:20
  Last stop time: 26/08/2009 19:03:19
  Last expiry time: 19/08/2009 18:12:39
```
Timer Name: [LSD Restart] Index:[4]
Duration: [60] Is running: NO
Last start time: 19/08/2009 17:44:26
Last stop time: 19/08/2009 17:44:26
Last expiry time: Never expired

Timer Name: [LSD Recovery] Index:[5]
Duration: [600] Is running: NO
Last start time: 19/08/2009 17:44:26
Last stop time: Never Stopped
Last expiry time: 19/08/2009 17:53:44

Timer Name: [Clearing in progress BW for the whole topology] Index:[6]
Duration: [60] Is running: YES
Last start time: 02/09/2009 11:57:50
Last stop time: Never Stopped
Last expiry time: 02/09/2009 11:57:50

This table describes the significant fields shown in the display.

<table>
<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 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 XR EXEC mode.

```
show mpls traffic-eng counters signaling
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</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 tunnel-name</td>
<td>Displays statistics for a specified tunnel.</td>
</tr>
<tr>
<td>summary</td>
<td>Displays a summary of signaling statistics.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.
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>Recv</th>
<th>Xmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>PathCreate</td>
<td>1</td>
<td>1</td>
<td>1</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>18</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BackupAssign</td>
<td>0</td>
<td>1</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 100.0.0.4
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>1</td>
<td>1</td>
<td>1</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>18</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BackupAssign</td>
<td>0</td>
<td>1</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: 100.0.0.4
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>1</td>
<td>1</td>
<td>1</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>1</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>
</tbody>
</table>
```
This table describes the significant fields shown in the display.

**Table 49: 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

This is sample output from the `show mpls traffic-eng counters signaling all` command that displays the `Signalled-Name` information:

```plaintext
RP/0/RP0/CPU0:router# show mpls traffic-eng counters signaling all
Tunnel Head: tunnel-te1
Signalled-Name: rtrA_t1
Cumulative Tunnel Counters:

<table>
<thead>
<tr>
<th>Signalling Events</th>
<th></th>
<th>Signalling Events</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Recv</td>
<td>Xmit</td>
<td></td>
</tr>
<tr>
<td>PathCreate</td>
<td>2</td>
<td>2</td>
<td>ResvCreate</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 XR EXEC mode.

```
show mpls traffic-eng forwarding [backup-name tunnel-name] [source source-address][tunnel-id tunnel-id] [interface {in | inout | out} type interface-path-id][{p2p}] {p2p} [detail]
```

<table>
<thead>
<tr>
<th>Syntax Description</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>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 tunnel-id 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>
</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>in</th>
<th>Displays information for the input interface.</th>
</tr>
</thead>
<tbody>
<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** XR EXEC mode
This command was introduced in Release 6.2.1.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID Operations ID

mpls-te read

Examples

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

```
RP/0/RP0/CPU0:router# show mpls traffic-eng forwarding
Tue Sep 15 14:22:39.609 UTC P2P tunnels

Tunnel ID Ingress IF Egress IF In lbl Out lbl
Backup tunnel
---------------------- ------------ ------------ -------- --------
2.2.2.2 2_2 HundredGigE0/0/0/3 HundredGigE0/0/0/4 16004 16020
unknown
6.6.6.6 1_23 tt1300 HundredGigE0/0/0/4 16000 3
tt1300
6.6.6.6 1100_9 unknown HundredGigE0/0/0/3 16002 16001
unknown
6.6.6.6 1200_9 unknown HundredGigE0/0/0/3 16001 16000
unknown
6.6.6.6 1300_2 unknown HundredGigE0/0/0/3 16005 16021
unknown
6.6.6.6 1400_9 unknown HundredGigE0/0/0/3 16003 16002
unknown

This table describes the significant fields shown in the display.

**Table 50: 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 XR EXEC mode.

show mpls traffic-eng forwarding-adjacency [IP-address]

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-address</td>
<td>(Optional) Destination IPv4 address for forwarding adjacency.</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>6.2.1</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 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)
```

This sample output displays information on IPv6 autoroute forwarding adjacency information for IS-IS IGP:

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

destination 3.3.3.3 has 1 tunnels
tunnel-te10  (traffic share 0, next-hop 3.3.3.3)
            (Adjacency Announced: yes, holdtime 0)
            (IS-IS 100, IPv4 unicast)
            (IS-IS 100, IPv6 unicast)
```
show mpls traffic-eng igp-areas

To display MPLS-TE internal area storage, use the `show mpls traffic-eng igp-areas` command in XR EXEC mode.

`show mpls traffic-eng igp-areas [detail]`

**Syntax Description**

- `detail` (Optional) Displays detailed information about the configured MPLS-TE igp-areas and communication statistics with IGPs.

**Command Default**

No default behavior or values

**Command Modes**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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 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 igp-areas` command:

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

MPLS-TE IGP Areas

Global router-id: 10.144.144.144
Global optical router-id: Not available

IS-IS 100

IGP ID: 0000.0000.0044
TE router ID configured: 10.144.144.144
in use: 10.144.144.144
Link connection: up
Topology/tunnel connection: up

level 2
TE index: 1
IGP config for TE: complete
Local links flooded in this IGP level: 1
Flooding beacon sent and received
P2P tunnel heads running over this IGP level: 1
1 AA, 0 FA
```
Tunnel loose-hops expanded over this IGP level: 0

OSPF 100

IGP ID: 10.144.144.144
TE router ID configured: 10.144.144.144
in use: 10.144.144.144
Link connection: up
Topology/tunnel connection: up

area 0
TE index: 0
IGP config for TE: complete
Local links flooded in this IGP area: 2
Flooding beacon sent and received
P2P tunnel heads running over this IGP area: 3
1 AA, 0 FA
Tunnel loose-hops expanded over this IGP area: 0

The following shows a sample output from the `show mpls traffic-eng igp-areas` command:

RP/0/RP0/CPU0:router# show mpls traffic-eng igp-areas

MPLS-TE IGP Areas
Global router-id: 0.0.0.0
Global optical router-id: Not available
OSPF 0
IGP ID: 101.0.0.1
TE router ID configured: 101.0.0.1
in use: 101.0.0.1
Link connection: up
Topology/tunnel connection: up
area 4
TE index: 0
IGP config for TE: complete
Number of links in this IGP area: 1
Number of tunnel heads running over this IGP area: 0
Number of tunnel loose-hops expanded over this IGP area: 0
area 3
TE index: 1
IGP config for TE: complete
Number of links in this IGP area: 1
Number of tunnel heads running over this IGP area: 0
Number of tunnel loose-hops expanded over this IGP area: 0
area 2
TE index: 2
IGP config for TE: complete
Number of links in this IGP area: 1
Number of tunnel heads running over this IGP area: 0
Number of tunnel loose-hops expanded over this IGP area: 0
area 1
TE index: 3
IGP config for TE: complete
Number of links in this IGP area: 1
Number of tunnel heads running over this IGP area: 0
Number of tunnel loose-hops expanded over this IGP area: 0
area 0
TE index: 4
IGP config for TE: complete
Number of links in this IGP area: 2
Number of tunnel heads running over this IGP area: 1
Number of tunnel loose-hops expanded over this IGP area: 0
This table describes the significant fields shown in the display.

Table 51: 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 XR EXEC mode.

show mpls traffic-eng link-management admission-control [interface type interface-path-id]

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</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**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Examples**

The following shows a sample output from the show mpls traffic-eng link-management admission-control command:

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

S System Information:
    Tunnels Count : 2
    Tunnels Selected : 2
Bandwidth descriptor legend:
    B0 - bw from pool 0, B1 - bw from pool 1, R - bw locked, H - bw held

<table>
<thead>
<tr>
<th>TUNNEL ID</th>
<th>UP IF</th>
<th>DOWN IF</th>
<th>PRI STATE</th>
<th>BW (kbits/sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
This table describes the significant fields shown in the display.

Table 52: 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</td>
</tr>
<tr>
<td></td>
<td>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.</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 HundredGigE 0/0/0/3

System Information::
  Links Count : 1

Link ID:: HundredGigE 0/0/0/3 (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
```
This table describes the significant fields shown in the display.

**Table 53: 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 Intf ID</td>
<td>Local interface ID.</td>
</tr>
<tr>
<td>Link Label Type</td>
<td>Label type of the link, for instance: PSC(^{18}), TDM(^{19}), FSC(^{20}).</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>

\(^{18}\) PSC = Packet switch capable.
\(^{19}\) TDM = Time-division multiplexing.
show mpls traffic-eng link-management admission-control

20  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 XR EXEC mode.

**Syntax Description**

This command has no arguments or keywords.

**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>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show mpls traffic-eng link-management advertisements` command has two output formats depending on the Diff-Serv TE Mode: one for prestandard mode and one for IETF mode.

The SRLG values are advertised for the link.

**Task ID**

<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</td>
</tr>
</tbody>
</table>

**Examples**

The following shows a sample output from the `show mpls traffic-eng link-management advertisements` command:

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

Link ID:: 0 (GigabitEthernet0/2/0/1)
  Link IP Address : 12.9.0.1
  O/G Intf ID     : 28
  Designated Router : 12.9.0.2
  TE Metric       : 1
  IGP Metric      : 1
  Physical BW     : 1000000 kbits/sec
  BCID            : RDM
  Max Reservable BW : 10000 kbits/sec
  Res Global BW   : 10000 kbits/sec
  Res Sub BW      : 0 kbits/sec
  SRLGs           : 10, 20

Downstream::
  Global Pool    Sub Pool
  --------------  --------
  Reservable BW[0]:  10000  0 kbits/sec
  Reservable BW[1]:  10000  0 kbits/sec
  Reservable BW[2]:   9800  0 kbits/sec
```
Reservable BW[3]: 9800 0 kbits/sec
Reservable BW[4]: 9800 0 kbits/sec
Reservable BW[5]: 9800 0 kbits/sec
Reservable BW[6]: 9800 0 kbits/sec
Reservable BW[7]: 9800 0 kbits/sec

Attribute Flags: 0x00000004
Attribute Names: red2

Link ID: 1 (GigabitEthernet0/2/0/2)
Link IP Address: 14.9.0.1
O/G Intf ID: 29
Designated Router: 14.9.0.4
TE Metric: 1
IGP Metric: 1
Physical BW: 1000000 kbits/sec
BCID: RDM
Max Reservable BW: 750000 kbits/sec
Res Global BW: 750000 kbits/sec
Res Sub BW: 0 kbits/sec

Downstream:

<table>
<thead>
<tr>
<th>Global Pool</th>
<th>Sub Pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reservable BW[0]: 750000 0 kbits/sec</td>
<td></td>
</tr>
<tr>
<td>Reservable BW[1]: 750000 0 kbits/sec</td>
<td></td>
</tr>
<tr>
<td>Reservable BW[2]: 750000 0 kbits/sec</td>
<td></td>
</tr>
<tr>
<td>Reservable BW[3]: 750000 0 kbits/sec</td>
<td></td>
</tr>
<tr>
<td>Reservable BW[4]: 750000 0 kbits/sec</td>
<td></td>
</tr>
<tr>
<td>Reservable BW[5]: 750000 0 kbits/sec</td>
<td></td>
</tr>
<tr>
<td>Reservable BW[6]: 750000 0 kbits/sec</td>
<td></td>
</tr>
<tr>
<td>Reservable BW[7]: 750000 0 kbits/sec</td>
<td></td>
</tr>
</tbody>
</table>

Attribute Flags: 0x00000000
Attribute Names:

This table describes the significant fields shown in the display.

