Nokia is a registered trademark of Nokia Corporation. Other products and company names mentioned herein may be trademarks or tradenames of their respective owners.

The information presented is subject to change without notice. No responsibility is assumed for inaccuracies contained herein.

© 2016-2017 Nokia.

Contains proprietary/trade secret information which is the property of Nokia and must not be made available to, or copied or used by anyone outside Nokia without its written authorization. Not to be used or disclosed except in accordance with applicable agreements.
Table of Contents

1 Preface .................................................................................................................. 13
1.1 About This Guide ......................................................................................... 13
1.1.1 Audience ............................................................................................. 14
1.1.2 List of Technical Publications ........................................................... 14
1.1.3 Technical Support ............................................................................... 15

2 7705 SAR MPLS Configuration Process ....................................................... 17

3 MPLS and RSVP-TE ....................................................................................... 19
3.1 Overview .................................................................................................... 20
3.2 MPLS ......................................................................................................... 21
3.2.1 Traffic Engineering for MPLS ............................................................... 21
3.2.1.1 TE Metric and IGP Metric ............................................................... 22
3.2.2 MPLS Label Stack ................................................................................. 23
3.2.2.1 Label Values .................................................................................... 24
3.2.3 MPLS Entropy Labels ........................................................................... 26
3.2.3.1 Overview of Entropy Labels ............................................................. 26
3.2.3.2 Inserting and Processing the Entropy Label .................................... 28
3.2.3.3 Entropy Label on OAM Packets ...................................................... 29
3.2.3.4 Entropy Label Configuration .......................................................... 30
3.2.4 Label Edge and Label Switch Routers .................................................. 31
3.2.5 LSP Types .......................................................................................... 31
3.3 RSVP and RSVP-TE .................................................................................. 33
3.3.1 RSVP-TE Overview ............................................................................. 33
3.3.1.1 Using RSVP-TE for MPLS ............................................................... 35
3.3.1.2 RSVP-TE Extensions for MPLS ...................................................... 35
3.3.1.3 Hello Protocol ................................................................................ 36
3.3.1.4 Authentication ................................................................................. 37
3.3.1.5 Non-Router ID Addresses as Destinations and Hops ....................... 39
3.4 RSVP-TE Signaling ................................................................................... 40
3.4.1 General Attributes of RSVP-TE ........................................................... 40
3.4.1.1 OAM: BFD ...................................................................................... 41
3.4.1.2 Timers ............................................................................................ 41
3.4.1.3 LSP Resignal Limit ......................................................................... 42
3.4.1.4 RSVP-TE Message Pacing .............................................................. 42
3.4.1.5 RSVP-TE Overhead Refresh Reduction .......................................... 43
3.4.1.6 RSVP-TE Reservation Styles .......................................................... 44
3.4.1.7 RSVP-TE Entropy Labels ................................................................. 44
3.4.1.8 LSP Redundancy ............................................................................ 45
3.4.1.9 Make-Before-Break (MBB) Procedures for LSP and Path Parameter
......................................................................................................................... 46
3.5 LSP Redundancy ....................................................................................... 45
3.5.1 Automatic Creation of RSVP-TE LSPs ................................................ 47
3.5.2 Automatic Creation of RSVP-TE LSP Mesh (Auto-LSP) ...................... 47
3.5.3 Multi-Area and Multi-Instance Support ............................................... 49
3.5.3.1 Mesh LSP Name Encoding ............................................................... 50
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.5.4</td>
<td>Automatic Creation of an RSVP-TE Single-Hop LSP</td>
</tr>
<tr>
<td>3.5.5</td>
<td>Automatic ABR Selection for Inter-area LSPs</td>
</tr>
<tr>
<td>3.5.5.1</td>
<td>Rerouting of Inter-area LSPs</td>
</tr>
<tr>
<td>3.5.5.2</td>
<td>Behavior of MPLS Options in Inter-area LSPs</td>
</tr>
<tr>
<td>3.5.5.3</td>
<td>Inter-area LSP Support of OSPF Virtual Links</td>
</tr>
<tr>
<td>3.5.6</td>
<td>ABR FRR Protection for Inter-area LSP</td>
</tr>
<tr>
<td>3.6</td>
<td>RSVP-TE Fast Reroute (FRR)</td>
</tr>
<tr>
<td>3.6.1</td>
<td>FRR Terminology</td>
</tr>
<tr>
<td>3.6.2</td>
<td>FRR Behavior</td>
</tr>
<tr>
<td>3.6.3</td>
<td>Dynamic and Manual Bypass LSPs</td>
</tr>
<tr>
<td>3.6.3.1</td>
<td>Bypass LSP Selection Rules for the PLR</td>
</tr>
<tr>
<td>3.6.3.2</td>
<td>FRR Node Protection (Facility Backup)</td>
</tr>
<tr>
<td>3.6.4</td>
<td>Admin Group Support on Facility Bypass Backup LSPs</td>
</tr>
<tr>
<td>3.6.5</td>
<td>FRR Over Unnumbered Interfaces</td>
</tr>
<tr>
<td>3.7</td>
<td>Shared Risk Link Groups</td>
</tr>
<tr>
<td>3.7.1</td>
<td>SRLGs for Secondary LSP Paths</td>
</tr>
<tr>
<td>3.7.2</td>
<td>SRLGs for FRR LSP Paths</td>
</tr>
<tr>
<td>3.7.3</td>
<td>Disjoint and Non-disjoint Paths</td>
</tr>
<tr>
<td>3.7.4</td>
<td>Enabling Disjoint Backup Paths</td>
</tr>
<tr>
<td>3.8</td>
<td>RSVP-TE Graceful Shutdown</td>
</tr>
<tr>
<td>3.9</td>
<td>RSVP-TE Support for Unnumbered Interfaces</td>
</tr>
<tr>
<td>3.10</td>
<td>PCEP Support for RSVP-TE LSPs</td>
</tr>
<tr>
<td>3.11</td>
<td>MPLS Service Usage</td>
</tr>
<tr>
<td>3.11.1</td>
<td>Service Destination Points</td>
</tr>
<tr>
<td>3.12</td>
<td>MPLS and RSVP-TE Configuration Process Overview</td>
</tr>
<tr>
<td>3.13</td>
<td>Configuration Notes</td>
</tr>
<tr>
<td>3.13.1</td>
<td>Reference Sources</td>
</tr>
<tr>
<td>3.14</td>
<td>Configuring MPLS and RSVP-TE with CLI</td>
</tr>
<tr>
<td>3.15</td>
<td>MPLS Configuration Overview</td>
</tr>
<tr>
<td>3.15.1</td>
<td>Router Interface</td>
</tr>
<tr>
<td>3.15.1.1</td>
<td>E-LSP for Differentiated Services</td>
</tr>
<tr>
<td>3.15.2</td>
<td>Paths</td>
</tr>
<tr>
<td>3.15.3</td>
<td>LSPs</td>
</tr>
<tr>
<td>3.15.4</td>
<td>Pseudowires</td>
</tr>
<tr>
<td>3.15.5</td>
<td>Signaling Protocol</td>
</tr>
<tr>
<td>3.16</td>
<td>Basic MPLS Configuration</td>
</tr>
<tr>
<td>3.17</td>
<td>Common Configuration Tasks</td>
</tr>
<tr>
<td>3.17.1</td>
<td>Configuring MPLS Components</td>
</tr>
<tr>
<td>3.17.2</td>
<td>Configuring Global MPLS Parameters</td>
</tr>
<tr>
<td>3.17.3</td>
<td>Configuring an MPLS Interface</td>
</tr>
<tr>
<td>3.17.4</td>
<td>Configuring MPLS Paths</td>
</tr>
<tr>
<td>3.17.5</td>
<td>Configuring an MPLS LSP</td>
</tr>
<tr>
<td>3.17.6</td>
<td>Configuring a Static LSP</td>
</tr>
<tr>
<td>3.17.6.1</td>
<td>Configuring a Fast-Retry Timer for Static LSPs</td>
</tr>
<tr>
<td>3.17.7</td>
<td>Configuring Manual Bypass Tunnels</td>
</tr>
<tr>
<td>3.17.8</td>
<td>Configuring RSVP-TE Parameters and Interfaces</td>
</tr>
<tr>
<td>3.17.9</td>
<td>Configuring RSVP-TE Message Pacing Parameters</td>
</tr>
<tr>
<td>3.18</td>
<td>MPLS Configuration Management Tasks</td>
</tr>
<tr>
<td>3.18.1</td>
<td>Deleting MPLS</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>3.18.2</td>
<td>Modifying MPLS Parameters</td>
</tr>
<tr>
<td>3.18.3</td>
<td>Modifying an MPLS LSP</td>
</tr>
<tr>
<td>3.18.4</td>
<td>Modifying MPLS Path Parameters</td>
</tr>
<tr>
<td>3.18.5</td>
<td>Modifying MPLS Static LSP Parameters</td>
</tr>
<tr>
<td>3.18.6</td>
<td>Deleting an MPLS Interface</td>
</tr>
<tr>
<td>3.19</td>
<td>RSVP-TE Configuration Management Tasks</td>
</tr>
<tr>
<td>3.19.1</td>
<td>Modifying RSVP-TE Parameters</td>
</tr>
<tr>
<td>3.19.2</td>
<td>Modifying RSVP-TE Message Pacing Parameters</td>
</tr>
<tr>
<td>3.19.3</td>
<td>Deleting an Interface from RSVP-TE</td>
</tr>
<tr>
<td>3.20</td>
<td>MPLS and RSVP-TE Command Reference</td>
</tr>
<tr>
<td>3.20.1</td>
<td>Command Hierarchies</td>
</tr>
<tr>
<td>3.20.1.1</td>
<td>MPLS Commands</td>
</tr>
<tr>
<td>3.20.1.2</td>
<td>RSVP-TE Commands</td>
</tr>
<tr>
<td>3.20.1.3</td>
<td>Show Commands</td>
</tr>
<tr>
<td>3.20.1.4</td>
<td>Clear Commands</td>
</tr>
<tr>
<td>3.20.1.5</td>
<td>Debug Commands</td>
</tr>
<tr>
<td>3.20.2</td>
<td>Command Descriptions</td>
</tr>
<tr>
<td>3.20.2.1</td>
<td>Configuration Commands (MPLS)</td>
</tr>
<tr>
<td>3.20.2.2</td>
<td>Configuration Commands (RSVP-TE)</td>
</tr>
<tr>
<td>3.20.2.3</td>
<td>Show Commands (MPLS)</td>
</tr>
<tr>
<td>3.20.2.4</td>
<td>Show Commands (RSVP)</td>
</tr>
<tr>
<td>3.20.2.5</td>
<td>Clear Commands</td>
</tr>
<tr>
<td>3.20.2.6</td>
<td>Debug Commands</td>
</tr>
<tr>
<td>4</td>
<td>PCEP</td>
</tr>
<tr>
<td>4.1</td>
<td>Introduction to the Path Computation Element (PCE)</td>
</tr>
<tr>
<td>4.2</td>
<td>Communication Protocol (PCE)</td>
</tr>
<tr>
<td>4.3</td>
<td>Base Implementation of Path Computation Elements (PCE)</td>
</tr>
<tr>
<td>4.4</td>
<td>PCEP Session Establishment and Maintenance</td>
</tr>
<tr>
<td>4.4.1</td>
<td>PCEP Parameters</td>
</tr>
<tr>
<td>4.4.2</td>
<td>Stateful PCE</td>
</tr>
<tr>
<td>4.4.3</td>
<td>LSP Initiation</td>
</tr>
<tr>
<td>4.4.4</td>
<td>PCC-Initiated and PCE-Computed or PCE-Controlled LSPs</td>
</tr>
<tr>
<td>4.5</td>
<td>PCEP Support for RSVP-TE LSPs</td>
</tr>
<tr>
<td>4.5.1</td>
<td>RSVP-TE LSP Configuration for a PCC Router</td>
</tr>
<tr>
<td>4.5.2</td>
<td>Behavior of the LSP Path Update</td>
</tr>
<tr>
<td>4.5.2.1</td>
<td>Path Update with Empty ERO</td>
</tr>
<tr>
<td>4.5.3</td>
<td>Behavior of LSP MBB</td>
</tr>
<tr>
<td>4.5.3.1</td>
<td>PCC-Controlled LSPs</td>
</tr>
<tr>
<td>4.5.3.2</td>
<td>PCE-Computed LSPs</td>
</tr>
<tr>
<td>4.5.3.3</td>
<td>PCE-Controlled LSPs</td>
</tr>
<tr>
<td>4.5.4</td>
<td>Behavior of Secondary LSP Paths</td>
</tr>
<tr>
<td>4.5.5</td>
<td>PCE Path Profile Support</td>
</tr>
<tr>
<td>4.6</td>
<td>LSP Path Diversity and Bidirectionality Constraints</td>
</tr>
<tr>
<td>4.7</td>
<td>Configuring RSVP-TE LSPs with PCEP Using the CLI</td>
</tr>
<tr>
<td>4.7.1</td>
<td>PCEP on the PCE Node and the PCC Node</td>
</tr>
<tr>
<td>4.7.2</td>
<td>MPLS on the PCC Node</td>
</tr>
<tr>
<td>4.8</td>
<td>PCEP Configuration Command Reference</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>5.8</td>
<td>Basic LDP Configuration</td>
</tr>
<tr>
<td>5.9</td>
<td>Common Configuration Tasks</td>
</tr>
<tr>
<td>5.9.1</td>
<td>Enabling LDP</td>
</tr>
<tr>
<td>5.9.2</td>
<td>Configuring Graceful Restart Helper Parameters</td>
</tr>
<tr>
<td>5.9.3</td>
<td>Applying Import and Export Policies</td>
</tr>
<tr>
<td>5.9.4</td>
<td>Configuring Interface Parameters</td>
</tr>
<tr>
<td>5.9.5</td>
<td>Specifying Targeted Session Parameters</td>
</tr>
<tr>
<td>5.9.6</td>
<td>Specifying Peer Parameters</td>
</tr>
<tr>
<td>5.9.7</td>
<td>Configuring LDP Support for Multicast VPN (MVPN)</td>
</tr>
<tr>
<td>5.9.8</td>
<td>Enabling LDP Signaling and Services</td>
</tr>
<tr>
<td>5.10</td>
<td>LDP Configuration Management Tasks</td>
</tr>
<tr>
<td>5.10.1</td>
<td>Disabling LDP</td>
</tr>
<tr>
<td>5.10.2</td>
<td>Modifying Targeted Session Parameters</td>
</tr>
<tr>
<td>5.10.3</td>
<td>Modifying Interface Parameters</td>
</tr>
<tr>
<td>5.11</td>
<td>LDP Command Reference</td>
</tr>
<tr>
<td>5.11.1</td>
<td>Command Hierarchies</td>
</tr>
<tr>
<td>5.11.1.1</td>
<td>LDP Commands</td>
</tr>
<tr>
<td>5.11.1.2</td>
<td>Show Commands</td>
</tr>
<tr>
<td>5.11.1.3</td>
<td>Clear Commands</td>
</tr>
<tr>
<td>5.11.1.4</td>
<td>Debug Commands</td>
</tr>
<tr>
<td>5.11.2</td>
<td>Command Descriptions</td>
</tr>
<tr>
<td>5.11.2.1</td>
<td>Configuration Commands</td>
</tr>
<tr>
<td>5.11.2.2</td>
<td>Show Commands</td>
</tr>
<tr>
<td>5.11.2.3</td>
<td>Clear Commands</td>
</tr>
<tr>
<td>5.11.2.4</td>
<td>Debug Commands</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Standards and Protocol Support</td>
<td>403</td>
</tr>
</tbody>
</table>
List of Tables

2  7705 SAR MPLS Configuration Process.................................17
   Table 1  Configuration Process .................................................17

3  MPLS and RSVP-TE.................................................................19
   Table 2  Packet/Label Field Description ..................................23
   Table 3  Ingress Label Values (Pop Labels) .................................25
   Table 4  Egress Label Values (Push Labels) .................................25
   Table 5  FRR Terminology .........................................................60
   Table 6  Disabled and Enabled Options for Bypass-Only ..............94
   Table 7  Show Router MPLS Admin-Group Output Fields ............170
   Table 8  Show Router MPLS Bypass-Tunnel Output Fields ..........171
   Table 9  Show Router MPLS Interface Output Fields .................173
   Table 10 Show Router MPLS Label Output Fields ..................175
   Table 11 Show Router MPLS Label Range Output Fields ...........176
   Table 12 Show Router MPLS LSP Output Fields ......................178
   Table 13 Show Router MPLS LSP Detail Output Fields .............179
   Table 14 Show Router MPLS LSP Path Detail Output Fields .......183
   Table 15 Show Router MPLS LSP Path MBB Output Fields ........186
   Table 16 Show Router MPLS Auto LSP Output Fields .................187
   Table 17 Show Router MPLS LSP Template Fields ................188
   Table 18 Show Router MPLS Path Output Fields ....................191
   Table 19 Show Router MPLS SRLG Group Output Fields ..........193
   Table 20 Show Router MPLS Static LSP Output Fields .............194
   Table 21 Show Router MPLS Status Output Fields ................196
   Table 22 Show Router RSVP-TE Interface Output Fields ........198
   Table 23 Show Router RSVP-TE Interface Detail Output Fields .....199
   Table 24 Show Router RSVP-TE Interface Statistics Output Fields 201
   Table 25 Show Router RSVP-TE Neighbor Output Fields ............203
   Table 26 Show Router RSVP-TE Session Output Fields .............204
   Table 27 Show Router RSVP-TE Statistics Output Fields ............205
   Table 28 Show Router RSVP-TE Status Output Fields ...............206

4  PCEP .................................................................................219
   Table 29  Base PCEP TLVs, Objects, and Messages ..................224
   Table 30  PCEP Stateful PCE Extension TLVs, Objects, and Messages 230
   Table 31  PCEP Path Profile Extension Objects and TLVs ..........246
   Table 32  Show PCEP PCC Output Fields .................................264
   Table 33  Show PCEP PCC Peer Output Fields .........................268
   Table 34  Show PCEP PCC Status Output Fields .......................269

5  Label Distribution Protocol ..................................................271
   Table 35  Hello Timeout Factor Default Values .......................330
   Table 36  Keepalive Timeout Factor Default Values .................332
   Table 37  LDP Auth-keychain Output Fields ..........................344
   Table 38  LDP Bindings Output Fields .....................................347
Table 39  LDP Discovery Output Fields .................................................................353
Table 40  FEC-Originate Output Fields .................................................................356
Table 41  LDP Interface Output Fields .................................................................357
Table 42  LDP Parameters Output Fields ...............................................................359
Table 43  LDP Peer Output Fields ......................................................................362
Table 44  LDP Peer-Parameter Output Fields .......................................................364
Table 45  LDP Session Output Fields ...................................................................366
Table 46  LDP Status Output Fields .................................................................367

6  List of Acronyms ...............................................................................................375
Table 47  Acronyms ...............................................................................................375

7  Standards and Protocol Support .................................................................403
Table 48  EMC Industrial Standards Compliance ...................................................404
Table 49  EMC Regulatory and Customer Standards Compliance ......................405
Table 50  Environmental Standards Compliance ..................................................408
Table 51  Safety Standards Compliance ..............................................................409
Table 52  Telecom Interface Compliance .............................................................411
Table 53  Directives, Regional Approvals and Certifications Compliance ..............412
## List of Figures

**3**  
MPLS and RSVP-TE ................................................................. 19  
Figure 1  
Label Structure ............................................................................. 23  
Figure 2  
Label Packet Placement ............................................................... 24  
Figure 3  
Entropy Label and Load Balancing ............................................... 30  
Figure 4  
Establishing LSPs ......................................................................... 34  
Figure 5  
LSP Using RSVP-TE Path Setup .................................................... 34  
Figure 6  
Automatic ABR Selection for Inter-Area LSP ................................. 53  
Figure 7  
ABR Protection Using Dynamic Bypass LSP ................................. 57  
Figure 8  
Bypass Tunnel Node Example ...................................................... 64  
Figure 9  
FRR Node-Protection Example ..................................................... 67  
Figure 10  
Disjoint Primary and Secondary LSPs ........................................... 72  
Figure 11  
Disjoint FRR Bypass LSPs ............................................................ 73  
Figure 12  
MPLS and RSVP-TE Configuration and Implementation Flow ............ 79  
Figure 13  
Manual Bypass Tunnels .............................................................. 93  

**4**  
PCEP ............................................................................................ 219  
Figure 14  
NSP Functional Modules ............................................................. 221  
Figure 15  
NRC-P Architecture ...................................................................... 222  
Figure 16  
PCEP Session Initialization ............................................................ 227  
Figure 17  
Multi-level IS-IS Topology in the NSP GUI ..................................... 250  
Figure 18  
Primary and Secondary RSVP-TE LSP Paths in the NSP GUI ............ 252  

**5**  
Label Distribution Protocol ............................................................. 271  
Figure 19  
LDP Subsystem Interrelationships ................................................. 276  
Figure 20  
Multicast LDP Fast Upstream Switchover ..................................... 298  
Figure 21  
LDP Configuration and Implementation ........................................ 300
1 Preface

1.1 About This Guide

This guide describes the services and protocol support provided by the 7705 SAR and presents examples to configure and implement MPLS (RSVP-TE and LDP) protocols.

This guide is organized into functional chapters and provides concepts and descriptions of the implementation flow, as well as Command Line Interface (CLI) syntax and command usage.

Note: This manual generically covers Release 8.0 content and may contain some content that will be released in later maintenance loads. Please refer to the 7705 SAR OS 8.0.Rx Software Release Notes, part number 3HE11057000xTQZZA, for information on features supported in each load of the Release 8.0 software.

Note:

As of Release 7.0, support for the following hardware has been deprecated:

- CSMv1
- 7705 SAR-F
- 8-port Ethernet Adapter card, version 1
- 16-port T1/E1 ASAP Adapter card, version 1

These components are no longer recognized in the release.
1.1.1 Audience

This guide is intended for network administrators who are responsible for configuring the 7705 SAR routers. It is assumed that the network administrators have an understanding of networking principles and configurations. Concepts described in this guide include the following:

- Multiprotocol Label Switching (MPLS)
- Resource Reservation Protocol for Traffic Engineering (RSVP-TE)
- Label Distribution Protocol (LDP)

1.1.2 List of Technical Publications

The 7705 SAR documentation set is composed of the following guides:

- 7705 SAR Basic System Configuration Guide
  This guide describes basic system configurations and operations.
- 7705 SAR System Management Guide
  This guide describes system security and access configurations as well as event logging and accounting logs.
- 7705 SAR Interface Configuration Guide
  This guide describes card and port provisioning.
- 7705 SAR Router Configuration Guide
  This guide describes logical IP routing interfaces, filtering, and routing policies.
- 7705 SAR MPLS Guide
  This guide describes how to configure Multiprotocol Label Switching (MPLS), Resource Reservation Protocol for Traffic Engineering (RSVP-TE), and Label Distribution Protocol (LDP).
- 7705 SAR Services Guide
  This guide describes how to configure service parameters such as service access points (SAPs), service destination points (SDPs), customer information, and user services.
- 7705 SAR Quality of Service Guide
  This guide describes how to configure Quality of Service (QoS) policy management.
• 7705 SAR Routing Protocols Guide
  This guide provides an overview of dynamic routing concepts and describes how to configure them.

• 7705 SAR OAM and Diagnostics Guide
  This guide provides information on Operations, Administration and Maintenance (OAM) tools.

1.1.3 Technical Support

If you purchased a service agreement for your 7705 SAR router and related products from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance. If you purchased a Nokia service agreement, follow this link to contact a Nokia support representative and to access product manuals and documentation updates:

Product Support Portal
2 7705 SAR MPLS Configuration Process

Table 1 lists the tasks that are required to configure MPLS, RSVP-TE, and LDP protocols.

This guide is presented in an overall logical configuration flow. Each section describes a software area and provides CLI syntax and command usage to configure parameters for a functional area.

Table 1 Configuration Process

<table>
<thead>
<tr>
<th>Area</th>
<th>Task/Description</th>
<th>Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol configuration</td>
<td>Configure MPLS parameters</td>
<td>MPLS</td>
</tr>
<tr>
<td></td>
<td>Configure RSVP-TE parameters</td>
<td>RSVP and RSVP-TE</td>
</tr>
<tr>
<td></td>
<td>Configure PCEP parameters</td>
<td>PCEP</td>
</tr>
<tr>
<td></td>
<td>Configure LDP parameters</td>
<td>Label Distribution Protocol</td>
</tr>
<tr>
<td>Reference</td>
<td>List of IEEE, IETF, and other proprietary entities</td>
<td>Standards and Protocol Support</td>
</tr>
</tbody>
</table>
3  MPLS and RSVP-TE

This chapter provides information required to configure Multiprotocol Label Switching (MPLS) and Resource Reservation Protocol for Traffic Engineering (RSVP-TE) for the 7705 SAR. For information on dynamic LSPs with LDP, refer to the chapter Label Distribution Protocol.

Topics in this chapter include:

- Overview
- MPLS
- RSVP and RSVP-TE
- RSVP-TE Signaling
- LSP Redundancy
- RSVP-TE Fast Reroute (FRR)
- Shared Risk Link Groups
- RSVP-TE Graceful Shutdown
- RSVP-TE Support for Unnumbered Interfaces
- PCEP Support for RSVP-TE LSPs
- MPLS Service Usage
- MPLS and RSVP-TE Configuration Process Overview
- Configuration Notes
- Configuring MPLS and RSVP-TE with CLI
- MPLS and RSVP-TE Command Reference
3.1 Overview

The 7705 SAR provides MPLS technology using static LSPs, RSVP-TE for traffic-engineered signaled routing of LSPs, and LDP for non-traffic-engineered signaled routing of LSPs. A network operator may choose to use any combination of static LSPs, RSVP-TE, and LDP to establish paths for services. Furthermore, the 7705 SAR can be used as an ingress and egress Label Edge Router (iLER and eLER), and as a transit router. A transit router is also referred to as a Label Switch Router (LSR). Consider RSVP-TE and LDP as the Layer 2.5 protocols.

OSPF and IS-IS are the interior gateway protocols with traffic engineering extensions (IGP-TE) available to the 7705 SAR. These are the Layer 3 protocols. Typically, one or the other of these gateway protocols will be in use in the network. Whichever protocol is the chosen gateway protocol, it must be working in order for LDP or RSVP-TE to function. These Layer 3 protocols identify the next hop, which is information needed by the Layer 2.5 protocols (LDP or RSVP-TE) in order to assign labels.

In addition, the 7705 SAR provides link and node redundancy protection through LSP redundancy and Fast Reroute (FRR) features.

The LSP redundancy and FRR features have the ability to take shared risk link groups (SRLGs) into consideration when the Constrained Shortest Path First (CSPF) algorithm is used to determine an alternate LSP. The selection of a route is determined by the IGP-TE protocol. The added constraints imposed by SRLGs and CSPF will ensure that the redundant route selected will be unique from the principal route (route being protected); that is, it will use physical equipment that is different from the equipment that carries the principal route. CSPF will constrain the alternate route to be the shortest possible alternative route. There may be more than one alternative route.
3.2  MPLS

Multiprotocol Label Switching (MPLS) is a label switching technology that provides the ability to set up connection-oriented paths over a connectionless IP network. MPLS facilitates network traffic flow and provides a mechanism to engineer network traffic patterns independently from routing tables. MPLS sets up a specific path for a sequence of packets. The packets are identified by a label inserted into each packet.

MPLS is independent of any routing protocol but is considered multiprotocol because it works with protocols such as IP, ATM, Ethernet, and circuit emulation.

This section contains the following topics:

- Traffic Engineering for MPLS
- MPLS Label Stack
- MPLS Entropy Labels
- Label Edge and Label Switch Routers
- LSP Types

3.2.1  Traffic Engineering for MPLS

Without traffic engineering (TE), routers route traffic according to the Shortest Path First (SPF) algorithm, disregarding congestion or packet types.

With traffic engineering, network traffic is routed efficiently to maximize throughput and minimize delay. Traffic engineering facilitates traffic flows to be mapped to the destination through a less-congested path than the one selected by the SPF algorithm.

MPLS directs a flow of IP packets along a label switched path (LSP). LSPs are simplex, meaning that the traffic flows in one direction (unidirectional) from an ingress router to an egress router. Two LSPs are required for duplex (bidirectional) traffic. Each LSP carries traffic in a specific direction, forwarding packets from one router to the next across the MPLS domain.

When an ingress router receives a packet, it adds an MPLS header to the packet and forwards it to the next hop in the LSP. The labeled packet is forwarded along the LSP path (from next hop to next hop) until it reaches the destination point. The MPLS header is removed and the packet is forwarded based on Layer 3 information such as the IP destination address. The physical path of the LSP is not constrained to the shortest path that the IGP would choose using SPF to reach the destination IP address.
3.2.1.1 TE Metric and IGP Metric

When the TE metric is selected for an LSP, the shortest path computation will select an LSP path based on the TE metric constraints instead of the IGP metric (for OSPF and IS-IS), which is the default metric. The user configures the TE metric under the `router>mpls> interface` context and the IGP metric under the `router>ospf>area>interface` context (for OSPF) and the `router>isis>if>level` context (for IS-IS). Both the TE and IGP metrics are advertised by OSPF and IS-IS for each link in the network.

The TE metric is part of the traffic engineering extensions of the IGP protocols. For more information on the OSPF and IS-IS routing protocols, refer to the 7705 SAR Routing Protocols Guide.

Typically, the TE metric is used to allow Constrained Shortest Path First (CSPF) to represent a dual TE topology for the purpose of computing LSP paths, where one TE topology is based on the RSVP-TE database and the other is based on the IGP-TE database.

An LSP dedicated to real-time and delay-sensitive user and control traffic has its path computed by CSPF using the TE metric. The user configures the TE metric to represent the amount of delay, or combined delay and jitter, of the link. In this case, the shortest path satisfying the constraints of the LSP path will effectively represent the shortest-delay path.

An LSP dedicated to non-delay-sensitive user and control traffic has its path computed by CSPF using the IGP metric. The IGP metric could represent the link bandwidth or some other value as required.

When the use of the TE metric is enabled for an LSP, the CSPF process will first eliminate all links in the network topology that do not meet the constraints specified for the LSP path; the constraints include bandwidth, admin-groups, and hop limit. CSPF will then run the SPF algorithm on the remaining links. The shortest path among all the SPF paths will be selected based on the TE metric instead of the IGP metric. The TE metric is only used in CSPF computations for MPLS paths and not in the regular SPF computation for IP reachability.

Operational metrics of LSPs that use the TE metric in CSPF path calculations can be overridden with the user-configured administrative LSP metric.
3.2.2  MPLS Label Stack

Routers that support MPLS are known as Label Edge Routers (LERs) and Label Switch Routers (LSRs). MPLS requires a set of procedures to enhance network layer packets with label stacks, which turns them into labeled packets. In order to initiate, transmit, or terminate a labeled packet on a particular data link, an LER or LSR must support the encoding technique which, when given a label stack and a network layer packet, produces a labeled packet.

In MPLS, packets can carry not just one label, but a set of labels in a stack. An LSR can swap the label at the top of the stack, pop the stack (that is, remove the top label), or swap the label and push one or more labels onto the stack. The processing of a labeled packet is completely independent of the level of hierarchy. The processing is always based on the top label, without regard for the possibility that other labels may have been above it in the past or that other labels may be below it at present.

As described in RFC 3032, *MPLS Label Stack Encoding*, the label stack is represented as a sequence of "label stack entries". Each label stack entry is represented by 4 octets. Figure 1 shows the structure of a label and Table 2 describes the fields. Figure 2 shows the label placement in a packet.

**Figure 1  Label Structure**

```
0 1 2 3
0 1 2 3
Label 1  Exp S TTL
```

**Table 2  Packet/Label Field Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>This 20-bit field carries the actual value (unstructured) of the label.</td>
</tr>
<tr>
<td>Exp</td>
<td>This 3-bit field is reserved for experimental use. It is currently used for Class of Service (CoS).</td>
</tr>
<tr>
<td>S</td>
<td>This bit is set to 1 for the last entry (bottom) in the label stack and 0 for all other label stack entries.</td>
</tr>
<tr>
<td>TTL</td>
<td>This 8-bit field is used to encode a time-to-live value.</td>
</tr>
</tbody>
</table>
A stack can carry several labels, organized in a last in/first out order. The top of the label stack appears first in the packet and the bottom of the stack appears last (Figure 2).

**Figure 2  Label Packet Placement**

The label value at the top of the stack is looked up when a labeled packet is received. A successful lookup reveals:

- the next hop where the packet is to be forwarded
- the operation to be performed on the label stack before forwarding

In addition, the lookup may reveal outgoing data link encapsulation and other information needed to properly forward the packet.

An empty label stack can be thought of as an unlabeled packet. An empty label stack has zero (0) depth. The label at the bottom of the stack is referred to as the Level 1 label. The label above it (if it exists) is the Level 2 label, and so on. The label at the top of the stack is referred to as the Level m label.

### 3.2.2.1 Label Values

The 7705 SAR uses RSVP-TE and LDP protocols for label forwarding. For packet-based services such as VLL, the 7705 SAR uses T-LDP for signaling PW labels between peer nodes.

Packets traveling along an LSP are identified by the packet label, which is the 20-bit, unsigned integer (see Label Edge and Label Switch Routers). The range is 0 through 1 048 575. Label values 0 to 15 are reserved and are defined below:

- A value of 0 represents the IPv4 Explicit NULL label. This label value is legal only at the bottom of the label stack if the label stack is immediately followed by an IPv4 header, in which case the packet forwarding is based on the IPv4 header. If the IPv4 Explicit NULL label is not at the bottom of the label stack, then the packet forwarding is based on the subsequent label.
• A value of 1 represents the router alert label. This label value is legal anywhere in the label stack except at the bottom. When a received packet contains this label value at the top of the label stack, it is delivered to a local software module for processing. The actual packet forwarding is determined by the label beneath it in the stack. However, if the packet is further forwarded, the router alert label should be pushed back onto the label stack before forwarding. The use of this label is analogous to the use of the router alert option in IP packets. Since this label cannot be at the bottom of the stack, it is not associated with a particular network layer protocol.