**Table 54: 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>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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SRLGs&lt;sup&gt;21&lt;/sup&gt;</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[&lt;i&gt;x&lt;/i&gt;]</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>

<sup>21</sup> 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 XR EXEC mode.

### show mpls traffic-eng link-management bandwidth-allocation [interface type interface-path-id]

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface</code></td>
<td>(Optional) Displays information on the specified interface.</td>
<td></td>
</tr>
<tr>
<td><code>type</code></td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
<td></td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or a virtual interface.</td>
<td></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
XR EXEC mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
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 HundredGigE 0/0/0/3

System Information::
  Links Count : 4
  Bandwidth Hold time : 15 seconds

Link ID: HundredGigE0/0/0/3 (7.2.2.1)
  Local Intf ID: 4
  Link Status:
  Link Label Type : PSC
```
Physical BW: 155520 kbits/sec
BCID: MAM
Max Reservable BW: 1000 kbits/sec (reserved: 0% in, 0% out)
BC0: 600 kbits/sec (reserved: 2% in, 2% out)
BC1: 400 kbits/sec (reserved: 0% in, 0% out)
MPLS-TE Link State: MPLS-TE on, RSVP on, admin-up, flooded
Inbound Admission: allow-all
Outbound Admission: allow-if-room
IGP Neighbor Count: 2
BW Descriptors: 1 (including 0 BC1 descriptors)
Admin Weight: 1 (OSPF), 10 (ISIS)
Up Thresholds: 15 30 45 60 75 80 85 90 95 96 97 98 99 100 (default)
Down Thresholds: 100 99 98 97 96 95 90 85 80 75 60 45 30 15 (default)

Bandwidth Information:

Downstream BC0 (kbits/sec):
<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></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<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>0</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></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<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 55: show mpls traffic-eng link-management bandwidth-allocation 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>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>Link Label type</td>
<td>Label type of the link, for example:</td>
</tr>
<tr>
<td></td>
<td>• PSC\textsuperscript{22}</td>
</tr>
<tr>
<td></td>
<td>• TDM\textsuperscript{23}</td>
</tr>
<tr>
<td></td>
<td>• FSC\textsuperscript{24}</td>
</tr>
<tr>
<td>Physical BW</td>
<td>Link bandwidth capacity (in bits per second).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</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>

22 PSC = Packet switch capable.
23 TDM = Time-division multiplexing.
24 FSC = Fiber switch capable.
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 XR EXEC mode.

```
show mpls traffic-eng link-management igp-neighbors [igp-id | isis isis-address | ospf ospf-id] [{interface type interface-path-id IP-address}]
```

**Syntax Description**

- **igp-id** (Optional) Displays the IGP neighbors that are using a specified IGP identification.
- **isis isis-address** Displays the specified Intermediate System-to-Intermediate System (IS-IS) neighbor system ID when neighbors are displayed by IGP ID.
- **ospf ospf-id** Displays the specified Open Shortest Path first (OSPF) neighbor OSPF router ID when neighbors are displayed by IGP ID.
- **interface** (Optional) Displays information on the specified interface.
- **type** Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id** Physical interface or a virtual interface.

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

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

- **IP-address** (Optional) IGP neighbors that are using a specified IGP IP address.

**Command Modes**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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 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 igp-neighbors` command:

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

Link ID: HundredGigE0/0/0/3
No Neighbors

Link ID: HundredGigE0/0/0/4
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 56: 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 XR EXEC mode.

```
show mpls traffic-eng link-management interfaces [type  interface-path-id]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</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.</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**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You cannot configure more than 250 links under MPLS-TE.

SRLG values can be configured for the link.

**Task ID**

```
Task ID Operations
mpls-te read
```

**Examples**

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

```
RP/0/RP0/CPU0:router# show mpls traffic-eng link-management interfaces HundredGigE 0/0/0/3

System Information::
    Links Count : 7 (Maximum Links Supported 250)

Link ID:: HundredGigE0/0/0/3 (12.9.0.1)
    Local Intf ID: 28
    Link Status:
        Link Label Type : PSC
        Physical BW : 1000000 kbits/sec
```
show mpls traffic-eng link-management interfaces

<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>SRLGs</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>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>
</tbody>
</table>

This table describes the significant fields shown in the display.

Table 57: show mpls traffic-eng link-management interfaces Command Field Descriptions
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>

25 SRLGs = Shared Risk Link Groups.
26 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 XR EXEC mode.

```
show mpls traffic-eng link-management statistics  [{summary | interface type interface-path-id}]
```

**Syntax Description**

- `summary` (Optional) Displays the statistics summary.
- `interface` (Optional) Displays the interface for which information is requested.
- `type` (Optional) Interface type. For more information, use the question mark (?) online help function.
- `interface-path-id` Physical interface or virtual interface.

**Note**

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

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

**Command Default**

No default behavior or values

**Command Modes**

XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The show mpls traffic-eng link-management statistics command displays resource and configuration information for all configured interfaces.

**Task ID**

- Task ID: mpls-te
- Operations ID: read

**Examples**

The following shows a sample output from the show mpls traffic-eng link-management statistics command using the summary keyword:

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

LSP Admission Statistics:

<table>
<thead>
<tr>
<th>Setup Requests</th>
<th>Setup Admits</th>
<th>Setup Rejects</th>
<th>Setup Errors</th>
<th>Tear Requests</th>
<th>Tear Admits</th>
<th>Tear Rejects</th>
<th>Tear Errors</th>
<th>Tear Preempts</th>
<th>Tear Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
Table 58: show mpls traffic-eng link-management statistics summary Command Field Descriptions, on page 379 describes the significant fields shown in the display.

<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 XR EXEC mode.

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

**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>6.2.1</td>
<td>This command was introduced</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
You cannot configure more than 250 links for MPLS-TE/FRR.

**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 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
```
This table describes the significant fields shown in the display.

**Table 59: 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 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>

27 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 XR EXEC mode.

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

XR EXEC mode

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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 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 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 60: show mpls traffic-eng maximum tunnels Command Field Descriptions, on page 383 describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Global Tunnel Count</td>
<td>Maximum number of tunnel interfaces (all TE tunnel types, tunnel-te, tunnel-mte, and tunnel-gte) that can be configured.</td>
</tr>
<tr>
<td>Maximum Global Tunnel Count</td>
<td>Maximum number of tunnel interfaces (all TE tunnel types and tunnel-te) 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>
</tbody>
</table>
### Field | Description
--- | ---
Current Count | Table heading for the current count in each category.
Maximum AutoTunnel Backup Count | Maximum number of automatic backup tunnels that can be configured.
Maximum GMPLS UNI Tunnel Count | Maximum number of Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI) tunnels that can be configured and the current tunnel count.
Maximum AutoTunnel Mesh Count | Maximum number of automatic mesh tunnels that can be configured.

`show mpls traffic-eng maximum tunnels`
show mpls traffic-eng preemption log

To display the log of preemption events, use the show mpls traffic-eng preemption log command in XR EXEC mode mode.

show mpls traffic-eng preemption log

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log</td>
<td>Displays a log of preemption events.</td>
</tr>
</tbody>
</table>

Command Default

None

Command Modes

XR EXEC mode

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID: mpls-te Operation: read

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</th>
<th>Pri</th>
<th>Bandwidth</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</td>
<td>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</td>
<td>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</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 XR EXEC mode.

```
show mpls traffic-eng topology  [IP-address]  [affinity]  [brief]  [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}]  [srlg][static]
```

**Syntax Description**

- **IP-address** (Optional) Node IP address (router identifier to interface address).
- **destination IP-address** Displays the LSP destination IPv4 address.
- **exclude-srlg** Specifies an IP address to get SRLG values from for exclusion.
- **explicit-path** Displays the explicit LSP path.
- **tunnel** Displays the topology path that is based on the Point-to-Point (P2P) tunnel number.
- **P2P-tunnel-number** P2P tunnel number. Range is 0 to 65535.
- **affinity** (Optional) Displays the attribute values that are required for links carrying this tunnel. A 32-bit decimal number. Range is 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.
- **priority level** (Optional) Displays the priority used when signaling a LSP for this tunnel, to determine which existing tunnels can be preempted.
- **isis nsap-address** (Optional) Displays the node router identification, if Intermediate System-to-Intermediate System (IS-IS) is enabled.
- **ospf ospf-address** (Optional) Displays the node router identifier, if Open Shortest Path First (OSPF) is enabled.
show mpls traffic-eng topology

<table>
<thead>
<tr>
<th>path</th>
<th>(Optional) Displays the path to a destination from this router.</th>
</tr>
</thead>
<tbody>
<tr>
<td>router</td>
<td>Displays the given OSPF address type of the router node.</td>
</tr>
<tr>
<td>network</td>
<td>Displays the given OSPF address type of the network node.</td>
</tr>
<tr>
<td>brief</td>
<td>(Optional) Displays the brief form of the output that provides a less detailed version of the topology.</td>
</tr>
<tr>
<td>srlg</td>
<td>(Optional) Displays the SRLG information.</td>
</tr>
<tr>
<td>static</td>
<td>(Optional) Displays the statically configured SRLG.</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>6.2.1</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 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 0xffffff
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:

```
The following shows a sample output from the `show mpls traffic-eng topology path destination` command specifying the topological path with SRLG exclusion:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng topology path destination 100.0.0.2 exclude-srlg 50.4.5.5 isis 1 level 2