• A value of 3 represents the Implicit NULL label. An LER advertises this when it is requesting penultimate hop popping and expecting unlabeled packets. Thus, the label value 3 should never appear in the label stack.

• A value of 7 represents the entropy label indicator (ELI). The ELI is a special-purpose MPLS label that indicates that the entropy label (the EL) follows it in the stack.

• Values 4 through 6 and 8 through 15 are reserved for future use.

Table 3 lists the label ranges available for use by ingress labels (pop labels).

**Table 3**  Ingress Label Values (Pop Labels)

<table>
<thead>
<tr>
<th>Label Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 through 31</td>
<td>Reserved for future use</td>
</tr>
<tr>
<td>32 through 1023</td>
<td>Available for static outer LSP tunnel label assignment</td>
</tr>
<tr>
<td>1024 through 2047</td>
<td>Reserved for future use</td>
</tr>
<tr>
<td>2048 through 18 431</td>
<td>Statically assigned for services (inner pseudowire label)</td>
</tr>
<tr>
<td>32 768 through 131 071</td>
<td>Dynamically assigned for both MPLS and services</td>
</tr>
<tr>
<td>131 072 through 1 048 575</td>
<td>Reserved for future use</td>
</tr>
</tbody>
</table>

Table 4 lists the label ranges available for use by egress labels (push labels).

**Table 4**  Egress Label Values (Push Labels)

<table>
<thead>
<tr>
<th>Label Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 through 1 048 575</td>
<td>Can be used for static LSP tunnel and static PW labels</td>
</tr>
<tr>
<td>16 through 1 048 575</td>
<td>Can be dynamically assigned for both MPLS tunnel labels and PW labels</td>
</tr>
</tbody>
</table>
3.2.3 MPLS Entropy Labels

This section contains information on the following topics:

- Overview of Entropy Labels
- Inserting and Processing the Entropy Label
- Entropy Label on OAM Packets
- Entropy Label Configuration

3.2.3.1 Overview of Entropy Labels

The 7705 SAR supports MPLS entropy labels on RSVP-TE LSPs, as per RFC 6790. The entropy label provides greater granularity for load balancing on an LSR where load balancing is typically based on the MPLS label stack.

The ability of a node to receive and process an entropy label for an LSP is signaled using capability signaling (referred to as entropy label-capable). Entropy labels are supported on RSVP-TE tunnels.

Inserting an entropy label adds two labels in the MPLS label stack: the entropy label itself and the entropy label indicator (ELI).

The entropy label is inserted directly below the tunnel label and closest to the service payload that has advertised entropy label capability (which may be above the bottom of the stack). The value of the entropy label is calculated at the iLER and is based on a hash of the packet payload header content and other system parameters at ingress. For more information on hashing inputs, see the “Per-Flow Hashing” section in the 7705 SAR Interface Configuration Guide.

The ELI is inserted by the iLER. The ELI is a special-purpose MPLS label (value = 7) that indicates that the entropy label is the next label in the stack.

Entropy label capability is advertised at the tunnel level by the far-end node (eLER). This capability can be advertised for an RSVP-TE FEC. Capability signaling is not supported for point-to-multipoint LSPs, BGP tunnels, or LDP FECs. An LSR used for RSVP-TE tunnels will pass the entropy label capability signal from the downstream LSP segment to upstream peers. However, earlier releases that do not support entropy label functionality will pass the capability flag transparently, without altering the value.
The insertion of an entropy label by the upstream LER on a tunnel enabled for entropy label capability is enabled on a per-service basis. The entropy label is only inserted if the downstream peer has signaled entropy label support. The upstream LER only inserts a single entropy label, even if multiple LSP labels exist in a label stack.

The 7705 SAR supports the entropy label feature for the following services:

- Epipe access to spoke SDP
- Epipe spoke SDP to spoke SDP (vc-switching)
- VPLS SAP to VPLS spoke SDP or mesh SDP
- VPLS spoke SDP to VPLS spoke SDP

Entropy label capability on RSVP-TE LSPs is enabled on the eLER using the `config>router>rsvp>entropy-label-capability` command.

At the iLER, the insertion of the entropy label into the label stack is enabled using the `config>service>epipe>spoke-sdp>entropy-label` command and the `config>service>vpls>spoke-sdp>entropy-label` and `mesh-sdp>entropy-label` commands.

In Release 8.0, the following items apply.

- There is no entropy label support for Layer 3 traffic riding over an IGP-shortcut LSP.
- For entropy labels that are supported on LDP tunnels with remote-LFA protection (that is, for `rsvp-shortcut`), only loop-free alternate protect (`lfa-protect`) and LFA (`lfa-only`) are allowed.
- Support of entropy labels over RSVP-TE tunnels is the only valid option, except when the 7705 SAR is the LER node with BGP labeled unicast (BGP-LU) tunnels. A 7705 SAR in an LER role can push and pop an entropy label for Epipe and VPLS services with a BGP-LU tunnel riding over an RSVP-TE LSP. Conversely, a 7705 SAR does not support being in an ABR or ASBR role with BGP-LU.
3.2.3.2 Inserting and Processing the Entropy Label

This section contains inserting and processing information on the following node types:

- Ingress LER
- LSR
- Egress LER

3.2.3.2.1 Ingress LER

The procedures at the iLER are as specified in section 4.2 of RFC 6790. In general, the router inserts an entropy label into the label stack if the downstream node for the LSP tunnel has signaled support for entropy label and the entropy label is enabled for the particular service.

RFC 6790 specifies that the iLER can insert several entropy labels in the label stack where the LSP hierarchy exists, one for each LSP in the hierarchy. However, this could result in unreasonably large label stacks. Therefore, when there are multiple LSPs in a hierarchy (for example, LDP over RSVP-TE), the router only inserts a single EL/ELI pair within the innermost LSP label closest to the service payload that has advertised entropy label capability.

The entropy label functionality is not available on first generation (Gen-1) adapter cards.

The router inserts an entropy label on a tunnel that is entropy label-capable when the service has entropy label enabled, even if an implicit or explicit NULL label has been signaled by the downstream LSR or LER. This ensures consistent behavior and ensures that the entropy label value as determined by the iLER is maintained where a tunnel with an implicit NULL label is stitched at a downstream LSR.
3.2.3.2.2 LSR

If an LSR is configured for load balancing and an entropy label is found in the label stack, the LSR will take the entropy label into account in the hashing algorithm as follows:

- **label-only**: the entropy label is used as input to the hash routine and the rest of the label stack is ignored.
- **label-ip**: the entropy label and the IP packet are used as input to the hash routine and the rest of the label stack is ignored.

The entropy label functionality is not available on first generation (Gen-1) adapter cards.

If PHP has been requested by a next-hop LER, the LSR will retain any entropy label found immediately below the tunnel label that is to be popped. The system will retain and use the entropy label information as input to the local hash routine if an applicable LSR load-balancing mode has been configured.

For more information on LSR load balancing, see the “LSR Hashing” section in the 7705 SAR Interface Configuration Guide.

3.2.3.2.3 Egress LER

At an eLER, if an ELI and entropy label are detected in the label stack, both the ELI and entropy label are popped and the packet processed as normal. This occurs whether or not the system has signaled entropy label capability.

If an ELI is popped that has the bottom of stack (BoS) bit set, the system will discard the packet.

3.2.3.3 Entropy Label on OAM Packets

Service OAM packets also include an entropy label and ELI if entropy label capability is signaled for the corresponding tunnel and entropy label is enabled for the service. The EL/ELI pair is inserted at the same level in the label stack as it is in user data packets; that is, within the innermost LSP label context closest to the service payload that has advertised entropy label capability. The EL/ELI pair will therefore always reside at a different level in the label stack from special-purpose labels related to the service payload (for example, the router alert label).

OAM packets at the LSP level, such as LSP ping and LSP trace, do not have the EL/ELI pair inserted.
3.2.3.4 Entropy Label Configuration

Figure 3 illustrates the use of entropy labels at the service level.

The iLER has entropy label enabled under an applicable service context and the eLER has entropy label capability enabled. The iLER inserts the ELI and the entropy label (EL) into the label stack. The entropy label value is based on the service ID for point-to-point Layer 2 services.

At the LSR, if hashing is enabled, the LSR recognizes the ELI and uses the entropy label value as the hash result. If the entropy-label command had been disabled at the iLER, the LSR would not find the ELI and would default to hashing based on the label stack, if applicable.

Figure 3 Entropy Label and Load Balancing

At the ingress LER:

```
config>service>epipe
    spoke-sdp> entropy-label
```

```
or
config>service>vpls
    spoke-sdp> entropy-label
```

```
or
config>service>vpls
    mesh-sdp> entropy-label
```

At the egress LER:

```
config>router>rsvp
    entropy-label-capability
```

The `per-service-hashing` command and the `l4-load-balancing` and `teid-load-balancing` commands are mutually exclusive.

For IP traffic, use the `l4-load-balancing` command. For IP traffic with mobile payload, use the `teid-load-balancing` command. For other types of flows, use the `per-service-hashing` command.
3.2.4 Label Edge and Label Switch Routers

A 7705 SAR performs different functions based on its position in an LSP—ingress, egress, or transit—as described in the following list:

• ingress Label Edge Router (iLER) — The router at the beginning of an LSP is the iLER. The ingress router encapsulates packets with an MPLS header and forwards the packets to the next router along the path. An LSP can only have one ingress router.

• Label Switching Router (LSR) — An LSR can be any intermediate router in the LSP between the ingress and egress routers, swapping the incoming label with the outgoing MPLS label and forwarding the MPLS packets it receives to the next router in the LSP. An LSP can have 0 to 253 transit routers.

• egress Label Edge Router (eLER) — The router at the end of an LSP is the eLER. The egress router strips the MPLS encapsulation, which changes it from an MPLS packet to a data packet, and then forwards the packet to its final destination using information in the forwarding table. An LSP can have only one egress router. The ingress and egress routers in an LSP cannot be the same router.

A router in a network can act as an ingress, egress, or transit router for one or more LSPs, depending on the network design.

Constrained-path LSPs are signaled and are confined to one Interior Gateway Protocol (IGP) area. These LSPs cannot cross an autonomous system (AS) boundary.

Static LSPs can cross AS boundaries. The intermediate hops are manually configured so that the LSP has no dependence on the IGP topology or a local forwarding table.

3.2.5 LSP Types

The following LSP types are supported:

• static LSPs — a static LSP specifies a static path. All routers that the LSP traverses must be configured manually with labels. No RSVP-TE or LDP signaling is required. Static LSPs are discussed in this chapter.
• signaled LSPs — LSPs are set up using the RSVP-TE or LDP signaling protocol. The signaling protocol allows labels to be assigned from an ingress router to the egress router. Signaling is triggered by the ingress routers. Configuration is required only on the ingress router and is not required on intermediate routers. Signaling also facilitates path selection. RSVP-TE is discussed in this chapter, and LDP is discussed in Label Distribution Protocol.

There are two types of signaled LSP:

– explicit-path LSPs — MPLS uses RSVP-TE to set up explicit-path LSPs. The hops within the LSP are configured manually. The intermediate hops must be configured as either strict or loose, meaning that the LSP must take either a direct path from the previous hop router to this router (strict) or can traverse other routers (loose). Thus, you can control how the path is set up. Explicit-path LSPs are similar to static LSPs but require less configuration. See RSVP and RSVP-TE. An explicit path that has not specified any hops will follow the IGP route.

– constrained-path LSPs — for constrained-path LSPs, the intermediate hops of the LSP are dynamically assigned. A constrained-path LSP relies on the Constrained Shortest Path First (CSPF) routing algorithm to find a path that satisfies the constraints for the LSP. In turn, CSPF relies on the topology database provided by an extended IGP such as OSPF or IS-IS.

Once the path is found by CSPF, RSVP-TE uses the path to request the LSP setup. CSPF calculates the shortest path based on the constraints provided, such as bandwidth, class of service, and specified hops.

If Fast Reroute (FRR) is configured, the ingress router signals the downstream routers so that each downstream router can preconfigure a detour route for the LSP that will be used if there is a failure on the original LSP. If a downstream router does not support FRR, the request is ignored and the router continues to support the original LSP. This can cause some of the detour routes to fail, but the original LSP is not impacted. For more information on FRR, see RSVP-TE Fast Reroute (FRR).

No bandwidth is reserved for the reroute path. If the user enters a value in the bandwidth parameter in the config>router>mpls>lsp>fast-reroute context, it will have no effect on establishing the backup LSP. The following warning message is displayed:

“The fast reroute bandwidth command is not supported in this release.”
3.3 RSVP and RSVP-TE

The Resource Reservation Protocol (RSVP) is a network control protocol used by a host to request specific qualities of service from the network for particular application data streams or flows. RSVP is also used by routers to deliver quality of service (QoS) requests to all nodes along the paths of the flows and to establish and maintain operational state to provide the requested service. In general, RSVP requests result in resources reserved in each node along the data path.

The Resource Reservation Protocol for Traffic Engineering (RSVP-TE) is an extended version of RSVP for MPLS. RSVP-TE uses traffic engineering extensions to support automatic signaling of LSPs. MPLS uses RSVP-TE to set up traffic-engineered LSPs. See RSVP-TE Extensions for MPLS for more information.

3.3.1 RSVP-TE Overview

RSVP-TE requests resources for simplex (unidirectional) flows. Therefore, RSVP-TE treats a sender as logically distinct from a receiver, although the same application process may act as both a sender and a receiver at the same time. Duplex flows require two LSPs, to carry traffic in each direction.

RSVP-TE is a signaling protocol, not a routing protocol. RSVP-TE operates with unicast and multicast routing protocols. Routing protocols determine where packets are forwarded. RSVP-TE consults local routing tables to relay RSVP-TE messages.

RSVP-TE uses two message types to set up LSPs, PATH and RESV. Figure 4 depicts the process to establish an LSP.

• The sender (the ingress LER (iLER)) sends PATH messages toward the receiver, (the egress LER (eLER)) to indicate the forwarding equivalence class (FEC) for which label bindings are desired. PATH messages are used to signal and request the label bindings required to establish the LSP from ingress to egress. Each router along the path observes the traffic type.

• PATH messages facilitate the routers along the path to make the necessary bandwidth reservations and distribute the label binding to the router upstream.

• The eLER sends label binding information in the RESV messages in response to PATH messages received.

• The LSP is considered operational when the iLER receives the label binding information.
Figure 4  Establishing LSPs

Figure 5 displays an example of an LSP path set up using RSVP-TE. The ingress label edge router (iLER 1) transmits an RSVP-TE PATH message (path: 30.30.30.1) downstream to the egress label edge router (eLER 4). The PATH message contains a label request object that requests intermediate LSRs and the eLER to provide a label binding for this path.

Figure 5  LSP Using RSVP-TE Path Setup

In addition to the label request object, an RSVP-TE PATH message can also contain a number of optional objects:

- explicit route object (ERO) — when the ERO is present, the RSVP-TE PATH message is forced to follow the path specified by the ERO (independent of the IGP shortest path)
- record route object (RRO) — allows the iLER to receive a listing of the LSRs that the LSP tunnel actually traverses
- session attribute object — controls the path setup priority, holding priority, and local rerouting features
Upon receiving a PATH message containing a label request object, the eLER transmits an RESV message that contains a label object. The label object contains the label binding that the downstream LSR communicates to its upstream neighbor. The RESV message is sent upstream towards the iLER, in a direction opposite to that followed by the PATH message. Each LSR that processes the RESV message carrying a label object uses the received label for outgoing traffic associated with the specific LSP. When the RESV message arrives at the ingress LSR, the LSP is established.

### 3.3.1.1 Using RSVP-TE for MPLS

Hosts and routers that support both MPLS and RSVP-TE can associate labels with RSVP-TE flows. When MPLS and RSVP-TE are combined, the definition of a flow can be made more flexible. Once an LSP is established, the traffic through the path is defined by the label applied at the ingress node of the LSP. The mapping of label to traffic can be accomplished using a variety of criteria. The set of packets that are assigned the same label value by a specific node are considered to belong to the same Forwarding Equivalence Class (FEC) that defines the RSVP-TE flow.

For use with MPLS, RSVP-TE already has the resource reservation component built in, making it ideal to reserve resources for LSPs.

### 3.3.1.2 RSVP-TE Extensions for MPLS

The RSVP-TE extensions enable MPLS to support the creation of explicitly routed LSPs, with or without resource reservation. Several of the features enabled by these extensions were implemented to meet the requirements for traffic engineering over MPLS, which enables the creation of traffic trunks with specific characteristics. None of the TE extensions result in backward compatibility problems with traditional RSVP implementations.

To run properly, the traffic engineering capabilities of RSVP-TE require an underlying TE-enabled IGP routing protocol. The 7705 SAR supports OSPF and IS-IS with TE extensions.

Routing protocols make it possible to advertise the constraints imposed over various links in the network. For example, in order for the nodes in a network to choose the best link for signaling a tunnel, the capacity of a particular link and the amount of reservable capacity must be advertised by the IGP. RSVP-TE makes use of these constraints to request the setup of a path or LSP that traverses only those links that are part of an administrative group (admin groups are described in the following list).
Thus, both RSVP-TE and the IGP-TE (that is, OSPF-TE or IS-IS-TE for the 7705 SAR) must be enabled and running simultaneously.

The following TE capabilities are supported:

- hop limit — the hop limit is the maximum number of LSRs that a given LSP can traverse, including the ingress and the egress LERs. Typically, the hop limit is used to control the maximum delay time for mission-critical traffic such as voice traffic.

  The hop limit applies to the primary LSP, any backup LSPs, and LSPs configured to be used in Fast Reroute (FRR) situations.

- admin groups — administrative groups provide a way to define which LSR nodes should be included or excluded while signaling an LSP. For example, it might be desirable to avoid some nodes or links that are known to be used heavily from being included in the path of an LSP, or to include a specific LSR node to ensure that a newly signaled RSVP-TE tunnel traverses that LSR node.

  Administrative groups apply to both primary and secondary LSPs. They are defined under the `config>router>if-attribute` context, and are applied at the MPLS interface level, as well as at the LSP and the primary and secondary LSP levels through `include` and `exclude` commands.

- bandwidth — the bandwidth capability (supported by RSVP-TE), is similar to the Connection Admission Control (CAC) function in ATM. During the establishment phase of RSVP-TE, the LSP PATH message contains the bandwidth reservation request. If the requested capacity is available, the RESV message confirms the reservation request. The amount of reserved bandwidth stated in the request is deducted from the amount of reservable bandwidth for each link over which the LSP traverses.

  The bandwidth capability applies to both primary and secondary LSPs, and LSPs configured to be used in Fast Reroute (FRR) situations.

### 3.3.1.3 Hello Protocol

The Hello protocol detects the loss of a neighbor node (node failure detection) or the reset of a neighbor’s RSVP-TE state information. In standard RSVP, neighbor monitoring occurs as part of the RSVP soft-state model. The reservation state is maintained as cached information that is first installed and then periodically refreshed by the ingress and egress LERs. If the state is not refreshed within a specified time interval, the LSR discards the state because it assumes that either the neighbor node has been lost or its RSVP-TE state information has been reset.
The Hello protocol extension is composed of a Hello message, a Hello request object and a Hello ACK object. Hello processing between two neighbors supports independent selection of failure detection intervals. Each neighbor can automatically issue Hello request objects. Each Hello request object is answered by a Hello ACK object.

### 3.3.1.4 Authentication

Protocol authentication protects against malicious attacks on the communications between routing protocol neighbors. These attacks could either disrupt communications or inject incorrect routing information into the systems routing table. The use of authentication keys can help to protect routing protocols from these types of attacks.

All RSVP-TE protocol exchanges can be authenticated. This guarantees that only trusted routers can participate in autonomous system routing.

Authentication must be explicitly configured and can be done using two separate mechanisms:

- configuration of an explicit authentication key and algorithm using the `authentication-key` command
- configuration of an authentication keychain using the `auth-keychain` command

Either the `authentication-key` command or the `auth-keychain` command can be used by RSVP-TE, but both cannot be supported at the same time. If both commands are configured, the `auth-keychain` configuration will be applied and the `authentication-key` command will be ignored.

By default, authentication is not enabled on an interface.

#### 3.3.1.4.1 Authentication Key

When enabled on an RSVP-TE interface with the `authentication-key` command, authentication of RSVP messages operates in both directions of the interface. A node maintains a security association with its neighbors for each authentication key. The following items are stored in the context of this security association:

- the HMAC-MD5 authentication algorithm
- the key used with the authentication algorithm
• the lifetime of the key. A key is a user-generated key using third-party software or hardware. The value is entered as a static string into the CLI configuration of the RSVP interface. The key will continue to be valid until it is removed from that RSVP interface.

• the source address of the sending system

• the latest sending sequence number used with this key identifier

The RSVP sender transmits an authenticating digest of the RSVP message, computed using the shared authentication key and a keyed hash algorithm. The message digest is included in an Integrity object that also contains a Flags field, a Key Identifier field, and a Sequence Number field. The RSVP sender complies with the procedures for RSVP message generation in RFC 2747, RSVP Cryptographic Authentication.

An RSVP receiver uses the key together with the authentication algorithm to process received RSVP messages.

If a point of local repair (PLR) node switches the path of the LSP to a bypass LSP, it does not send the integrity object in the RSVP messages over the bypass tunnel. If an integrity object is received from the merge point (MP) node, then the message is discarded since there is no security association with the next-next-hop MP node.

The 7705 SAR MD5 implementation does not support the authentication challenge procedures in RFC 2747.

### 3.3.1.4.2 Authentication Keychains

The keychain mechanism allows for the creation of keys used to authenticate RSVP-TE communications. Each keychain entry defines the authentication attributes to be used in authenticating RSVP-TE messages from remote peers or neighbors; the entry must include at least one key entry to be valid. The keychain mechanism also allows authentication keys to be changed without affecting the state of the RSVP-TE adjacencies and supports stronger authentication algorithms than plain text and MD5.

Keychains are configured in the `config>system>security>keychain` context. For more information about configuring keychains, refer to the 7705 SAR System Management Guide, “TCP Enhanced Authentication and Keychain Authentication”.

The keychain is then associated with an RSVP-TE interface with the `auth-keychain` command.
For a key entry to be valid, it must include a valid key, the current system clock value must be within the begin and end time of the key entry, and the algorithm specified must be supported by RSVP-TE.

RSVP-TE supports the following authentication algorithms:

- HMAC-MD5
- HMAC-SHA-1-96
- HMAC-SHA-1
- HMAC-SHA-256

Keychain errors are handled as follows.

- If a keychain exists but there are no active key entries with an authentication type that matches the type supported by RSVP-TE, inbound RSVP-TE packets will not be authenticated and will be discarded and no outbound RSVP-TE packets will be sent.
- If a keychain exists but the last key entry has expired, a log entry will be raised indicating that all keychain entries have expired.

RSVP-TE requires that the protocol continue to authenticate inbound and outbound traffic using the last valid authentication key.

3.3.1.5 Non-Router ID Addresses as Destinations and Hops

The address of a configured loopback interface, other than the router ID, can be used as the destination of an RSVP LSP. For a constrained-path LSP, CSPF searches for the best path that matches the constraints across all areas or levels of the IGP where this address is reachable. If the address is the router ID of the destination node, then CSPF selects the best path across all areas or levels of the IGP for that router ID, regardless of which area or level the router ID is reachable for as an interface.

The address of a loopback interface other than the router ID can also be configured as a hop in the LSP path hop definition. If the hop is “strict” and corresponds to the router ID of the node, the CSPF path may use any TE-enabled link to the downstream node based on best cost. If the hop is “strict” and does not correspond to the router ID of the node, CSPF will fail.
3.4 RSVP-TE Signaling

RSVP-TE-based signaling provides a means to establish tunnels dynamically.

RSVP-TE uses the Downstream on Demand (DOD) label distribution mode, sending PATH messages from the ingress LER node to the egress LER, and RESV messages in the reverse direction. DOD label distribution is a router’s response to an explicit request from another router for label binding information. The DOD mode is in contrast to LDP on the 7705 SAR, which uses the Downstream Unsolicited (DU) label distribution mode for both PWs and LSPs. A router in DU mode will distribute label bindings to another router that has not explicitly requested the label bindings.

RSVP-TE signaling is supported when the 7705 SAR is deployed as an LER and as an LSR. When used as an LER, the 7705 SAR uses RSVP-TE signaling to set up constrained paths because only the LER knows all the constraints imposed on the LSP. When used as an LSR, the 7705 SAR uses RSVP-TE to interpret the RSVP-TE messages (including all the constraints).

With RSVP-TE, users can choose which services and PWs may use a particular LSP. One-to-one or many-to-one scenarios for binding PWs to RSVP-TE LSPs is supported, which is similar to binding PWs to static LSPs. Furthermore, each RSVP-TE LSP can be configured with its own set of attributes and constraints.

3.4.1 General Attributes of RSVP-TE

The following general attributes of RSVP-TE on the 7705 SAR are supported:

- OAM: BFD
- Timers
- LSP Resignal Limit
- RSVP-TE Message Pacing
- RSVP-TE Overhead Refresh Reduction
- RSVP-TE Reservation Styles
- RSVP-TE Entropy Labels
3.4.1.1 OAM: BFD

Bidirectional Forwarding Detection (BFD) is supported on the 7705 SAR. In the case of BFD for RSVP-TE, an RSVP-TE enabled link is registered with the BFD state machine, and if a failure occurs the RSVP-TE interface is taken out of service. The BFD implementation on the 7705 SAR works on a hop-by-hop basis, and if BFD detects a link failure, only the two directly connected MPLS nodes are aware of that failure. If the node that detects the link failure is an LSR node, it generates PATH-ERR messages to the originators (the LER nodes) of the failing LSPs. If FRR is configured, the detecting node takes corrective action itself. See LSP Redundancy and RSVP-TE Fast Reroute (FRR) for more information on these topics.

3.4.1.2 Timers

The following timers are implemented to ensure the successful operation of RSVP-TE:

- hold-timer — the hold timer defines the amount of time before an LSP is brought up and is in service, which provides protection against unreliable nodes and links
- resignal-timer — the resignal timer is used in conjunction with the route optimization process, especially after a reroute has occurred. If the newly computed path for an LSP has a better metric than the currently recorded hop list, then an attempt is made to resignal that LSP, and if the attempt is successful, then a make-before-break switchover occurs. If the attempt to resignal an LSP fails, the LSP continues to use the existing path and another resignal attempt is made the next time the timer expires.

When the resignal timer expires, a trap and syslog message are generated.
- retry-timer — the retry timer defines a period of time before a resignal attempt is made after an LSP failure. This delay time protects network resources against excessive signaling overhead.
3.4.1.3 LSP Resignal Limit

When an LSP fails, an LER node tries to resignal it. The following limit can be configured:

• retry-limit — the retry limit defines the number of ressignaling attempts in order to conserve the resources of the nodes in the network. There could be a serious loss of capacity due to a link failure where an infinite number of retries generate unnecessary message overhead.

3.4.1.4 RSVP-TE Message Pacing

RSVP-TE message pacing provides a means to limit the overwhelming number of RSVP-TE signaling messages that can occur in large MPLS networks during node failures. RSVP-TE message pacing allows the messages to be sent in timed intervals.

To protect nodes from receiving too many messages, the following message pacing parameters can be configured:

• msg-pacing — message pacing can be enabled or disabled
• max-burst — maximum burst defines the number of RSVP-TE messages that can be sent in the specified period of time
• period — period defines the interval of time used in conjunction with the max-burst parameter to send message pacing RSVP-TE messages

Message pacing needs to be enabled on all the nodes in a network to ensure the efficient operation of tier-1 nodes. Message pacing affects the number of RSVP-TE messages that a particular node can generate, not the number of messages it can receive. Thus, each node must be paced at a rate that allows the most loaded MPLS nodes to keep up with the number of messages they receive.

Note: Typically, a tier-1 node is an aggregator of tier-2 node transmissions, which is an aggregator of tier-3 node transmissions. Tier-1 nodes are often installed at an MTSO, while tier-3 nodes are often installed at cell sites.
3.4.1.5 RSVP-TE Overhead Refresh Reduction

RFC 2961, *RSVP Refresh Overhead Reduction Extensions*, defines enhancements to the RSVP-TE signaling protocol that reduce refresh overhead, which are in addition to the message pacing function.

These extensions are:

- RSVP-TE message bundling — RSVP-TE message bundling reduces the total number of RSVP-TE messages by aggregating the status information of multiple LSPs into a single RSVP-TE PDU. The 7705 SAR supports the receipt and processing of bundled RSVP-TE messages but not the transmission of bundled messages as specified in RFC 2961, section 3.3.

- reliable message delivery — reliable message delivery extends RSVP-TE to support MESSAGE_ACK. Each RSVP-TE PDU has a unique message-id for sequence tracking purposes. When an RSVP-TE message arrives, the recipient acknowledges the reception of the specific message-id (this is similar to TCP ACK messages). Lost PDUs can be detected and re-sent with this method, which helps reduce the refresh rate because there are two endpoints tracking the received/lost messages.

- summary refresh — the summary refresh capability uses a single message-id list to replace many individual refresh messages and sends negative ACKs (NACKs) for any message-id that cannot be matched (verified). The summary refresh capability reduces the number of message exchanges and message processing between peers. It does not reduce the amount of soft state stored in the node. The term soft state refers to the control state in hosts and routers that will expire if not refreshed within a specified amount of time (see RFC 2205 for information on soft state).

These capabilities can be enabled on a per-RSVP-TE interface basis and are referred to collectively as “refresh overhead reduction extensions”. When refresh-reduction is enabled on a 7705 SAR RSVP-TE interface, the node indicates this to its peer by setting a refresh-reduction-capable bit in the flags field of the common RSVP-TE header. If both peers of an RSVP-TE interface set this bit, all three of the capabilities listed above can be used. The node monitors the setting of this bit in received RSVP-TE messages from the peer on the interface. If the bit is cleared, the node stops sending summary refresh messages. If a peer did not set the refresh-reduction-capable bit, a 7705 SAR node does not attempt to send summary refresh messages.

Also, reliable delivery of RSVP-TE messages over the RSVP-TE interface can be enabled using the **reliable-delivery** option.
3.4.1.6 RSVP-TE Reservation Styles

LSPs can be signaled with explicit reservation styles for the reservation of resources, such as bandwidth. A reservation style describes a set of attributes for a reservation, including the sharing attributes and sender selection attributes. The style information is part of the LSP configuration. The 7705 SAR supports two reservation styles:

- fixed filter (FF) — the fixed filter (FF) reservation style specifies an explicit list of senders and a distinct reservation for each of them. Each sender has a dedicated reservation that is not shared with other senders. Each sender is identified by an IP address and a local identification number, the LSP ID. Because each sender has its own reservation, a unique label and a separate LSP can be constructed for each sender-receiver pair. For traditional RSVP applications, the FF reservation style is ideal for a video distribution application in which each channel (or source) requires a separate pipe for each of the individual video streams.

- shared explicit (SE) — the shared explicit (SE) reservation style creates a single reservation over a link that is shared by an explicit list of senders. Because each sender is explicitly listed in the RESV message, different labels can be assigned to different sender-receiver pairs, thereby creating separate LSPs.

If the FRR option is enabled for the LSP and the facility FRR method is selected at the head-end node, only the SE reservation style is allowed. Furthermore, if a 7705 SAR PLR node receives a PATH message with fast reroute requested with facility method and the FF reservation style, it will reject the reservation. The one-to-one backup method supports both FF and SE styles.

3.4.1.7 RSVP-TE Entropy Labels

The 7705 SAR supports entropy labels as described in MPLS Entropy Labels.
3.5 LSP Redundancy

Each primary LSP can be protected by up to two secondary LSPs. When the LER detects a primary LSP failure, it signals its secondary LSPs, if any have been configured, and automatically switches to the first one that is available. LSP redundancy supports shared risk link groups (SRLG). See Shared Risk Link Groups for more information on SRLG.

LSP redundancy differs from the Fast Reroute (FRR) feature in that LSP redundancy is controlled by the LER that initiated the LSP, whereas FRR uses the node that detects the failure to take recovery action. This means that LSP redundancy takes longer to reroute traffic than FRR because failure messages need to traverse multiple hops to reach the LER and activate LSP redundancy, whereas an FRR-configured node responds immediately to bypass the failed node or link. See RSVP-TE Fast Reroute (FRR) for more information on FRR.

The following parameters can be configured for primary and secondary LSPs:

- **bandwidth** — the amount of bandwidth needed for the secondary LSP can be reserved and can be any value; it does not need to be identical to the value reserved by the primary LSP. Bandwidth reservation can be set to 0, which is equivalent to reserving no bandwidth.

- **inclusion and exclusion of nodes** — by including or excluding certain nodes, you can ensure that the primary and secondary LSPs do not traverse the same nodes and therefore ensure successful recovery. Each secondary LSP can have its own list of included and excluded nodes.

- **hop limit** — the hop limit is the maximum number of LSRs that a secondary LSP can traverse, including the ingress and egress LERs.

- **standby (secondary LSPs only)** — when a secondary LSP is configured for standby mode, it is signaled immediately and is ready to take over traffic the moment the LER learns of a primary LSP failure. This mode is also called hot-standby mode.