Tue Oct 6 13:13:44.053 UTC
Path Setup to 100.0.0.2:
bw 0 (CT0), min_bw 0, metric: 20
setup_pri 7, hold_pri 7
affinity_bits 0x0, affinity_mask 0xffffffff
Exclude SRLG Intf Addr : 50.4.5.5
SRLGs Excluded: 10, 30, 77, 88, 1500, 10000000, 4294967290, 4294967295
Hop0:50.5.1.5
Hop1:50.5.1.1
Hop2:51.1.2.1
Hop3:51.1.2.2
Hop4:100.0.0.2
```

The following shows a sample output from the `show mpls traffic-eng topology path destination` command specifying the topological path based on a given explicit path:
show mpls traffic-eng topology path destination 100.0.0.2 explicit-path
name exclude-srlg isis 1 level 2

Tue Oct 6 13:16:44.233 UTC
Path Setup to 100.0.0.2:
bw 0 (CT0), min_bw 0, metric: 20
setup_pri 7, hold_pri 7
affinity_bits 0x0, affinity_mask 0xffff
SRLGs Excluded: 10, 30, 77, 88, 1500, 10000000
4294967290, 4294967295, 1, 2, 3, 4
5, 6, 7, 8
Hop0:50.5.1.5
Hop1:50.5.1.1
Hop2:50.1.2.1
Hop3:50.1.2.2
Hop4:100.0.0.2
show mpls traffic-eng tunnels

To display information about MPLS-TE tunnels, use the `show mpls traffic-eng tunnels` command in XR EXEC mode.

Syntax:
```
show mpls traffic-eng tunnels [tunnel-number] [affinity] [all] [auto-bw] [attribute-set {all|tunnel-name}] [auto-tunnel] [backup] [destination {name tunnel-name} | {p2p}] [property { backup-tunnel | fast-reroute}] [protection { [frr | path | tunnel-id | tunnel-id | tabular]} [reoptimized within-last [interval]] [role {all | head | tail | middle | soft-preemption {desired | triggered} }]] [source source-address] [summary] [tabular] [up] [class-type ct]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>tunnel-number</code></td>
<td>(Optional) Number of the tunnel. Range is from 0 to 65535.</td>
</tr>
<tr>
<td><code>attribute-set</code></td>
<td>(Optional) Restricts the display of tunnels with an attribute set.</td>
</tr>
<tr>
<td><code>affinity</code></td>
<td>(Optional) Displays the affinity attributes for all outgoing links.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>(Optional) Displays all MPLS-TE tunnels.</td>
</tr>
<tr>
<td><code>auto-bw</code></td>
<td>(Optional) Restricts the display to tunnels when the automatic bandwidth is enabled.</td>
</tr>
<tr>
<td><code>auto-tunnel</code></td>
<td>(Optional) Restricts the display of automatically created tunnels.</td>
</tr>
<tr>
<td><code>mesh mesh-value</code></td>
<td>Displays the tunnels that belong to the specified auto-tunnel mesh group.</td>
</tr>
<tr>
<td><code>backup</code></td>
<td>(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.</td>
</tr>
<tr>
<td><code>name tunnel-name</code></td>
<td>(Optional) Displays the tunnel with given name.</td>
</tr>
<tr>
<td><code>protected-interface</code></td>
<td>(Optional) Displays FRR protected interfaces.</td>
</tr>
<tr>
<td><code>static</code></td>
<td>(Optional) Displays static backup tunnels.</td>
</tr>
<tr>
<td><code>auto-tunnel</code></td>
<td>(Optional) Displays protected automatic backup tunnels.</td>
</tr>
</tbody>
</table>
### show mpls traffic-eng tunnels

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>brief</strong></td>
<td>(Optional) Displays the brief form of this command.</td>
</tr>
<tr>
<td><strong>destination</strong></td>
<td>(Optional) Restricts the display to tunnels destined for the specified IP address.</td>
</tr>
<tr>
<td><strong>detail</strong></td>
<td>(Optional) Displays detail information about headend tunnels.</td>
</tr>
<tr>
<td><strong>down</strong></td>
<td>(Optional) Displays tunnels that are down.</td>
</tr>
<tr>
<td><strong>interface in</strong></td>
<td>(Optional) Displays tunnels that use the specified input interface.</td>
</tr>
<tr>
<td><strong>interface out</strong></td>
<td>(Optional) Displays tunnels that use the specified output interface.</td>
</tr>
<tr>
<td><strong>interface inout</strong></td>
<td>(Optional) Displays tunnels that use the specified interface as an input or output 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 a virtual interface.</td>
</tr>
<tr>
<td><strong>p2p</strong></td>
<td>(Optional) Displays only P2P tunnels.</td>
</tr>
<tr>
<td><strong>property backup-tunnel</strong></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><strong>property fast-reroute</strong></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>
</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>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>frr</td>
<td>(Optional) Displays all protected tunnels (configured as fast-reroutable).</td>
</tr>
<tr>
<td>path</td>
<td>(Optional) Displays information for the path-protection.</td>
</tr>
<tr>
<td>tunnel-id</td>
<td>(Optional) Displays information for the path-protection for a particular tunnel.</td>
</tr>
<tr>
<td>tunnel-id</td>
<td>(Optional) Tunnel identifier. The range is from 0 to 65535.</td>
</tr>
<tr>
<td>tabular</td>
<td>(Optional) Displays information for the path protection tunnel in tabular format.</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>
</tbody>
</table>
show mpls traffic-eng tunnels

suboptimal constraints none  (Optional) Displays tunnels whose path metric is greater than the shortest unconstrained path.

summary  (Optional) Displays summary of configured tunnels.

tabular  (Optional) Displays a table showing TE LSPs, with one entry per line.

up  (Optional) Displays tunnels when the tunnel interface is up.

class-type  ct  (Optional) Displays tunnels using the given class-type value configuration.

28  FRR = Fast Reroute.
29  LSPs = Label Switched Paths.

Command Default
None

Command Modes
XR EXEC mode

Command History
Release 6.2.1  This command was introduced.

Usage Guidelines
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.

To display the path-protection summary fields, you must configure the options for the path-protection.

Task ID  Operations Task ID
mpls-te  read, write

Examples
This sample output is not changed when no area is specified for the active path-option. If the area is specified, it is added on a line of its own after the existing path-option information.

RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels 20 detail

Signalling Summary:
LSP Tunnels Process: running
RSVP Process: running
Forwarding: enabled
Periodic reoptimization: every 3600 seconds, next in 2400 seconds
Periodic FRR Promotion: every 300 seconds, next in 16 seconds
Auto-bw enabled tunnels: 6

Name: tunnel-te20   Destination: 130.130.130.130
Status:
   Admin:    up   Oper:    up   Path:    valid   Signalling: connected
   path option 1, type explicit r1r2r3gig_path (Basis for Setup, path weight 200)
   G-PID: 0x0800 (derived from egress interface properties)
   Bandwidth Requested: 113 kbps  CT0

Config Parameters:
   Bandwidth: 100 kbps (CT0) Priority: 7 7 Affinity: 0x0/0xffff
   Metric Type: TE (interface)
   AutoRoute: enabled LockDown: disabled Policy class: not set
   Forwarding-Adjacency: disabled
   Loadshare: 0 equal loadshares
   Auto-bw: enabled
   Last BW Applied: 113 kbps CT0 BW Applications: 1
   Last Application Trigger: Periodic Application
   Bandwidth Min/Max: 0-4294967295 kbps
   Application Frequency: 5 min Jitter: 0s Time Left: 4m 19s
   Collection Frequency: 1 min
   Samples Collected: 0 Next: 14s
   Highest BW: 0 kbps Underflow BW: 0 kbps
   Adjustment Threshold: 10% 10 kbps
   Overflow Detection disabled
   Underflow Detection disabled
   Fast Reroute: Disabled, Protection Desired: None
   Path Protection: Not Enabled

History:
   Tunnel has been up for: 00:18:54
   Current LSP:
      Uptime: 00:05:41
   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: HundredGigE0/0/0/3, 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 HundredGigE0/0/0/3

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: 0x0/0xffffffff
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 61: 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>
</tbody>
</table>
## MPLS Command Reference for Cisco NCS 5000 Series Routers

### show mpls traffic-eng tunnels

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<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 thes 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>

30 LSP = Link-State Packet.
31 FRR = Fast Reroute.

This sample output shows the link attributes of links that are traversed by the tunnel (color information):

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels 11 affinity

Signalling Summary:
  LSP Tunnels Process: running
  RSVP Process: running
  Forwarding: enabled
  Periodic reoptimization: every 3600 seconds, next in 2710 seconds
  Periodic FRR Promotion: every 300 seconds, next in 27 seconds

Auto-bw enabled tunnels: 0 (disabled)

Name: tunnel-te11 Destination: 3.3.3.3
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 1, type explicit gige_1_2_3 (Basis for Setup, path weight 2)
  G-FID: 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
```
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# 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_t6010</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>
<tr>
<td>Tunnel_PE10-PE21</td>
<td>10.21.21.21</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>PE21_C12406_t2106</td>
<td>10.6.6.6</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>PE21_C12406_t2107</td>
<td>10.7.7.7</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>PE21_C12406_t2108</td>
<td>10.8.8.8</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>PE21_C12406_t2109</td>
<td>10.9.9.9</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>PE21_C12406_t2110</td>
<td>10.10.10.10</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>PE6_C12406_t6070</td>
<td>10.7.7.7</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>PE7_C12406_t7060</td>
<td>10.6.6.6</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>tunnel-te1</td>
<td>200.0.0.3</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>HundredGigE0/0/3</td>
<td>100.0.0.1</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>HundredGigE0/0/4</td>
<td>200.0.0.1</td>
<td>up</td>
<td>up</td>
</tr>
</tbody>
</table>
```

Displayed 1 (of 1) heads, 20 (of 20) midpoints, 0 (of 0) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads

This section shows a sample output that results when automatic backup tunnels are created:
show mpls traffic-eng tunnels brief

<table>
<thead>
<tr>
<th>TUNNEL NAME</th>
<th>DESTINATION</th>
<th>STATUS</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel-te0</td>
<td>200.0.0.3</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>tunnel-te1</td>
<td>200.0.0.3</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>tunnel-te2</td>
<td>200.0.0.3</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>*tunnel-te50</td>
<td>200.0.0.3</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>*tunnel-te60</td>
<td>200.0.0.3</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>*tunnel-te70</td>
<td>200.0.0.3</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>*tunnel-te80</td>
<td>200.0.0.3</td>
<td>up</td>
<td>up</td>
</tr>
</tbody>
</table>

* = automatically created backup tunnel

This is sample output that shows a summary of configured tunnels by using the summary keyword:

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

Path Protection Summary:
20 standby configured tunnels, 15 connected, 10 path protected
2 link-diverse, 4 node-diverse, 4 node-link-diverse