When a secondary LSP is not in standby mode, then it is only signaled when the primary LSP fails. If there is more than one secondary LSP, they are all signaled at the same time (upon detection of a primary LSP failure) and the first one to come up is used.
3.5.1 Make-Before-Break (MBB) Procedures for LSP and Path Parameter Configuration Changes

The Make-Before-Break (MBB) procedure allows an LSP to switch from an existing working path to a new path without interrupting service. The MBB procedure does this by first signaling the new path when it is operationally up, having the ingress LER move the traffic to the new path, and then allowing the ingress LER to tear down the original path.

The MBB procedure is invoked during the following operations:

- timer-based and manual resignal of an LSP path
- Fast Reroute (FRR) global revertive procedures
- Traffic Engineering (TE) graceful shutdown procedures
- update of the secondary path due to an update to the primary path SRLG
- LSP primary or secondary path name change
- LSP or path configuration parameter change

MBB procedure coverage has been extended to most of the other LSP-level and path-level parameters as follows:

- including or excluding admin groups at the LSP and path levels
- enabling or disabling the LSP-level CSPF option
- enabling or disabling LSP-level `use-te-metric` parameters when the CSPF option is enabled
- enabling or disabling the LSP-level hop-limit option in the fast-reroute context
- enabling the LSP-level least-fill option
- enabling or disabling the LSP-level `adspec` option
- changing between node-protect and no node-protect (link-protect) values in the LSP-level fast-reroute option
- changing the LSP-level and path-level hop-limit parameter values
- enabling or disabling primary or secondary path record or record-label options

The MBB procedure is not supported on a manual bypass LSP.
### 3.5.2 Automatic Creation of RSVP-TE LSPs

Automatic creation of RSVP-TE LSPs enables the automated creation of point-to-point RSVP-TE LSPs within a single IGP IS-IS level or OSPF area that can subsequently be used by services and/or IGP shortcuts. The feature is divided into two modes: creation of an RSVP-TE LSP mesh, and creation of single-hop RSVP-TE LSPs.

When creating an RSVP-TE LSP mesh, the mesh can be full or partial, the extent of which is governed by a prefix list containing the system addresses of all nodes that should form part of the mesh. When using single-hop RSVP-TE LSPs, point-to-point LSPs are established to all directly connected neighbors.

The use of automatically created RSVP-TE LSPs avoids manual configuration of RSVP-TE LSP meshes. Even when provisioning tools are used to automatically provision these LSPs, automatic creation of a mesh still provides a benefit by avoiding increased configuration file sizes.

### 3.5.3 Automatic Creation of RSVP-TE LSP Mesh (Auto-LSP)

This feature enables the automatic creation of an RSVP-TE point-to-point LSP to a destination node whose router ID matches a prefix in the specified peer prefix policy. This LSP type is referred to as an auto-created LSP mesh. To start the process of automatically creating an RSVP-TE LSP mesh, the user must create a route policy referencing a prefix list. This prefix list contains the system addresses of all nodes that are required to be in the mesh, and can be entered as a series of /32 addresses, or simply as a range.

After the route policy is created, the user must create an LSP template containing the common parameters that are used to establish all point-to-point LSPs within the mesh. The template must be created with the keyword `mesh-p2p`:

```
config>router>mpls>lsp-template template-name mesh-p2p
```

Upon creation of the template, CSPF is automatically enabled and cannot be disabled. The template must also reference a default path before it can be placed in a `no shutdown` state.
Next, the user must associate the LSP template with the previously defined route policy, and this is accomplished using the `auto-lsp lsp-template` command:

```
cfg>router>mpls>auto-lsp lsp-template template-name policy peer-prefix-policy
```

Once the `auto-lsp lsp-template` command is entered, the system starts the process of establishing the point-to-point LSPs. The prefixes defined in the prefix list are checked, and if a prefix corresponds to a router ID that is present in the Traffic Engineering (TE) database, the system instantiates a CSPF-computed primary path to that prefix using the parameters specified in the LSP template.

Multiple templates can be associated with the same or different peer prefix policies. Each application of an LSP template with a given prefix in the prefix list results in the instantiation of a single CSPF-computed LSP primary path using the LSP template parameters, as long as the prefix corresponds to a router ID for a node in the TE database. Auto LSP does not support the automatic signaling of a secondary path for an LSP. If the signaling of multiple LSPs to the same destination node is required, a separate LSP template must be associated with a prefix list that contains the same destination node address. Each instantiated LSP will have a unique LSP ID and a unique tunnel ID.

The auto-created LSP is installed in the Tunnel Table Manager (TTM) and is available to applications such as resolution of BGP label routes, and resolution of BGP, IGP, and static routes. The auto-created LSP can also be used for auto-binding by a VPRN service. The auto-created LSP cannot be used as a provisioned SDP for explicit binding by services.

The auto-created LSP mesh can be signaled over both numbered and unnumbered RSVP-TE interfaces.

Up to five peer prefix policies can be associated with an LSP template. Every time the user executes the `auto-lsp` command with the same or different prefix policy associations or changes the prefix policy associated with an LSP template, the system re-evaluates the prefix policy. The outcome of the re-evaluation indicates to MPLS whether an existing LSP must be torn down or a new LSP must be signaled to a destination address that is already in the TE database.

If a /32 prefix is added to or removed from a prefix list associated with an LSP template, or if a prefix range is expanded or narrowed, the prefix policy re-evaluation is performed. Whether the prefix list contains one or more specific /32 addresses or a range of addresses, MPLS requires an external trigger to instantiate an LSP to a node whose address matches an entry in the prefix list. The external trigger is when the router with a router ID matching an address in the prefix list appears in the TE database. The TE database provides the trigger to MPLS.
The user must perform a no shutdown of the template before it takes effect. When a template is in use, the user must shut down the template before changing any parameters except for those LSP parameters for which the change can be handled with the Make-Before-Break (MBB) procedures (see Make-Before-Break (MBB) Procedures for LSP and Path Parameter Configuration Changes). When the template is shut down and parameters are added, removed, or modified, the existing instances of the LSP using this template are torn down and ressignaled.

MBB procedures for manual and timer-based ressignaling of the LSP, and for TE graceful shutdown, are supported.

The tools>perform>router>mpls>update-path command is not supported for mesh LSPs.

The one-to-one option under the fast-reroute command is also not supported.

If the TE database loses the router ID while the LSP is up, it will perform an update to the MPLS that states that the router ID is no longer in the TE database. This occurs whether the bypass backup path is activated or not. This will cause MPLS to tear down all mesh LSPs to this router ID. However, if the destination router is not a neighbor of the ingress LER and the user shuts down the IGP instance on the destination router, the router ID corresponding to the IGP instance will only be deleted from the TE database on the ingress LER after the LSA/LSP times out. If the user brings the IGP instance back up before the LSA/LSP times out, the ingress LER will delete and reinstall the same router ID at the receipt of the updated LSA/LSP. The RSVP-TE LSPs destined for this router ID will be deleted and re-established. All other failure conditions will cause the LSP to activate the bypass backup LSP or to go down without being deleted.

### 3.5.3.1 Multi-Area and Multi-Instance Support

A router that does not have TE links within a given IGP area or level will not have its router ID discovered in the TE database by other routers in this area or level. In other words, an auto-created LSP mesh cannot be signaled to a router that does not participate in the area or level of the ingress LER.

A mesh LSP can be signaled using TE links that belong to the same IGP area even if the router ID of the ingress and egress routers are interfaces reachable in a different area. In this case, the LSP is considered to be an intra-area LSP.

If multiple instances of IS-IS are configured on a router, each with its own router ID, the TE database on other routers will be able to discover TE links advertised by each instance. In this case, an instance of an LSP can be signaled to each router ID with a CSPF path computed using TE links within each instance.
If multiple instances of IS-IS are configured on a destination router, each with the same router ID, a single instance of LSP will be signaled from other routers. If the user shuts down one IGP instance, this will have no impact as long as the other IGP instances remain up. The LSP will remain up and will forward traffic using the same TE links. The same behavior exists with a provisioned LSP.

3.5.3.2 Mesh LSP Name Encoding

When the ingress LER signals the path of an auto-created mesh LSP, it includes the name of the LSP and the path name in the Session Name field of the Session Attribute object in the Path message. The encoding is as follows:

Session Name: <lsp-name::path-name>, where the lsp-name component is encoded as follows:

TemplateName-DestIpv4Address-TunnelId

where DestIpv4Address is the address of the destination of the auto-created LSP.

3.5.4 Automatic Creation of an RSVP-TE Single-Hop LSP

If the one-hop option is specified instead of a prefix policy, the auto-lsp command enables the automatic signaling of single-hop, point-to-point LSPs using the specified template to all directly connected neighbors. This LSP type is referred to as auto-created single-hop LSPs of type one-hop. Unlike the automatically created RSVP-TE LSP mesh, the automatically created single-hop RSVP-TE LSPs have no requirement for a prefix list to be referenced.

The first requirement is to create an LSP template containing the common parameters used to establish each single-hop LSP. The template must be created with the keyword one-hop-p2p:

config>router>mpls>lsp-template template-name one-hop-p2p

Upon creation of the template, CSPF is automatically enabled (and cannot be disabled), and the hop-limit is set to a value of two. The hop-limit defines the number of nodes the LSP may traverse, and since these are single-hop LSPs to adjacent neighbors, a limit of two is sufficient. The template must also reference a default path before it can be placed in the no shutdown state.
The next requirement is to trigger the creation of single-hop LSPs using the `auto-lsp lsp-template` command:

```
config>router>mpls>auto-lsp lsp-template template-name one-hop
```

The LSP and path parameters and options supported in an LSP template of type `one-hop-p2p` are the same as those in the LSP template of type `mesh-p2p`. The show command for `auto-lsp` will display the actual outgoing interface address in the “from” field.

The auto-created single-hop LSP can be signaled over both numbered and unnumbered RSVP-TE interfaces.

When the `one-hop` command is executed, the TE database keeps track of each TE link to a directly connected IGP neighbor whose router ID is discovered. MPLS then signals an LSP with a destination address matching the router ID of the neighbor and with a strict hop consisting of the address of the interface used by the TE link. The `auto-lsp` command with the `one-hop` option results in one or more LSPs signaled to the IGP neighbor.

Only the router ID of the first IGP instance of the neighbor that advertises a TE link causes the LSP to be signaled. If another IGP instance with a different router ID advertises the same TE link, no action is taken and the existing LSP is kept up. If the router ID originally used disappears from the TE database, the LSP is kept up and is now associated with the other router ID.

The state of a single-hop LSP that is signaled displays the following behavior.

- If the interface used by the TE link goes down or BFD times out and the RSVP-TE interface is registered with BFD, the LSP path moves to the bypass backup LSP if the primary path is associated with one.
- If the association of the TE link with a router ID is removed from the TE database while the single-hop LSP is up, the single-hop LSP is torn down whether the bypass backup path is activated or not. This occurs if the interface used by the TE link is deleted or if the interface is shut down in the context of RSVP-TE.
- If the TE database loses the router ID while the LSP is up, it will perform two separate updates to MPLS, whether the bypass backup path is activated or not. The first one updates the loss of the TE link association, which will cause the single-hop LSP to be torn down. The other update states that the router ID is no longer in the TE database, which will cause MPLS to tear down all mesh LSPs to this router ID. A shutdown at the neighbor of the IGP instance that advertised the router ID will cause the router ID to be removed from the ingress LER node immediately after the last IGP adjacency is lost and not be subject to time-out as it is for a non-directly connected destination router.
All other feature behavior and limitations are the same as for an auto-created LSP mesh.

### 3.5.5 Automatic ABR Selection for Inter-area LSPs

Inter-area RSVP point-to-point LSPs support automatic area border router (ABR) selection at the ingress LER. The ABR does not need to be included as a loose hop in the LSP path definition.

CSPF can now compute all segments of a multi-segment, inter-area LSP path in one operation. Previously, MPLS made separate requests to CSPF for each segment.

For LSP path establishment, the explicit route object (ERO) in the path message is expanded on ABRs where the next hop is a loose hop in the LSP path definition. For ERO expansion to operate, the `cspf-on-loose-hop` command must be enabled under the `mpls` context on the ABR to allow the ABR to perform a CSPF calculation. If CSPF calculations are not performed, CSPF for the LSP path fails at the head-end node as TE information for links in another area are not available.

*Figure 6* illustrates the role of each node in the signaling of an inter-area LSP with automatic ABR selection.
CSPF for an inter-area LSP operates as follows:

1. CSPF in the ingress LER node determines that an LSP is inter-area by performing a route lookup with the destination address of a point-to-point LSP, such as the address in the "to" field of the LSP configuration. If there is no intra-area route to the destination address, the LSP is considered to be inter-area.

2. When the path of the LSP is empty, CSPF computes a single-segment, intra-area path to an ABR that advertised a prefix matching the destination address of the LSP.

3. If the path of the LSP contains one or more hops, CSPF computes a multi-segment, intra-area path including the hops that are in the area of the ingress LER node.

4. If all hops are in the area of the ingress LER, the calculated path ends on an ABR that advertised a prefix matching the destination address of the LSP.

5. When there are one or more hops that are not in the area of the ingress LER, the calculated path ends on an ABR that advertised a prefix matching the first-hop address that is not in the area of the ingress LER.
6. Note the following special case of a multi-segment, inter-area LSP. If CSPF hits a hop that can be reached via an intra-area path but that resides on an ABR, CSPF only calculates a path up to that ABR. This is because there is a better chance to reach the destination of the LSP by first signaling the LSP up to that ABR and continuing the path calculation from there on by having the ABR expand the remaining hops in the ERO.

7. If there is more than one ABR that advertised a prefix, CSPF calculates a path for all ABRs. Only the shortest path is withheld. If more than one path is the shortest path, CSPF picks a path randomly or based on the least-fill criterion if least-fill is enabled. If more than one ABR satisfies the least-fill criterion, CSPF also picks one path randomly.

8. The path for an intra-area LSP cannot exit and re-enter the local area of the ingress LER. This behavior was possible in prior implementations when the user specified a loose hop outside the local area or when the only available path was via TE links outside the local area.

3.5.5.1 Rerouting of Inter-area LSPs

In prior implementations, an inter-area LSP path would have been rerouted if a failure or a topology change occurred in the local area or in a remote area while the ABR loose hop in the path definition was still up. If the transit/inter-area (exit) ABR failed or was put into node TE graceful shutdown, or if IS-IS went into overload mode, the LSP path would remain down at the ingress LER.

With automatic ABR selection, the ingress LER can reroute an inter-area LSP primary path via a different ABR in the following situations:

- When the local exit ABR fails, there are two cases to consider:
  - If the primary path is not protected at the ABR, and is therefore torn down by the previous hop in the path, then the ingress LER retries the LSP primary path via the ABR that currently has the best path for the destination prefix of the LSP.
  - If the primary path is protected at the ABR with a manual or dynamic bypass LSP, the ingress LER will receive a PathErr message with a notification of protection becoming active downstream and a RESV with a Local-Protection-In-Use flag set. At the receipt of the first of these two messages, the ingress LER performs a Global Revertive MBB procedure to optimize the LSP primary path via the ABR that currently has the best path for the destination prefix of the LSP.
- When the local exit ABR node goes into IS-IS overload or is put into node TE graceful shutdown, the ingress LER performs an MBB procedure to optimize the LSP primary path via the ABR that currently has the best path for the destination prefix of the LSP. The MBB is performed at the receipt of the PathErr message for the node TE shutdown, or at the next timer or manual optimization of the LSP path if the IS-IS overload bit is received.

3.5.5.2 Behavior of MPLS Options in Inter-area LSPs

The automatic ABR selection for an inter-area LSP does not change the prior implementation of inter-area LSP behavior for many of the LSP-level and path-level options. However, there are a number of enhancements introduced by the automatic ABR selection feature.

- Features such as path bandwidth reservation and admin-groups continue to operate within the scope of all areas since they rely on propagating the parameter information in the Path message across the area boundary.
- The TE graceful shutdown feature continues to support MBB of the LSP path to avoid the link or node that originated the PathErr message as long as the link or node is in the local area of the ingress LER. If the PathErr originated in a remote area, the ingress LER is not able to avoid the link or node when it performs the MBB since it computes the path to the local exit ABR only. However, there is an exception to this. An enhancement has been added to cause the upstream ABRs in the current path of the LSP to record the link or node to avoid and use the record in subsequent ERO expansions. This means that if the ingress LER computes a new MBB path that goes through the same exit ABR as the current path, and all ABRs upstream of the node or link that originated the PathErr message are also selected in the new MBB path when the ERO is expanded, then the new path will also avoid this link or node.
- MBB support has been expanded to avoid the ABR when the node is put into TE graceful shutdown.
- The use-te-metric option in CSPF cannot be propagated across the area boundary and thus operates within the scope of the local area of the ingress LER. This is a new behavior.
- The srlg option on the bypass LSP continues to operate locally at each PLR within each area. The PLR protecting the ABR checks the SRLG constraint for the path of the bypass within the local area.
- The srlg option on the secondary path is allowed to operate within the scope of the local area of the ingress LER with the automatic ABR selection feature.
- The least-fill option support with an inter-area LSP is introduced with the automatic ABR selection feature. When this option is enabled, CSPF applies the least-fill criterion to select the path segment to the exit ABR in the local area.
• The PLR must indicate to CSPF that a request to a one-to-one detour LSP path must remain within the local area. If the destination for the detour, which is the same as that of the LSP, is outside of the area, CSPF must return no path.

• With the automatic ABR selection feature, timer-based resignaling of the inter-area LSP path is supported and the path is resignaled if the cost of the path segment to the local exit ABR changes. The cost shown for the inter-area LSP at the ingress LER is the cost of the path segments to the ABR.

### 3.5.5.3 Inter-area LSP Support of OSPF Virtual Links

The OSPF virtual link extends area 0 for a router that is not connected to area 0 (OSPF backbone area). All prefixes in area 0 appear to be reachable via an intra-area path. However, the prefixes are not reachable since the path crosses the transit area through which the virtual link is set up to reach the area 0 remote nodes.

The TE database in a router learns all of the remote TE links in area 0 from the ABR connected to the transit area, but an intra-area LSP path using these TE links cannot be signaled within area 0 since none of these links are directly connected to this node.

The inter-area LSP feature can identify when the destination of an LSP is reachable via a virtual link. In that case, CSPF automatically computes and signals an inter-area LSP via the ABRs that are connected to the transit area.

However, when the ingress LER for the LSP is the ABR connected to the transit area, and the destination of the LSP is the address corresponding to another ABR router-id in that same transit area, CSPF computes and signals an intra-area LSP using the transit area TE links, even when the destination router-id is only part of area 0.

### 3.5.6 ABR FRR Protection for Inter-area LSP

For protection of the ABR, the upstream node of the ABR acts as a PLR, and the next-hop node to the protected domain border router is the merge point (MP). Both manual and dynamic bypass are available to protect the ABR.

Manual bypass protection only works when a proper completely strict path is provisioned that avoids the ABR.

Dynamic bypass protection provides for the automatic computation, signaling, and association with the primary path of an inter-area point-to-point LSP to provide ABR protection. Figure 7 illustrates the role of each node in ABR protection using a dynamic bypass LSP.
In order for a PLR within the local area of the ingress LER to provide ABR protection, it must dynamically signal a bypass LSP and associate it with the primary path of the inter-area LSP using the following procedures:

- The PLR must inspect the RRO node-id of the LSP primary path to determine the address of the node immediately downstream of the ABR in the other area.
- The PLR signals an inter-area bypass LSP with a destination address set to the address downstream of the ABR and with the exclude route object (XRO) set to exclude the node-id of the protected ABR.
- The request to CSPF is for a path to the merge point (that is, the next-next-hop in the RRO received in the RESV for the primary path) along with the constraint to exclude the protected ABR and the include/exclude admin groups of the primary path. If CSPF returns a path that can only go to an intermediate hop, then the PLR signals the dynamic bypass and automatically includes the XRO with the address of the protected ABR and propagates the admin-group constraints of the primary path into the Session Attribute object of the bypass LSP. Otherwise, the PLR signals the dynamic bypass directly to the merge point node with no XRO in the Path message.
• If a node-protect dynamic bypass cannot be found or signaled, the PLR attempts a link-protect dynamic bypass LSP. As with the existing implementation of dynamic bypass within the same area, the PLR attempts in the background to signal a node-protect bypass at the receipt of every third Resv refresh message for the primary path.

• Refresh reduction over dynamic bypass only works if the RRO node-id also contains the interface address. Otherwise, the neighbor is not created once the bypass is activated by the PLR. The Path state then times out after three refreshes following the activation of the bypass backup LSP.

A one-to-one detour backup LSP cannot be used at the PLR for the protection of the ABR. As a result, a 7705 SAR, acting as a PLR, will not signal a one-to-one detour LSP for ABR protection. In addition, an ABR will reject a Path message, received from a third party implementation, with a detour object and with the ERO having the next hop loose. This is performed whether the `cspf-on-loose` option is enabled or not on the 7705 SAR. In other words, the 7705 SAR, working as a transit ABR for the detour path, rejects the signaling of an inter-area detour backup LSP.
3.6 RSVP-TE Fast Reroute (FRR)

FRR is a mechanism to protect against RSVP-TE signaled LSP failures by reacting to these failures as soon as possible. FRR is set up from the iLER, which signals the transit routers to precompute their backup LSPs. FRR creates a precomputed backup LSP from each node in the LSP path. If a link or LSP between two routers fails, traffic is rerouted immediately onto the precomputed backup LSP.

**Note:** In order for FRR to work, CSPF must be enabled.

The 7705 SAR supports FRR facility backup and one-to-one backup.

Facility backup mode allows FRR to be enabled on an aggregate basis and protects a whole node or a whole link, regardless of the number of LSPs using that link. In other words, facility backup mode creates a common bypass tunnel to protect all LSP-paths traversing a common facility path. It provides flexibility, faster provisioning, and faster convergence times compared with one-to-one backup or LSP redundancy. One-to-one backup allows FRR to be enabled on a per-LSP basis.

With both methods, MPLS switches build many possible detour routes on the nodes between the ingress and egress nodes of an LSP. The facility backup method creates a detour route between two nodes, called a bypass tunnel, which is a single tunnel that follows the primary LSP path except where the link or node has failed. Traffic then switches to the bypass tunnel. The bypass tunnel merges with the original LSP path at the merge point (MP) as soon as possible. The one-to-one backup method creates a detour route, called a detour LSP, for each LSP that needs to be rerouted. Unlike the bypass tunnel, the detour LSP takes the best path to the termination point, and does not merge with the original LSP as soon as possible. The detour LSPs of a one-to-one backup LSP can merge at a detour merge point (DMP), which can either be at the termination point or at a point along the primary LSP.

One of the major differences between facility and one-to-one backup is the scalability offered by the protection method. In facility backup mode, all LSPs of the same type are rerouted over the bypass tunnel. Hence they are all protected against the failure of a node or link in the network. In facility backup mode, each LSR along the path verifies that it has a bypass tunnel available to meet its requirements; otherwise, if it can, it signals a new bypass tunnel based on the requirements. If a new LSP is configured for FRR facility backup, the existing backup tunnels are scanned and if any one of them can be used for recovery, it is preferred. If there are no common links, then a new bypass tunnel will be signaled, assuming that the LSP requirements can be met. One-to-one backup mode uses similar reroute and protection methods except a detour route is applied on a per-LSP basis.
The 7705 SAR uses CSPF to calculate the explicit route and dynamically signal the FRR LSP.

With facility backup mode, routers check the contents of the Record Route Object (RRO) in the received RESV message to determine the bypass tunnel endpoint in the FRR facility. For link protection, the router uses the RRO to check the IP address of the next-hop router attached to the far end of the link along with the label allocation information and to build the bypass tunnel. This label is preserved until the LSP is merged at the MP. For node protection, the router uses the RRO to determine the next-next-hop router and the label it is expecting. The collection of RRO information is enabled through the `record` and `record-label` options.

If, after this process, another LSP requests FRR using the facility backup method, the router checks and compares its session object to the existing session objects and if there is a match, the router binds that LSP to the same bypass tunnel. If there is no match, another bypass is created.

### 3.6.1 FRR Terminology

Table 5 provides definitions of terms used for FRR.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup path</td>
<td>The LSP that is responsible for backing up a protected LSP. A backup path can be a backup tunnel (facility backup) or a detour LSP (one-to-one backup).</td>
</tr>
<tr>
<td>Backup tunnel</td>
<td>The LSP that is used to back up one of the many LSPs in FRR facility (many-to-one backup)</td>
</tr>
<tr>
<td>Bypass tunnel</td>
<td>An LSP that is used to protect a set of LSPs passing over a common facility in FRR facility backup. A bypass tunnel can be configured manually or dynamically (see Dynamic and Manual Bypass LSPs).</td>
</tr>
<tr>
<td>CSPF</td>
<td>Constraint-based shortest path first</td>
</tr>
<tr>
<td>Detour route</td>
<td>Any alternate route that protects the primary path, such as a secondary path, FRR bypass tunnel, or FRR detour LSP. The term “detour route” should not be confused with the term “detour LSP”. Detour route is a general term that refers to any alternate route, while detour LSP is a specific term that applies to one-to-one backup.</td>
</tr>
</tbody>
</table>
Detour LSP
The LSP that is used to reroute traffic around a failure in FRR one-to-one backup. The term “detour LSP” should not be confused with the term “detour route”. Detour route is a general term that refers to any alternate route, while detour LSP is a specific term that applies to one-to-one backup.

DMP
Detour merge point
In the case of one-to-one backup, this is an LSR where multiple detours converge. Only one detour is signaled beyond that LSR.

Disjoint
See SRLG disjoint

Facility backup
A local repair method in which a single bypass tunnel is used to protect one or more LSPs that traverse the PLR, the resource being protected, and the Merge Point (in that order). Facility backup is distinct from a one-to-one backup tunnel, which has one backup path per protected path.

MP
Merge point
The LSR where one or more backup tunnels rejoin the path of the protected LSP downstream of the potential failure. The same LSR may be both an MP and a PLR simultaneously.

NHOP bypass tunnel
Next-hop bypass tunnel
A backup tunnel that bypasses a single link of the protected LSP

NNHOP bypass tunnel
Next-next-hop bypass tunnel
A backup tunnel that bypasses a single node of the protected LSP

One-to-one backup
A local repair method in which a backup LSP is separately created for each protected LSP at a PLR

PLR
Point of local repair
The head-end router of a backup tunnel or a detour LSP, where the term local repair refers to techniques used to repair an LSP tunnel quickly when a node or link along an LSP path fails

Primary path
An LSP that uses the routers specified by the path defined by the primary path-name command

Protected LSP
An LSP is protected at a given hop if it has one or more associated backup tunnels originating at that hop

Reroutable LSP
Any LSP for which the head-end router requests local protection

Secondary path
An LSP that protects a primary path that uses LSP redundancy protection rather than FRR protection

<table>
<thead>
<tr>
<th>Table 5</th>
<th>FRR Terminology (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>Detour LSP</td>
<td>The LSP that is used to reroute traffic around a failure in FRR one-to-one backup. The term “detour LSP” should not be confused with the term “detour route”. Detour route is a general term that refers to any alternate route, while detour LSP is a specific term that applies to one-to-one backup.</td>
</tr>
<tr>
<td>DMP</td>
<td>Detour merge point In the case of one-to-one backup, this is an LSR where multiple detours converge. Only one detour is signaled beyond that LSR.</td>
</tr>
<tr>
<td>Disjoint</td>
<td>See SRLG disjoint</td>
</tr>
<tr>
<td>Facility backup</td>
<td>A local repair method in which a single bypass tunnel is used to protect one or more LSPs that traverse the PLR, the resource being protected, and the Merge Point (in that order). Facility backup is distinct from a one-to-one backup tunnel, which has one backup path per protected path.</td>
</tr>
<tr>
<td>MP</td>
<td>Merge point The LSR where one or more backup tunnels rejoin the path of the protected LSP downstream of the potential failure. The same LSR may be both an MP and a PLR simultaneously.</td>
</tr>
<tr>
<td>NHOP bypass tunnel</td>
<td>Next-hop bypass tunnel A backup tunnel that bypasses a single link of the protected LSP</td>
</tr>
<tr>
<td>NNHOP bypass tunnel</td>
<td>Next-next-hop bypass tunnel A backup tunnel that bypasses a single node of the protected LSP</td>
</tr>
<tr>
<td>One-to-one backup</td>
<td>A local repair method in which a backup LSP is separately created for each protected LSP at a PLR</td>
</tr>
<tr>
<td>PLR</td>
<td>Point of local repair The head-end router of a backup tunnel or a detour LSP, where the term local repair refers to techniques used to repair an LSP tunnel quickly when a node or link along an LSP path fails</td>
</tr>
<tr>
<td>Primary path</td>
<td>An LSP that uses the routers specified by the path defined by the primary path-name command</td>
</tr>
<tr>
<td>Protected LSP</td>
<td>An LSP is protected at a given hop if it has one or more associated backup tunnels originating at that hop</td>
</tr>
<tr>
<td>Reroutable LSP</td>
<td>Any LSP for which the head-end router requests local protection</td>
</tr>
<tr>
<td>Secondary path</td>
<td>An LSP that protects a primary path that uses LSP redundancy protection rather than FRR protection</td>
</tr>
</tbody>
</table>
3.6.2 FRR Behavior

The FRR MPLS facility backup method and one-to-one backup method are configured on the ingress LER (iLER) by using the fast-reroute command.

The behavior of an LSP at an iLER with both FRR and a standby LSP path configured is as follows.

- When a downstream detour route (alternative path) becomes active at a Point of Local Repair (PLR):
  The iLER switches to the standby LSP path as soon as it is notified of the reroute. If the primary LSP path is subsequently repaired at the PLR, the LSP switches back to the primary path. If the standby path goes down, the LSP is switched back to the primary path, even though the primary path is still on the detour route at the PLR.
- If the primary path goes down at the iLER while the LSP is on the standby path, the detour route at the iLER is torn down and, for one-to-one backup detour routes, a “path tear” is sent for the detour route. In other words, the detour route at the iLER does not protect the standby LSP. If and when the primary LSP is again successfully resignaled, the iLER detour route will be restarted.
- When the primary LSP fails at the iLER:
  The LSP switches to the detour route. If the primary path undergoes a global revertive recovery, the LSP switches back to the primary path. If the LSP is on the detour route and the detour route fails, the LSP is switched to the standby path.
- Administrative groups are not taken into account when creating the detour routes for LSPs.

<table>
<thead>
<tr>
<th>Table 5</th>
<th>FRR Terminology (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>SRLG disjoint</td>
<td>A path is considered to be SRLG disjoint from a given link or node if the path does not use any links or nodes that belong to the same SRLG as the given link or node</td>
</tr>
</tbody>
</table>
3.6.3 Dynamic and Manual Bypass LSPs

Users can disable dynamic bypass creation on a per-node basis using the `config>router>mpls>dynamic-bypass` command. Disabling dynamic bypass means that manual bypass is enabled. Dynamic bypass is enabled by default.

Dynamic bypass tunnels are implemented as per RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*. When an LSP is signaled and the Local Protection flag in the Session_attribute object is set, or the FRR object in the PATH message indicates that facility backup is desired, the PLR establishes a bypass tunnel to provide node and link protection. If there exists a bypass LSP that merges with the protected LSP at a downstream node, and if this LSP satisfies the constraints in the FRR object, then this bypass tunnel is selected and used. The `frr-object` command specifies whether facility backup is signaled in the FRR object.

The manual bypass feature allows an LSP to be preconfigured from a Point of Local Repair (PLR) that will be used exclusively for bypass protection. When a PATH message for a new LSP requests bypass protection, the node first checks for a manual bypass tunnel that satisfies the path constraints. If one is found, it is selected and used. If no manual bypass tunnel is found, the 7705 SAR dynamically signals a bypass LSP in the default behavior. To configure a manual bypass LSP, use the `bypass-only` option in the `config>router>mpls>lsp lsp-name [bypass-only]` command.

When a PLR activates a bypass backup LSP and subsequently receives a RESV refresh message for the original primary LSP path reservation over the restored interface, the PLR does not generate a ResvErr packet downstream. In addition, the MP node, once it becomes active, does not propagate a downstream ResvErr message received packet for the original primary LSP path reservation.

Refer to Configuring Manual Bypass Tunnels for configuration information.

3.6.3.1 Bypass LSP Selection Rules for the PLR

*Figure 8* shows an example of a network used to illustrate the LSP selection rules for a PLR bypass scenario.
The PLR uses the following rules to select a bypass LSP from among multiple bypass LSPs (manually and dynamically created) when establishing the primary LSP path or when searching for a bypass for a protected LSP that does not have an association with a bypass tunnel.

1. The MPLS/RSVP-TE task in the PLR node checks for an existing manual bypass tunnel that satisfies the constraints. If the PATH message for the primary LSP path indicated that node protection is desired, which is the default LSP FRR setting at the head-end node, then the MPLS/RSVP-TE task searches for a node-protect bypass LSP. If the PATH message for the primary LSP path indicated that link protection is desired, then it searches for a link-protect bypass LSP.

2. If multiple manual bypass LSPs satisfying the path constraints exist, the PLR will prefer a manual bypass LSP terminating closer to the PLR over a manual bypass LSP terminating further away. If multiple manual bypass LSPs satisfying the path constraints terminate on the same downstream node, the PLR selects the one with the lowest IGP path cost, or if there is a tie, it picks the first one available.

3. If none of the manual bypass LSPs satisfy the constraints and dynamic bypass tunnels have not been disabled on the PLR node, then the MPLS/RSVP-TE task in the PLR node checks to determine if any of the already established dynamic bypass LSPs of the requested type satisfy the constraints.

4. If none of the dynamic bypass LSPs satisfy the constraints, then the MPLS/RSVP-TE task will ask CSPF to check if a new dynamic bypass of the requested type, node-protect or link-protect, can be established.

5. If the PATH message for the primary LSP path indicated node protection is desired, and no manual bypass was found after Step 1, and/or no dynamic bypass LSP was found after three attempts to perform Step 3, the MPLS/RSVP-TE task will repeat Steps 1 to 3 looking for a suitable link-protect bypass LSP. If none are found, the primary LSP will have no protection and the PLR node must clear the Local Protection Available flag in the IPv4 address sub-object of the RRO, starting in the next RESV refresh message it sends upstream.
6. If the PATH message for the primary LSP path indicated link protection is desired, and no manual bypass was found after Step 1, and/or no dynamic bypass LSP was found after performing Step 3, the primary LSP will have no protection and the PLR node must clear the Local Protection Available flag in the IPv4 address sub-object of the RRO, starting in the next RESV refresh message it sends upstream. The PLR will not search for a node-protect bypass LSP in this case.

7. If the PLR node successfully makes an association, it must set the Local Protection Available flag in the IPv4 address sub-object of the RRO, starting in the next RESV refresh message it sends upstream.

8. For all primary LSPs that requested FRR protection but are not currently associated with a bypass tunnel, the PLR node—upon reception of an RESV refresh message on the primary LSP path—repeats Steps 1 to 7.

If the user disables dynamic bypass tunnels on a node while dynamic bypass tunnels are activated and passing traffic, traffic loss will occur on the protected LSP. Furthermore, if no manual bypass tunnel exists that satisfies the constraints of the protected LSP, the LSP will remain without protection.

If the user configures a bypass tunnel on Node B (Figure 8) and dynamic bypass tunnels have been disabled, LSPs that had been previously signaled and that were not associated with any manual bypass tunnel (for example, none existed) will be associated with the manual bypass tunnel, if it is suitable. The node checks for the availability of a suitable bypass tunnel for each of the outstanding LSPs every time an RESV message is received for these LSPs.

If the user configures a bypass tunnel on Node B and dynamic bypass tunnels have not been disabled, LSPs that had been previously signaled over dynamic bypass tunnels will not automatically be switched to the manual bypass tunnel, even if the manual bypass tunnel is a more optimized path. The user must perform a make-before-break switchover at the head end of these LSPs. The make-before-break process is enabled using the adaptive option.

If the manual bypass tunnel goes into the down state on Node B and dynamic bypass tunnels have been disabled, Node B (PLR) will clear the “protection available” flag in the RRO IPv4 sub-object in the next RESV refresh message for each affected LSP. It will then try to associate each of these LSPs with one of the manual bypass tunnels that are still up. If it finds one, it will make the association and set the “protection available” flag in the next RESV refresh message for each of these LSPs. If it cannot find one, it will keep checking for one every time an RESV message is received for each of the remaining LSPs. When the manual bypass tunnel is back up, the LSPs that did not find a match are associated back with this tunnel and the protection available flag is set starting in the next RESV refresh message.
If the manual bypass tunnel goes into the down state on Node B and dynamic bypass tunnels have not been disabled, Node B will automatically signal a dynamic bypass tunnel to protect the LSPs if a suitable one does not exist. Similarly, if an LSP is signaled while the manual bypass tunnel is in the down state, the node will only signal a dynamic bypass tunnel if the user has not disabled dynamic tunnels. When the manual bypass tunnel is back up, the node will not switch the protected LSPs from the dynamic bypass tunnel to the manual bypass tunnel.

### 3.6.3.2 FRR Node Protection (Facility Backup)

The MPLS Fast Reroute (FRR) functionality enables PLRs to be aware of the lack of node protection and lets them regularly probe for a node bypass via the `node-protect` command.

When enabled, the `node-protect` command provides node protection for the specified LSP. If node protection cannot be provided, link protection is attempted. If link protection cannot be provided, no protection is provided. When disabled via the `no` form of the command, link protection is attempted, and if link protection cannot be provided, no protection is provided.

For example, assume the following for the LSP scenario in Figure 9.

1. LSP_1 is between PE_1 and PE_2 (via P1 and P2), and has CSPF, FRR facility backup, and FRR node protection enabled.
2. P1 protects P2 with bypass nodes P1 - P3 - P4 - PE_4 - PE_3.
3. If P4 fails, P1 tries to establish the bypass node three times.
4. When the bypass node creation fails (there is no bypass route), P1 will protect link P1-P2.
5. P1 protects the link to P2 through P1 - P5 - P2.
6. P4 returns online.
LSP_1 had requested node protection, but due to lack of an available path it could only obtain link protection. Therefore, every 60 s, the PLR for LSP_1 will search for a new path that might be able to provide node protection. When P4 is back online and such a path is available, a new bypass tunnel will be signaled and LSP_1 will be associated with this new bypass tunnel.

### 3.6.4 Admin Group Support on Facility Bypass Backup LSPs

Admin group support on facility bypass backup LSPs provides for the inclusion of the LSP primary path admin-group constraints in the computation of an FRR facility bypass backup LSP to protect the primary LSP path. Admin group constraints are honored by all nodes in the LSP path both for primary and FRR backup LSPs.

This feature is supported on primary paths of an RSVP point-to-point LSP in both intra-area and inter-area TE where applicable.

This feature is not supported on one-to-one detour backup LSPs.
3.6.5 FRR Over Unnumbered Interfaces

When the PLR is the ingress LER node and the outgoing interface of the bypass LSP is unnumbered, the user must assign a borrowed IP address to the interface that is different from the system interface; otherwise, the bypass LSP will not come up.

In addition, the PLR node includes the IF_ID RSVP_HOP object (C-Type = 3) in the PATH message if the outgoing interface of the bypass LSP is unnumbered. If the outgoing interface of the bypass LSP is numbered, the PLR node includes the IPv4 RSVP_HOP object (C-Type = 1).

When the MP node receives the PATH message over the bypass LSP, it creates the merge-point context for the protected LSP and associates it with the existing state if any of the following is satisfied:

- the C-Type value of the RSVP_HOP object has changed
- the C-Type is the value for the IF_ID RSVP_HOP object (C-Type = 3) and it has not changed, but the IF_ID TLV is different
- the IPv4 Next/Previous Hop Address field in the RSVP_HOP object has changed, regardless of the C-Type value

This behavior at the PLR and MP nodes is the same for both link protection and node protection FRR.

**Note:** If node protection FRR is enabled but the MP does not support an unnumbered interface, the PATH message is rejected at the MP and the path is torn down.

See [RSVP-TE Support for Unnumbered Interfaces](#) for information on unnumbered interfaces.
3.7 Shared Risk Link Groups

A shared risk link group (SRLG) represents a set of interfaces (or links) that share the same risk of failing because they may be subjected to the same resource failures or defects. Two examples where the same risk of failure exists are fiber links that share the same conduit, and multiple wavelengths that share the same fiber.

SRLGs are supported by both LSP redundancy protection and FRR protection. SRLGs allow the user to prepare a detour route that is disjoint from the primary LSP path. See Disjoint and Non-disjoint Paths.

The SRLG feature ensures that a primary and secondary LSP path, or a bypass tunnel or detour LSP path, do not share SRLGs. That is, they do not share the same sets of links that are considered to have a similar (or identical) chance of failure.

To use SRLGs, the user first creates an SRLG by assigning one or more routers to the SRLG. Then, the user links the SRLG to an MPLS interface and enables the SRLG feature on the LSP path. SRLGs cannot be assigned to the system interface.

3.7.1 SRLGs for Secondary LSP Paths

SRLGs for secondary LSP paths apply when LSP redundancy protection is used.

When setting up the secondary path, enable the srlg option on the secondary path to ensure that CSPF includes the SRLG constraint in its route calculation. To make an accurate computation, CSPF requires that the primary LSP be established and in the up state (because the head-end LER needs the most current explicit route object (ERO) for the primary path, and the most current ERO is built during primary path CSPF computation). The ERO includes the list of SRLGs.

At the establishment of a secondary path with the SRLG constraint, the MPLS/RSVP-TE task queries CSPF again, which provides the list of SRLGs to be avoided. CSPF prunes all links having interfaces that belong to the same SRLGs as the interfaces included in the ERO of the primary path. If CSPF finds an eligible path, the secondary path is set up. If CSPF does not find an eligible path, MPLS/RSVP-TE keeps retrying the requests to CSPF.
3.7.2 SRLGs for FRR LSP Paths

When setting up the FRR bypass or detour LSP, enable the `srlg-frr` option on FRR to ensure that CSPF includes the SRLG constraint in its route calculation. CSPF prunes all links that are in the SRLG being used by the primary LSP during the calculation of the FRR path. If one or more paths are found, CSPF sets up the FRR bypass or detour LSP based on the best cost and signals the FRR LSP.

If there is no path found based on the above calculation and the `srlg-frr` command has the `strict` option set, then the FRR LSP is not set up and the MPLS/RSVP-TE task keeps trying to set up a path. If the `strict` option is not set, then the FRR LSP is set up based on the other TE constraints (that is, excluding the SRLG constraint).

3.7.3 Disjoint and Non-disjoint Paths

A path is considered to be SRLG disjoint from a given link (or node) if the path does not use any links (or nodes) that belong to the same SRLG as the given link (or node). Eligible disjoint paths are found by CSPF when the SRLG constraint is included in the CSPF route calculation (referred to as the strict SRLG condition).

When LSP redundancy is used, the secondary LSP is always signaled with a strict SRLG condition.

When FRR is used, the FRR bypass or detour LSP may have a strict or non-strict SRLG condition. If the `strict` option is used with the `srlg-frr` command, then the bypass LSP must be on the list of eligible paths found by the CSPF calculation that included the SRLG constraint. If the `strict` option is not used, then it is possible for the bypass or detour LSP to be non-disjoint. The non-disjoint case is supported only if the SRLG is not strict.

At the PLR, if an FRR tunnel is needed to protect a primary LSP, the priority order for selecting that FRR tunnel is as follows:

1. Manual bypass disjoint
2. Manual bypass non-disjoint (eligible only if `srlg-frr` is non-strict)
3. Dynamic bypass disjoint
4. Dynamic bypass non-disjoint (eligible only if `srlg-frr` is non-strict)

A bypass or a detour LSP path is not guaranteed to be SRLG disjoint from the primary path. This is because only the SRLG constraint of the outgoing interface at the PLR that the primary path is using is considered in the CSPF calculation.
3.7.4 Enabling Disjoint Backup Paths

A typical application of the SRLG feature is to provide automatic setup of secondary LSPs or FRR bypass or detour LSPs, in order to minimize the probability that they share the same failure risks with the primary LSP path (see Figure 10 and Figure 11).

Figure 10 illustrates SRLG when LSP redundancy is used, where SRLG_1 contains the interfaces that define links A-B, B-C, and C-D. The primary path uses these links to connect node A to node D. In the event of a failure along the primary path, the secondary path cannot use any of the links in SRLG_1 and takes the path from node A to nodes E, F, G, H, J, and D.

Figure 11 illustrates SRLG when FRR bypass is used, where SRLG_1 is the same as in Figure 10. Since FRR bypass is used, the following possible reroutes may occur, depending on where the failure occurs:

- if node B fails, the bypass is from node A to nodes E, F, G, H, and C
- if node C fails, the bypass is from node B to nodes F, G, H, J, and D
- if link C-D fails, the bypass is from node C to nodes H, J, and D

The SRLG feature is supported on OSPF and IS-IS interfaces for which RSVP-TE is enabled.

The following steps describe how to enable SRLG disjoint backup paths for LSP redundancy and FRR.

LSP Redundancy for Primary/Secondary (standby) SRLG Disjoint Configuration

- Create an SRLG-group (similar to creating an admin group).
- Link the SRLG-group to MPLS interfaces.
- Configure primary and secondary LSP paths, and enable SRLG on the secondary LSP path. The SRLG secondary LSP paths will always perform a strict CSPF query.

The setting of the srlg-frr command is irrelevant in this case (see the srlg-frr command).
FRR Bypass Tunnel or Detour LSP SRLG Disjoint Configuration

- Create an SRLG-group (similar to creating an admin group).
- Link the SRLG-group to MPLS interfaces.
- Enable the **strict** option on the `srlg-frr` command, which is a system-wide command that forces the CSPF calculation for every LSP path to take any configured SRLG memberships into account.
- Configure primary FRR (facility backup or one-to-one backup) LSP paths. Each PLR will create a bypass or detour LSP that will only avoid the SRLG memberships configured on the primary LSP path egress interface. For one-to-one backup, detour-detour merging is out of the control of the PLR. The PLR will not ensure that the FRR detour will be prohibited from merging with a colliding detour LSP. For facility backup, given that there are several bypass types to bind to, the priority rules shown in *Disjoint and Non-disjoint Paths* are used.

Manually configured bypasses that do not use CSPF are not considered as possible backup paths.

*Figure 10*  
**Disjoint Primary and Secondary LSPs**
**Figure 11** Disjoint FRR Bypass LSPs

Legend:
- Primary path
- FRR bypasses taking SRLG_1 into account
- Bypassing A-B
- Bypassing B-C
- Bypassing C-D
3.8 RSVP-TE Graceful Shutdown

RSVP-TE graceful shutdown provides a method to reroute transit LSPs in a bulk fashion away from a node prior to maintenance of that node. A PathErr message with the error code “Local Maintenance on TE Link required Flag” (if the affected network element is a link) or the error code “Local node maintenance required” (if the affected network element is the node) is sent before the links or node are taken out of service.

When an LER receives the message, it performs a make-before-break on the LSP path to move the LSPs away from the links/nodes whose IP addresses are indicated in the PathErr message and reroute them. Affected link/node resources are flagged in the TE database so that other routers will signal LSPs using the affected resources only as a last resort.

Graceful shutdown can be enabled on a per-interface basis or on all interfaces on the node if the whole node must be taken out of service.
3.9 RSVP-TE Support for Unnumbered Interfaces

Unnumbered interfaces are point-to-point interfaces that are not explicitly configured with a dedicated IP address and subnet; instead, they borrow (or link to) an IP address from another interface on the system (the system IP address, another loopback interface, or any other numbered interface) and use it as the source IP address for packets originating from the interface. For more information on support for unnumbered interfaces, refer to the 7705 SAR Router Configuration Guide, "Unnumbered Interfaces".

Unnumbered IP interfaces can be used via RSVP-TE for signaling traffic engineering (TE) LSPs.

Supporting RSVP-TE over unnumbered interfaces requires the ability to:

• carry TE information over unnumbered links in IS-IS-TE or OSPF-TE extensions
• specify unnumbered interfaces in RSVP-TE signaling

An unnumbered IP interface is identified uniquely on a router in the network by the tuple (router ID, ifindex). An LSR at each end of the link assigns a system-wide unique interface index to the unnumbered interface. IS-IS, OSPF, MPLS (RSVP-TE, LDP), and OAM use this tuple to advertise the link information, signal LSPs over the interface, or send and respond to an MPLS echo request message over an unnumbered interface.

The borrowed IP address for an unnumbered interface is configured using the following CLI command, with the default value set to the system interface address:

```
config>router>interface>unnumbered {ip-int-name | ip-address}.
```

Note: The borrowed IP address is used exclusively as the source address for IP packets that originate from the interface. For FRR, this address must be configured to an address different from the system interface in order for the FRR bypass LSP to come up at the ingress LER. See RSVP-TE Fast Reroute (FRR) for information on FRR.

To support unnumbered TE links in IS-IS, a new sub-TLV of the extended IS reachability TLV is added, which encodes the link local identifiers and link remote identifiers as defined in RFC 5307, *IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*.

To support unnumbered TE links in OSPF, a new sub-TLV of the Link TLV is added, which encodes the link local identifiers and link remote identifiers as defined in RFC 4203, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*.
To support unnumbered TE links in RSVP-TE, a new sub-object of the Explicit Route Object (ERO) is added to specify unnumbered links and a new sub-object of the Route Record Object (RRO) is added to record that the LSP traversed an unnumbered link, as per RFC 3477, *Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)*. As well, a new IF_ID RSVP_HOP object with a C-Type of 3 is added as per section 8.1.1 of RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*. The IPv4 Next/Previous Hop Address field in the object is set to the borrowed IP interface address.

The unnumbered IP interface address is advertised by IS-IS-TE or OSPF-TE, and CSPF can include it in the computation of a path for a point-to-point LSP. However, this feature does not support defining an unnumbered interface as a hop in the path definition of an LSP.

A router creates an RSVP neighbor over an unnumbered interface using the tuple (router ID, ifindex). The router ID of the router that advertised an unnumbered interface index is obtained from the TE database. Therefore, if traffic engineering is disabled in IS-IS or OSPF, a non-CSPF LSP that has its next hop over an unnumbered interface will not come up at the ingress LER because the router ID of the neighbor that has the next hop of the PATH message cannot be looked up. The LSP path will remain operationally down with the error “noRouteToDestination”. If a PATH message is received at the LSR for which traffic engineering was disabled and the next hop for the LSP is over an unnumbered interface, a PathErr message is sent back to the ingress LER with the error code of 24 “Routing Problem” and an error value of 5 “No route available toward destination”.

All MPLS (RSVP-TE and LDP) features supported for numbered IP interfaces are supported for unnumbered interfaces, with the following exceptions:

- configuration of a router ID with a value other than system interface
- signaling of an LSP with an ERO based on a loose or strict hop using an unnumbered TE link in the path hop definition
- signaling of a one-to-one detour LSP over an unnumbered interface
- RSVP Hello messages and all Hello-related capabilities, such as Graceful-Restart Helper
- RSVP refresh reduction on an unnumbered interface

The unnumbered interface feature also extends the support of LSP ping and LSP traceroute to point-to-point LSPs that have unnumbered TE links in their path.
3.10 PCEP Support for RSVP-TE LSPs

The Path Computation Element Communication Protocol (PCEP) is one of several protocols used for communication between a wide area network (WAN) software-defined network (SDN) controller and network elements.

The 7705 SAR operates as a PCE Client (PCC) only, supporting PCC capabilities for RSVP-TE LSPs.

The following MPLS-level and LSP-level CLI commands are used to configure RSVP-TE LSPs in a router acting as a PCC. See MPLS and RSVP-TE Command Reference for command descriptions. See the PCEP Support for RSVP-TE LSPs section in the PCEP chapter for information on using these commands.

• config>router>mpls>
   pce-report rsvp-te {enable | disable}
• config>router>mpls>lsp>
   path-profile profile-id [path-group group-id]
   pce-computation
   pce-control
   pce-report {enable | disable | inherit}
• config>router>mpls>lsp-template>
   pce-report {enable | disable | inherit}
3.11 MPLS Service Usage

The 7705 SAR routers enable service providers to deliver virtual private networks (VPNs) and Internet access using Generic Routing Encapsulation (GRE), IP, and/or MPLS tunnels, with Ethernet and/or SONET/SDH interfaces.

3.11.1 Service Destination Points

A service destination point (SDP) acts as a logical way of directing traffic from one 7705 SAR router to another through a unidirectional (one-way) service tunnel. The SDP terminates at the far-end 7705 SAR router, which directs packets to the correct service egress service access point (SAP) on that device. All services mapped to an SDP use the GRE, IP, or MPLS transport encapsulation type.

For information about service transport tunnels, refer to the 7705 SAR Services Guide. Service transport tunnels can support up to eight forwarding classes and can be used by multiple services.
3.12 MPLS and RSVP-TE Configuration Process Overview

Figure 12 displays the process to configure MPLS and RSVP-TE parameters.

**Figure 12**  MPLS and RSVP-TE Configuration and Implementation Flow

![Diagram](image-url)
3.13 Configuration Notes

Network and system interfaces must be configured in the `config>router>interface` context before they can be specified in MPLS. Refer to the 7705 SAR Router Configuration Guide for interface configuration information.

This section describes MPLS and RSVP-TE guidelines and caveats.

- Interfaces must already be configured in the `config>router>interface` context before they can be specified in MPLS and RSVP.
- A router interface must be specified in the `config>router>mpls` context in order to apply it or modify parameters in the `config>router>rsvp` context.
- A system interface must be configured and specified in the `config>router>mpls` context.
- Paths must be created before they can be applied to an LSP.
- CSPF must be enabled in order for administrative groups and SRLGs to be relevant.

3.13.1 Reference Sources

For information on supported IETF drafts and standards, as well as standard and proprietary MIBs, refer to Standards and Protocol Support.
3.14 Configuring MPLS and RSVP-TE with CLI

This section provides information to configure MPLS and RSVP-TE using the CLI.

Topics in this section include:

- MPLS Configuration Overview
- Basic MPLS Configuration
- Common Configuration Tasks
- MPLS Configuration Management Tasks
- RSVP-TE Configuration Management Tasks
3.15 MPLS Configuration Overview

MPLS enables routers to forward traffic based on a label embedded in the packet header. A router examines the label to determine the next hop for the packet, instead of router address lookups to the next node when forwarding packets.

To implement MPLS on an LSP for outer tunnel and pseudowire assignment, the following entities must be configured:

- Router Interface
- Paths
- LSPs
- Pseudowires
- Signaling Protocol (for RSVP-TE or LDP)

3.15.1 Router Interface

At least one router interface and one system interface must be defined in the `config>router>interface` context in order to configure MPLS on an interface.

3.15.1.1 E-LSP for Differentiated Services

An EXP-inferred LSP (E-LSP) is an LSP that can support a variety of VLLs or traffic types. Up to eight types of traffic can be multiplexed over an E-LSP.

The prioritization of mission-critical traffic is handled by the settings of the three EXP bits. The EXP bits designate the importance of a particular packet. The classification and queuing at the Provider (P) or Provider Edge (PE) nodes typically take place based on the value of the EXP bits. Refer to the 7705 SAR Quality of Service Guide for more information on the use of EXP bits and differentiated services on the 7705 SAR.

3.15.2 Paths

To configure signaled LSPs, you must first create one or more named paths on the ingress router using the `config>router>mpls>path` command. For each path, the transit routers (hops) in the path are specified.
3.15.3 LSPs

The 7705 SAR supports static and dynamic LSPs.

To configure MPLS-signaled (dynamic) LSPs, the LSP must run from an ingress LER to an egress LER. Configure the dynamic LSP only at the ingress router, and either configure the LSP to allow the router software to make the forwarding decisions or configure some or all routers in the LSP path statically. The LSP is set up by RSVP-TE signaling messages. The 7705 SAR automatically manages label values. Labels that are automatically assigned have values ranging from 1024 through 1 048 575 (see Label Values).

A static LSP is a manually configured LSP where the next hop IP address and the outgoing label are explicitly specified.

To establish a static LSP, an LSP must be configured from an ingress LER to an egress LER. Labels must be manually assigned and the label values must be within the range of 32 to 1023 (see Label Values).

3.15.4 Pseudowires

To configure PW/VLL labels, the PW/VLL service must be configured. PW/VLL labels can be configured manually as statically allocated labels using any unused label within the static label range. Pseudowire/VLL labels can also be dynamically assigned by targeted LDP. Statically allocated labels and dynamically allocated labels are designated differently in the label information base.

PW/VLL labels are uniquely identified against a 7705 SAR, not against an interface or module.

As defined in RFC 3036, LDP Specification, and RFC 4447 Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP), label distribution is handled in the Downstream Unsolicited (DU) mode. Generic Label TLV is used for all setup and maintenance operations.
3.15.5 Signaling Protocol

For static LSPs, the path and the label mappings and actions configured at each hop must be specified manually. RSVP-TE or LDP is not required for static LSPs.

For dynamic LSPs, RSVP-TE or LDP must be turned on. See RSVP and RSVP-TE or Label Distribution Protocol.

To implement dynamic pseudowire/VLL labels, entities must be enabled as follows:

- MPLS must be enabled on all routers that are part of a static LSP
- LDP must be enabled on the ingress and egress LERs

When MPLS is enabled and either RSVP-TE or LDP is also enabled, MPLS uses RSVP-TE or LDP to set up the configured LSPs. For example, when you configure an LSP with both MPLS and RSVP-TE running, RSVP-TE initiates a session to create the LSP. RSVP-TE uses the local router as the RSVP-TE session sender and the LSP destination as the RSVP-TE session receiver. Once the RSVP-TE session is created, the LSP is set up on the path created by the session. If the session is not successfully created, RSVP-TE notifies MPLS; MPLS can then either initiate backup paths or retry the initial path.
3.16 Basic MPLS Configuration

This section provides information to configure MPLS and gives configuration examples of common configuration tasks. To enable MPLS on a 7705 SAR router, you must configure at least one MPLS interface. The MPLS interface is configured in the `config>router> mpls` context. The other MPLS configuration parameters are optional.

The following example displays an MPLS configuration output. The `admin-group` is configured in the `config>router>if-attribute` context and associated with the MPLS interface in the `config>router>mpls@interface` context.

```
A:ALU-1>config>router>if-attr# info
------------------------------------------
  admin-group "green" 15
  admin-group "yellow" 20
  admin-group "red" 25
------------------------------------------

A:ALU-1>config>router>mpls# info
------------------------------------------
  interface "system"
  exit
  interface "StaticLabelPop"
    admin-group "green"
    label-map 50
      pop
      no shutdown
    exit
  exit
  interface "StaticLabelPop"
    label-map 35
      swap 36 nexthop 10.10.10.91
      no shutdown
    exit
  exit
  path "to-NYC"
    hop 1 10.10.10.104 strict
    no shutdown
  exit
  path "secondary-path"
    no shutdown
  exit
  lsp "lsp-to-eastcoast"
    to 10.10.10.104
    from 10.10.10.103
    fast-reroute one-to-one
    exit
  primary "to-NYC"
  exit
  secondary "secondary-path"
  exit
  no shutdown
  exit
```

static-lsp "StaticLabelPush"
  to 10.10.11.105
  push 60 nexthop 10.10.11.105
  no shutdown
exit
no shutdown
--------
A:ALU-1>config>router>mpls#
3.17 Common Configuration Tasks

This section provides a brief overview of the tasks to configure MPLS and provides the CLI commands.

The following protocols must be enabled on each participating router:

- MPLS
- RSVP-TE (for RSVP-TE-signaled MPLS only)
- LDP

In order for MPLS to run, you must configure at least one MPLS interface in the `config>router>mpls` context.

- An interface must be created in the `config>router>interface` context before it can be applied to MPLS.
- In the `config>router>mpls` context, configure the path parameters. A path specifies some or all hops from ingress to egress. A path can be used by multiple LSPs.
- When an LSP is created, the egress router must be specified in the to command and at least one primary or secondary path must be specified. All other settings under the LSP hierarchy are optional.

3.17.1 Configuring MPLS Components

Use the MPLS and RSVP-TE CLI syntax shown in the following information for:

- Configuring Global MPLS Parameters
- Configuring an MPLS Interface
- Configuring MPLS Paths
- Configuring an MPLS LSP
- Configuring a Static LSP
- Configuring Manual Bypass Tunnels
- Configuring RSVP-TE Parameters and Interfaces
- Configuring RSVP-TE Message Pacing Parameters
3.17.2 Configuring Global MPLS Parameters

Admin groups can signify link colors, such as red, yellow, or green, or some other link quality. Shared risk link groups (SRLGs) are lists of interfaces that share the same risk of failure due to shared resources. MPLS interfaces advertise the admin groups and SRLGs that they support. CSPF uses the information when paths are computed for constraint-based LSPs. CSPF must be enabled in order for admin groups and SRLGs to be relevant.

Admin groups and SRLGs are created in the `config>router>if-attribute` context. Other global parameters are created in the `config>router>mpls` context.

To configure global MPLS parameters, enter the following commands:

**CLI Syntax:**

```
config>router>if-attribute
   admin-group group-name value group-value
   srlg-group group-name value group-value
```

```
config>router>mpls
   dynamic-bypass [enable | disable]
   frr-object
   hold-timer seconds
   resignal-timer minutes
   srlg-frr [strict]
```

**Example:**

```
config>router# if-attribute
config>router# if-attr# admin-group "green" value 15
config>router# if-attr# admin-group "red" value 25
config>router# if-attr# admin-group "yellow" value 20
config>router# if-attr# srlg-group "SRLG_fiber_1" value 50
config>router# if-attr# exit
config>router# mpls
config>router# mpls# frr-object
config>router# mpls# hold-timer 3
config>router# mpls# resignal-timer 500
config>router# mpls# srlg-frr strict
```
The following example displays a global MPLS configuration output.

A:ALU-1>config>router>if-attr# info
----------------------------------------------
admin-group "green" 15
admin-group "red" 25
admin-group "yellow" 20
srlg-group "SRLG_fiber_1" 50
----------------------------------------------
A:ALU-1>config>router>mpls# info
----------------------------------------------
frr-object
hold-timer 3
resignal-timer 500
srlg-frr strict
----------------------------------------------
A:ALU-1>config>router>mpls# info

3.17.3 Configuring an MPLS Interface

The interface must exist in the system before it can be configured as an MPLS interface; refer to the 7705 SAR Router Configuration Guide for more information.

Once the MPLS protocol instance is created, the `no shutdown` command is not required since MPLS is administratively enabled upon creation. Configure the `label-map` parameters if the interface is used in a static LSP.

Use the following CLI syntax to configure an MPLS interface on a router:

**CLI Syntax:**
```
config>router>mpls
    interface ip-int-name
        admin-group group-name [group-name...(up to 5 max)]
        label-map in-label
          pop
          swap out-label next-hop ip-address
          no shutdown
        srlg-group group-name [group-name...(up to 5 max)]
        te-metric value
        no shutdown
```

**Example:**
```
config>router# mpls
config>router>mpls# interface to-104
config>router>mpls>if# label-map 35
config>router>mpls>if>label-map# swap 36 next-hop 10.10.10.91
config>router>mpls>if>label-map# no shutdown
```
The following example displays the interface configuration output.

```
A:ALU-1>config>router>mpls# info
----------------------------------------------
interface "to-104"
  admin-group "green"
  admin-group "red"
  admin-group "yellow"
  label-map 35
       swap 36 nexthop 10.10.10.91
       no shutdown
  srlg-group "SRLG_fiber_1"
  exit
exit
no shutdown
```

### 3.17.4 Configuring MPLS Paths

Configure an MPLS path for use by LSPs. When configuring an MPLS path, the IP address of each hop that the LSP should traverse on its way to the egress router must be specified. The intermediate hops must be configured as either **strict** or **loose**, meaning that the LSP must take either a direct path from the previous hop router to this router (strict) or can traverse other routers (loose).

Use the following CLI syntax to configure a path:

**CLI Syntax:**
```
config>router>mpls
path path-name
    hop hop-index ip-address {strict|loose}
    no shutdown
```

The following example displays a path configuration output.

```
A:ALU-1>config>router>mpls# info
------------------------------------------
interface "system"
exit
path "to-NYC"
    hop 1 10.10.10.103 strict
    hop 2 10.10.0.210 strict
    hop 3 10.10.0.215 loose
exit
path "secondary-path"
    hop 1 10.10.0.121 strict
    hop 2 10.10.0.145 strict
```
3.17.5 Configuring an MPLS LSP

Configure an LSP for MPLS. When configuring an LSP, you must specify the IP address of the egress router in the to statement. Specify the primary path to be used. Secondary paths can be explicitly configured or signaled upon the failure of the primary path. All other statements are optional.

The following displays an MPLS LSP configuration.

```
A:ALU-1>config>router>mpls# info
...  
  lsp "lsp-to-eastcoast"
    to 192.168.200.41
    rsvp-resv-style ff
cspf
    include "red"
    exclude "green"
adspec
    fast-reroute one-to-one
exit
primary "to-NYC"
    hop-limit 10
exit
secondary "secondary-path"
    bandwidth 50000
exit
no shutdown
exit
no shutdown
```

A:ALU-1>config>router>mpls#
### 3.17.6 Configuring a Static LSP

An LSP can be explicitly (manually) configured. The reserved range of static LSP labels is 32 to 1023. Static LSPs are configured on every node along the LSP path. The label’s forwarding information includes the address of the next hop router.

Use the following CLI syntax to configure a static LSP:

**CLI Syntax:**

```
config>router>mpls
    static-lsp lsp-name
    to ip-address
    push label nexthop ip-address
    no shutdown
```

**Example:**

```
config>router# mpls
config>router>mpls# static-lsp static-LSP
to 10.10.10.124
push 60 nexthop 10.10.42.3
no shutdown
config>router>mpls>static-lsp# exit
```

The following example displays the static LSP configuration output.

```
ALU-1>config>router>mpls# info
----------------------------------------------
... static-lsp "static-LSP"
to 10.10.10.124
push 60 nexthop 10.10.42.3
no shutdown
exit
----------------------------------------------
```

### 3.17.6.1 Configuring a Fast-Retry Timer for Static LSPs

A fast-retry timer can be configured for static LSPs. When a static LSP is trying to come up, MPLS tries to resolve the ARP entry for the next hop of the LSP. This request may fail because the next hop might still be down or unavailable. In that case, MPLS starts a retry timer before making the next request. The fast-retry command allows the user to configure the retry timer so that the LSP comes up shortly after the next hop is available.
Use the following CLI syntax to configure a fast-retry timer for static LSPs:

**CLI Syntax:**
```
config>router>mpls
    static-lsp-fast-retry seconds
```

**Example:**
```
config>router# mpls
config>router>mpls# static-lsp-fast-retry 15
```

### 3.17.7 Configuring Manual Bypass Tunnels

Consider the following network setup in Figure 13. Assume that a manual bypass tunnel must be configured on Node B.

**Figure 13  Manual Bypass Tunnels**

![Diagram of network setup](image)

**Step 1.** Disable dynamic bypass tunnels on Node B.
The CLI syntax for this configuration is:
```
config>router>mpls>dynamic-bypass [disable | enable]
```
By default, dynamic bypass tunnels are enabled.

**Step 2.** Configure an LSP on Node B, such as B-E-F-C, which will be used only as a bypass. Specify each hop in the path and assign its *strict* or *loose* option; in this case, the bypass LSP will have a strict path. Designate the LSP as a primary LSP.
The CLI syntax for this configuration is:
```
config>router>mpls>path path-name>hop hop-index ip-address [strict | loose]
config>router>mpls>lsp lsp-name bypass-only
```
(see also the configuration example below)
Including the *bypass-only* keyword disables some options under the LSP configuration. See Table 6.
Step 3. Configure an LSP from A to D and indicate fast-reroute bypass protection by selecting facility as the FRR method.