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

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

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

  tunnel170
  LSP Head, Admin: up, Oper: up
  Src: 10.20.20.20, Dest: 10.10.10.10, Instance: 945
  Fast Reroute Protection: Requested
    Outbound: FRR Ready
    Backup tunnel160 to LSP nhop
tunnel160: out I/f: HundredGigE0/0/0/3
  LSP signalling info:
    Original: out I/f: HundredGigE0/0/0/4, label: 3, nhop: 10.10.10.10
    With FRR: out I/f: tunnel160, label: 3
  LSP bw: 10 kbps, Backup level: any unlimited, type: CT0
```

This table describes the significant fields shown in the display.

**Table 62: 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>

32 LSP = Link-State Packet.
33 LSP = Label Switched Path

This is sample output from the `show mpls traffic-eng tunnels` command using the `backup` keyword. This command selects every MPLS-TE tunnel known to the router, and displays information about the FRR protection that each selected tunnel provides for interfaces on this route. The command does not generate output for tunnels that do not provide FRR protection of interfaces on this router:
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: HundredGigE0/0/0/3
    Protected lsps: 0
  Backup BW: any-class unlimited, Inuse: 0 kbps

This table describes the significant fields shown in the display.

**Table 63: 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

Interface: HundredGigE0/0/0/3
  Tunnel100  UNUSED : out I/f: Admin: down Oper: down

Interface: HundredGigE0/0/0/4
  Tunnel160 NHOP : out I/f: HundredGigE0/0/0/5 Admin: up Oper: up

This table describes the significant fields shown in the display.

**Table 64: 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>
</tbody>
</table>
show mpls traffic-eng tunnels

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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` command using the `up` within-last keywords:

RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels up within-last 200

Signalling Summary:

- LSP Tunnels Process: running
- RSVP Process: running
- Forwarding: enabled
- Periodic reoptimization: every 3600 seconds, next in 3381 seconds
- Periodic FRR Promotion: every 300 seconds, next in 81 seconds
- Periodic auto-bw collection: disabled

Name: tunnel-te11 Destination: 30.30.30.30

Status:
- Admin: up
- Oper: up
- Path: valid
- Signalling: connected

path option 1, type explicit back (Basis for Setup, path weight 1)
G-PID: 0x0800 (derived from egress interface properties)

Config Parameters:
- Bandwidth: 0 kbps (CT0)
- Priority: 7
- 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
- Direction: unidirectional
- Auto-bw: disabled(0/0)
- 0 Bandwidth Requested: 0
- Endpoint switching capability: unknown, encoding type: unassigned
- Transit switching capability: unknown, encoding type: unassigned

History:
- Tunnel has been up for: 00:00:21
- Current LSP:
  - Uptime: 00:00:21
  - Prior LSP:
    - ID: path option 1 [4]
    - Removal Trigger: tunnel shutdown

Path info (ospf area 0):
- Hop0: 7.4.4.2
- Hop1: 30.30.30.30

Displayed 1 (of 3) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads

This shows a sample output from the `show mpls traffic-eng tunnels` command using the `reoptimized` within-last keywords:

RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels reoptimized within-last 600

Signalling Summary:
LSP Tunnels Process: running
RSVP Process: running
Forwarding: enabled
Periodic reoptimization: every 60000 seconds, next in 41137 seconds
Periodic FRR Promotion: every 300 seconds, next in 37 seconds
Periodic auto-bw collection: disabled

Name: tunnel-te1 Destination: 30.30.30.30
Status:
  Admin: up  Oper: up  Path: valid  Signalling: connected

path option 1, type explicit prot1 (Basis for Setup, path weight 1)
G-PID: 0x0800 (derived from egress interface properties)

Config Parameters:
  Bandwidth: 66 kbps (CT0)  Priority: 7 7  Affinity: 0x0/0xffff
  Metric Type: IGP (global)
  AutoRoute: enabled  LockDown: disabled  Loadshare: 66 bw-based
  Auto-bw: disabled(0/0) 0  Bandwidth Requested: 66
  Direction: unidirectional

Endpoint switching capability: unknown, encoding type: unassigned
Transit switching capability: unknown, encoding type: unassigned

History:
  Tunnel has been up for: 00:14:04
  Current LSP:
    Uptime: 00:03:52
    Selection: reoptimization
  Prior LSP:
    ID: path option 1 [2017]
    Removal Trigger: reoptimization completed

Path info (ospf area 0):
  Hop0: 7.2.2.2
  Hop1: 7.3.3.2
  Hop2: 30.30.30.30
Displayed 1 (of 1) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads

This is a sample output from the show mpls traffic-eng tunnels command using the detail keyword:

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
show mpls traffic-eng tunnels

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: HundredGigE0/0/0/3, Outgoing Label: implicit-null
  Path Info:
    Explicit Route:
      Strict, 100.0.0.3
      Strict, 24.24.24.24
    Record Route: None
    Tspec: avg rate=2488320 kbits, burst=1000 bytes, peak rate=2488320 kbits
  Resv Info:
    Record Route:
      IPv4 100.0.0.3, flags 0x0
    Fspec: avg rate=2488320 kbits, burst=1000 bytes, peak rate=2488320 kbits
Protecting LSP Info:
  Instance: 72, Signaling Area: ospf optical area 0
  Incoming Label: explicit-null
  Outgoing Interface: HundredGigE0/0/0/4, Outgoing Label: implicit-null
  Path Info:
    Explicit Route:
      Strict, 101.0.0.3
      Strict, 24.24.24.24
    Record Route: None
    Tspec: avg rate=2488320 kbits, burst=1000 bytes, peak rate=2488320 kbits
  Resv Info:
    Record Route:
      IPv4 101.0.0.3, flags 0x0
    Fspec: avg rate=2488320 kbits, burst=1000 bytes, peak rate=2488320 kbits
Reoptimized LSP Info (Install Timer Remaining 11 Seconds):
Cleaned LSP Info (Cleanup Timer Remaining 19 Seconds):

This is a sample output that shows the path-protection options for tunnel-te 100 using the detail keyword.

RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels 100 detail

Signalling Summary:
  LSP Tunnels Process: running
  RSVP Process: running
  Forwarding: enabled
  Periodic reoptimization: every 60 seconds, next in 31 seconds
  Periodic FRR Promotion: every 300 seconds, next in 299 seconds
  Auto-bw enabled tunnels: 0 (disabled)

Name: tunnel-te100 Destination: 33.3.33.3
Status:
  Admin: up Oper: up (Up for 02:06:14)
  Path: valid Signalling: connected

Path options:
path-option 5 explicit name to-gmpls3 verbatim lockdown OSPF 0 area 0
Info: Destination IP address, 1.2.3.4, not found in topology
path-option 10 dynamic
path option 15 explicit name div-wrt-to-gmpls3 verbatim
path option 20 dynamic standby OSPF 0 area 0
(Basis for Standby, path weight 2)
G-PID: 0x0800 (derived from egress interface properties)
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
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
Path Protection: enabled

Reoptimization Info in Inter-area:
Better Path Queries sent = 13; Preferred Path Exists received = 0
Last better path query was sent 00:08:22 ago
Last preferred path exists was received 00:00:00 ago

History:
Tunnel has been up for: 02:15:56
Current LSP:
  Uptime: 02:15:56
Prior LSP:
  ID: path option 10 [22]
  Removal Trigger: path verification failed
Current LSP Info:
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: disabled Direction: unidirectional
Endpoint switching capability: unknown, encoding type: unassigned
Transit switching capability: unknown, encoding type: unassigned
Fast Reroute: Disabled, Protection Desired: None

Reoptimization Info in Inter-area:
Better Path Queries sent = 13; Preferred Path Exists received = 0
Last better path query was sent 00:08:22 ago
Last preferred path exists was received 00:00:00 ago
Path Protection Info:
Standby Path: Node and Link diverse Last switchover 00:08:22 ago
Switchover Reason: Path delete request
Number of Switchovers 13, Standby Ready 15 times

History:
Prior LSP:
  ID: path option 10 [188]
  Removal Trigger: path option removed
Tunnel has been up for: 00:03:58
Current LSP:
  Uptime: 00:03:58
Reopt. LSP:
  Setup Time: 272 seconds
Current LSP Info:
  Instance: 1, Signaling Area: OSPF 0 area 0
Uptime: 00:03:58
Outgoing Interface: HundredGigE0/0/0/3, Outgoing Label: implicit-null
Router-IDs: local 222.22.2.2
downstream 33.3.33.3

Path Info:
Outgoing:
Explicit Route:
Strict, 23.0.0.3
Strict, 33.3.33.3
Record Route: None
Tspec: avg rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Session Attributes: Local Prot: Not Set, Node Prot: Not Set, BW Prot: Not Set
Resv Info:
Record Route: None
Fspec: avg rate=0 kbits, burst=1000 bytes, peak rate=0 kbits

Standby LSP Info:
Instance: 1, Signaling Area: OSPF 0 area 0
Uptime: 00:03:58
Outgoing Interface: HundredGigE0/0/0/3, Outgoing Label: implicit-null
Router-IDs: local 222.22.2.2
downstream 33.3.33.3

Path Info:
Outgoing:
Explicit Route:
Strict, 23.0.0.3
Strict, 33.3.33.3
Record Route: None
Tspec: avg rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Session Attributes: Local Prot: Not Set, Node Prot: Not Set, BW Prot: Not Set
Resv Info:
Record Route: None
Fspec: avg rate=0 kbits, burst=1000 bytes, peak rate=0 kbits

Reoptimized LSP Info:
Instance: 5, Signaling Area: OSPF 0 area 0
Outgoing Interface: HundredGigE0/0/0/4, Outgoing Label: 16000

Path Info:
Outgoing:
Explicit Route:
Strict, 26.0.0.6
Strict, 36.0.0.3
Strict, 33.3.33.3
Record Route: None
Tspec: avg rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Session Attributes: Local Prot: Not Set, Node Prot: Not Set, BW Prot: Not Set
Resv Info:
Record Route: None
Fspec: avg rate=0 kbits, burst=1000 bytes, peak rate=0 kbits

Delayed Clean Standby LSP Info:
Instance: 1, Signaling Area: OSPF 0 area 0
Uptime: 00:03:58
Outgoing Interface: HundredGigE0/0/0/3, Outgoing Label: implicit-null
Router-IDs: local 222.22.2.2
downstream 33.3.33.3

Path Info:
Outgoing:
Explicit Route:
Strict, 23.0.0.3
Strict, 33.3.33.3
Record Route: None
Tspec: avg rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Session Attributes: Local Prot: Not Set, Node Prot: Not Set, BW Prot: Not Set
Resv Info:
Record Route: None
Fspec: avg rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
This is a sample output from the `show mpls traffic-eng tunnels` command using the `role mid` keyword:

```
RP/0/RP0/CPU0# 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: HundredGigE0/0/0/3, 33
  OutLabel: HundredGigE0/0/0/4, implicit-null
  Signalling Info:
    Src 10.10.10.10 Dst 30.30.30.30, Tunnel ID 1, Tunnel Instance 5508
    Path Info:1
      Incoming Address: 7.3.3.1
      Incoming Explicit Route:
        Strict, 7.3.3.1
        Loose, 30.30.30.30
      ERO Expansion Info:
        ospf 100 area 0, Metric 1 (TE), Affinity 0x0, Mask 0xffffffff, Queries 0
        Outgoing Explicit Route:
          Strict, 7.2.2.1
          Strict, 30.30.30.30
      Record Route: None
      Tspec: avg rate=10 kbits, burst=1000 bytes, peak rate=10 kbits
      Resv Info:
        Record Route:
          IPv4 30.30.30.30, flags 0x20
          Label 3, flags 0x1
          IPv4 7.3.3.2, flags 0x0
          Label 3, flags 0x1
        Fspec: avg rate=10 kbits, burst=1000 bytes, peak rate=10 kbits
```

This sample output shows a tabular table for TE LSPs by using the `tabular` keyword:

```
RP/0/RP0/CPU0# 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>LSP Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel-mte100</td>
<td>1</td>
<td>2.2.2.2</td>
<td>60.60.60.60</td>
<td>up</td>
<td>Inact</td>
<td>Head</td>
</tr>
<tr>
<td>tunnel-mte300</td>
<td>1</td>
<td>2.2.2.2</td>
<td>60.60.60.60</td>
<td>up</td>
<td>Inact</td>
<td>Head</td>
</tr>
<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>
</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>
</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>
</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>
</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>
</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>
</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>
</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>
</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>
</tr>
</tbody>
</table>
```

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>State</th>
<th>FRR State</th>
<th>LSP Role</th>
<th>Prot</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel-te0</td>
<td>549</td>
<td>200.0.0.3</td>
<td>200.0.0.1</td>
<td>up</td>
<td>Inact</td>
<td>Head</td>
<td>InAct</td>
</tr>
<tr>
<td>tunnel-te1</td>
<td>546</td>
<td>200.0.0.3</td>
<td>200.0.0.1</td>
<td>up</td>
<td>Inact</td>
<td>Head</td>
<td>InAct</td>
</tr>
<tr>
<td>tunnel-te2</td>
<td>6</td>
<td>200.0.0.3</td>
<td>200.0.0.1</td>
<td>up</td>
<td>Inact</td>
<td>Head</td>
<td>InAct</td>
</tr>
<tr>
<td>*tunnel-te50</td>
<td>6</td>
<td>200.0.0.3</td>
<td>200.0.0.1</td>
<td>up</td>
<td>Active</td>
<td>Head</td>
<td>InAct</td>
</tr>
<tr>
<td>*tunnel-te60</td>
<td>4</td>
<td>200.0.0.3</td>
<td>200.0.0.1</td>
<td>up</td>
<td>Active</td>
<td>Head</td>
<td>InAct</td>
</tr>
<tr>
<td>*tunnel-te70</td>
<td>4</td>
<td>200.0.0.3</td>
<td>200.0.0.1</td>
<td>up</td>
<td>Active</td>
<td>Head</td>
<td>InAct</td>
</tr>
<tr>
<td>*tunnel-te80</td>
<td>3</td>
<td>200.0.0.3</td>
<td>200.0.0.1</td>
<td>up</td>
<td>Active</td>
<td>Head</td>
<td>InAct</td>
</tr>
</tbody>
</table>

* = automatically created backup tunnel
```

This table describes the significant fields shown in the display.

### Table 65: show mpls traffic-eng tunnels tabular Command Field Descriptions

<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>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 a path protection for tunnel ID 10:
show mpls traffic-eng tunnels protection path tunnel-id 10

Tun ID 10, Src 22.2.22.2 Dst 66.6.66.6, Ext ID 22.2.22.2
Switchover 00:08:22 ago, Standby Path: {Not found | Link diverse | Node diverse | Node and Link diverse}
Current LSP: LSP ID 10022, Up time 12:10:24,
Local lbl: 16001, Out Interface: HundredGigE0/0/0/3, Out lbl: implicit-null
Path: 1.1.1.1, 2.2.2.2, 3.3.3.3, 8.8.8.8
Standby LSP: None | LSP ID, Up time 12:00:05,
Local lbl: 16002, Out Interface: HundredGigE0/0/0/4, Out lbl: implicit-null
Path 4.4.4.4, 5.5.5.5, 6.6.6.6, 7.7.7.7

This sample output shows the path protection in a tabular format:

show mpls traffic-eng tunnels protection path tabular

<table>
<thead>
<tr>
<th>Tunnel ID</th>
<th>Current LSP ID</th>
<th>Standby LSP ID</th>
<th>Protected State</th>
<th>Standby Diversity</th>
</tr>
</thead>
<tbody>
<tr>
<td>155</td>
<td>10</td>
<td>11</td>
<td>Ready</td>
<td>Node and Link Diverse</td>
</tr>
<tr>
<td>1501</td>
<td>11</td>
<td>12</td>
<td>Ready</td>
<td>Node and Link Diverse</td>
</tr>
<tr>
<td>1502</td>
<td>10</td>
<td>11</td>
<td>Ready</td>
<td>Node and Link Diverse</td>
</tr>
<tr>
<td>1504</td>
<td>10</td>
<td>11</td>
<td>Ready</td>
<td>Node and Link Diverse</td>
</tr>
<tr>
<td>1505</td>
<td>10</td>
<td>11</td>
<td>Ready</td>
<td>Node and Link Diverse</td>
</tr>
</tbody>
</table>

This table describes the significant fields shown in the display.

*Table 66: show mpls traffic-eng tunnels protection path tabular Command Field Descriptions*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel ID</td>
<td>Identifier of the tunnel.</td>
</tr>
<tr>
<td>Current LSP ID</td>
<td>Identifier of the LSP that is carrying traffic.</td>
</tr>
<tr>
<td>Standby LSP ID</td>
<td>Identifier of the standby LSP that is protecting traffic.</td>
</tr>
<tr>
<td>Protected State</td>
<td>Values are Ready and Not Ready.</td>
</tr>
<tr>
<td>Standby Diversity</td>
<td>Values are Node and Link Diverse along with Node Diverse and Link Diverse. Values that state that the current and standby LSP do not have nodes or links in common. The current and standby LSP do not have nodes in common (but can share a link), or they have no links in common (but can share nodes).</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:

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
- Affinity: 0x0/0xffffffff
- 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 67: 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>
</tbody>
</table>
### Field | Description
--- | ---
Samples Collected | Number of samples that are collected during the current application period. This field is replaced by the Collection Disabled field if Collection Frequency is not currently configured.

Highest BW | Highest bandwidth that is collected for the application period.

Next | Time left before the next collection event.

Overflow Threshold | Overflow threshold that is configured. The Overflow field appears only if the overflow detection is configured in the tunnel automatic bandwidth configuration.

Limit | Consecutive overflow detected or configured limit.

Early BW Applications | Number of early bandwidth applications that are triggered by an overflow condition.

This is sample output from the `show mpls traffic-eng tunnels` command after the NNHOP SRLG preferred automatic backup tunnel is configured:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels 1

Signalling Summary:
  LSP Tunnels Process: running
  RSVP Process: running
  Forwarding: enabled
  Periodic reoptimization: every 3600 seconds, next in 2524 seconds
  Periodic FRR Promotion: every 300 seconds, next in 49 seconds
  Auto-bw enabled tunnels: 1

Name: tunnel-te1 Destination: 200.0.0.3 (auto backup)
  Status: Admin: up Oper: up Path: valid Signalling: connected
    path option 10, type explicit (autob_nnhop_srlg_tunnel1) (Basis for Setup, path weight 11)
    path option 20, type explicit (autob_nnhop_tunnel1)
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 0 kbps CT0
    Creation Time: Fri Jul 10 01:53:25.581 PST (1h 25m 17s ago)

Config Parameters:
  Bandwidth: 0 kbps (CT0) Priority: 7 7 Affinity: 0x0/0xffff
  Metric Type: TE (default)
  AutoRoute: disabled LockDown: disabled Policy class: not set
  Forwarding-Adjacency: disabled

Loadshare: 0 equal loadshares
  Auto-bw: disabled
  Fast Reroute: Disabled, Protection Desired: None
  Path Protection: Not Enabled
  Auto Backup:
    Protected LSPs: 4
    Protected S2L Sharing Families: 0
    Protected S2Ls: 0
    Protected i/f: HundredGigE0/0/0/2 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 68: 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>
<tr>
<td>Protected i/f</td>
<td>Interface and NNHOP node protected by this backup.</td>
</tr>
<tr>
<td>Protected node</td>
<td>Type of protection provided by this backup.</td>
</tr>
<tr>
<td>Protection: NNHOP+SRLG</td>
<td>Note Protection can be different when a preferred SRLG is configured and an SRLG path is not found.</td>
</tr>
<tr>
<td>Example when backup is in use:</td>
<td>Unused removal timeout: not running</td>
</tr>
<tr>
<td>Example when backup is unused:</td>
<td>Unused removal timeout: 1h26m</td>
</tr>
</tbody>
</table>

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: Fri Jan 14 23:35:58 2017 (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 Fri Jan 14 23:36:10 EST 2017)
Current LSP:
Uptime: 00:00:30 (since Fri Jan 14 23:36:10 EST 2017)
Current LSP Info:
Instance: 2, Signaling Area: OSPF 100 area 16909060
Uptime: 00:00:30 (since Fri Jan 14 23:36:10 EST 2017)
Outgoing Interface: HundredGigE0/0/0/4, Outgoing Label: 16005
Router-IDs: local 3.3.3.3
downstream 2.2.2.2
Soft Preemption: None
Path Info:
Outgoing:
Explicit Route:
Strict, 23.9.0.2
Strict, 12.9.0.2
Strict, 12.9.0.1
Strict, 1.1.1.1

Record Route: Disabled
Tspec: avg rate=300 kbits, burst=1000 bytes, peak rate=300 kbits
Session Attributes: Local Prot: Set, Node Prot: Not Set, BW Prot: Not Set
Soft Preemption Desired: Not Set

Resv Info:
Record Route:
IPv4 2.2.2.2, flags 0x20
Label 16005, flags 0x1
IPv4 23.9.0.2, flags 0x0
Label 16005, flags 0x1
IPv4 1.1.1.1, flags 0x20
Label 3, flags 0x1
IPv4 12.9.0.1, flags 0x0
Label 3, flags 0x1
Fspec: avg rate=300 kbits, burst=1000 bytes, peak rate=300 kbits Displayed 1 (of 8) heads, 0 (of 3) midpoints, 0 (of 0) tails Displayed 1 up, 0 down, 0 recovering, 0 recovered heads