The CLI syntax for this configuration is:

```
config>router>mpls>lsp lsp-name>fast-reroute facility
```

If the LSP from A to D goes through Node B and bypass is requested, the next hop is Node C, and there is a manually configured bypass-only tunnel from B to C that excludes link BC (that is, path BEFC), then Node B uses the bypass-only tunnel.

The following example displays a bypass tunnel configuration output.

```
A:ALU-48>config>router>mpls># info
-------------------------------------------
...                               
path "BEFC"
    hop 10 10.10.10.11 strict
    hop 20 10.10.10.12 strict
    hop 30 10.10.10.13 strict
    no shutdown
exit
lsp "bypass-BC" bypass-only
to 10.10.10.15
primary "BEFC"
exit
no shutdown
...                               
-------------------------------------------
```

### Table 6  
Disabled and Enabled Options for Bypass-Only

<table>
<thead>
<tr>
<th>Disabled Options</th>
<th>Enabled Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>• bandwidth</td>
<td>• adaptive</td>
</tr>
<tr>
<td>• fast-reroute</td>
<td>• adspec</td>
</tr>
<tr>
<td>• secondary</td>
<td>• cspf</td>
</tr>
<tr>
<td></td>
<td>• exclude</td>
</tr>
<tr>
<td></td>
<td>• hop-limit</td>
</tr>
<tr>
<td></td>
<td>• include</td>
</tr>
<tr>
<td></td>
<td>• metric</td>
</tr>
</tbody>
</table>

Table 6: | Disabled and Enabled Options for Bypass-Only

<table>
<thead>
<tr>
<th>Disabled Options</th>
<th>Enabled Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>• bandwidth</td>
<td>• adaptive</td>
</tr>
<tr>
<td>• fast-reroute</td>
<td>• adspec</td>
</tr>
<tr>
<td>• secondary</td>
<td>• cspf</td>
</tr>
<tr>
<td></td>
<td>• exclude</td>
</tr>
<tr>
<td></td>
<td>• hop-limit</td>
</tr>
<tr>
<td></td>
<td>• include</td>
</tr>
<tr>
<td></td>
<td>• metric</td>
</tr>
</tbody>
</table>
3.17.8 Configuring RSVP-TE Parameters and Interfaces

RSVP-TE is used to set up LSPs. RSVP-TE must be enabled on the router interfaces that are participating in signaled LSPs. The default values can be modified in the config>router>rsvp context.

Initially, interfaces are configured in the config>router>mpls>interface context. Only these existing (MPLS) interfaces are available to be modified in the config>router>rsvp context. Interfaces cannot be directly added in the rsvp context.

The following example displays an RSVP-TE configuration output.

A:ALU-1>config>router>rsvp# info
---------------------------------------------------------------------
  keep-multiplier 3
  refresh-time 30
  no msg-pacing
  rapid-retransmit-time 5
  rapid-retry-limit 3
  refresh-reduction-over-bypass disable
  no graceful-shutdown
  no entropy-label-capability
  node-id-in-rro exclude
  interface "system"
    no shutdown
  exit
  interface to-104
    hello-interval 4000
    no shutdown
  exit
  no shutdown
---------------------------------------------------------------------
A:ALU-1>config>router>rsvp#
### 3.17.9 Configuring RSVP-TE Message Pacing Parameters

RSVP-TE message pacing maintains a count of the messages that were dropped because the output queue for the egress interface was full.

Use the following CLI syntax to configure RSVP-TE message pacing parameters:

**CLI Syntax:**
```
config>router>rsvp
   no shutdown
   msg-pacing
       period milli-seconds
       max-burst number
```

The following example displays an RSVP-TE message pacing configuration output.

```
A:ALU-1>config>router>rsvp# info
-----------------------------------------------
  keep-multiplier 5
  refresh-time 60
  msg-pacing
      period 400
      max-burst 400
  exit
  interface "system"
      no shutdown
  exit
  interface to-104
      hello-interval 4000
      no shutdown
  exit
  no shutdown
-----------------------------------------------
A:ALU-1>config>router>rsvp#
```
3.18 MPLS Configuration Management Tasks

This section discusses the following MPLS configuration management tasks:

- Deleting MPLS
- Modifying MPLS Parameters
- Modifying an MPLS LSP
- Modifying MPLS Path Parameters
- Modifying MPLS Static LSP Parameters
- Deleting an MPLS Interface

3.18.1 Deleting MPLS

The no form of the mpls command typically removes an MPLS instance and all associated information. However, MPLS must be disabled (shut down) and all SDP bindings to LSPs removed before an MPLS instance can be deleted. Once MPLS is shut down, the no mpls command deletes the protocol instance and removes all configuration parameters for the MPLS instance.

If MPLS is not shut down first, when the no mpls command is executed, a warning message on the console indicates that MPLS is still administratively up.

To delete the MPLS instance:

1. Disable the MPLS instance using the shutdown command.
2. Remove the MPLS instance from the router using the no mpls command.

**CLI Syntax:**
```
config>router# no mpls
```

3.18.2 Modifying MPLS Parameters

**Note:** You must shut down MPLS entities in order to modify parameters. Re-enable (no shutdown) the entity for the change to take effect.
3.18.3 Modifying an MPLS LSP

Some MPLS LSP parameters (such as primary and secondary), must be shut down before they can be edited or deleted from the configuration.

The following example displays an MPLS LSP configuration output. Refer to Configuring an MPLS Interface.

A:ALU-1>>config>router>mpls>lsp# info
----------------------------------------------
shutdown
to 10.10.10.104
from 10.10.10.103
rsvp-resv-style ff
include "red"
exclude "green"
fast-reroute one-to-one
exit
primary "to-NYC"
hop-limit 50
exit
secondary "secondary-path"
exit
----------------------------------------------
A:ALU-1>config>router>mpls#

3.18.4 Modifying MPLS Path Parameters

In order to modify path parameters, the config>router>mpls>path context must be shut down first.

The following example displays an MPLS path configuration output. Refer to Configuring MPLS Paths.

A:ALU-1>config>router>mpls# info
#------------------------------------------
echo "MPLS"
#------------------------------------------
...
p
ath "secondary-path"
  hop 1 10.10.0.111 strict
  hop 2 10.10.0.222 strict
  hop 3 10.10.0.123 strict
  no shutdown
exit
path "to-NYC"
  hop 1 10.10.10.104 strict
  hop 2 10.10.0.210 strict
  no shutdown
exit
#------------------------------------------
3.18.5 Modifying MPLS Static LSP Parameters

Use the `show>service>router>static-lsp` command to display a list of LSPs.

In order to modify static LSP parameters, the `config>router>mpls>static-lsp lsp-name` context must be shut down.

To modify an LSP:

1. Access the specific LSP by specifying the LSP name, and then shut it down.
2. Enter the parameter to modify and then enter the new information.

Example:

```
config>router# mpls
config>router>mpls# static-lsp "static-LSP"
config>router>mpls>static-lsp# shutdown
config>router>mpls>static-lsp# to 10.10.0.234
config>router>mpls>static-lsp# push 1023 nexthop 10.10.8.114
config>router>mpls>static-lsp# no shutdown
config>router>mpls>static-lsp# exit
```

The following example displays the static LSP configuration output.

```
ALU-1>config>router>mpls# info
-----------------------------------------------
... static-lsp "static-LSP"
   to 10.10.10.234
   push 1023 nexthop 10.10.8.114
   no shutdown
   exit
no shutdown
-----------------------------------------------
ALU-1>config>router>mpls#
```
3.18.6 Deleting an MPLS Interface

To delete an interface from the MPLS configuration:

1. Administratively disable the interface using the `shutdown` command.
2. Delete the interface with the `no interface` command.

CLI Syntax:

```
mpls
  interface ip-int-name
    shutdown
    exit
  no interface ip-int-name
```

Example:
```
config>router# mpls
config>router>mpls# interface to-104
config>router>mpls>if# shutdown
config>router>mpls>if# exit
config>router>mpls# no interface to-104
```

The following example displays the configuration output when interface “to-104” has been deleted.

```
A:ALU-1>config>router>mpls# info
----------------------------------------------
... admin-group "green" 15
    admin-group "red" 25
    admin-group "yellow" 20
    interface "system"
    exit
    no shutdown
----------------------------------------------
A:ALU-1>config>router>mpls#
```
3.19 RSVP-TE Configuration Management Tasks

This section discusses the following RSVP-TE configuration management tasks:

- Modifying RSVP-TE Parameters
- Modifying RSVP-TE Message Pacing Parameters
- Deleting an Interface from RSVP-TE

3.19.1 Modifying RSVP-TE Parameters

Only interfaces configured in the MPLS context can be modified in the `rsvp` context.

The **no rsvp** command deletes this RSVP-TE protocol instance and removes all configuration parameters for this RSVP-TE instance. The **shutdown** command suspends the execution and maintains the existing configuration.

The following example displays a modified RSVP-TE configuration output.

```
A:ALU-1>config>router>rsvp# info
----------------------------------------------
  keep-multiplier 5
  refresh-time 60
  msg-pacing
    period 400
    max-burst 400
  exit
  rapid-retransmit-time 5
  rapid-retry-limit 3
  refresh-reduction-over-bypass disable
  no graceful-shutdown
  no entropy-label-capability
  node-id-in-rro exclude
  interface "system"
  exit
  interface "test1"
    hello-interval 5000
  exit
  no shutdown
----------------------------------------------
A:ALU-1>config>router>rsvp#
```
3.19.2 Modifying RSVP-TE Message Pacing Parameters

RSVP-TE message pacing maintains a count of the messages that were dropped because the output queue for the egress interface was full.

The following example displays a modified RSVP-TE message pacing configuration output. Refer to Configuring RSVP-TE Message Pacing Parameters.

```
A:ALU-1>config>router>rsvp# info
----------------------------------------------
keep-multiplier 5
refresh-time 60
msg-pacing
  period 200
  max-burst 200
exit
interface "system"
exit
interface "to-104"
exit
no shutdown
----------------------------------------------
A:ALU-1>config>router>rsvp#
```

3.19.3 Deleting an Interface from RSVP-TE

Interfaces cannot be deleted directly from the RSVP-TE configuration. Because an interface is created in the mpls context and then configured in the rsvp context, it can only be deleted in the mpls context. This removes the association from RSVP-TE.

Refer to Deleting an MPLS Interface.
3.20  MPLS and RSVP-TE Command Reference

3.20.1  Command Hierarchies

- MPLS Commands
- RSVP-TE Commands
- Show Commands
- Tools Commands (refer to Tools section of 7705 SAR OAM and Diagnostics Guide)
- Clear Commands
- Debug Commands
3.20.1.1 MPLS Commands

config
  — router [router-name]
    — [no] mpls
      — [no] admin-group-frr
      — auto-lsp lsp-template template-name (policy peer-prefix-policy peer-prefix-policy...(up to 5 max)] | one-hop)
      — no auto-lsp lsp-template template-name
      — [no] cspf-on-loose-hop
      — dynamic-bypass [enable | disable]
      — [no] frr-object
      — hold-timer seconds
      — no hold-timer
      — [no] interface ip-int-name
        — [no] admin-group group-name [group-name...(up to 5 max)]
        — [no] label-map in-label
          — [no] pop
          — swap out-label nexthop ip-address
          — no swap
          — [no] shutdown
        — [no] shutdown
        — [no] srlg-group group-name [group-name...(up to 5 max)]
        — te-metric value
        — no te-metric
        — least-fill-min-thd percent
        — no least-fill-min-thd
        — least-fill-reoptim-thd percent
        — no least-fill-reoptim-thd
        — [no] logger-event-bundling
      — [no] lsp lsp-name [bypass-only]
        — [no] adaptive
        — [no] adspec
        — bgp-transport-tunnel (include | exclude)
        — [no] cspf [use-te-metric]
        — [no] exclude group-name [group-name...(up to 5 max)]
        — [no] fast-reroute [frr-method]
          — hop-limit limit
          — no hop-limit
          — [no] node-protect
          — [no] propagate-admin-group
        — from ip-address
        — hop-limit number
        — no hop-limit
        — igp-shortcut [lfa-protect | lfa-only | relative-metric [offset]]
        — no igp-shortcut
        — [no] include group-name [group-name...(up to 5 max)]
        — [no] least-fill
        — metric metric
        — path-profile profile-id [path-group group-id]
        — no path-profile profile-id
        — [no] pce-computation
        — [no] pce-control
- `pce-report {enable | disable | inherit}
- [no] primary path-name
  - [no] adaptive
  - bandwidth rate-in-mbps
  - no bandwidth
  - [no] exclude group-name [group-name...(up to 5 max)]
  - hop-limit number
  - no hop-limit
  - [no] include group-name [group-name...(up to 5 max)]
  - [no] record
  - [no] record-label
  - [no] shutdown
- [no] propagate-admin-group
- retry-limit number
- no retry-limit
- retry-timer seconds
- no retry-timer
- `rsvp-resv-style [se | ff]
- [no] secondary path-name
  - [no] adaptive
  - bandwidth rate-in-mbps
  - no bandwidth
  - [no] exclude group-name [group-name...(up to 5 max)]
  - hop-limit number
  - no hop-limit
  - [no] include group-name [group-name...(up to 5 max)]
  - [no] record
  - [no] record-label
  - [no] shutdown
  - [no] srlg
  - [no] standby
  - [no] shutdown
  - to ip-address
  - `vprn-auto-bind [include | exclude]
  - no vprn-auto-bind
- `lsp-template template-name
- `lsp-template template-name mesh-p2p
- `lsp-template template-name one-hop-p2p
  - no lsp-template template-name [one-hop-p2p | mesh-p2p]
  - [no] adaptive
  - [no] adspec
  - bgp-transport-tunnel {include | exclude}
  - [no] csdp [use-te-metric]
  - [no] default-path path-name
  - [no] exclude group-name [group-name...(up to 5 max)]
  - [no] fast-reroute [frr-method]
    - hop-limit limit
    - no hop-limit
  - [no] node-protect
  - [no] propagate-admin-group
  - from ip-address
  - hop-limit number
  - no hop-limit
  - `igp-shortcut [ifa-protect | ifa-only] [relative-metric [offset]]
--- no  igp-shortcut
--- [no]  include  group-name  [group-name...(up to 5 max)]
--- [no]  least-fill
--- metric  metric
--- pce-report  {enable | disable | inherit}
--- [no]  propagate-admin-group
--- retry-limit  number
--- no  retry-limit
--- retry-timer  seconds
--- no  retry-timer
--- [no]  shutdown
--- vprn-auto-bind  [include | exclude]
--- [no]  path  path-name
--- hop  hop-index  ip-address  {strict | loose}
--- no  hop  hop-index
--- [no]  shutdown
--- pce-report  rsvp-te  {enable | disable}
--- resignal-timer  minutes
--- no  resignal-timer
--- srlg-frr  [strict]
--- no  srlg-frr
--- [no]  shutdown
--- [no]  static-lsp  lsp-name
--- push  label  nexthop  ip-address
--- no  push  label
--- to  ip-address
--- [no]  shutdown
--- static-lsp-fast-retry  seconds
--- no  static-lsp-fast-retry

3.20.1.2 RSVP-TE Commands

    config
    --- router
    --- [no]  rsvp
    --- [no]  entropy-label-capability
    --- [no]  graceful-shutdown
    --- [no]  interface  ip-int-name
        --- auth-keychain  name
        --- no  auth-keychain
        --- authentication-key  {authentication-key | hash-key}  [hash | hash2]
        --- no  authentication-key
        --- [no]  bfd-enable
        --- [no]  graceful-shutdown
        --- hello-interval  milli-seconds
        --- no  hello-interval
        --- [no]  refresh-reduction
            --- [no]  reliable-delivery
        --- [no]  shutdown
        --- subscription  percentage
        --- no  subscription
3.20.1.3 Show Commands

show
  — router
  — mpls
    — admin-group group-name
    — bypass-tunnel [to ip-address] [protected-lsp [lsp-name]] [dynamic | manual] [detail]
    — interface [ip-int-name | ip-address] [label-map [label]]
    — interface [ip-int-name | ip-address] statistics
    — label start-label [end-label] [in-use] [label-owner]
    — label-range
    — lsp [lsp-name] [status {up | down}] [from ip-address] [to ip-address] [detail] [auto-lsp {all | mesh-p2p | one-hop-p2p}]
    — lsp [transit | terminate] [status {up | down}] [from ip-address] [to ip-address] [lsp-name name] [detail]
    — lsp count
    — lsp [lsp-name] activepath [auto-lsp {all | mesh-p2p | one-hop-p2p}]
    — lsp [lsp-name] path [path-name] [status {up | down}] [detail] [auto-lsp {all | mesh-p2p | one-hop-p2p}]
    — lsp [lsp-name] path [path-name] mbb [auto-lsp {all | mesh-p2p | one-hop-p2p}]
    — lsp-template [lsp-template-name] bindings
    — lsp-template [lsp-template-name] detail
    — path [path-name] [lsp-binding]
    — static-lsp [lsp-name]
    — static-lsp [lsp-type]
    — static-lsp count
    — srlg-group [group-name]
    — status

show
  — router
  — rsvp
— interface [ip-int-name | ip-address] statistics [detail]
— neighbor [ip-address] [detail]
— session [session-type] [from ip-address] to [ip-address] [lsp-name name]
  [status (up | down)] [detail]
— statistics
— status

3.20.1.4 Clear Commands

clear
  — router
    — mpls
      — interface [ip-int-name] [statistics]
      — lsp [lsp-name]
    — rsvp
      — interface [ip-int-name] [statistics]
      — statistics

3.20.1.5 Debug Commands

debug
  — router
    — [no] mpls [lsp lsp-name] [sender source-address] [endpoint endpoint-address]
      [tunnel-id tunnel-id] [lsp-id lsp-id] [interface ip-int-name]
    — [no] event
      — all [detail]
      — no all
      — frr [detail]
      — no frr
      — iom [detail]
      — no iom
      — lsp-setup [detail]
      — no lsp-setup
      — mbb [detail]
      — no mbb
      — misc [detail]
      — no misc
      — xc [detail]
      — no xc
    — [no] rsvp [lsp lsp-name] [sender sender-address] [endpoint endpoint-address]
      [tunnel-id tunnel-id] [lsp-id lsp-id] [interface ip-int-name]
    — [no] event
      — all [detail]
      — no all
      — auth
      — no auth
      — misc [detail]
      — no misc
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nbr</td>
<td>neighbor</td>
</tr>
<tr>
<td>no nbr</td>
<td></td>
</tr>
<tr>
<td>path</td>
<td>path</td>
</tr>
<tr>
<td>no path</td>
<td></td>
</tr>
<tr>
<td>resv</td>
<td>reservation</td>
</tr>
<tr>
<td>no resv</td>
<td></td>
</tr>
<tr>
<td>rr</td>
<td></td>
</tr>
<tr>
<td>no rr</td>
<td></td>
</tr>
<tr>
<td>[no] packet</td>
<td></td>
</tr>
<tr>
<td>ack</td>
<td>acknowledgement</td>
</tr>
<tr>
<td>no ack</td>
<td></td>
</tr>
<tr>
<td>all</td>
<td>all</td>
</tr>
<tr>
<td>no all</td>
<td></td>
</tr>
<tr>
<td>bundle</td>
<td>bundle</td>
</tr>
<tr>
<td>no bundle</td>
<td></td>
</tr>
<tr>
<td>hello</td>
<td>hello</td>
</tr>
<tr>
<td>no hello</td>
<td></td>
</tr>
<tr>
<td>path</td>
<td>path</td>
</tr>
<tr>
<td>no path</td>
<td></td>
</tr>
<tr>
<td>patherr</td>
<td>path error</td>
</tr>
<tr>
<td>no patherr</td>
<td></td>
</tr>
<tr>
<td>pathtear</td>
<td>path tear</td>
</tr>
<tr>
<td>no pathtear</td>
<td></td>
</tr>
<tr>
<td>resv</td>
<td>reservation</td>
</tr>
<tr>
<td>no resv</td>
<td></td>
</tr>
<tr>
<td>resverr</td>
<td>reservation error</td>
</tr>
<tr>
<td>no resverr</td>
<td></td>
</tr>
<tr>
<td>resvtear</td>
<td>reservation tear</td>
</tr>
<tr>
<td>no resvtear</td>
<td></td>
</tr>
<tr>
<td>srefresh</td>
<td>refresh</td>
</tr>
<tr>
<td>no srefresh</td>
<td></td>
</tr>
</tbody>
</table>
3.20.2 Command Descriptions

- Configuration Commands (MPLS)
- Configuration Commands (RSVP-TE)
- Show Commands (MPLS)
- Show Commands (RSVP)
- Clear Commands
- Debug Commands
3.20.2.1 Configuration Commands (MPLS)

- Generic Commands
- MPLS Global Commands
- Interface Commands
- Interface Label-Map Commands
- LSP and LSP Template Commands
- Primary and Secondary Path Commands
- LSP Path Commands
- Static LSP Commands
3.20.2.1.1 Generic Commands

shutdown

Syntax
[no] shutdown

Context
config>router>mpls
config>router>mpls>interface
config>router>mpls>if>label-map
config>router>mpls>path
config>router>mpls>static-lsp

Description
The shutdown command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many objects must be shut down before they can be deleted. Many entities must be explicitly enabled using the no shutdown command.

In the label-map context, all packets that match the specified in-label are dropped when the label map is shut down.

In the path context, this command disables the existing LSPs using this path. All services using these LSPs are affected. Binding information, however, is retained in those LSPs. Paths are created in the shutdown state.

The no form of this command places the entity into an administratively enabled state. In the mpls and mpls>interface contexts, this triggers any LSPs that were previously defined under the associated context to come back up. In the path context, the no form of this command administratively enables the path and all LSPs—where the path is defined as a primary or a standby secondary path—are (re)established.

Default
mpls — no shutdown
interface — shutdown
label-map — no shutdown
path — shutdown
static-lsp — shutdown
### 3.20.2.1.2 MPLS Global Commands

**mpls**

**Syntax**

```
[no] mpls
```

**Context**

```
config>router
```

**Description**

This command creates the MPLS protocol instance and enables MPLS configuration. The MPLS protocol instance is not created by default, but once it is created, a **no shutdown** command is not required since MPLS is enabled automatically. The **shutdown** command administratively disables MPLS.

The **no** form of this command deletes this MPLS protocol instance and all configuration parameters for this MPLS instance.

MPLS must be shut down and all SDP bindings to LSPs removed before the MPLS instance can be deleted. If MPLS is not shut down, when the **no mpls** command is executed, a warning message on the console indicates that MPLS is still administratively up.

**admin-group-frr**

**Syntax**

```
[no] admin-group-frr
```

**Context**

```
config>router>mpls
```

**Description**

This command enables the use of admin-group constraints in the association of a manual or dynamic bypass LSP with the primary LSP path at a Point-of-Local Repair (PLR) node.

When this command is enabled, each PLR node reads the admin-group constraints in the FAST_REROUTE object in the PATH message of the LSP primary path. If the FAST_REROUTE object is not included in the PATH message, the PLR reads the admin-group constraints from the SESSION_ATTRIBUTE object in the PATH message.

If the PLR is also the ingress LER for the LSP primary path, it only uses the admin-group constraint from the LSP and/or path level configurations.

The PLR node then uses the admin-group constraints along with other constraints, such as hop-limit and SRLG, to select a manual or dynamic bypass LSP among those that are already in use.

If none of the manual or dynamic bypass LSPs satisfies the admin-group constraints and/or the other constraints, the PLR node will request CSPF for a path that merges the closest to the protected link or node and includes or excludes the specified admin-group IDs.

Changes to this command (enabling or disabling) will apply only to new attempts to find a valid bypass.
The `no` form of this command disables the use of administrative group constraints on a FRR backup LSP at a PLR node.

**Default**

```
no admin-group-frr
```

### auto-lsp

**Syntax**

```
auto-lsp lsp-template template-name (policy peer-prefix-policy [peer-prefix-policy...(up to 5 max)]) | one-hop)
```

```
no auto-lsp lsp-template template-name
```

**Context**

```
config>router>mpls
```

**Description**

This command enables the automatic creation of an RSVP-TE point-to-point LSP within a single IGP IS-IS level or OSPF area that can subsequently be used by services and/or IGP shortcuts. It can be used to create an RSVP-TE LSP mesh to a destination node whose router ID matches a prefix in a specified previously created peer prefix policy, or to create single-hop RSVP-TE LSPs. These LSP types are referred to as auto-LSP of type mesh or auto-LSP of type one-hop.

Multiple templates can be associated with the same or different peer prefix policies. Each application of an LSP template with a given prefix in the prefix list results in the instantiation of a single CSPF-computed LSP primary path using the LSP template parameters, as long as the prefix corresponds to a router ID for a node in the TE database. Auto LSP does not support the automatic signaling of a secondary path for an LSP. If the signaling of multiple LSPs to the same destination node is required, a separate LSP template must be associated with a prefix list that contains the same destination node address. Each instantiated LSP will have a unique LSP ID and a unique tunnel ID. Auto LSP also does not support the signaling of a non-CSPF LSP. The selection of the `no csfp` option in the LSP template is blocked.

Up to five peer prefix policies can be associated with an LSP template. Every time the user executes the above command with the same or different prefix policy associations or a prefix policy associated with the LSP template, the system re-evaluates the prefix policy. The outcome of the re-evaluation indicates to MPLS whether an existing LSP must be torn down or a new LSP must be signaled to a destination address that is already in the TE database.

If a `/32` prefix is added to or removed from a prefix list associated with the template, or if a prefix range is expanded or narrowed, the prefix policy re-evaluation described above is performed.

A `no shutdown` of the template must be performed before it takes effect. When a template is in use, it must be shut down before the user can make any changes to the parameters except for LSP parameters for which the change can be handled with the Make-Before-Break (MBB) procedures. This includes `fast-reroute` with or without the `hop-limit` or `node-protect` options. When the template is shut down and parameters are added, removed or modified, the existing instances of the LSP using this template are torn down and resignalled.
The trigger to signal the LSP is when the router with a router ID matching a prefix in the prefix list appears in the TE database. The signaled LSP is installed in the Tunnel Table Manager (TTM) and is available to applications such as resolution of BGP label routes, and resolution of BGP, IGP, and static routes. It can also be used for auto-binding by a VPRN service but cannot be used as a provisioned SDP for explicit binding.

Except for the MBB limitations to the configuration parameter change in the LSP template, MBB procedures for manual and timer-based resignaling of the LSP, and for TE graceful shutdown, are supported.

The **one-to-one** option under fast-reroute is not supported.

If the **one-hop** option is specified instead of a prefix policy, this command enables the automatic signaling of single-hop, point-to-point LSPs using the specified template to all directly connected neighbors. This LSP type is referred to as auto LSP of type **one-hop**. When the above command is executed, the TE database keeps track of each TE link to a directly connected IGP neighbor whose router ID is discovered. It then instructs MPLS to signal an LSP with a destination address matching the router ID of the neighbor and with a strict hop consisting of the address of the interface used by the TE link. This results in one or more LSPs signaled to the neighboring router.

For an LSP mesh, the **no** form of this command deletes all LSPs signaled using the specified template and prefix policy. When the **one-hop** option is used, the **no** form of the command deletes all single-hop LSPs signaled using the specified template to all directly connected neighbors.

**Default**

n/a

**Parameters**

- **template-name** — specifies an LSP template name
- **one-hop** — specifies that the template type is one-hop LSP, rather than LSP mesh
- **peer-prefix-policy** — specifies a peer prefix policy name. The prefix policy must already be defined.

---

cspf-on-loose-hop

**Syntax**

[no] cspf-on-loose-hop

**Context**

config>router>mpls

**Description**

This command enables the option to perform CSPF calculations to the next loose hop or the final destination of the LSP on the LSR. On receiving a PATH message on the LSR and processing all local hops in the received ERO, if the next hop is loose, then the LSR does a CSPF calculation to the next loose hop (this is known as ERO expansion). On successful completion of the CSPF calculation, the ERO in the PATH message is modified to include the newly calculated intermediate hops and the message is propagated forward to the next hop. This allows for the setting up of inter-area LSPs based on the ERO expansion method.
The LSP may fail to set up if this option is enabled on an LSR that is not an ABR and that receives a PATH message without a proper next loose hop in the ERO. The `cspf-on-loose-hop` configuration can change dynamically and is applied to the new LSP setup after changes are made.

**Default**

`no cspf-on-loose-hop`

dynamic-bypass

**Syntax**

`dynamic-bypass [enable | disable]`

**Context**

`config>router>mpls`

**Description**

This command disables the creation of dynamic bypass LSPs in FRR. One or more manual bypass LSPs must be configured to protect the primary LSP path at the PLR nodes.

**Default**

`enable`

frr-object

**Syntax**

`[no] frr-object`

**Context**

`config>router>mpls`

**Description**

This command specifies whether signaling the FAST_REROUTE object is on or off. The value is ignored if fast reroute is disabled for the LSP or if the LSP is using one-to-one backup.

**Default**

`frr-object — by default, the value is inherited by all LSPs`

hold-timer

**Syntax**

`hold-timer seconds`

`no hold-timer`

**Context**

`config>router>mpls`

**Description**

This command specifies the amount of time that the ingress node waits before programming its data plane and declaring to the service module that the LSP status is up.

The `no` form of the command disables the hold-timer.

**Parameters**

`seconds — specifies the hold time, in seconds`

**Values**

0 to 10
least-fill-min-thd

Syntax  least-fill-min-thd percent
        no least-fill-min-thd

Context  config>router>mpls

Description  This parameter is used in the least-fill path selection process. See the description of the least-fill command for information on the least-fill path selection process. When comparing the percentages of least available link bandwidth across the available paths, whenever two percentages differ by less than the value configured as the least-fill minimum threshold, CSPF considers them to be equal and applies a random number generator to select the path.

The no form of the command resets this parameter to its default value.

Default  5

Parameters  percent — specifies the least fill minimum threshold value as a percentage

Values  1 to 100

least-fill-reoptim-thd

Syntax  least-fill-reoptim-thd percent
        no least-fill-reoptim-thd

Context  config>router>mpls

Description  This parameter is used in the least-fill path selection process. See the description of the least-fill command for information on the least-fill path selection process.

During a timer-based resignaling of an LSP path that has the least-fill option enabled, CSPF first updates the least-available bandwidth value for the current path of this LSP. It then applies the least-fill path selection method to select a new path for this LSP. If the new computed path has the same cost as the current path, CSPF compares the least-available bandwidth values of the two paths and if the difference exceeds the user-configured optimization threshold, MPLS generates a trap to indicate that a better least-fill path is available for this LSP. This trap can be used by an external SNMP-based device to trigger a manual resignaling of the LSP path, since the timer-based resignaling will not resignal the path in this case. MPLS generates a path update trap at the first MBB event that results in the resignaling of the LSP path. This clears the eligibility status of the path at the SNMP device.

The no form of the command resets this parameter to its default value.

Default  10

Parameters  percent — specifies the least fill reoptimization threshold value as a percentage

Values  1 to 100
logger-event-bundling

**Syntax**  
[no] logger-event-bundling

**Context**  
config>router>mpls

**Description**  
This command merges two of the most commonly generated MPLS traps, vRtrMplsXCCreate and vRtrMplsXCDelete, which can be generated at both the LER and LSR, into the new vRtrMplsSessionsModified trap. In addition, this command bundles traps of multiple RSVP sessions, such as LSPs, into this new trap.

This trap bundling allows the user to minimize trap generation in an MPLS network. MPLS trap throttling is not applied to the vRtrMplsSessionsModified trap.

The **no** version of the command disables the merging and bundling of the vRtrMplsXCCreate and vRtrMplsXCDelete traps.

pce-report

**Syntax**  
pce-report rsvp-te {enable | disable}

**Context**  
config>router>mpls

**Description**  
This command configures the reporting modes to a PCE for RSVP-TE LSPs.

The PCC LSP database is synchronized with the PCE LSP database using the PCEP PCRpt (PCE Report) message for PCC-controlled, PCE-computed, and PCE-controlled LSPs.

This global MPLS-level **pce-report** command can be used to enable or disable PCE reporting for all RSVP-TE LSPs during PCE LSP database synchronization. The PCC reports both CSPF and non-CSPF LSPs.

The LSP-level **pce-report** command overrides the global configuration for the reporting of an LSP to the PCE (see **config>router>mpls>lsp>pce-report**). The default configuration is to inherit the global MPLS-level configuration.

The default configuration is disabled. This default configuration is meant to control the introduction of a PCE into an existing network and let the operator decide whether all RSVP-TE LSPs need to be reported. If PCE reporting is disabled for an LSP, either due to inheritance of the global MPLS configuration or due to LSP-level configuration, enabling the **pce-control** option for the LSP has no effect.

**Default**  
pce-report rsvp-te disable

**Parameters**  
rsvp-te {enable | disable} — specifies to enable or disable PCE reporting for all RSVP-TE LSPs
resignal-timer

Syntax  
resignal-timer minutes  
no resignal-timer

Context  
config>router>mpls

Description  
This command specifies the value for the LSP resignal timer. The resignal timer is the time, in minutes, that the 7705 SAR software waits before attempting to resignal the LSPs.

When the resignal timer expires, if the newly computed path for an LSP has a better metric than that for the currently recorded hop list, an attempt is made to resignal that LSP using the make-before-break (MBB) mechanism. If the attempt to resignal an LSP fails, the LSP will continue to use the existing path and a resignal will be attempted the next time the timer expires.

When the resignal timer expires, a trap and syslog message are generated.

The no form of the command disables timer-based LSP resignalizing.