This is sample output from the **show mpls traffic-eng tunnels** command using the **auto-tunnel backup** keywords:

```
RP/0/RP0/CPU0# 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>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>
</tbody>
</table>

This table describes the significant fields shown in the display.

*Table 69: 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>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>
<tr>
<td>Cumulative Counters</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>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/O/RP0/CPU0# 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 FCALC Error [Reopt]: Fri Jan 13 16:40:24 2017
    Info: Can't reach 10.10.10.2 on 192.168.0.2, from node 192.168.0.1 (bw)
```
Last Signalled Error: Fri Jan 13 16:38:53 2017
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 Jan 13 15:46:45 2017 (00:53:44 ago)
Config Parameters:
- Bandwidth: 30000 kbps (CT0) Priority: 7 7 Affinity: 0x0/0xffffffff
- 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: Fri Jan 13 16:38:53 2017 (00:01:36 ago)
  Addresses of preempting links:
  10.10.10.1: Fri Jan 13 16:38:53 2017 (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 Jan 13 15:47:43 EDT 2017)
- Current LSP:
  Uptime: 00:52:46 (since Thu Jan 13 15:47:43 EDT 2017)
- Reopt. LSP:
  Last Failure:
  LSP not signalled, has no S2Ls
  Date/Time: Thu Jan 13 16:40:24 EDT 2017 [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 Jan 13 15:47:43 EDT 2017)
- Outgoing Interface: HundredGigE0/0/0/3, Outgoing Label: 16002
- Router-IDs: local 192.168.0.1
downstream 192.168.0.2
- Soft Preemption: Pending
  Preemption Link: HundredGigE0/0/0/3; Address: 10.10.10.1
  Preempted at: Fri Jan 13 16:38:53 2017 (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
Fsacle: avg rate=30000 kbits, burst=1000 bytes, peak rate=30000 kbits
Displayed 1 (of 4) heads, 0 (of 0) midpoints, 0 (of 2) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads

This is sample output from the show mpls traffic-eng tunnels command with the mesh keyword:

RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels auto-tunnel
Signalling Summary:
LSP Tunnels Process: running
RSVP Process: running
Forwarding: enabled
Periodic reoptimization: every 3600 seconds, next in 3098 seconds
Periodic FRR Promotion: every 300 seconds, next in 238 seconds
Auto-bw enabled tunnels: 1000

Name: tunnel-te9000  Destination: 20.20.20.20 (auto-tunnel mesh)
Status:
Admin: up  Oper: up  Path: valid  Signalling: connected
path option 10, type dynamic (Basis for Setup, path weight 11)
G-VID: 0x0800 (derived from egress interface properties)
Bandwidth Requested: 0 kbps  CT0
Creation Time: Fri Jan 14 09:09:31 2010 (01:41:20 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
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 Fri Jan 14 09:09:58 EST 2010)
Current LSP:
Uptime: 01:41:00 (since Fri Jan 14 09:09:51 EST 2010)
Reopt. LSP:
Last Failure:
LSP not signalled, identical to the [CURRENT] LSP
Date/Time: Fri Jan 14 09:42:30 EST 2010 [01:08:21 ago]
Path info (OSPF 100 area 0):
Hop0: 7.0.15.1
Hop1: 20.20.20.20

This shows an auto-tunnel mesh summary sample output from the show mpls traffic-eng tunnels command using the summary keyword:

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

This sample output displays the Signalled-Name information:

```
RP/0/RP0/CPU0:router#show mpls traffic-eng tunnels
Name: tunnel-te1 Destination: 192.168.0.4
Signalled-Name: rtrA_t1
Status:
   Admin: up Oper: up Path: valid Signalling: connected

This sample output displays the cost-limit configuration information:

RP/0/RP0/CPU0:router#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: Fri Jan 15 13:00:29 2014 (5d06h ago)
Config Parameters:
   Bandwidth: 0 kbps (CT0) Priority: 7 7 Affinity: 0x0/0xffffffff
   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: HundredGigE0/0/0/3; Address: 14.14.14.2
    Traffic switched to FRR backup tunnel-te 1000
    Preempted at: Fri Jan 27 12:56:14 2017 (00:00:03 ago)
    Time left before hard preemption: 96 seconds
.
.
.

MPLS Command Reference for Cisco NCS 5000 Series Routers
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**
XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
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 70: 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>
<tr>
<td>LSP ID</td>
<td>ID of the Label Switched Path that is used by the tunnel.</td>
</tr>
<tr>
<td>Last appl BW (kbps)</td>
<td>Last bandwidth applied (for example, requested) by the automatic-bandwidth feature for the tunnel.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requested BW (kbps)</td>
<td>Bandwidth that is requested for the tunnel.</td>
</tr>
<tr>
<td>Signalled BW (kbps)</td>
<td>Bandwidth that is actually signalled for the tunnel.</td>
</tr>
<tr>
<td>Highest BW (kbps)</td>
<td>Highest bandwidth measured since the last start of the application interval.</td>
</tr>
<tr>
<td>Application Time Left</td>
<td>Time left until the application period ends for this tunnel.</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 XR EXEC mode.

show mpls traffic-eng link-management soft-preemption [interface type interface-path-id]

Syntax Description

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

XR EXEC mode

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</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 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 link-management soft-preemption command:

RP/0/RP0/CPU0:router# show mpls traffic-eng link-management soft-preemption interface HundredGigE0/0/0/3
Name: HundredGigE0/0/0/3; IPv4 Address: 10.2.1.10
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>10.4.4.40</td>
<td>10.1.1.10</td>
<td>2/2</td>
<td>400</td>
<td>BC0</td>
<td>100</td>
</tr>
<tr>
<td>51</td>
<td>11</td>
<td>10.4.4.40</td>
<td>10.1.1.10</td>
<td>2/2</td>
<td>600</td>
<td>BC0</td>
<td>100</td>
</tr>
<tr>
<td>52</td>
<td>12</td>
<td>10.4.4.40</td>
<td>10.1.1.10</td>
<td>3/3</td>
<td>200</td>
<td>BC0</td>
<td>80</td>
</tr>
<tr>
<td>53</td>
<td>11</td>
<td>10.4.4.40</td>
<td>10.1.1.10</td>
<td>3/3</td>
<td>500</td>
<td>BC1</td>
<td>90</td>
</tr>
<tr>
<td>54</td>
<td>12</td>
<td>10.4.4.40</td>
<td>10.1.1.10</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 XR EXEC mode.

```
show srlg [group group-name] [inherit-location {location}] [interface type interface-path-id] [location {name | mgmt-nodes}] [mapping {locationname}] [name name] [optical-interface {locationinterface-id}] [producers name] [value value-number] [trace {file filename original | hexdump | last entries | reverse | stats | tailf | unique | verbose | wrapping}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>group</code></td>
<td>(Optional) Specifies a group.</td>
</tr>
<tr>
<td><code>group-name</code></td>
<td>(Optional) Specifies a particular location.</td>
</tr>
<tr>
<td><code>inherit-location</code></td>
<td>(Optional) Specifies a particular location.</td>
</tr>
<tr>
<td><code>location</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>type</code></td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Node ID. The node-id argument is entered in the rack/slot/module notation.</td>
</tr>
<tr>
<td><code>node-id</code></td>
<td>Specifies a node.</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>mapping</code></td>
<td>(Optional) Specifies a mapping</td>
</tr>
<tr>
<td><code>location</code></td>
<td>Node location</td>
</tr>
<tr>
<td><code>name</code></td>
<td>Name of the mapping</td>
</tr>
<tr>
<td><code>name name</code></td>
<td>(Optional) Specifies an SRLG name.</td>
</tr>
<tr>
<td><code>optical-interface</code></td>
<td>(Optional) Specifies an optical interface.</td>
</tr>
<tr>
<td><code>interface-id</code></td>
<td>(Optional) Specifies a SRLG producer.</td>
</tr>
<tr>
<td><code>producers</code></td>
<td>(Optional) Specifies a SRLG producer.</td>
</tr>
<tr>
<td><code>value</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</code></td>
<td>(Optional) Displays trace information for a specific file name.</td>
</tr>
<tr>
<td><code>filename</code></td>
<td></td>
</tr>
</tbody>
</table>

For more information about the syntax for the router, use the question mark (?) online help function.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>original</td>
<td>Displays the original location of the file.</td>
</tr>
<tr>
<td>hexdump</td>
<td>(Optional) Displays traces in hexadecimal format.</td>
</tr>
<tr>
<td>last</td>
<td>(Optional) Displays trace information for a specific number of entries.</td>
</tr>
<tr>
<td>entries</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>reverse</td>
<td>(Optional) Displays the latest traces first.</td>
</tr>
<tr>
<td>stats</td>
<td>(Optional) Displays the statistics in the command output.</td>
</tr>
<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**
XR EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.2.1</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>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)
```
show srlg

Interface : HundredGigE0/0/0/3, Value Count : 2
SRLG Values : 10,20

Interface : HundredGigE0/0/0/3, Value Count : 2
SRLG Values : 10,30

Interface : HundredGigE0/0/0/3, Value Count : 2
SRLG Values : 10,40

Interface : HundredGigE0/0/0/3, Value Count : 1
SRLG Values : 100
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>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

```
Task ID
mpls-te read, write
```

**Examples**

The following example shows how to set the tunnel name:

```
RP/0/RP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RP0/CPU0:router(config-if)# signalled-name tunnel-from-NY-to-NJ
```
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>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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
```
### 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 XR Config mode. To disable this behavior, use the `no` form of this command.

**Syntax**

```
snmp traps mpls traffic-eng [notification-option] preempt
no snmp traps mpls traffic-eng [notification-option]
```

**Syntax Description**

<table>
<thead>
<tr>
<th><code>notification-option</code> (Optional) Notification option to enable the sending of notifications to indicate changes in the status of MPLS-TE tunnels. Use one of these values:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• up</td>
</tr>
<tr>
<td>• down</td>
</tr>
<tr>
<td>• reoptimize</td>
</tr>
<tr>
<td>• reroute</td>
</tr>
<tr>
<td>• cisco-ext</td>
</tr>
</tbody>
</table>

**preempt**

Enables MPLS-TE tunnel preempt trap.

**Command Default**

None

**Command Modes**

XR Config mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the command is entered without the `notification-option` argument, all MPLS-TE notification types are enabled.

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

The `snmp-server enable traps mpls traffic-eng` command enables both traps and inform requests for the specified notification types. To specify whether the notifications should be sent as traps or informs, use the `snmp-server host` command and specify the keyword `trap` or `informs`.

If you do not enter the `snmp traps mpls traffic-eng` command, no MPLS-TE notifications controlled by this command are sent. To configure the router to send these MPLS-TE SNMP notifications, you must enter at least one `snmp enable traps mpls traffic-eng` command. If you enter the command with no keywords, all MPLS-TE notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. To enable multiple types of MPLS-TE notifications, you must issue a separate `snmp traps mpls traffic-eng` command for each notification type and notification option.

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

For a host to receive an MPLS-TE notification controlled by this command, both the `snmp traps mpls traffic-eng` command and the `snmp host` command for that host must be enabled.
Task ID  | Operations ID
-------|---------------
mpls-te | read/write

Examples

This example shows how to configure a router to send MPLS-TE tunnel up SNMP notifications when a configured MPLS-TE tunnel leaves the down state and enters the up state:

```
RP/0/RP0/CPU0:router(config)# snmp traps mpls traffic-eng up
```
**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><code>timeout seconds</code></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>6.2.1</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>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)#
```
**soft-preemption frr-rewrite**

To enable LSP traffic over backup tunnel, when LSP is soft-preempted, use the `soft-preemption frr-rewrite` command in MPLS TE configuration mode. To disable the LSP traffic over backup tunnel, use the `no` form of this command.