Default  
no resignal-timer

Parameters  
minutes — specifies the time the software waits before attempting to resignal the LSPs, in minutes

Values  
30 to 10080
srlg-frr

Syntax srlg-frr [strict]
no srlg-frr

Context config>router>mpls

Description This system-wide command enables or disables the use of the shared risk link group (SRLG) constraint in the computation of an FRR bypass or detour LSP for any primary LSP path on the system. When srlg-frr is enabled, CSPF includes the SRLG constraint in the computation of an FRR bypass or detour LSP for protecting the primary LSP path.

The strict option is a system-wide option that forces the CSPF to consider any configured SRLG membership lists in its calculation of every LSP path.

CSPF and FRR

CSPF prunes all links with interfaces that belong to the same SRLG as the interface being protected, where the interface being protected is the outgoing interface at the PLR used by the primary path. If one or more paths are found, the MPLS/RSVP-TE task selects one path based on best cost and signals the setup of the FRR bypass or detour LSP. If no path is found and the user included the strict option, the FRR bypass or detour LSP is not set up and the MPLS/RSVP-TE task keeps retrying the request to CSPF. If no path is found and the strict option is disabled, if a path exists that meets all the TE constraints except the SRLG constraint, then the FRR bypass or detour LSP is set up.

An FRR bypass or detour LSP is not guaranteed to be SRLG disjoint from the primary path. This is because only the SRLG constraint of the outgoing interface at the PLR that the primary path is using is checked.

When the MPLS/RSVP-TE task is searching for an SRLG bypass tunnel to associate with the primary path of the protected LSP, the task does the following steps.

- First, the task checks for any configured manual bypass LSP that has CSPF enabled and that satisfies the SRLG constraints.
- The task skips any non-CSPF bypass LSP since there is no ERO returned with which to check the SRLG constraint.
- If no path is found, the task checks for an existing dynamic bypass LSP that satisfies the SRLG and other primary path constraints.
- If no bypass path is found, then the task makes a request to CSPF to try to create one.

Primary Path and FRR Behavior

Once the primary path of the LSP is set up and is operationally up, any subsequent changes to the SRLG membership of an interface that the primary path is using will not be considered by the MPLS/RSVP-TE task at the PLR for FRR bypass or detour LSP association until the next opportunity that the primary path is resignaled. The path may be resignedaled due to a failure or to a make-before-break (MBB) operation. A make-before-break operation occurs as a result of a global revertive operation, a reoptimization of the LSP path (timer-based or manual), or a change by the user to any of the path constraints.
Once the FRR bypass or detour LSP is set up and is operationally up, any subsequent change to the SRLG membership of an interface that the FRR bypass or detour LSP is using will not be considered by the MPLS/RSVP-TE task at the PLR until the next opportunity that the association with the primary LSP path is rechecked. The association is rechecked if the FRR bypass or detour LSP is reoptimized. Detour routes are not reoptimized and are resignal if the primary path is down.

The user must first shut down MPLS before enabling or disabling the `srlg-frr` option in CLI.

An RSVP-TE interface can belong to a maximum of 64 SRLGs. The user creates SRLGs using the `config>router>mpls>srlg-group` command. The user associates the SRLGs with an RSVP-TE interface using the `srlg-group` command in the `config>router>mpls>interface` context.

The `no` form of the command reverts to the default value.

```
Default
no srlg-frr

Parameters
strict — specifies that the CSPF calculation for the FRR backup must include the SRLG constraint and the backup must be on the resulting list of eligible backup paths

Values
non-strict:srlg-frr
strict:srlg-frr strict
```
3.20.2.1.3  Interface Commands

interface

Syntax  
[no] interface ip-int-name

Context  
config>router>mpls

Description  
This command enables MPLS protocol support on an IP interface. MPLS commands are not executed on an IP interface where MPLS is not enabled.

The no form of this command deletes all MPLS commands that are defined under the interface, such as label-map. The interface must be shut down before it can be deleted. If the interface is not shut down, the no interface ip-int-name command issues a warning message on the console indicating that the interface is administratively up.

Default  
shutdown

Parameters  
ip-int-name — identifies the network IP interface. The interface name character string cannot be in the form of an IP address. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

admin-group

Syntax  
[no] admin-group group-name [group-name...(up to 5 max)]

Context  
config>router>mpls>interface

Description  
This command associates admin groups with this interface. The admin group must already be defined in the config>router>if-attribute context (refer to the 7705 SAR Router Configuration Guide, “IP Router Command Reference”).

Up to five groups can be specified with one command. When an admin group is bound to one or more interfaces, its value cannot be changed until all bindings are removed.

When associated with MPLS interfaces, the interfaces can be included or excluded in the LSP path definition by matching on the admin-group name. CSPF will calculate a path that satisfies the admin-group include and exclude constraints.

The configured admin-group membership is applied in all levels or areas that the interface is participating in. The same interface cannot have different memberships in different levels or areas.

The admin groups bound to an MPLS interface are advertised area-wide in TE link TLVs and sub-TLVs when the traffic-engineering option is enabled in IS-IS or OSPF.
The no form of this command deletes the association of this interface with one or more of the admin groups.

**Default**

no admin-group

**Parameters**

group-name — specifies the name of the group. The group names should be the same across all routers in the MPLS domain.

---

### srlg-group

**Syntax**

[no] srlg-group group-name [group-name...(up to 5 max)]

**Context**

config>router>mpls>interface

**Description**

This command associates an MPLS interface with one or more SRLGs. The SRLG must already be defined in the config>router>if-attribute context (refer to the 7705 SAR Router Configuration Guide, “IP Router Command Reference”).

Up to five SRLGs can be specified with one command. When an SRLG is bound to one or more interfaces, its value cannot be changed until all bindings are removed.

When SRLGs are associated with MPLS interfaces, CSPF at an LER will exclude the SRLGs of interfaces used by the LSP primary path when calculating the route of the secondary path. CSPF at an LER or LSR will also exclude the SRLGs of the outgoing interface of the primary LSP path in the calculation of the path of the FRR backup LSP. This provides a path disjoint between the primary path and the secondary path or FRR backup path of an LSP.

The configured SRLG membership is applied in all levels or areas that the interface is participating in. The same interface cannot have different memberships in different levels or areas.

SRLGs bound to an MPLS interface are advertised area-wide in TE link TLVs and sub-TLVs when the traffic-engineering option is enabled in IS-IS or OSPF.

The no form of this command deletes the association of this interface with one or more of the SRLGs.

**Default**
	n/a

**Parameters**

group-name — specifies the name of the SRLG. The group names should be the same across all routers in the MPLS domain.
te-metric

**Syntax**

```
  te-metric  value
  no  te-metric
```

**Context**

```
config>router>mpls>interface
```

**Description**

This command configures the traffic engineering metric used on the interface. This metric is in addition to the interface metric used by IGP for the shortest path computation.

This metric is flooded as part of the TE parameters for the interface using an opaque LSA or an LSP. The OSPF-TE metric is encoded as a sub-TLV type 5 in the Link TLV. The metric value is encoded as a 32-bit unsigned integer. The IS-IS-TE metric is encoded as sub-TLV type 18 as part of the extended IS reachability TLV. The metric value is encoded as a 24-bit unsigned integer.

When the use of the TE metric is enabled for an LSP, CSPF will first prune all links in the network topology that do not meet the constraints specified for the LSP path. Such constraints include bandwidth, admin-groups, and hop limit. Then, CSPF will run an SPF on the remaining links. The shortest path among the all SPF paths will be selected based on the TE metric instead of the IGP metric, which is used by default.

The TE metric in CSPF LSP path computation can be configured by entering the command

```
config>router>mpls>lsp  lsp-name>csfp  use-te-metric.
```

The TE metric is only used in CSPF computations for MPLS paths and not in the regular SPF computation for IP reachability.

The **no** form of the command reverts to the default value.

**Default**

```
  no  te-metric
```

**Parameters**

```
  value  —  1 to 16777215
```
### 3.20.2.1.4 Interface Label-Map Commands

#### label-map

**Syntax**  
`[no] label-map in-label`

**Context**  
`config>router>mpls>interface`

**Description**  
This command is used on either transit or egress LSP routers when a static LSP is defined. The static LSP on the ingress router is initiated using the `config>router>mpls>static-lsp lsp-name` command. The `in-label` is associated with a `pop` action or a `swap` action, but not both. If both actions are specified, the last action specified takes effect.

The `no` form of this command deletes the static LSP configuration associated with the `in-label`.

**Parameters**  
`in-label` — specifies the incoming MPLS label on which to match

**Values**  
32 to 1023

#### pop

**Syntax**  
`[no] pop`

**Context**  
`config>router>mpls>if>label-map`

**Description**  
This command specifies that the incoming label must be popped (removed). No label stacking is supported for a static LSP. The service header follows the top label. Once the label is popped, the packet is forwarded based on the service header.

The `no` form of this command removes the `pop` action for the `in-label`.

**Default**  
n/a

#### swap

**Syntax**  
`swap out-label nexthop ip-address`

`no swap`

**Context**  
`config>router>mpls>if>label-map`

**Description**  
This command swaps the incoming label and specifies the outgoing label and next-hop IP address on an LSR for a static LSP.

The `no` form of this command removes the swap action associated with the `in-label`.

**Default**  
n/a
Parameters  

out-label — specifies the label value to be swapped with the in-label. Label values 16 through 1048575 are defined as follows:
- Label values 16 through 31 are 7705 SAR reserved
- Label values 32 through 1023 are available for static assignment
- Label values 1024 through 2047 are reserved for future use
- Label values 2048 through 18431 are statically assigned for services
- Label values 28672 through 131071 are dynamically assigned for both MPLS and services
- Label values 131072 through 1048575 are reserved for future use

Values  

16 to 1048575

ip-address — specifies the IP address to forward to. If an ARP entry for the next hop exists, then the static LSP will be marked operational. If an ARP entry does not exist, software will set the operational status of the static LSP to down and continue to ARP for the configured next-hop at a fixed interval.
### 3.20.2.1.5 LSP and LSP Template Commands

#### lsp

**Syntax**

```plaintext
[no] lsp lsp-name [bypass-only]
```

**Context**

```
config>router>mpls
```

**Description**

This command creates an LSP that is signaled dynamically by the 7705 SAR.

When the LSP is created, the egress router must be specified using the `to` command and at least one primary or secondary path must be specified. All other statements under the LSP hierarchy are optional.

LSPs are created in the administratively down (shutdown) state.

The `no` form of this command deletes the LSP. All configuration information associated with this LSP is lost. The LSP must be administratively shut down and unbound from all SDPs before it can be deleted.

**Default**

n/a

**Parameters**

- `lsp-name` — specifies the name that identifies the LSP. The LSP name can be up to 32 characters long and must be unique.

- `bypass-only` — defines an LSP as a manual bypass LSP exclusively. When a PATH message for a new LSP requests bypass protection, the PLR first checks if a manual bypass tunnel satisfying the path constraints exists. If one is found, the 7705 SAR selects it. If no manual bypass tunnel is found, the 7705 SAR dynamically signals a bypass LSP as the default behavior. The CLI for this feature includes a command that provides the user with the option to disable dynamic bypass creation on a per-node basis.

#### lsp-template

**Syntax**

```plaintext
lsp-template template-name
lsp-template template-name mesh-p2p
lsp-template template-name one-hop-p2p
no lsp-template template-name
```

**Context**

```
config>router>mpls
```

**Description**

This command creates an LSP template that is referenced when dynamic LSP creation is required. The LSP template type, `mesh-p2p` or `one-hop-p2p`, must be specified when the template is first created.

The `no` form of this command deletes the LSP template. The LSP template cannot be deleted if a client application is using it.
**Parameters**

- `template-name` — specifies an LSP template name up to 32 characters in length. The LSP template name and the LSP name cannot be the same.

- `mesh-p2p | one-hop-p2p` — This command specifies the type of LSP the template signals

**adaptive**

**Syntax**

```plaintext
[no] adaptive
```

**Context**

```plaintext
config>router>mpls>lsp
config>router>mpls>lsp-template
```

**Description**

This command enables the make-before-break (MBB) functionality for an LSP, LSP path, or LSP instance created using an LSP template. When enabled for the LSP, a make-before-break operation will be performed for the primary path and all the secondary paths of the LSP.

**Default**

adaptive

**adspec**

**Syntax**

```plaintext
[no] adspec
```

**Context**

```plaintext
config>router>mpls>lsp
config>router>mpls>lsp-template
```

**Description**

When enabled, the advertised data (ADSPEC) object will be included in RSVP-TE messages.

**Default**

no adspec

**bgp-transport-tunnel**

**Syntax**

```plaintext
bgp-transport-tunnel {include | exclude}
```

**Context**

```plaintext
config>router>mpls>lsp
config>router>mpls>lsp-template
```

**Description**

This command allows an RSVP-TE LSP to be used as a transport LSP for BGP tunnel routes or blocks it from being used.

**Default**

include

**Parameters**

- `include` — allows an RSVP-TE LSP to be used as a transport LSP from the ASBR to a local PE router, from an ingress PE to the ASBR in the local AS or between multihop EBGP peers with ASBR-to-ASBR adjacency
**exclude** — blocks an RSVP-TE LSP from being used as a transport LSP from the ASBR to a local PE router, from an ingress PE to the ASBR in the local AS or between multihop EBGP peers with ASBR-to-ASBR adjacency.

---

**cspf**

**Syntax**

```plaintext
[no] cspf [use-te-metric]
```

**Context**

```
config>router>mpls>lsp
cfg>router>mpls>lsp-template
```

**Description**

This command enables Constrained Shortest Path First (CSPF) computation for constrained-path LSPs. Constrained-path LSPs are the LSPs that take configuration constraints into account. CSPF is also used to calculate the FRR bypass or detour LSP routes when fast reroute is enabled.

Explicitly configured LSPs where each hop from ingress to egress is specified do not use CSPF. The LSP is set up using RSVP-TE signaling from ingress to egress.

If an LSP is configured with **fast-reroute** specified but does not enable CSPF, then neither global revertive nor local revertive will be available for the LSP to recover.

When an LSP template is created, CSPF is automatically enabled and cannot be disabled.

**Default**

```plaintext
no cspf
```

**Parameters**

- **use-te-metric** — specifies to use the TE metric for the purpose of the LSP path computation by CSPF

---

**default-path**

**Syntax**

```plaintext
default-path path-name
```

**Context**

```
config>router>mpls>lsp-template
```

**Description**

This command specifies the default path to be used for signaling an LSP created using the LSP template. You must reference a default path before the template is put in a **no shutdown** state.

**Parameters**

- **path-name** — specifies the default path name to be used

---

**exclude**

**Syntax**

```plaintext
[no] exclude group-name [group-name...(up to 5 max)]
```

**Context**

```
config>router>mpls>lsp
cfg>router>mpls>lsp-template
```
**Description**

This command specifies the admin groups to be excluded when an LSP is set up in the primary or secondary contexts. Each single operation of the exclude command allows a maximum of 5 groups to be specified at a time. However, a maximum of 32 groups can be specified per LSP through multiple operations. The admin groups are defined in the config>router>mpls>admin-group context.

Use the no form of the command to remove the exclude command.

**Default**

no exclude

**Parameters**

*group-name* — specifies the existing group name to be excluded when an LSP is set up

---

**fast-reroute**

**Syntax**

[no] fast-reroute [frr-method]

**Context**

config>router>mpls>lsp
config>router>mpls>lsp-template

**Description**

This command creates a precomputed protection LSP from each node in the path of the LSP. If a link or LSP failure occurs between two nodes, traffic is immediately rerouted on the precomputed protection LSP. When fast-reroute is specified, the default fast-reroute method is the facility method.

When fast-reroute is enabled, each node along the path of the LSP tries to establish a protection LSP as follows.

- Each upstream node sets up a protection LSP that avoids only the immediate downstream node, and merges back onto the actual path of the LSP as soon as possible.
- If it is not possible to set up a protection LSP that avoids the immediate downstream node, a protection LSP can be set up to the downstream node on a different interface.
- The protection LSP may take one or more hops (see igp-shortcut) before merging back onto the main LSP path.
- When the upstream node detects a downstream link or node failure, the ingress router switches traffic to a standby path if one was set up for the LSP.

FRR is available only for the primary path. No configuration is required on the transit hops of the LSP. The ingress router will signal all intermediate routers using RSVP-TE to set up their protection LSP. TE must be enabled for fast reroute to work.

CSPF must be enabled for fast reroute to work. If an LSP is configured with fast-reroute frr-method specified but does not enable CSPF, then neither global revertive nor local revertive will be available for the LSP to recover.

The one-to-one fast reroute method creates a separate detour LSP for each backed-up LSP. One-to-one is not supported for LSP templates.
The facility fast reroute method, sometimes called many-to-one, takes advantage of the MPLS label stack. Instead of creating a separate LSP for every backed-up LSP, a single LSP is created that serves to back up a set of LSPs. This LSP tunnel is called a bypass tunnel. The bypass tunnel must intersect the path of the original LSPs somewhere downstream of the point of local repair (PLR). This constrains the set of LSPs being backed up via that bypass tunnel to those LSPs that pass through a common downstream node. All LSPs that pass through the PLR and through this common node which do not also use the facilities involved in the bypass tunnel are candidates for this set of LSPs.

The no form of the fast-reroute command removes the protection LSP from each node on the primary path. This command will also remove configuration information about the hop-limit and the bandwidth for the detour routes.

**Parameters**

frr-method — specifies the fast reroute method to use

**Values**

- one-to-one, facility
- Default: facility

**hop-limit**

**Syntax**

```
hop-limit limit
no hop-limit
```

**Context**

```
config>router>mpls>lsp>fast-reroute
config>router>mpls>lsp-template>fast-reroute
```

**Description**

For fast reroute, this command defines how many more routers a protection tunnel is allowed to traverse compared with the LSP itself. For example, if an LSP traverses four routers, any protection tunnel for the LSP can be no more than 10 router hops, including the ingress and egress routers.

The no form of the command reverts to the default value.

**Default**

16

**Parameters**

- limit — specifies the maximum number of hops
  - **Values**
    - 0 to 255

**node-protect**

**Syntax**

```
[no] node-protect
```

**Context**

```
config>router>mpls>lsp>fast-reroute
config>router>mpls>lsp-template>fast-reroute
```
**Description**

This command enables or disables node and link protection on the specified LSP. Node protection ensures that traffic from an LSP traversing a neighboring router will reach its destination even if the neighboring router fails.

When `node-protect` is enabled, the 7705 SAR provides node protection on the specified LSP. If node protection cannot be provided, link protection is attempted. If link protection cannot be provided, there will be no protection.

The **no** form of this command provides link protection. If link protection cannot be provided, there will be no protection.

**Default**

`node-protect`

---

**propagate-admin-group**

**Syntax**

```
[no] propagate-admin-group
```

**Context**

```
config>router>mpls>lsp>fast-reroute
config>router>mpls>lsp-template>fast-reroute
```

**Description**

The command enables the signaling of the primary LSP path admin-group constraints in the FAST_REROUTE object at the ingress LER.

When this command is executed, the admin-group constraints configured in the context of the point-to-point LSP primary path, or the constraints configured in the context of the LSP and inherited by the primary path, are copied into the FAST_REROUTE object. The admin-group constraints are copied into the “include-any” or “exclude-any” fields.

The ingress LER propagates these constraints to the downstream nodes during the signaling of the LSP so that the downstream nodes can include the constraints in the selection of the FRR backup LSP for the LSP primary path.

The ingress LER inserts the FAST_REROUTE object by default in a primary LSP path message.

The same admin-group constraints can be copied into the SESSION_ATTRIBUTE object using the `propagate-admin-group` command at the `config>router>mpls>lsp` level. They are intended for the use of an LSR, typically an ABR, to expand the ERO of an inter-area LSP path. They are also used by any LSR node in the path of a CSPF or non-CSPF LSP to check the admin-group constraints against the ERO whether the hop is strict or loose.

The primary path admin-group constraints can be copied into the FAST_REROUTE object only, the SESSION_ATTRIBUTE object only, or both. The PLR rules for processing the admin-group constraints can make use of either of the two objects.

If the FAST_REROUTE object is disabled (no `frr-object`), the admin-group constraints will not be propagated.

**Default**

`no propagate-admin-group`
from

**Syntax**  
from *ip-address*

**Context**  
config>router>mpls>lsp  
config>router>mpls>lsp-template

**Description**  
This command specifies the IP address of the ingress router for the LSP. When this command is not specified, the system IP address is used. IP addresses that are not defined in the system are allowed.

If an invalid IP address is entered, LSP bring-up fails and an error is logged. This command is only allowed for an LSP template of type **mesh-p2p**.

If an interface IP address is specified as the *from* address, and the egress interface of the next-hop IP address is a different interface, the LSP is not signaled. As the egress interface changes due to changes in the routing topology, an LSP recovers if the *from* IP address is the system IP address and not a specific interface IP address.

Only one *from* address can be configured.

**Default**  
system IP address

**Parameters**  
- *ip-address* — specifies the IP address of the ingress router. This can be either the interface or the system IP address. If the IP address is local, the LSP must egress through that local interface, which ensures local strictness.

  **Values**  
  - system IP or network interface IP addresses

  **Default**  
  - system IP address

hop-limit

**Syntax**  
hop-limit *number*  
no hop-limit

**Context**  
config>router>mpls>lsp  
config>router>mpls>lsp-template

**Description**  
This command specifies the maximum number of hops that an LSP can traverse, including the ingress and egress routers. An LSP is not set up if the hop limit is exceeded. This value can be changed dynamically for an LSP that is already set up, with the following implications:

- If the new value is less than the current number of hops of the established LSP, the LSP is brought down. The 7705 SAR then tries to re-establish the LSP within the new **hop-limit** number. If the new value is equal to or greater than the current number of hops of the established LSP, the LSP is not affected.

The **no** form of this command returns the parameter to the default value.
### Default

- **255 (LSP and LSP mesh template)**
- **2 (one-hop template)**

### Parameters

- **number** — specifies the number of hops the LSP can traverse, expressed as an integer

  **Values**
  - 2 to 255

---

#### igp-shortcut

**Syntax**

```
igp-shortcut [lfa-protect | lfa-only] [relative-metric [offset]]
```

**no igp-shortcut**

**Context**

```
config>router>mpls>lsp
config>router>mpls>lsp-template
```

**Description**

This command enables the use of an RSVP-TE LSP by OSPF or IS-IS routing protocols as a shortcut or as a forwarding adjacency for resolving IGP routes.

When the `rsvp-shortcut` or the `advertise-tunnel-link` command is enabled at the OSPF or IS-IS instance level, all RSVP-TE LSPs originating on this node are eligible by default as long as the destination address of the LSP, as configured with the `config>router>mpls>lsp>to` command, corresponds to a router ID of a remote node.

If the command is used with no options, and the `rsvp-shortcut` command is enabled, the LSP is included in the main SPF but not in the LFA SPF algorithm. If the `advertise-tunnel-link` command is enabled, the tunnel is advertised as a point-to-point link if it has the best LSP metric, is included in the main SPF if advertised, but is not included in the LFA SPF algorithm.

If the command is used with the `lfa-protect` option, and the `rsvp-shortcut` command is enabled, an LSP can be included in both the main SPF and the LFA SPF algorithm. If the `advertise-tunnel-link` command is enabled, the tunnel is advertised as a point-to-point link if it has the best LSP metric, is included in the main SPF if advertised, and is included in the LFA SPF algorithm whether it is advertised or not.

For a given prefix, the LSP can be used either as a primary next hop or as an LFA next hop, but not both. If the main SPF calculation selects a tunneled primary next hop for a prefix, the LFA SPF calculation will not select an LFA next hop for this prefix and the protection of this prefix will rely on the RSVP-TE LSP FRR protection. If the main SPF calculation selects a direct primary next hop, the LFA SPF calculation will select an LFA next hop for this prefix but will prefer a direct LFA next hop over a tunneled LFA next hop.

If the command is used with the `lfa-only` option, and the `rsvp-shortcut` command is enabled, an LSP can be included in the LFA SPF algorithm only. If the `advertise-tunnel-link` command is enabled, the tunnel is not advertised as a point-to-point link, is not included in the main SPF, and is only included in the LFA SPF algorithm.
When the **lfa-only** option is enabled, the introduction of IGP shortcuts does not affect the main SPF decision. For a given prefix, the main SPF calculation always selects a direct primary next hop. The LFA SPF calculation will select an LFA next hop for this prefix but will prefer a direct LFA next hop over a tunneled LFA next hop.

When the **relative-metric** option is enabled, IGP will apply the shortest IGP cost between the endpoints of the LSP plus the value of the offset (instead of the LSP operational metric) when calculating the cost of a prefix that is resolved to the LSP. The offset value is optional and defaults to zero. The minimum net cost for a prefix is one (1) after applying the offset. The Tunnel Table Manager (TTM) continues to show the LSP operational metric as provided by MPLS; therefore, applications such as BGP and static route shortcuts will continue to use the LSP operational metric.

The **relative-metric** option and the **lfa-protect** or the **lfa-only** options are mutually exclusive. An LSP with the **relative-metric** option enabled cannot be included in the LFA SPF calculation and the **relative-metric** option cannot be enabled if the LSP is included in the LFA SPF calculation when the **rsvp-shortcut** option is enabled in the IGP.

The **relative-metric** option is ignored when forwarding adjacency is enabled in OSPF or IS-IS. In this case, IGP advertises the LSP as a point-to-point unnumbered link along with the LSP operational metric as returned by MPLS and capped to the maximum link metric allowed in that IGP.

Both the main SPF and the LFA SPF algorithms use the local IGP database to resolve the routes.

The **no** form of this command disables the use of an RSVP-TE LSP by OSPF or IS-IS as a shortcut or a forwarding adjacency for resolving IGP routes.

For more information on IGP shortcuts and LFA, refer to the 7705 SAR Routing Protocols Guide, “LDP and IP Fast Reroute (FRR) for OSPF Prefixes” and “LDP and IP Fast Reroute (FRR) for IS-IS Prefixes”.

**Default**

- igp-shortcut — all RSVP-TE LSPs originating on this node are eligible by default as long as the destination address of the LSP corresponds to a router ID of a remote node

**Parameters**

- **lfa-protect** — an LSP is included in both the main SPF and the LFA SPF calculation
- **lfa-only** — an LSP is included in the LFA SPF calculation only
- **relative-metric** [**offset**] — the shortest IGP cost between the endpoints of the LSP plus the configured offset, instead of the LSP operational metric returned by MPLS, is used when calculating the cost of prefix resolved to this LSP. The **offset** parameter is optional. If the **relative-metric** option is enabled without specifying the **offset** parameter value, a value of 0 is used.

**Values**

-10 to +10
include

Syntax
[no] include group-name [group-name...(up to 5 max)]

Context
config>router>mpls>lsp
config>router>mpls>lsp>primary
config>router>mpls>lsp>secondary
config>router>mpls>lsp-template

Description
This command specifies the admin groups to be included when an LSP is set up. Up to 5
groups per operation can be specified, and up to 32 maximum.

The no form of the command deletes the specified groups in the specified context.

Default
no include

Parameters
group-name — specifies admin groups to be included when an LSP is set up

least-fill

Syntax
[no] least-fill

Context
config>router>mpls>lsp
config>router>mpls>lsp-template

Description
This command enables the use of the least-fill path selection method for the computation of
the path of this LSP.

When MPLS requests the computation of a path for this LSP, CSPF finds all equal-cost
shortest paths that satisfy the constraints of this path. Then, CSPF identifies the single link in
each of these paths that has the least available bandwidth as a percentage of its maximum
reservable bandwidth. It then selects the path that has the highest percentage available
bandwidth. CSPF identifies the least-available bandwidth link in each equal-cost path after it
has accounted for the bandwidth of the new requested path of this LSP.

CSPF applies the least-fill path selection method to all requests for a path, primary and
secondary, of an LSP for which this option is enabled. The bandwidth of the path can be any
value, including zero.

MPLS resignals and move the LSP to the new path in the following cases:

• initial LSP path signaling
• retry of an LSP path after failure
• MBB due to an LSP path configuration change, that is, a user change to the bandwidth
  parameter of the primary or secondary path, or a user enabling of the fast-reroute option
  for the LSP
• MBB of the path due to an update to the primary path SRLG
• MBB due to fast reroute global revertive procedures on the primary path
• manual resignaling of an LSP path or of all LSP paths by the user

During a manual resignaling of an LSP path, MPLS always resignals the path even if the new path is the same as the current path and even if the metric of the new path is the same as the metric of the current path.

During a timer-based resignaling of an LSP path that has the least-fill option enabled, MPLS only resignals the path if the metric of the new path is different from the metric of the current path.

Default
no least-fill - the path of an LSP is randomly chosen among a set of equal-cost paths

metric

Syntax metric metric

Context config>router>mpls>lsp
config>router>mpls>lsp-template

Description This command specifies the metric for this LSP, which is used to select an LSP from among a set of LSPs that are destined for the same egress router. The LSP with the lowest metric will be selected.

The operational metric for an LSP that uses the TE metric in CSPF path calculations can be overridden by the configured administrative LSP metric parameter.

Default 1

Parameters metric — specifies the metric for this LSP

Values 1 to 16777215

path-profile

Syntax path-profile profile-id [path-group group-id]
no path-profile profile-id

Context config>router>mpls>lsp

Description This command configures the PCE path profile and path group ID.

The PCE supports the computation of disjoint paths for two different LSPs originating or terminating on the same or different PE routers. In order to indicate this constraint to the PCE, the user must configure the PCE path profile ID and path group ID that the PCE-computed or PCE-controlled LSP belongs to. These parameters are passed transparently by the PCC to the PCE and are thus opaque data to the router.
The association of the optional path group ID is to allow the PCE to determine which profile ID this path group ID must be used with. One path group ID is allowed per profile ID. The user can, however, enter the same path group ID with multiple profile IDs by executing this command multiple times. A maximum of five entries of `path-profile [path-group]` can be associated with the same LSP.

**Parameters**

- `profile-id` — specifies the profile ID
  - **Values**
  - 1 to 4294967295
- `group-id` — specifies the path group ID
  - **Values**
  - 0 to 4294967295

### pce-computation

**Syntax**

```
[no] pce-computation
```

**Context**

```
config>router>mpls>lsp
```

**Description**

This command enables a PCE-computed LSP mode of operation for an RSVP-TE LSP.

The user can grant only path computation requests (PCE-computed) or both path computation requests and path update (PCE-controlled) to a PCE for a specific LSP.

The `pce-computation` option allows the path computation request to be sent to the PCE instead of the local CSPF. Enabling this option allows the PCE to perform path computations for the LSP at the request of the PCC router only. This is used in cases where the operator wants to make use of the PCE-specific path computation algorithm instead of the local router CSPF algorithm.

The default configuration is `no pce-computation`. The enabling of the `pce-computation` option or `pce-control` option requires that the `cspf` option first be enabled; otherwise, this configuration will be rejected. Conversely, an attempt to disable the `cspf` option on an RSVP-TE LSP that has the `pce-computation` option or `pce-control` option enabled will be rejected.

**Default**

`no pce-computation`

### pce-control

**Syntax**

```
[no] pce-control
```

**Context**

```
config>router>mpls>lsp
```

**Description**

This command enables a PCE-controlled LSP mode of operation for an RSVP-TE LSP.

The `pce-control` option means that the PCC router delegates full control of the LSP to the PCE (PCE-controlled). Enabling PCE control means that the PCE is acting in active stateful mode for this LSP; the PCE will be able to reroute the path following a failure or reoptimize the path and update the router without the PCC router requesting the update.
The user can delegate CSPF and non-CSPF LSPs, or LSPs that have the **pce-computation** option enabled or disabled. The LSP maintains its latest active path computed by the PCE or the PCC router at the time it is delegated. The PCE will only make an update to the path at the next network event or reoptimization.

The default configuration is **no pce-control**. The enabling of the **pce-control** option or **pce-computation** option requires that the **cspf** option first be enabled; otherwise, this configuration will be rejected. Conversely, an attempt to disable the **cspf** option on an RSVP-TE LSP that has the **pce-control** option or **pce-computation** option enabled will be rejected.

If PCE reporting is disabled for the LSP, either due to inheritance from the MPLS-level configuration or due to LSP-level configuration, enabling the **pce-control** option for the LSP has no effect.

**Default**  
**no pce-control**

### pce-report

**Syntax**  
pce-report {enable | disable | inherit}

**Context**  
config>router>mpls>lsp  
config>router>mpls>lsp-template

**Description**  
This command configures the reporting mode to a PCE for an RSVP-TE LSP.

The PCC LSP database is synchronized with the PCE LSP database using the PCEP PCRpt (PCE Report) message for PCC-controlled, PCE-computed, and PCE-controlled LSPs.

The global MPLS-level **pce-report** command can be used to enable or disable PCE reporting for all RSVP-TE LSPs during PCE LSP database synchronization (see **config>router>mpls>pce-report**).

The LSP-level **pce-report** command overrides the global configuration for the reporting of an LSP to the PCE. The default configuration is to inherit the global MPLS-level configuration. The **inherit** option reconfigures the LSP to inherit the global configuration.

**Default**  
pce-report inherit

**Parameters**  
enable — enables PCE reporting  
disable — disables PCE reporting  
inherit — inherits the global configuration for PCE reporting

### propagate-admin-group

**Syntax**  
[no] propagate-admin-group

**Context**  
config>router>mpls>lsp
config>router>mpls>lsp-template

Description
This command enables propagation of the SESSION_ATTRIBUTE object with resource affinity (C-type 1) in the PATH message. If a SESSION_ATTRIBUTE object with resource affinity is received at an LSR, the LSR will check the compatibility of admin groups received in the PATH message against configured admin groups on the egress interface of the LSP.

To support admin groups for inter-area LSPs, the ingress node must configure the propagation of admin groups within the SESSION_ATTRIBUTE object. If a PATH message is received by an LSR node that has the cspf-on-loose-hop option enabled and the message includes admin groups, then the ERO expansion by CSPF to calculate the path to the next loose hop will include the admin-group constraints received from the ingress node.