```plaintext
soft-preemption frr-rewrite
no soft-preemption frr-rewrite
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

FRR LSP traffic over backup tunnel is disabled.

**Command Modes**

MPLS TE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The fast re-route backup tunnel must be available and ready for the traffic of the preempted LSP to be moved onto the FRR backup. The traffic will not be moved to the backup tunnel, if an LSP is already soft-preempted.

**Task ID**

`mpls-te` read, write

This example shows how to enable FRR LSP traffic over backup tunnels, when the LSP is soft-preempted.

```
RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)#mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)#soft-preemption frr-rewrite
```
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**

- MPLS-TE interface configuration
- XR Config mode

**Command History**

- **Release 6.2.1**: This command was introduced.

**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**

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

**Examples**

The following example shows how to configure an SRLG with 10 member links:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# interface HundredGigE 0/0/0/3
RP/0/RP0/CPU0:router(config-mpls-te-if)# srlg 10

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# srlg
RP/0/RP0/CPU0:router(config-srlg)# interface HundredGigE 0/0/0/3
RP/0/RP0/CPU0:router(config-srlg-if)# value 10
```
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>Release 6.2.1</td>
<td>This command was introduced</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
No specific guidelines impact the use of this command.

**Task ID**
- Task ID
  - mpls-te read, write

**Examples**
The following example shows how to the period between retries after path errors to 300 seconds:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# timers loose-path retry-period 300
```
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>Release 6.2.1</td>
<td>This command was introduced</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `unused` auto-tunnel backup tunnel is the tunnel that is not assigned to protect any FRR tunnel.

**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 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
```
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 Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>timeout seconds</code>  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>Release 6.2.1</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>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>Release 6.2.1</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 ID**: 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
```
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>Release 6.2.1</td>
<td>This command was introduced</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you increase the tunnel ID range, the automatic backup tunnels that failed earlier will get created the next time automatic backup assignments are processed.

**Restrictions:**

- Command is rejected if the `max` value minus `min` value is >= 1K.
- Command is rejected if `min` value > `max` value.
- Command is rejected if `min` value is greater than the tunnel ID of an existing automatic backup tunnel.
- Command is rejected if `max` value is smaller than the tunnel ID of an existing automatic backup tunnel.
- Command is rejected if a statically configured tunnel ID matches with the configured `min` and `max` range of values.
- Command is rejected if a static backup assignment is already configured to a tunnel with an ID within the `min` value / `max` value range.

**Task ID**

- `mpls-te` read,
  write

---

MPLS Command Reference for Cisco NCS 5000 Series Routers
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
```
tunnel-id (auto-tunnel backup)
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 442
- echo disable-vendor-extension, on page 443
- mpls oam, on page 444
- ping mpls ipv4, on page 445
- show mpls oam, on page 450
- show mpls oam database, on page 452
- traceroute mpls ipv4, on page 453
- traceroute mpls multipath, on page 457
# clear mpls oam counters

To clear MPLS OAM counters, use the `clear mpls oam counters` command in XR EXEC mode.

```
clear mpls oam counters  {global | interface  [{type  interface-path-id}] | packet}
```

## Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>global</strong></td>
<td>Clears global counters.</td>
</tr>
<tr>
<td><strong>interface</strong></td>
<td>Clears counters on a specified interface.</td>
</tr>
<tr>
<td><strong>type</strong></td>
<td>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>
</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

XR EXEC mode

## 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

No specific guidelines impact the use of this command.

## Task ID

### Task ID Operations

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<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>6.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

No specific guidelines impact the use of this command.

**Task ID**

```
Task ID    Operations
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
```
To enable MPLS OAM LSP verification, use the `mpls oam` command in XR Config 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**

XR Config mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 6.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `mpls oam` command and OAM functionality is described in the RFC 4379.

**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-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 XR EXEC mode.

```
ping mpls ipv4  address/mask [destination start-address end-address increment] [dsmap] [exp exp-bits] [force-explicit-null] [interval min-send-delay] [output interface type interface-path-id [nexthop nexthop-address]] [pad pattern] [repeat count] [reply {dscp dscp-value | reply mode {ipv4 | no-reply | router-alert} | reply pad-tlv}] [size packet-size] [source source-address] [sweep min-value max-value increment] [timeout timeout] [ttl value] [verbose] [fec-type {bgp | generic | ldp}]
```

### Syntax Description

<table>
<thead>
<tr>
<th><strong>address/mask</strong></th>
<th>Address prefix of the target and number of bits in the target address network mask.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>destination</strong></td>
<td>(Optional) Specifies a network 127/8 address to be used as the destination address in the echo request packet.</td>
</tr>
<tr>
<td><strong>start address</strong></td>
<td>Start of the network address.</td>
</tr>
<tr>
<td><strong>end address</strong></td>
<td>Start of the ending network address.</td>
</tr>
<tr>
<td><strong>address increment</strong></td>
<td>Incremental value of the network address, which is expressed as a decimal number value or IP address.</td>
</tr>
<tr>
<td><strong>dsmap</strong></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><strong>exp exp-bits</strong></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><strong>force-explicit-null</strong></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><strong>interval min-send-delay</strong></td>
<td>(Optional) Specifies a send interval, in milliseconds, between requests. Range is 0 to 3600000. Default is 0.</td>
</tr>
<tr>
<td><strong>output interface</strong></td>
<td>(Optional) Specifies the output interface where echo request packets are sent.</td>
</tr>
<tr>
<td><strong>type</strong></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</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.</td>
</tr>
<tr>
<td></td>
<td>For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>nexthop</td>
<td>(Optional) Specifies the nexthop 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>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>source source-address</td>
<td>(Optional) Specifies the source address used in the echo request packet.</td>
</tr>
</tbody>
</table>
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.

fec-type

(Optional) Specifies FEC type to be used.

generic

Use FEC type as generic

ldp

Use FEC type as LDP

Command Default

exp exp bits: 0

interval min-send-delay: 0

repeat count: 5

reply-mode: IPv4

timeout timeout: 2

Command Modes

XR EXEC mode

Command History

Release Modification

Release 6.0 This command was introduced.

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.

**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.

**Examples**

The following example shows the destination type as a label distribution protocol (LDP) prefix and specifies a range of sizes for the echo packets sent:

```
RP/0/RP0/CPU0:router# ping mpls ipv4 7.7.7.7/32 verbose sweep 100 200 15 repeat 1

Sending 1, [100..200]-byte MPLS Echos to 7.7.7.7/32, timeout is 2 seconds, send interval is 0 msec:


Type escape sequence to abort.

! size 100, reply addr 178.0.0.1, return code 3
! size 115, reply addr 178.0.0.1, return code 3
! size 130, reply addr 178.0.0.1, return code 3
! size 145, reply addr 178.0.0.1, return code 3
! size 160, reply addr 178.0.0.1, return code 3
! size 175, reply addr 178.0.0.1, return code 3
! size 190, reply addr 178.0.0.1, return code 3

Success rate is 100 percent (7/7), round-trip min/avg/max = 2/2/4 ms
```

The following example shows the destination type as a label distribution protocol (LDP) prefix and specifies FEC type as generic and verbose option:

```
RP/0/RP0/CPU0:router# ping mpls ipv4 7.7.7.7/32 fec-type generic output interface TenGigE 0/0/0/11 nexthop 79.1.0.2 verbose

Sending 5, 100-byte MPLS Echos to 7.7.7.7/32, timeout is 2 seconds, send interval is 0 msec:


Type escape sequence to abort.

! size 100, reply addr 178.0.0.1, return code 3
! size 130, reply addr 178.0.0.1, return code 3
! size 145, reply addr 178.0.0.1, return code 3
! size 160, reply addr 178.0.0.1, return code 3
! size 175, reply addr 178.0.0.1, return code 3
! size 190, reply addr 178.0.0.1, return code 3

Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/4 ms
```
'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

! size 100, reply addr 178.0.0.1, return code 3
! size 100, reply addr 178.0.0.1, return code 3
! size 100, reply addr 178.0.0.1, return code 3
! size 100, reply addr 178.0.0.1, return code 3
! size 100, reply addr 178.0.0.1, return code 3

Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
show mpls oam

To display MPLS OAM information, use the **show mpls oam** command in XR 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>client</td>
<td>Displays clients registered with LSPV server.</td>
</tr>
<tr>
<td>counters global</td>
<td>Displays LSP verification global counters.</td>
</tr>
<tr>
<td>counters packet</td>
<td>Displays LSP verification packet counters.</td>
</tr>
<tr>
<td>interface</td>
<td>Displays LSP verification information for a specific 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.

**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>Release 6.0</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-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//RP0//CPU0:router# show mpls oam client
Client Process: l2vpn_mgr Node: 0/RP0/CPU0 Pid: 7200 Service: 3
Client Process: mpls_ldp Node: 0/RP0/CPU0 Pid: 7201 Service: 2
Client Process: bgp Node: 0/RP0/CPU0 Pid: 7488 Service: 5
```
This table describes the significant fields shown in the display.

Table 71: 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 XR EXEC mode.

```
show mpls oam database  { requests | tt-requests} [detail] [handle  handle-value ]
```

### Syntax Description
- **requests**: Displays request database
- **tt-requests**: Displays tree trace request database
- **detail**: (Optional) Displays displayed information.
- **handle**: (Optional) Displays handle information.
- **handle-value**: Generic handle value. Range is from 0 to 4294967295.

### Command Default
No default behavior or values

### Command Modes
XR EXEC mode

### Command History
- **Release 6.0**: This command was introduced.

### Usage Guidelines
No specific guidelines impact the use of this command.

### Task ID
- **Task ID**
  - **mpls-ldp**: read
  - **mpls-static**: read

### Examples
The following example shows how to display detailed MPLS OAM database information:

```
RP/0/RP0/CPU0:router# show mpls oam database request detail
```
**traceroute mpls ipv4**

To learn the routes that packets follow when traveling to their Label Distribution Protocol (LDP) IPv4 destination, use the **traceroute mpls** command in XR EXEC mode.

```
traceroute mpls ipv4address/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] | [nexthop nexthop-address]]] [reply {dscp dscp-value | reply mode {ipv4 | router-alert}}] [source source-address] [timeout timeout] [ttl value] [verbose] [fec-type {bgp | generic | ldp}]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</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 start-address end-address address-increment</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>Note</td>
<td>Use the <strong>show interfaces</strong> command to see a list of all interfaces currently configured on the router.</td>
</tr>
<tr>
<td></td>
<td>For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>nexthop</td>
<td>(Optional) Specifies the IP address for the next hop.</td>
</tr>
</tbody>
</table>
### traceroute mpls ipv4

- **nexthop-address**: (Optional) IP address for the next hop.

- **reply dscp dscp-value**: (Optional) Specifies the differentiated service codepoint value for an MPLS echo reply.

- **reply mode** { **ipv4** | **router-alert** }:
  - (Optional) Specifies the reply mode for the echo request packet.
  - **ipv4**: Reply with IPv4 UDP packet (this is the default)
  - **router-alert**: Reply with IPv4 UDP packet with router alert

- **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.

- **fec-type**: (Optional) Specifies FEC type to be used.
  - **bgp**: Use FEC type as BGP
  - **generic**: Use FEC type as generic
  - **ldp**: Use FEC type as LDP

### Command Default
- **exp exp-bits**: 0
- **reply mode**: IPv4
- **timeout timeout**: 2

### Command Modes
- XR EXEC mode

### 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

**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 System Monitoring Configuration Guide.

### Examples

The following example shows how to trace a destination:

RP/0/RP0/CPU0:router# traceroute mpls ipv4 7.7.7.7/32 destination 127.0.0.10 127.0.0.15 1

Tracing MPLS Label Switched Path to 7.7.7.7/32, timeout is 2 seconds

Codes: '!'-success, 'Q'-request not sent, '.'-timeout,  
'L'-labeled output interface, 'B'-unlabeled output interface,  
'D'-DS Map mismatch, 'F'-no FEC mapping, 'f'-FEC mismatch,  
'M'-malformed request, 'm'-unsupported tlvs, 'N'-no rx label,  
'P'-no rx intf label prot, 'p'-premature termination of LSP,  
'R'-transit router, 'I'-unknown upstream index,  
'X'-unknown return code, 'x'-return code 0

Type escape sequence to abort.

Destination address 127.0.0.10  
0 79.4.0.1 MRU 1500 [Labels: 24008 Exp: 0]  
L 1 79.4.0.2 MRU 1500 [Labels: implicit-null Exp: 0] 5 ms  
! 2 178.0.0.1 4 ms

Destination address 127.0.0.11  
0 79.5.0.1 MRU 1500 [Labels: 24008 Exp: 0]  
L 1 79.5.0.2 MRU 1500 [Labels: implicit-null Exp: 0] 3 ms  
! 2 178.0.0.1 2 ms

Destination address 127.0.0.12  
0 79.1.0.1 MRU 1500 [Labels: 24008 Exp: 0]  
L 1 79.1.0.2 MRU 1500 [Labels: implicit-null Exp: 0] 3 ms  
! 2 178.0.0.1 2 ms

Destination address 127.0.0.13  
0 79.4.0.1 MRU 1500 [Labels: 24008 Exp: 0]  
L 1 79.4.0.2 MRU 1500 [Labels: implicit-null Exp: 0] 3 ms  
! 2 178.0.0.1 2 ms

Destination address 127.0.0.14  
0 79.4.0.1 MRU 1500 [Labels: 24008 Exp: 0]  
L 1 79.4.0.2 MRU 1500 [Labels: implicit-null Exp: 0] 3 ms  
! 2 178.0.0.1 2 ms

The following example shows how to trace a destination with FEC type specified as generic and verbose option:

RP/0/RP0/CPU0:router# router#traceroute mpls ipv4 7.7.7.7/32 fec-type generic output interface TenGigE 0/0/0/11.1 nexthop 79.1.0.2 verbose
Tracing MPLS Label Switched Path to 7.7.7.7/32, timeout is 2 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

0 79.1.0.1 79.1.0.2 MRU 1500 [Labels: 24008 Exp: 0]
L 1 79.1.0.2 178.0.0.1 MRU 1500 [Labels: implicit-null Exp: 0] 4 ms, ret code 8
! 2 178.0.0.1 3 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 XR EXEC mode.

```
traceroute mpls multipath ipv4 address/mask [destination start-address/end-address] [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] [nexthop nexthop-address]] [reply dscp dscp-value | reply mode {ipv4 | router-alert}] [retry-count count] [source source-address] [timeout timeout] [ttl value] [verbose] [fec-type {bgp | generic | ldp}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ipv4</strong></td>
<td>Specifies the destination type as a Label Distribution Protocol (LDP) IPv4 address.</td>
</tr>
<tr>
<td><strong>address/mask</strong></td>
<td>Address prefix of the target and number of bits in the target address network mask.</td>
</tr>
<tr>
<td><strong>destination</strong></td>
<td>(Optional) Specifies a network 127 address to be used as the destination address in the echo request packet.</td>
</tr>
<tr>
<td><strong>start-address</strong></td>
<td>Start of the network address.</td>
</tr>
<tr>
<td><strong>end-address</strong></td>
<td>End of the network address.</td>
</tr>
<tr>
<td><strong>exp exp-bits</strong></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><strong>flags fec</strong></td>
<td>(Optional) Specifies that forwarding equivalent class (FEC) stack checking is to be performed at transit routers.</td>
</tr>
<tr>
<td><strong>force-explicit-null</strong></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><strong>hashkey ipv4 bitmap bit-size</strong></td>
<td>(Optional) Allows user control of the hash key/multipath settings. Range is 0 to 256. The default is 32.</td>
</tr>
<tr>
<td><strong>interval min-send-delay</strong></td>
<td>(Optional) Specifies a send interval, in milliseconds, between requests. Range is 0 to 3600000. Default is 0.</td>
</tr>
<tr>
<td><strong>output interface</strong></td>
<td>(Optional) Specifies the output interface where echo request packets are sent.</td>
</tr>
<tr>
<td><strong>type</strong></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
</tbody>
</table>
interface-path-id | Physical interface or virtual interface.

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

For more information, use the question mark (?) online help function.

| nexthop | (Optional) Specifies the IP address for the next hop.
| nexthop-address | (Optional) IP address for the next hop.
| reply dscp `dscp-value` | (Optional) Specifies the differentiated service codepoint value for an MPLS echo reply.
| reply mode [ `ipv4` | `router-alert` ] | (Optional) Specifies the reply mode for the echo request packet.
| reply mode `ipv4` | Reply with IPv4 UDP packet (this is the default)
| reply mode `router-alert` | Reply with IPv4 UDP packet with router alert
| retry-count `count` | (Optional) Specifies the number of retry attempts during multipath LSP traceroute. A retry is attempted if an outstanding echo request
| | • times out waiting for the corresponding echo reply.
| | • fails to find a valid destination address set to exercise a specific outgoing path. Range is 0 to 10. Default is 3.
| 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.
| fec-type | (Optional) Specifies FEC type to be used.

- **bgp**
  Use FEC type as BGP

- **generic**
  Use FEC type as generic

- **ldp**
  Use FEC type as LDP

**Command Default**

- `exp exp-bits : 0`
- `hashkey ipv4 bitmap bit-size: 4`
interval min-send-delay: 0
reply mode: IPv4
retry-count: 3
timeout: 2

Command Modes
XR EXEC mode

Command History
Release Modification
Release 6.0 This command was introduced.

Usage Guidelines
The hashkey ipv4 bitmap keyword and bit-size value control how many addresses are encoded in the DSMP 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
mpls-ldp read, write

Examples
The following example shows how to specify the destination type as an LDP IPv4 prefix:

RP/0/RP0/CPU0:router# traceroute mpls multipath ipv4 7.7.7.32 verbose force-explicit-null

Starting LSP Path Discovery for 7.7.7.32

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.

L!
Path 0 found,
output interface TenGigE0/0/0/11.1 nexthop 79.1.0.2
source 79.1.0.1 destination 127.0.0.0
  0 79.1.0.1 79.1.0.2 MRU 1500 [Labels: 24008/explicit-null Exp: 0/0] multipaths 0
  L 1 79.1.0.2 178.0.0.1 MRU 1500 [Labels: implicit-null/explicit-null Exp: 0/0] ret code 8
  multipaths 1
  ! 2 178.0.0.1, ret code 3 multipaths 0
L!
Path 1 found,
output interface TenGigE0/0/0/11.1 nexthop 79.2.0.2
source 79.2.0.1 destination 127.0.0.0
  0 79.2.0.1 79.2.0.2 MRU 1500 [Labels: 24008/explicit-null Exp: 0/0] multipaths 0
  L 1 79.2.0.2 178.0.0.1 MRU 1500 [Labels: implicit-null/explicit-null Exp: 0/0] ret code 8
  multipaths 1
  ! 2 178.0.0.1, ret code 3 multipaths 0
L!
Path 2 found,
output interface TenGigE0/0/0/11.4 nexthop 79.4.0.2
  source 79.4.0.1 destination 127.0.0.0
  0 79.4.0.1 79.4.0.2 MRU 1500 [Labels: 24008/explicit-null Exp: 0/0] multipaths 0
L 1 79.4.0.2 178.0.0.1 MRU 1500 [Labels: implicit-null/explicit-null Exp: 0/0] ret code 8 multipaths 1
  ! 2 178.0.0.1, ret code 3 multipaths 0
L! Path 3 found,
output interface TenGigE0/0/0/11.5 nexthop 79.5.0.2
  source 79.5.0.1 destination 127.0.0.0
  0 79.5.0.1 79.5.0.2 MRU 1500 [Labels: 24008/explicit-null Exp: 0/0] multipaths 0
L 1 79.5.0.2 178.0.0.1 MRU 1500 [Labels: implicit-null/explicit-null Exp: 0/0] ret code 8 multipaths 1
  ! 2 178.0.0.1, ret code 3 multipaths 0
Paths (found/broken/unexplored) (4/0/0)
  Echo Request (sent/fail) (8/0)
  Echo Reply (received/timeout) (8/0)
  Total Time Elapsed 44 ms

The following example shows how to specify the FEC type as LDP with verbose option:

RP/0/RP0/CPU0:router# traceroute mpls multipath ipv4 7.7.7.7/32 fec-type ldp output interface TenGigE 0/0/0/11 nexthop 79.1.0.2

Starting LSP Path Discovery for 7.7.7.7/32

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.

L! Path 0 found,
output interface TenGigE0/0/0/11.1 nexthop 79.1.0.2
  source 79.1.0.1 destination 127.0.0.0
  0 79.1.0.1 79.1.0.2 MRU 1500 [Labels: 24008 Exp: 0] multipaths 0
L 1 79.1.0.2 178.0.0.1 MRU 1500 [Labels: implicit-null/explicit-null Exp: 0] ret code 8 multipaths 1
  ! 2 178.0.0.1, ret code 3 multipaths 0
Paths (found/broken/unexplored) (1/0/0)
  Echo Request (sent/fail) (2/0)
  Echo Reply (received/timeout) (2/0)
  Total Time Elapsed 10 ms
INDEX

W

window-size (RSVP) command  211