If this command is disabled, the SESSION_ATTRIBUTE object without resource affinity (C-Type 7) is propagated in the PATH message and CSPF at the LSR node will not include admin-group constraints.

If the configuration of this command is changed (enabled or disabled), the LSP will perform a make-before-break (MBB).

Default
no propagate-admin-group

retry-limit

Syntax
retry-limit number
no retry-limit

Context
config>router>mpls>lsp
config>router>mpls>lsp-template

Description
This optional command specifies the number of attempts software should make to re-establish the LSP after it has failed. After each successful attempt, the counter is reset to zero.

When the specified number is reached, no more attempts are made and the LSP path is put into the shutdown state.

Use the config>router>mpls>lsp lsp-name=no shutdown command to bring up the path after the retry limit is exceeded.

The no form of this command resets the parameter to the default value.

Default
0

Parameters
number — specifies the number of times that the 7705 SAR software will attempt to re-establish the LSP after it has failed. Allowed values are integers in the range of 0 to 10000, where 0 indicates to retry forever.

Values
0 to 10000
retry-timer

Syntax  retry-timer seconds
        no retry-timer

Context  config>router>mpls>lsp
         config>router>mpls>lsp-template

Description  This command configures the time, in seconds, between LSP re-establishment attempts after
             the LSP has failed.

             The no form of this command reverts to the default value.

Default  30

Parameters  seconds — specifies the amount of time, in seconds, between attempts to re-establish
           the LSP after it has failed

Values  1 to 600

rsvp-resv-style

Syntax  rsvp-resv-style [se | ff]

Context  config>router>mpls>lsp

Description  This command specifies the RSVP-TE reservation style, shared explicit (se) or fixed filter (ff).
             A reservation style is a set of control options that specify a number of supported parameters.
             The style information is part of the LSP configuration.

Default  se

Parameters  ff  — fixed filter is single reservation with an explicit scope. This reservation style
            specifies an explicit list of senders and a distinct reservation for each of them. A
            specific reservation request is created for data packets from a particular sender. The
            reservation scope is determined by an explicit list of senders.

            se  — shared explicit is shared reservation with a limited scope. This reservation style
            specifies a shared reservation environment with an explicit reservation scope. This
            reservation style creates a single reservation over a link that is shared by an explicit
            list of senders. Because each sender is explicitly listed in the RESV message,
            different labels can be assigned to different sender-receiver pairs, thereby creating
            separate LSPs.
shutdown

Syntax  [no] shutdown

Context  config>router>mpls>lsp
         config>router>mpls>lsp>primary
         config>router>mpls>lsp>secondary
         config>router>mpls>lsp-template

Description  This lsp form of this command disables the existing LSP, including the primary and any standby secondary paths.

The primary and secondary forms of this command administratively disable an LSP path and disable an existing LSP. Shutting down an LSP path does not change other configuration parameters for the LSP path.

To shut down only the primary path, enter the config>router>mpls>lsp lsp-name>primary path-name> shutdown command.

To shut down a specific standby secondary path, enter the config>router>mpls>lsp lsp-name>secondary path-name> shutdown command. The existing configuration of the LSP is preserved.

The lsp-template form of this command disables the existing LSP template.

Use the no form of this command to restart the LSP or LSP template. LSPs and LSP templates are created in a shutdown state. Use this command to administratively bring up the LSP or LSP template.

Default  lsp — shutdown
         primary — no shutdown
         secondary — no shutdown
         lsp-template — shutdown

to

Syntax  to ip-address

Context  config>router>mpls>lsp

Description  This command specifies the IP address of the egress router for the LSP. This command is mandatory to create an LSP.

An IP address for which a route does not exist is allowed in the configuration. If the LSP signaling fails because the destination is not reachable, an error is logged and the LSP operational status is set to down.
If the to address does not match the SDP address, the LSP is not included in the SDP definition.

**Default**

n/a

**Parameters**

*ip-address* — specifies the IP address of the egress router

## vprn-auto-bind

**Syntax**

vprn-auto-bind [include | exclude]

**Context**

config>router>mpls>lsp
cfgconfig>router>mpls>lsp-template

**Description**

This command determines whether the associated LSP can be used as part of the auto-bind feature for VPRN services. By default, an LSP is allowed to be used by the auto-bind feature. When VPRN auto-bind is set to *exclude*, the associated LSP is not used by the auto-bind feature for VPRN services.

**Default**

include

**Parameters**

*include* — allows an associated LSP to be used by auto-bind for VPRN services

*exclude* — prevents the associated LSP from being used with the auto-bind feature for VPRN services
3.20.2.1.6 Primary and Secondary Path Commands

**primary**

**Syntax**

[no] primary path-name

**Context**

config>router>mpls>lsp

**Description**

This command specifies a preferred path for the LSP. This command is optional only if the secondary path-name is included in the LSP definition. Only one primary path can be defined for an LSP.

Some of the attributes of the LSP, such as the bandwidth and hop limit, can be optionally specified as the attributes of the primary path. The attributes specified in the primary path-name command override the comparable LSP attributes that are defined in the config>router>mpls>lsp context.

The no form of this command deletes the association of this path-name from the lsp lsp-name. All configurations specific to this primary path, such as record, bandwidth, and hop limit, are deleted. The primary path must be shut down first in order to delete it. The no primary command will not result in any action except a warning message on the console indicating that the primary path is administratively up.

**Default**

n/a

**Parameters**

path-name — specifies the case-sensitive alphanumeric name label for the LSP path, up to 32 characters in length

**secondary**

**Syntax**

[no] secondary path-name

**Context**

config>router>mpls>lsp

**Description**

This command specifies an alternative path that the LSP uses if the primary path is not available. This command is optional and is not required if the config>router>mpls>lsp lsp-name> primary path-name command is specified. After the switchover from the primary path to the secondary path, the 7705 SAR software continuously tries to revert to the primary path. The switch back to the primary path is based on the retry-timer interval.

Up to two secondary paths can be specified. Both secondary paths are considered equal, and the first available path is used. The 7705 SAR software will not switch back between secondary paths.

The 7705 SAR software starts signaling all non-standby secondary paths at the same time. Retry counters are maintained for each unsuccessful attempt. Once the retry limit is reached on a path, software will not attempt to signal the path and administratively shuts down the path. The first successfully established path is made the active path for the LSP.
The **no** form of this command removes the association between this *path-name* and *lsp-name*. All specific configurations for this association are deleted. The secondary path must be shut down first in order to delete it. The **no secondary path-name** command will not result in any action except a warning message on the console indicating that the secondary path is administratively up.

**Default**
- n/a

**Parameters**
- *path-name* — specifies the case-sensitive alphanumeric name label for the LSP path, up to 32 characters in length

### adaptive

**Syntax**
- [no] adaptive

**Context**
- config>router>mpls>lsp>primary
- config>router>mpls>lsp>secondary

**Description**
This command enables the make-before-break (MBB) functionality for an LSP or a primary or secondary LSP path. When enabled for the LSP, a make-before-break operation will be performed for the primary path and all the secondary paths of the LSP.

**Default**
- adaptive

### bandwidth

**Syntax**
- bandwidth *rate-in-mbps*
  - **no bandwidth**

**Context**
- config>router>mpls>lsp>primary
- config>router>mpls>lsp>secondary

**Description**
This command specifies the amount of bandwidth to be reserved for the LSP path. The **no** form of this command resets bandwidth parameters (no bandwidth is reserved).

**Default**
- no bandwidth — bandwidth setting in the global LSP configuration

**Parameters**
- *rate-in-mbps* — specifies the amount of bandwidth reserved for the LSP path in Mb/s

**Values**
- 0 to 100000
exclude

Syntax   [no] exclude group-name [group-name...(up to 5 max)]

Context   config>router>mpls>lsp>primary
            config>router>mpls>lsp>secondary

Description   This command specifies the admin groups to be excluded when an LSP is set up. Up to 5
groups per operation can be specified, up to 32 maximum. The admin groups are defined in the
config>router>mpls>admin-group context.

Use the no form of the command to remove the exclude command.

Default   no exclude

Parameters   group-name — specifies the existing group name to be excluded when an LSP is set up

hop-limit

Syntax   hop-limit number
            no hop-limit

Context   config>router>mpls>lsp>primary
            config>router>mpls>lsp>secondary

Description   This optional command overrides the config>router>mpls>lsp lsp-name>hop-limit
command. This command specifies the total number of hops that an LSP traverses, including
the ingress and egress routers.

This value can be changed dynamically for an LSP that is already set up with the following
implications:

• If the new value is less than the current number of hops of the established LSP, then the
LSP is brought down. MPLS then tries to re-establish the LSP within the new hop-limit
number. If the new value is equal to or greater than the current hops of the established
LSP, then the LSP will be unaffected.

The no form of this command resets the hop limit to the value defined under the LSP
definition using the config>router>mpls>lsp lsp-name>hop-limit command.

Default   no hop-limit

Parameters   number — specifies the number of hops the LSP can traverse, expressed as an integer

    Values   2 to 255
record

**Syntax**

```
[no] record
```

**Context**

```
config>router>mpls>lsp>primary
config>router>mpls>lsp>secondary
```

**Description**

This command enables recording of all the hops that an LSP path traverses. Enabling `record` increases the size of the PATH and RESV refresh messages for the LSP, since this information is carried end-to-end along the path of the LSP. The increase in control traffic per LSP may impact scalability.

The `no` form of this command disables the recording of all the hops for the given LSP. There are no restrictions as to when the `no` command can be used. The `no` form of this command also disables the `record-label` command.

**Default**

`record`

record-label

**Syntax**

```
[no] record-label
```

**Context**

```
config>router>mpls>lsp>primary
config>router>mpls>lsp>secondary
```

**Description**

This command enables recording of all the labels at each node that an LSP path traverses. Enabling the `record-label` command will also enable the `record` command, if it is not already enabled.

The `no` form of this command disables the recording of the hops that an LSP path traverses.

**Default**

`record-label`

srlg

**Syntax**

```
[no] srlg
```

**Context**

```
config>router>mpls>lsp>secondary
```

**Description**

This command enables the use of the SRLG constraint in the CSPF computation of a secondary path for an LSP at the head-end LER. When this feature is enabled, CSPF includes the SRLG constraint in the computation of the secondary LSP path.
CSPF and SRLGs for Secondary Paths

CSPF requires that the primary LSP be established already and in the up state, since the head-end LER needs the most current ERO computed by CSPF for the primary path and CSPF includes the list of SRLGs in the ERO during the CSPF computation of the primary path. At a subsequent establishment of a secondary path with the SRLG constraint, the MPLS/RSVP-TE task queries CSPF again, which provides the list of SRLG numbers to be avoided. CSPF prunes all links with interfaces that belong to the same SRLGs as the interfaces included in the ERO of the primary path. If CSPF finds a path, the secondary path is set up. If CSPF does not find a path, MPLS/RSVP-TE keeps retrying the requests to CSPF.

If CSPF is not enabled on the LSP (using the `lsp lsp-name>cspf` command), then a secondary path of that LSP that includes the SRLG constraint is shut down and a specific failure code indicates the exact reason for the failure in the `show>router>mpls>lsp<path>detail` output.

Primary Path and Secondary Path Behavior

At initial primary LSP path establishment, if the primary path does not come up or is not configured, the SRLG secondary path is not signaled and is put in the down state. A specific failure code indicates the exact reason for the failure in the `show>router>mpls>lsp<path>detail` output. However, if a non-SRLG secondary path was configured, such as a secondary path with the SRLG option disabled, MPLS/RSVP-TE task signals it and the LSP uses it.

As soon as the primary path is configured and successfully established, MPLS/RSVP-TE moves the LSP to the primary path and signals all SRLG secondary paths.

Any time the primary path is reoptimized, has undergone a make-before-break (MBB) operation, or has come back up after being down, the MPLS/RSVP-TE task checks with CSPF to determine if the SRLG secondary path should be signaled. If the MPLS/RSVP-TE task finds that the current secondary path is no longer SRLG disjoint — for example, the path became ineligible — it puts the path on a delayed make-before-break immediately after the expiry of the retry timer. If MBB fails on the first try, the secondary path is torn down and the path is put on retry.

At the next opportunity (that is, when the primary path goes down), the LSP uses of an eligible SRLG secondary path if the secondary path is in the up state. If all secondary eligible SRLG paths are in the down state, MPLS/RSVP-TE uses a non-SRLG secondary path if the path is configured and in the up state. If, while the LSP is using a non-SRLG secondary path, an eligible SRLG secondary path comes back up, MPLS/RSVP-TE will not switch the path of the LSP to it. As soon as the primary path is signaled and comes up with a new SRLG list, MPLS/RSVP-TE resignals the secondary path using the new SRLG list.

A secondary path that becomes ineligible as a result of an update to the SRLG membership list of the primary path will have its ineligibility status removed when any of the following events occurs:

- A successful MBB operation of the standby SRLG path occurs, making it eligible again.
• The standby path goes down, in which case MPLS/RSVP-TE puts the standby on retry when the retry timer expires. If successful, it becomes eligible. If not successful after the retry timer expires or the number of retries reaches the configured retry-limit value, it is left down.

• The primary path goes down, in which case the ineligible secondary path is immediately torn down and will only be resigaled when the primary path comes back up with a new SRLG list.

Changes to SRLG Membership List

Once the primary path of the LSP is set up and is operationally up, any subsequent changes to the SRLG membership of an interface that the primary path is using is not considered until the next opportunity that the primary path is resigaled. The primary path may be resigaled due to a failure or to a make-before-break operation. A make-before-break operation occurs as a result of a global revertive operation, a timer-based or manual reoptimization of the LSP path, or a change by the user to any of the path constraints.

Once an SRLG secondary path is set up and is operationally up, any subsequent changes to the SRLG membership of an interface that the secondary path is using is not considered until the next opportunity that the secondary path is resigaled. The secondary path is resigaled due to a failure, to a resigaling of the primary path, or to a make-before-break operation. A make-before-break operation occurs as a result of a timer-based or manual reoptimization of the secondary path, or a change by the user to any of the path constraints of the secondary path, including enabling or disabling the SRLG constraint itself.

In addition, any user-configured include or exclude admin group statements for this secondary path are checked along with the SRLG constraints by CSPF.

The no form of the command reverts to the default value.

Default

table

standby

Syntax [no] standby

Context config>router>mpls>lsp>secondary

Description

The secondary path LSP is normally sigaled if the primary path LSP fails. The standby keyword ensures that the secondary path LSP is sigaled and maintained indefinitely in a hot-standby state. When the primary path is re-established, the traffic is switched back to the primary path LSP.

The no form of this command specifies that the secondary LSP is sigaled when the primary path LSP fails.

Default n/a
### 3.20.2.1.7 LSP Path Commands

**path**

**Syntax**

```
[no] path path-name
```

**Context**

```
config>router>mpls
```

**Description**

This command creates the path to be used for an LSP. A path can be used by multiple LSPs. A path can specify some or all hops from ingress to egress and they can be either **strict** or **loose**. A path can also be empty (no `path-name` specified), in which case the LSP is set up based on the IGP (best effort) calculated shortest path to the egress router. Paths are created in a **shutdown** state. A path must be shut down before making any changes (adding or deleting hops) to the path. When a path is shut down, any LSP using the path becomes operationally down.

To create a strict path from the ingress to the egress router, the ingress and the egress routers must be included in the path statement.

The **no** form of this command deletes the path and all its associated configuration information. All the LSPs that are currently using this path will be affected. Additionally, all the services that are actively using these LSPs will be affected. A path must be shut down and unbound from all LSPs using the path before it can be deleted. The **no path path-name** command will not result in any action except a warning message on the console indicating that the path may be in use.

**Default**

n/a

**Parameters**

`path-name` — specifies the unique case-sensitive alphanumeric name label for the LSP path, up to 32 characters in length

**hop**

**Syntax**

```
no hop hop-index ip-address {strict | loose}
```

```
o hop hop-index
```

**Context**

```
config>router>mpls>path
```

**Description**

This command specifies the IP address of the hops that the LSP should traverse on its way to the egress router. The IP address can be the interface IP address, a loopback IP address, or the system IP address. If the system IP address is specified, the LSP can choose the best available interface.

Optionally, the LSP ingress and egress IP address can be included as the first and the last hop. A hop list can include the ingress interface IP address, the system IP address, and the egress IP address of any of the hops being specified.
The **no** form of this command deletes hop list entries for the path. All the LSPs currently using this path are affected. Additionally, all services actively using these LSPs are affected. The path must be shut down first in order to delete the hop from the hop list. The **no hop hop-index** command will not result in any action except a warning message on the console indicating that the path is administratively up.

**Default**

n/a

**Parameters**

*hop-index* — specifies the hop index, which is used to order the specified hops. The LSP always traverses from the lowest hop index to the highest. The hop index does not need to be sequential.

**Values**

1 to 1024

*ip-address* — specifies the system or network interface IP address of the transit router. The IP address can be the interface IP address or the system IP address. If the system IP address is specified, the LSP can choose the best available interface. A hop list can also include the ingress interface IP address, the system IP address, and the egress IP address of any of the specified hops.

*strict* — specifies that the LSP must take a direct path from the previous hop router to this router. No transit routers between the previous router and this router are allowed. If the IP address specified is the interface address, then that is the interface the LSP must use. If there are direct parallel links between the previous router and this router and if the system IP address is specified, then any one of the available interfaces can be used by the LSP. The user must ensure that the previous router and this router have a direct link. Multiple hop entries with the same IP address are flagged as errors. Either the **loose** or **strict** keyword must be specified.

*loose* — specifies that the route taken by the LSP from the previous hop to this hop can traverse other routers. Multiple hop entries with the same IP address are flagged as errors. Either the **loose** or **strict** keyword must be specified.
### 3.20.2.1.8 Static LSP Commands

#### static-lsp

**Syntax**

```
[no] static-lsp lsp-name
```

**Context**

```
config>router>mpls
```

**Description**

This command configures static LSPs on the ingress router. The static LSP is a manually configured LSP where the next-hop IP address and the outgoing label (push) must be specified.

The **no** form of this command deletes this static LSP and associated information.

The LSP must be shut down before it can be deleted. If the LSP is not shut down, the **no static-lsp lsp-name** command generates a warning message on the console indicating that the LSP is administratively up.

**Parameters**

- **lsp-name** — identifies the LSP. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

#### push

**Syntax**

```
push label nexthop ip-address
no push label
```

**Context**

```
config>router>mpls>static-lsp
```

**Description**

This command specifies the label to be pushed onto the label stack and the next-hop IP address for the static LSP.

The **no** form of this command removes the association of the label to push for the static LSP.

**Parameters**

- **label** — specifies the label to push on the label stack
  
  Label values 16 through 31 are 7705 SAR reserved
  Label values 32 through 1023 are available for static assignment
  Label values 1024 through 2047 are reserved for future use
  Label values 2048 through 18431 are statically assigned for services
  Label values 28672 through 131071 are dynamically assigned for both MPLS and services
  Label values 131072 through 1048575 are reserved for future use.

**Values**

16 to 1048575
**ip-address** — specifies the IP address of the next hop towards the LSP egress router. If an ARP entry for the next hop exists, then the static LSP is marked operational. If an ARP entry does not exist, the software sets the operational status of the static LSP to down and continues to send an ARP request for the configured next hop at fixed intervals.

### Syntax
```
static-lsp-fast-retry seconds
```

### Context
```
config＞router＞mpls
```

### Description
This command specifies the fast-retry timer that can be configured for static LSPs. When a static LSP is trying to come up, MPLS tries to resolve the ARP entry for the next hop of the LSP. If the next hop is still down or unavailable, the request may fail. In that case, MPLS starts a non-configurable timer of 30 seconds before making the next request. The fast-retry timer allows the user to configure a shorter retry timer so that the LSP comes up shortly after the next hop is available.

**Default**
30

**Parameters**
- **seconds** — fast-retry timer value, in seconds
  - **Values**: 1 to 30
3.20.2.2 Configuration Commands (RSVP-TE)

- Generic Commands
- RSVP-TE Global Commands
- Interface Commands
- Message Pacing Commands
### 3.20.2.2.1 Generic Commands

**shutdown**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>[no] shutdown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context</td>
<td>config&gt;router&gt;rsvp&lt;br&gt;config&gt;router&gt;rsvp&gt;interface</td>
</tr>
<tr>
<td>Description</td>
<td>This command disables the RSVP-TE protocol instance or the RSVP-related functions for the interface. The RSVP-TE configuration information associated with this interface is retained. When RSVP-TE is administratively disabled, all the RSVP-TE sessions are torn down. The <strong>no</strong> form of this command administratively enables RSVP-TE on the interface.</td>
</tr>
<tr>
<td>Default</td>
<td>shutdown</td>
</tr>
</tbody>
</table>
3.20.2.2.2 RSVP-TE Global Commands

rsvp

Syntax  [no] rsvp

Context  config>router

Description  This command creates the RSVP-TE protocol instance and enables RSVP-TE configuration. RSVP-TE is enabled by default. RSVP-TE is used to set up LSPs. RSVP-TE should be enabled on all router interfaces that participate in signaled LSPs.

The no form of this command deletes this RSVP-TE protocol instance and removes all configuration parameters for this RSVP-TE instance. To suspend the execution and maintain the existing configuration, use the shutdown command. RSVP-TE must be shut down before the RSVP-TE instance can be deleted. If RSVP-TE is not shut down, the no rsvp command does nothing except issue a warning message on the console indicating that RSVP-TE is still administratively enabled.

Default  no shutdown

entropy-label-capability

Syntax  [no] entropy-label-capability

Context  config>router>rsvp

Description  This command enables or disables the entropy label capability for an RSVP-TE LSP. When enabled, the egress LER (eLER) signals to the ingress LER (iLER) that the LSP is capable of using entropy labels.

The no form of the command disables entropy label capability.

Default  no entropy-label-capability
graceful-shutdown

Syntax  

[no] graceful-shutdown

Context  
config>router>rsvp
config>router>rsvp>interface

Description  
This command initiates a graceful shutdown of the specified RSVP interface (referred to as a maintenance interface) or all RSVP interfaces on the node (referred to as a maintenance node). When this command is executed, the node performs the following operations in no specific order.

A PathErr message with an error sub-code of "Local Maintenance on TE Link required" is generated for each LSP that is in transit at this node and is using a maintenance interface as its outgoing interface. A PathErr message with the error code "Local node maintenance required" is generated if all interfaces are affected.

A single make-before-break attempt is performed for all adaptive CSPF LSPs that originate on the node and whose paths make use of the maintenance interfaces listed in the PathErr message. If an alternative path for an affected LSP is not found, the LSP is maintained on its current path. The maintenance node also tears down and resignals any bypass or detour LSP that uses the maintenance interfaces as soon as they are not active. The maintenance node floods an IGP TE LSA/LSP containing a Link TLV for the links under graceful shutdown with the Traffic Engineering metric set to 0xffffffff and the Unreserved Bandwidth parameter set to zero (0).

Upon receipt of the PathErr message, an intermediate LSR tears down and resignals any bypass LSP whose path makes use of the listed maintenance interfaces as soon as no associations with a protected LSP are active. The node does not take any action on a detour LSP whose path makes use of the listed maintenance interfaces.

Upon receipt of the PathErr message, a head-end LER performs a single make-before-break attempt on the affected adaptive CSPF LSP. If an alternative path is not found, the LSP is maintained on its current path.

A node does not take any action on the paths of the following originating LSPs after receiving the PathErr message:

• an adaptive CSPF LSP for which the PathErr indicates a node address in the address list and the node corresponds to the destination of the LSP. In this case, there are no alternative paths that can be found.
• an adaptive CSPF LSP whose path has explicit hops defined using the listed maintenance interfaces or node
• a CSPF LSP that has the adaptive option disabled and whose current path is over the listed maintenance interfaces in the PathErr message. These are not subject to make-before-break.
• a non-CSPF LSP whose current path is over the listed maintenance interfaces in the PathErr message
Upon receipt of the updated IPG TE LSA/LSP for the maintenance interfaces, the head-end LER updates the TE database. This information will be used at the next scheduled CSPF computation for any LSP whose path might traverse any of the maintenance interfaces.

The `no` form of the command disables the graceful shutdown operation at the RSVP interface level or at the RSVP level. The configured TE parameters of the maintenance links are restored and the maintenance node floods the links.

**Default**: n/a

### keep-multiplier

**Syntax**

```
[no] keep-multiplier number
no keep-multiplier
```

**Context**

```
config>router>rsvp
```

**Description**

This command is used by RSVP-TE to declare that a reservation is down or the neighbor is down. The `keep-multiplier number` is used with the `refresh-time` command to determine when RSVP-TE will declare the session down.

The `no` form of this command reverts to the default value.

**Default**: 3

**Parameters**

- `number` — specifies the `keep-multiplier` value
  - **Values**: 1 to 255

### node-id-in-rro

**Syntax**

```
node-id-in-rro {include | exclude}
```

**Context**

```
config>router>rsvp
```

**Description**

This command enables the option to include the node-id sub-object in the RRO. Propagation of the node-id sub-object is required to provide fast reroute protection for an LSP that spans multiple area domains.

**Default**: exclude

**Parameters**

- `include` — the node-id sub-object is included in the RRO
- `exclude` — the node-id sub-object is not included in the RRO
rapid-retransmit-time

**Syntax**

```
rapid-retransmit-time hundred-milliseconds
no rapid-retransmit-time
```

**Context**

`config>router>rsvp`

**Description**

This command is used to define the value of the rapid retransmission interval. This is used in the retransmission mechanism based on an exponential backoff timer in order to handle unacknowledged message-_id objects. The RSVP-TE message with the same message-id is retransmitted every $2 \times \text{rapid-retransmit-time}$ interval. The node will stop retransmission of unacknowledged RSVP-TE messages whenever the updated backoff interval exceeds the value of the regular refresh interval or the number of retransmissions reaches the value of the rapid-retry-limit parameter, whichever comes first.

The rapid retransmission interval must be smaller than the regular refresh interval configured in `config>router>rsvp>refresh-time`.

The **no** form of this command reverts to the default value.

**Default**

5 (which represents 500 msec)

**Parameters**

- `hundred-milliseconds` — 1 to 100, in units of 100 msec

rapid-retry-limit

**Syntax**

```
rapid-retry-limit number
no rapid-retry-limit
```

**Context**

`config>router>rsvp`

**Description**

This command is used to define the value of the rapid retry limit. This is used in the retransmission mechanism based on an exponential backoff timer in order to handle unacknowledged message_id objects. The RSVP-TE message with the same message_id is retransmitted every $2 \times \text{rapid-retransmit-time}$ interval. The node will stop retransmission of unacknowledged RSVP-TE messages whenever the updated backoff interval exceeds the value of the regular refresh interval or the number of retransmissions reaches the value of the rapid-retry-limit parameter, whichever comes first.

The **no** form of this command reverts to the default value.

**Default**

3

**Parameters**

- `number` — 1 to 6, integer values
refresh-reduction-over-bypass

Syntax
refresh-reduction-over-bypass [enable | disable]

Context
config>router>rsvp

Description
This command enables the refresh reduction capabilities over all bypass tunnels originating on this 7705 SAR PLR node or terminating on this 7705 SAR Merge Point (MP) node.

By default, this is disabled. Since a bypass tunnel may merge with the primary LSP path in a node downstream of the next hop, there is no direct interface between the PLR and the MP node and it is possible that the latter will not accept summary refresh messages received over the bypass.

When disabled, the node as a PLR or MP will not set the “Refresh-Reduction-Capable” bit on RSVP-TE messages pertaining to LSP paths tunneled over the bypass. It will also not send message-id in RSVP-TE messages. This effectively disables summary refresh.

Default
disable

refresh-time

Syntax
refresh-time seconds
no refresh-time

Context
config>router>rsvp

Description
This command controls the interval, in seconds, between the successive PATH and RESV refresh messages. RSVP-TE declares the session down after it misses keep-multiplier number consecutive refresh messages.

The no form of this command reverts to the default value.

Default
30

Parameters
seconds — specifies the refresh time in seconds

Values
1 to 65535
3.20.2.2.3 Interface Commands

interface

Syntax  
[no] interface ip-int-name

Context  
config>router>rsvp

Description  
This command enables RSVP-TE protocol support on an IP interface. No RSVP-TE commands are executed on an IP interface where RSVP-TE is not enabled.

The no form of this command deletes all RSVP-TE commands such as hello-interval and subscription, which are defined for the interface. The RSVP-TE interface must be shut down before it can be deleted. If the interface is not shut down, the no interface ip-int-name command does nothing except issue a warning message on the console indicating that the interface is administratively up.

Parameters  
ip-int-name — specifies the network IP interface. The interface name cannot be in the form of an IP address. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Values  
1 to 32 alphanumeric characters

auth-keychain

Syntax  
auth-keychain name

no auth-keychain

Context  
config>router>rsvp>interface

Description  
This command associates an authentication keychain with the RSVP-TE interface. The keychain is a collection of keys used to authenticate RSVP-TE messages from remote peers. The keychain allows the rollover of authentication keys during the lifetime of a session and also supports stronger authentication algorithms than clear text and MD5.

The keychain must already be defined in the config>system>security>keychain context.

Either the authentication-key command or the auth-keychain command can be used by RSVP-TE, but both cannot be supported at the same time. If both commands are configured, the auth-keychain configuration will be applied and the authentication-key command will be ignored.

By default, authentication is not enabled.

Default  
no auth-keychain

Parameters  
name — the name of an existing keychain, up to 32 characters
authentication-key

Syntax:  

**authentication-key** \(\{\text{authentication-key} \mid \text{hash-key}\}\) [\text{hash} \mid \text{hash2}]

**no authentication-key**

Context:  

config>router>rsvp>interface

Description:  

This command specifies the authentication key to be used between RSVP-TE neighbors to authenticate RSVP-TE messages. Authentication uses the MD5 message-based digest.

When enabled on an RSVP-TE interface, authentication of RSVP-TE messages operates in both directions of the interface.

A 7705 SAR node maintains a security association using one authentication key for each interface to a neighbor. The following items are stored in the context of this security association:

- the HMAC-MD5 authentication algorithm
- the key used with the authentication algorithm
- the lifetime of the key; the user-entered key is valid until the user deletes it from the interface
- the source address of the sending system
- the latest sending sequence number used with this key identifier

A 7705 SAR RSVP-TE sender transmits an authenticating digest of the RSVP-TE message, computed using the shared authentication key and a keyed hash algorithm. The message digest is included in an integrity object that also contains a flags field, a key identifier field, and a sequence number field. The 7705 SAR RSVP-TE sender complies with the procedures for RSVP-TE message generation in RFC 2747, *RSVP Cryptographic Authentication*.

A 7705 SAR RSVP-TE receiver uses the key together with the authentication algorithm to process received RSVP-TE messages.

When a PLR node switches the path of the LSP to a bypass LSP, it does not send the integrity object in the RSVP-TE messages sent over the bypass tunnel. If the PLR receives an RSVP-TE message with an integrity object, it will perform the digest verification for the key of the interface over which the packet was received. If this fails, the packet is dropped. If the received RSVP-TE message is an RESV message and does not have an integrity object, then the PLR node will accept it only if it originated from the MP node.

A 7705 SAR MP node will accept RSVP-TE messages received over the bypass tunnel with and without the integrity object. If an integrity object is present, the proper digest verification for the key of the interface over which the packet was received is performed. If this fails, the packet is dropped.

The 7705 SAR MD5 implementation does not support the authentication challenge procedures in RFC 2747.
Either the `authentication-key` command or the `auth-keychain` command can be used by RSVP-TE, but both cannot be supported at the same time. If both commands are configured, the `auth-keychain` configuration will be applied and the `authentication-key` command will be ignored.

The **no** form of this command disables authentication.

**Default**

- **no authentication-key** — the authentication key value is the null string

**Parameters**

- **authentication-key** — specifies the authentication key. The key can be any combination of ASCII characters up to 16 characters in length (unencrypted). If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

  - **hash-key** — specifies the hash key. The key can be any combination of up to 33 alphanumeric characters. If spaces are used in the string, enclose the entire string in quotation marks (" ").
  
  This is useful when a user must configure the parameter, but for security purposes, the actual unencrypted key value is not provided.

- **hash** — specifies the key is entered in an encrypted form. If the **hash** keyword is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

- **hash2** — specifies the key is entered in a more complex encrypted form. If the **hash2** keyword is not used, the less-encrypted **hash** form is assumed.
bfd-enable

**Syntax**

```plaintext
[no] bfd-enable
```

**Context**

```
config> router> rsvp> interface
```

**Description**

This command enables the use of bidirectional forwarding (BFD) to control the state of the associated RSVP-TE interface. This causes RSVP-TE to register the interface with the BFD session on that interface.

The user configures the BFD session parameters, such as `transmit-interval`, `receive-interval`, and `multiplier`, under the IP interface in the `config> router> if> bfd` context.

The BFD session on the interface might already have been started because of a prior registration with another protocol; for example, OSPF or IS-IS.

The registration of an RSVP-TE interface with BFD is performed when a neighbor gets its first session, which means registration occurs when this node sends or receives a new PATH message over the interface. However, if the session did not come up due to not receiving an RESV for a new PATH message sent after the maximum number of retries, the LSP is shut down and the node deregisters with BFD. In general, the registration of RSVP-TE with BFD is removed as soon as the last RSVP-TE session is cleared.

The registration of an RSVP-TE interface with BFD is performed independently of whether RSVP-TE hello is enabled on the interface or not. However, hello timeout clears all sessions toward the neighbor and RSVP-TE deregisters with BFD at the clearing of the last session.

An RSVP-TE session is associated with a neighbor based on the interface address that the PATH message is sent to. If multiple interfaces exist to the same node, each interface is treated as a separate RSVP-TE neighbor. The user must enable BFD on each interface, and RSVP-TE will register with the BFD session running with each of those neighbors independently.

Similarly, disabling BFD on the interface results in removing registration of the interface with BFD.

When a BFD session transitions to the down state, the following actions are triggered. For RSVP-TE signaled LSPs, this triggers activation of FRR bypass or detour backup LSPs (PLR role), global revertive (head-end role), and switchover to secondary (if any) (head-end role) for affected LSPs with FRR enabled. It triggers a switchover to secondary (if any) and scheduling of retries for signaling the primary path of the non-FRR-affected LSPs (head-end role).

The `no` form of this command removes BFD from the associated RSVP-TE protocol adjacency.

**Default**

```
no bfd-enable
```
hello-interval

Syntax       hello-interval  *milli-seconds*
             no  hello-interval

Context       config>router>rsvp>interface

Description  This command configures the time interval between RSVP-TE hello messages.

RSVP-TE hello packets are used to detect loss of RSVP-TE connectivity with the neighboring node. Hello packets detect the loss of a neighbor more quickly than it would take for the RSVP-TE session to time out based on the refresh interval. After the loss of the of keep-multiplier number consecutive hello packets, the neighbor is declared to be in a down state.

The no form of this command reverts to the default value of the hello-interval. To disable sending hello messages, set the value to zero.

Default       3000

Parameters    *milli-seconds* — specifies the RSVP-TE hello interval in milliseconds, in multiples of 1000. A 0 (zero) value disables the sending of RSVP-TE hello messages.

Values        0 to 60000 milliseconds (in multiples of 1000)

refresh-reduction

Syntax       [no]  refresh-reduction

Context       config>router>rsvp>interface

Description  This command enables the use of the RSVP-TE overhead refresh reduction capabilities on this RSVP-TE interface.

When this option is enabled, a 7705 SAR node will enable support for three capabilities:

- it will accept bundle RSVP-TE messages from its peer over this interface
- it will attempt to perform reliable RSVP-TE message delivery to its peer
- it will use summary refresh messages to refresh PATH and RESV states

The reliable message delivery must be explicitly enabled by the user after refresh reduction is enabled. The other two capabilities are enabled immediately.

A bundle RSVP-TE message is intended to reduce the overall message handling load. A bundle message consists of a bundle header followed by one or more bundle sub-messages. A sub-message can be any regular RSVP-TE message except another bundle message. A 7705 SAR node will only process received bundle RSVP-TE messages but will not generate them.
When reliable RSVP-TE message delivery is supported by both the node and its peer over the RSVP-TE interface, an RSVP-TE message is sent with a message_id object. A message_id object can be added to any RSVP-TE message when sent individually or as a sub-message of a bundle message.

If the sender sets the ack_desired flag in the message_id object, the receiver acknowledges the receipt of the RSVP-TE message by piggy-backing a message_ack object to the next RSVP-TE message it sends to its peer. Alternatively, an ACK message can also be used to send the message_ack object. In both cases, one or many message_ack objects could be included in the same message.

The 7705 SAR supports the sending of separate ACK messages only, but is capable of processing received message_ack objects piggy-backed to hop-by-hop RSVP-TE messages, such as PATH and RESV.

The 7705 SAR sets the ack_desired flag only in non-refresh RSVP-TE messages and in refresh messages that contain new state information.

A retransmission mechanism based on an exponential backoff timer is supported in order to handle unacknowledged message_id objects. The RSVP-TE message with the same message_id is retransmitted every $2 \times$ rapid-retransmit-time interval. The rapid-retransmit-time is referred to as the rapid retransmission interval because it must be smaller than the regular refresh interval configured in the `config>router>rsvp>refresh-time` context. There is also a maximum number of retransmissions of an unacknowledged RSVP-TE message rapid-retry-limit. The node will stop retransmission of unacknowledged RSVP-TE messages whenever the updated backoff interval exceeds the value of the regular refresh-time interval or the number of retransmissions reaches the value of the rapid-retry-limit parameter, whichever comes first. These two parameters are configurable globally on a system in the `config>router>rsvp` context.

Summary refresh consists of sending a summary refresh message containing a message_id list object. The fields of this object are populated each with the value of the message_identifier field in the message_id object of a previously sent individual PATH or RESV message. The summary refresh message is sent every refresh regular interval as configured by the user using the refresh-time command in the `config>router>rsvp` context. The receiver checks each message_id object against the saved PATH and RESV states. If a match is found, the state is updated as if a regular PATH or RESV refresh message was received from the peer. If a specific message_identifier field does not match, then the node sends a message_id_nack object to the originator of the message.

The above capabilities are referred to collectively as “refresh overhead reduction extensions”. When the refresh-reduction is enabled on a 7705 SAR RSVP-TE interface, the node indicates this to its peer by setting a “refresh-reduction-capable” bit in the flags field of the common RSVP-TE header. If both peers of an RSVP-TE interface set this bit, all the above three capabilities can be used. Furthermore, the node monitors the settings of this bit in received RSVP-TE messages from the peer on the interface. As soon as this bit is cleared, the 7705 SAR stops sending summary refresh messages. If a peer did not set the “refresh-reduction-capable” bit, a node does not attempt to send summary refresh messages.
However, if the peer did not set the “refresh-reduction-capable” bit, then a node with refresh reduction enabled and reliable message delivery enabled will still attempt to perform reliable message delivery with this peer. If the peer does not support the message_id object, it returns the error message “unknown object class”. In this case, the 7705 SAR node retransmits the RSVP-TE message without the message_id object and reverts to using this method for future messages destined for this peer.

The no form of the command reverts to the default value.

**Default**

no refresh-reduction

---

**reliable-delivery**

**Syntax**

[no] reliable-delivery

**Context**

config>router>rsvp>if>refresh-reduction

**Description**

This command enables reliable delivery of RSVP-TE messages over the RSVP-TE interface. When refresh-reduction is enabled on an interface and reliable-delivery is disabled, then the 7705 SAR will send a message_id and not set ACK desired in the RSVP-TE messages over the interface. Thus, the 7705 SAR does not expect an ACK but will accept it if received. The node will also accept message ID and reply with an ACK when requested. In this case, if the neighbor set the “refresh-reduction-capable” bit in the flags field of the common RSVP-TE header, the node will enter summary refresh for a specific message_id it sent regardless of whether it received an ACK or not to this message from the neighbor.

Finally, when the reliable-delivery option is enabled on any interface, RSVP-TE message pacing is disabled on all RSVP-TE interfaces of the system; for example, the user cannot enable the msg-pacing option in the config>router>rsvp context, and an error message is returned in CLI. When the msg-pacing option is enabled, the user cannot enable the reliable-delivery option on any interface on this system. An error message will also be generated in CLI after such an attempt.

The no form of the command reverts to the default value.

**Default**

no reliable-delivery
subscription

Syntax  subscription percentage
       no subscription

Context  config>router>rsvp>interface

Description  This command configures the percentage of the link bandwidth that RSVP-TE can use for reservation and sets a limit for the amount of over-subscription or under-subscription allowed on the interface.

When the subscription is set to zero, no new sessions are permitted on this interface. If the percentage is exceeded, the reservation is rejected and a log message is generated.

The no form of this command resets the percentage to the default value.

Default  100

Parameters  percentage — specifies the percentage of the interface’s bandwidth that RSVP-TE allows to be used for reservations

Values   0 to 1000
### 3.20.2.2.4 Message Pacing Commands

**msg-pacing**

**Syntax**

```
[no] msg-pacing
```

**Context**

```
config>router>rsvp
```

**Description**

This command enables RSVP-TE message pacing, which is defined by the `max-burst` and `period` commands. A count is kept of the messages that were dropped because the output queue for the interface used for message pacing was full.

**Default**

`no msg-pacing`

**max-burst**

**Syntax**

```
max-burst number
```

```
no max-burst
```

**Context**

```
config>router>rsvp>msg-pacing
```

**Description**

This command specifies the maximum number of RSVP-TE messages that can be sent under normal operating conditions, as specified by the `period` command. The `no` form of this command reverts to the default value.

**Default**

650

**Parameters**

- `number` — maximum number of RSVP-TE messages

**Values**

- 100 to 1000, in increments of 10

**period**

**Syntax**

```
period milli-seconds
```

```
no period
```

**Context**

```
config>router>rsvp>msg-pacing
```

**Description**

This command specifies the time interval, in milliseconds, during which the router can send RSVP-TE messages, as specified by the `max-burst` command. The `no` form of this command reverts to the default value.

**Default**

100

**Parameters**

- `milli-seconds` — the time interval during which the router can send RSVP-TE messages

**Values**

- 100 to 1000 milliseconds, in increments of 10 milliseconds
3.20.2.3 Show Commands (MPLS)

**Note:** The following command outputs are examples only; actual displays may differ depending on supported functionality and user configuration.

**admin-group**

**Syntax**

```
admin-group group-name
```

**Context**

```
show>router>mpls
```

**Description**

This command displays MPLS administrative group information.

**Parameters**

- `group-name` — specifies the administrative group name

**Output**

The following output is an example of MPLS administrative group information, and Table 7 describes the fields.

**Output Example**

```
A:ALU-1# show router mpls admin-group
=================================================================
MPLS Administrative Groups
=================================================================
Group Name  Group Value
---------------------------------------------------
green       15
red         25
yellow      20
---------------------------------------------------
No. of Groups: 3
=================================================================
A:ALU-1#
```

**Table 7**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>The name of the administrative group. The name identifies the administrative group within a router instance.</td>
</tr>
<tr>
<td>Group Value</td>
<td>The unique group value associated with the administrative group. If the value displays “-1”, then the group value for this entry has not been set.</td>
</tr>
<tr>
<td>No. of Groups</td>
<td>The total number of configured administrative groups within the router instance</td>
</tr>
</tbody>
</table>
bypass-tunnel

Syntax
bypass-tunnel [to ip-address] [protected-lsp [lsp-name]] [dynamic | manual] [detail]

Context
show>router>mpls

Description
If fast reroute is enabled on an LSP and the facility method is selected, instead of creating a separate LSP for every LSP that is to be backed up, a single LSP is created that serves as a backup for a set of LSPs. This type of LSP tunnel is called a bypass tunnel.

Parameters
- ip-address — specifies the IP address of the egress router
- lsp-name — specifies the name of the LSP protected by the bypass tunnel
- dynamic — displays dynamically assigned labels for bypass protection
- manual — displays manually assigned labels for bypass protection
- detail — displays detailed information

Output
The following output is an example of MPLS bypass tunnel information, and Table 8 describes the fields.

Output Example
A:ALU-12>show>router>mpls# bypass-tunnel to 10.20.1.4
===============================================================================
Legend : m - Manual d - Dynamic
===============================================================================
To State Out I/F Out Label Reserved Protected Type
BW (Kbps) LSP Count
-------------------------------------------------------------------------------
10.20.1.4 Up lag *-* 131071 0
-------------------------------------------------------------------------------
Bypass Tunnels : 1
===============================================================================
A:ALU-12>show>router>mpls#

Table 8 Show Router MPLS Bypass-Tunnel Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To</td>
<td>The system IP address of the egress router</td>
</tr>
<tr>
<td>State</td>
<td>The administrative state of the LSP</td>
</tr>
<tr>
<td>Out I/F</td>
<td>The name of the network IP interface</td>
</tr>
<tr>
<td>Out Label</td>
<td>The incoming MPLS label on which to match</td>
</tr>
<tr>
<td>Reserved BW (Kbps)</td>
<td>The amount of bandwidth in kilobytes per second (Kbps) reserved for the LSP</td>
</tr>
<tr>
<td>Protected LSP Count</td>
<td>The number of times this LSP has used a protected LSP</td>
</tr>
</tbody>
</table>
interface

Syntax  interface [ip-int-name | ip-address] [label-map [label]]

interface [ip-int-name | ip-address] statistics

Context  show-router>mpls

Description  This command displays MPLS interface information.

Parameters  ip-int-name — identifies the network IP interface. The interface name cannot be in the form of an IP address. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

ip-address — specifies the system or network interface IP address

label-map label — specifies the MPLS label on which to match

Values  32 to 1023

statistics — displays IP address and the number of packets and octets sent and received on an interface basis

Output  The following output is an example of MPLS interface information, and Table 9 describes the fields.

Output Example

ALU-12# show router mpls interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port-id</th>
<th>Adm</th>
<th>Opr</th>
<th>TE-metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>vport-1</td>
<td>Up</td>
<td>Up</td>
<td>None</td>
</tr>
<tr>
<td>Admin Groups</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Srlg Groups</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip-10.10.1.2</td>
<td>1/1/1</td>
<td>Up</td>
<td>Up</td>
<td>None</td>
</tr>
<tr>
<td>Admin Groups</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Srlg Groups</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip-10.10.4.2</td>
<td>1/1/2</td>
<td>Up</td>
<td>Up</td>
<td>None</td>
</tr>
<tr>
<td>Admin Groups</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Srlg Groups</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip-10.10.3.2</td>
<td>1/1/3</td>
<td>Up</td>
<td>Up</td>
<td>None</td>
</tr>
<tr>
<td>Admin Groups</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Srlg Groups</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Interfaces : 4

*A:ALU-48>config>router>mpls# show router mpls interface "to-104" label-map 35

MPLS Interface : to-104 (Label-Map 35)

<table>
<thead>
<tr>
<th>In Label</th>
<th>In I/F</th>
<th>Out Label</th>
<th>Out I/F</th>
<th>Next Hop</th>
<th>Type</th>
<th>Adm</th>
<th>Opr</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>1/1/1</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>Static</td>
<td>Up</td>
<td>Down</td>
</tr>
</tbody>
</table>

Interfaces : 1
*A:ALU-48>config>router>mpls#

ALU-12# show router mpls interface statistics

MPLS Interface (statistics)

Interface : ip-10.10.1.1
  Transmitted: Pkts - 6 Octets - 540
  Received: Pkts - 0 Octets - 0
  Invalid: Labels - 0
  Invalid: IPoMPLS Pkts - 0
  Invalid: Stack Too Big Pkts - 0
  Invalid: TTL Expired Pkts - 0
  Invalid: Other Discard Pkts - 0
  Last Invalid: Label Value - 0
  Last Invalid: Label Position - 0

Interface : ip-10.10.2.1
  Transmitted: Pkts - 0 Octets - 0
  Received: Pkts - 0 Octets - 0
  Invalid: Labels - 0
  Invalid: IPoMPLS Pkts - 0
  Invalid: Stack Too Big Pkts - 0
  Invalid: TTL Expired Pkts - 0
  Invalid: Other Discard Pkts - 0
  Last Invalid: Label Value - 0
  Last Invalid: Label Position - 0

ALU-12#

**Table 9** Show Router MPLS Interface Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface name</td>
</tr>
<tr>
<td>Port-id</td>
<td>The port ID in the <em>slot/mda/port</em> format</td>
</tr>
<tr>
<td>Adm</td>
<td>The administrative state of the interface</td>
</tr>
<tr>
<td>Opr</td>
<td>The operational state of the interface</td>
</tr>
<tr>
<td>Te-metric</td>
<td>The traffic engineering metric used on the interface</td>
</tr>
</tbody>
</table>
### Table 9  Show Router MPLS Interface Output Fields  (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Srlg Groups</td>
<td>The shared risk link group (SRLG)</td>
</tr>
<tr>
<td>Interfaces</td>
<td>The total number of interfaces</td>
</tr>
<tr>
<td>Transmitted</td>
<td>The number of packets and octets transmitted from the interface</td>
</tr>
<tr>
<td>Received</td>
<td>The number of packets and octets received</td>
</tr>
<tr>
<td>In Label</td>
<td>The ingress label</td>
</tr>
<tr>
<td>In I/F</td>
<td>The ingress interface</td>
</tr>
<tr>
<td>Out Label</td>
<td>The egress label</td>
</tr>
<tr>
<td>Out I/F</td>
<td>The egress interface</td>
</tr>
<tr>
<td>Next Hop</td>
<td>The next-hop IP address for the static LSP</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates whether the label value is statically or dynamically assigned</td>
</tr>
<tr>
<td>Invalid</td>
<td>Labels — the number of incoming packets discarded due to invalid labels</td>
</tr>
<tr>
<td></td>
<td>IPoMPLS Pkts — the number of incoming labeled packets discarded due to invalid IP packet headers in the packet</td>
</tr>
<tr>
<td></td>
<td>Stack Too Big Pkts — the number of incoming packets discarded due to having greater than the maximum number of labels in the label stack (that is, greater than five)</td>
</tr>
<tr>
<td></td>
<td>TTL Expired Pkts — the number of incoming packets discarded due to exceeding the maximum Time-To-Live (TTL) value</td>
</tr>
<tr>
<td></td>
<td>Other Discard Pkts — the number of incoming packets discarded due to internal errors (for example, memory corruption or invalid label table programming)</td>
</tr>
<tr>
<td>Last Invalid</td>
<td>Label Value — the value of the last invalid label received</td>
</tr>
<tr>
<td></td>
<td>Label Position — the position in the label stack of the last invalid label received</td>
</tr>
</tbody>
</table>
label

**Syntax**

`label start-label [end-label | in-use | label-owner]`

**Context**

`show>router>mpls`

**Description**

This command displays MPLS labels exchanged.

**Parameters**

- `start-label` — specifies the label value assigned at the ingress router
- `end-label` — specifies the label value assigned for the egress router
- `in-use` — specifies the number of in-use labels displayed
- `label-owner` — specifies the owner of the label

**Values**

`static, tldp`

**Output**

The following output is an example of MPLS label information, and Table 10 describes the fields.

**Output Example**

```
ALU-12# show router mpls label 32
================================================================
MPLS Label 32
================================================================
Label  Label Type  Label Owner
--------------------------
32   static-lsp   Not-in-use
================================================================
In-use labels in entire range : 7
================================================================
ALU-12#
```

**Table 10**  
Show Router MPLS Label Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>The value of the label</td>
</tr>
<tr>
<td>Label Type</td>
<td>Specifies whether the label value is statically or dynamically assigned</td>
</tr>
<tr>
<td>Label Owner</td>
<td>The label owner</td>
</tr>
<tr>
<td>In-use labels in entire range</td>
<td>The total number of labels being used</td>
</tr>
</tbody>
</table>
label-range

**Syntax**

```
label-range
```

**Context**

```
show>router>mpls
```

**Description**

This command displays the MPLS label range.

**Output**

The following output is an example of MPLS label range information, and Table 11 describes the fields.

**Output Example**

```
ALU-12# show router mpls label-range
==============================================================================
Label Ranges
==============================================================================
Label Type  Start Label  End Label  Aging  Total Available
------------------------------------------------------------------------------
static-lsp  32          1023      -       991
static-svc 2048        18431     -       16383
dynamic    32768       131071    0       98301
==============================================================================
ALU-12#
```

**Table 11**

**Show Router MPLS Label Range Output Fields**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label Type</td>
<td>Displays information about static-lsp, static-svc, and dynamic label types</td>
</tr>
<tr>
<td>Start Label</td>
<td>The label value assigned at the ingress router</td>
</tr>
<tr>
<td>End Label</td>
<td>The label value assigned for the egress router</td>
</tr>
<tr>
<td>Aging</td>
<td>The number of labels released from a service that are transitioning back to the label pool. Labels are aged 15 seconds.</td>
</tr>
<tr>
<td>Total Available</td>
<td>The number of label values available</td>
</tr>
</tbody>
</table>
The following outputs are examples of MPLS LSP information:

- MPLS LSP (Output Example, Table 12)
- MPLS LSP Detail (Output Example, Table 13)
- MPLS LSP Path Detail (Output Example, Table 14)
- MPLS LSP Path MBB (Output Example, Table 15)
- MPLS Auto LSP (Output Example, Table 16)
Output Example

A:ALU-48# show router mpls lsp

MPLS LSPs (Originating)

<table>
<thead>
<tr>
<th>LSP Name</th>
<th>To</th>
<th>FastFail Config</th>
<th>Adm</th>
<th>Opr</th>
</tr>
</thead>
<tbody>
<tr>
<td>to-104</td>
<td>10.10.10.104</td>
<td>Yes</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>to-103</td>
<td>0.0.0.0</td>
<td>Yes</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>to-99</td>
<td>10.10.10.99</td>
<td>No</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>to-100</td>
<td>10.10.10.100</td>
<td>No</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>to-49</td>
<td>10.20.30.49</td>
<td>No</td>
<td>Dwn</td>
<td>Up</td>
</tr>
</tbody>
</table>

LSPs : 5

*A:ALU-48#*

*A:ALU-48#* show router mpls lsp to-104

MPLS LSPs (Originating)

<table>
<thead>
<tr>
<th>LSP Name</th>
<th>To</th>
<th>FastFail Config</th>
<th>Adm</th>
<th>Opr</th>
</tr>
</thead>
<tbody>
<tr>
<td>to-104</td>
<td>10.10.10.104</td>
<td>Yes</td>
<td>Up</td>
<td>Dwn</td>
</tr>
</tbody>
</table>

LSPs : 1

*A:ALU-48#*

**Table 12** Show Router MPLS LSP Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP Name</td>
<td>The name of the LSP used in the path</td>
</tr>
<tr>
<td>To</td>
<td>The system IP address of the egress router for the LSP</td>
</tr>
<tr>
<td>FastFail Config</td>
<td>enabled — fast reroute is enabled. In the event of a failure, traffic is immediately rerouted on the precomputed protection LSP, thus minimizing packet loss</td>
</tr>
<tr>
<td></td>
<td>disabled — there is no protection LSP from each node on the primary path</td>
</tr>
<tr>
<td>Adm State</td>
<td>Down — the path is administratively disabled</td>
</tr>
<tr>
<td></td>
<td>Up — the path is administratively enabled</td>
</tr>
<tr>
<td>Oper State</td>
<td>Down — the path is operationally down</td>
</tr>
<tr>
<td></td>
<td>Up — the path is operationally up</td>
</tr>
<tr>
<td>LSPs</td>
<td>The total number of LSPs configured</td>
</tr>
</tbody>
</table>
### Output Example

```
*A:ALU-48# show router mpls lsp to-104 detail
===============================================================================
MPLS LSPs (Originating) (Detail)
===============================================================================
Type : Originating
-------------------------------------------------------------------------------
LSP Name : to-104 LSP Tunnel ID : 1
From : 10.10.10.103 To : 10.10.10.104
Adm State : Up Oper State : Down
LSP Up Time : 0d 00:00:00 LSP Down Time : 0d 00:46:50
Transitions : 0 Path Changes : 0
Retry Limit : 0 Retry Timer : 30 sec
Signaling : RSVP Resv. Style : FF
Hop Limit : 10 Negotiated MTU : 0
Adaptive : Enabled
FastReroute : Enabled Oper FR : Disabled
FR Method : Facility FR Hop Limit : 16
FR Bandwidth: 0 Mbps FR Node Protect: Enabled
FR Object : Enabled
CSPF : Enabled ADSPEC : Enabled
Metric : 1 Use TE metric : Disabled
Include Grps: None Exclude Grps : None
Type : RegularLsp
-------------------------------------------------------------------------------
Auto BW : Disabled
LdpOverRsvp : Disabled VprnAutoBind : Disabled
IGP Shortcut: Enabled
IGP LFA : Disabled IGP Rel Metric : -1
BGPTransTun : Enabled
Oper Metric : 20
Prop Adm Grp: Disabled
-------------------------------------------------------------------------------
Secondary : secondary-path Down Time : 0d 00:46:50
Bandwidth : 50000 Mbps
Primary : to-NYC Down Time : 0d 00:46:50
Bandwidth : 0 Mbps
-------------------------------------------------------------------------------
```

### Table 13

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP Name</td>
<td>The name of the LSP used in the path</td>
</tr>
<tr>
<td>From</td>
<td>The IP address of the ingress router for the LSP</td>
</tr>
<tr>
<td>To</td>
<td>The system IP address of the egress router for the LSP</td>
</tr>
<tr>
<td>Adm State</td>
<td>Down — the path is administratively disabled</td>
</tr>
<tr>
<td></td>
<td>Up — the path is administratively enabled</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Oper State</td>
<td>Down — the path is operationally down</td>
</tr>
<tr>
<td></td>
<td>Up — the path is operationally up</td>
</tr>
<tr>
<td>LSP Up Time</td>
<td>The length of time the LSP has been operational</td>
</tr>
<tr>
<td>LSP Down Time</td>
<td>The total time in increments that the LSP path has not been operational</td>
</tr>
<tr>
<td>Transitions</td>
<td>The number of transitions that have occurred for the LSP</td>
</tr>
<tr>
<td>Path Changes</td>
<td>The number of path changes this LSP has had. For every path change (path down, path up, path change), a corresponding syslog/trap (if enabled) is generated.</td>
</tr>
<tr>
<td>Retry Limit</td>
<td>The number of attempts that the software should make to re-establish the LSP after it has failed</td>
</tr>
<tr>
<td>Retry Timer</td>
<td>The time, in seconds, for LSP re-establishment attempts after an LSP failure</td>
</tr>
<tr>
<td>Signaling</td>
<td>Specifies the signaling style</td>
</tr>
<tr>
<td>Resv Style</td>
<td>se — specifies a shared reservation environment with a limited reservation scope. This reservation style creates a single reservation over a link that is shared by an explicit list of senders.</td>
</tr>
<tr>
<td></td>
<td>ff — specifies a shared reservation environment with an explicit reservation scope. Specifies an explicit list of senders and a distinct reservation for each of them.</td>
</tr>
<tr>
<td>Hop Limit</td>
<td>The maximum number of hops that an LSP can traverse, including the ingress and egress routers</td>
</tr>
<tr>
<td>Negotiated MTU</td>
<td>The size of the maximum transmission unit (MTU) that is negotiated during establishment of the LSP</td>
</tr>
<tr>
<td>Adaptive</td>
<td>Indicates whether make-before-break is enabled or disabled for resignalized paths</td>
</tr>
<tr>
<td>Fast Reroute</td>
<td>Enabled — fast reroute is enabled. In the event of a failure, traffic is immediately rerouted on the pre-computed protection LSP, thus minimizing packet loss.</td>
</tr>
<tr>
<td></td>
<td>Disabled — there is no protection LSP from each node on the primary path</td>
</tr>
<tr>
<td>Oper FR</td>
<td>Indicates whether FRR has been enabled or disabled</td>
</tr>
<tr>
<td>FR Method</td>
<td>The type of Fast Reroute (FRR) that is used by the path</td>
</tr>
</tbody>
</table>
### Table 13  Show Router MPLS LSP Detail Output Fields (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FR Hop Limit</td>
<td>The total number of hops a protection LSP can take before merging back onto the main LSP path</td>
</tr>
<tr>
<td>FR Bandwidth</td>
<td>The amount of bandwidth reserved for fast reroute</td>
</tr>
<tr>
<td>FR Node Protect</td>
<td>Indicates whether FRR has node protection enabled or disabled</td>
</tr>
<tr>
<td>FR Object</td>
<td>Indicates whether signaling the frr-object is on or off</td>
</tr>
<tr>
<td>CSPF</td>
<td>Indicates whether CSPF has been enabled or disabled</td>
</tr>
<tr>
<td>ADSPEC</td>
<td>enabled — the LSP will include advertising data (ADSPEC) objects in RSVP-TE messages</td>
</tr>
<tr>
<td></td>
<td>disabled — the LSP will not include advertising data (ADSPEC) objects in RSVP-TE messages</td>
</tr>
<tr>
<td>Metric</td>
<td>The TE metric value</td>
</tr>
<tr>
<td>Use TE metric</td>
<td>Indicates whether the use of the TE metric is enabled or disabled</td>
</tr>
<tr>
<td>Include Grps</td>
<td>The admin groups that are to be included by an LSP when signaling a path</td>
</tr>
<tr>
<td>Exclude Grps</td>
<td>The admin groups that are to be avoided by an LSP when signaling a path</td>
</tr>
<tr>
<td>Type</td>
<td>The type of LSP</td>
</tr>
<tr>
<td>IGP Shortcut</td>
<td>Indicates whether this LSP can be used as a shortcut by OSPF or IS-IS</td>
</tr>
<tr>
<td>IGP LFA</td>
<td>Indicates whether the LSP is included in the LFA SPF calculation</td>
</tr>
<tr>
<td>IGP Rel Metric</td>
<td>The relative metric of the LSP</td>
</tr>
<tr>
<td>Secondary</td>
<td>The alternate path that the LSP will use if the primary path is not available</td>
</tr>
<tr>
<td>Down Time</td>
<td>The length of time that the path has been down</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>The amount of bandwidth in megabits per second (Mbps) reserved for the LSP path</td>
</tr>
<tr>
<td>Primary</td>
<td>The preferred path for the LSP</td>
</tr>
</tbody>
</table>
Output Example

*A:ALU-48# show router mpls lsp path detail
===============================================================================
MPLS LSP Path (Detail)
===============================================================================
Legend :
  @ - Detour Available  # - Detour In Use
  b - Bandwidth Protected  n - Node Protected
===============================================================================
LSP 1 Path 1
-------------------------------------------------------------------------------
LSP Name : 1  Path LSP ID : 30226
From : 10.20.1.1  To : 10.20.1.2
Adm State : Up  Oper State : Up
Path Name : 1  Path Type : Primary
Path Admin : Up  Path Oper : Up
OutInterface: 1/1/1  Out Label : 131071
Path Up Time: 0d 00:59:39  Path Dn Time: 0d 00:00:00
Retry Limit : 20  Retry Timer : 30 sec
RetryAttempt: 0  Next Retry *: 0 sec
Bandwidth : 200 Mbps  Oper Bandwi*: 50 Mbps
Hop Limit : 255
Record Route: Record  Record Label: Record
Oper MTU : 1500  Neg MTU : 1500
Adaptive : Enabled
Include Grps:  None
Exclude Grps: None
Path Trans : 9  CSPF Queries: 205
Failure Code: noError  Failure Node: n/a
ExplicitHops:
  No Hops Specified
Actual Hops :
  10.20.1.1, If Index : 2 @ n  Record Label : N/A
  -> 10.20.1.2, If Index : 2 @ n  Record Label : 131071
  -> 10.20.1.4, If Index : 2  Record Label : 131071
  -> 10.20.1.6, If Index : 2  Record Label : 131071
ComputedHops:
  10.20.1.1, If Index : 2(S)
  -> 10.20.1.2, If Index : 2(S)
  -> 10.20.1.4, If Index : 2(S)
  -> 10.20.1.6, If Index : 2(S)
LastResignalAttempt: 2008/04/08 11:42:33.22 PST  Metric : 1000
Last MBB:
  MBB Type : Timer-based Resignal  MBB State : Success/Failed
  Ended at : 2008/04/08 11:12:23.76 PST  Old Metric : 3000
In Progress MBB:
  MBB Type : Config Change  NextRetryIn : 16 sec
  Started at : 2008/04/08 12:01:02.20 PST  RetryAttempt : 3
  Failure Code: noCspfRouteToDestination  Failure Node: 10.20.1.1
===============================================================================
*A:ALU-48#
### Table 14  Show Router MPLS LSP Path Detail Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP Name</td>
<td>The name of the LSP used in the path</td>
</tr>
<tr>
<td>Path LSP ID</td>
<td>The LSP ID for the path</td>
</tr>
<tr>
<td>From</td>
<td>The IP address of the ingress router for the LSP</td>
</tr>
<tr>
<td>To</td>
<td>The system IP address of the egress router for the LSP</td>
</tr>
<tr>
<td>Adm State</td>
<td>Down — the path is administratively disabled</td>
</tr>
<tr>
<td></td>
<td>Up — the path is administratively enabled</td>
</tr>
<tr>
<td>Oper State</td>
<td>Down — the path is operationally down</td>
</tr>
<tr>
<td></td>
<td>Up — the path is operationally up</td>
</tr>
<tr>
<td>Path Name</td>
<td>The alphanumeric name of the path</td>
</tr>
<tr>
<td>Path Type</td>
<td>The type of path: primary or secondary</td>
</tr>
<tr>
<td>Path Admin</td>
<td>The administrative status of the path</td>
</tr>
<tr>
<td>Path Oper</td>
<td>The operational status of the path</td>
</tr>
<tr>
<td>OutInterface</td>
<td>The output interface of the LSP</td>
</tr>
<tr>
<td>Out Label</td>
<td>The output label of the LSP</td>
</tr>
<tr>
<td>Path Up Time</td>
<td>The length of time that the path has been operationally up</td>
</tr>
<tr>
<td>Path Down Time</td>
<td>The length of time that the path has been operationally down</td>
</tr>
<tr>
<td>Retry Limit</td>
<td>The number of times an LSP will retry before giving up</td>
</tr>
<tr>
<td>Retry Timer</td>
<td>The length of time between LSP signaling attempts</td>
</tr>
<tr>
<td>Retry Attempt</td>
<td>The number of attempts that have been made to re-establish the LSP</td>
</tr>
<tr>
<td>Next Retry</td>
<td>The time when the next attempt to re-establish the LSP will occur</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>The amount of bandwidth in megabits per second (Mbps) reserved for the LSP</td>
</tr>
<tr>
<td>Oper Bandwidth</td>
<td>The bandwidth reserved by the LSP</td>
</tr>
<tr>
<td>Hop Limit</td>
<td>The limit on the number of hops taken by the LSP</td>
</tr>
<tr>
<td>Record Route</td>
<td>Indicates whether a list of routers for the LSP has been recorded</td>
</tr>
<tr>
<td>Record Label</td>
<td>Indicates whether a list of router labels has been recorded</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Oper MTU</td>
<td>The operational MTU of the connection to the next hop</td>
</tr>
<tr>
<td>Neg MTU</td>
<td>The MTU negotiated between the router and its next hop</td>
</tr>
<tr>
<td>Adaptive</td>
<td>Indicates whether make-before-break is enabled or disabled for resig</td>
</tr>
<tr>
<td>Include Grps</td>
<td>The admin groups that are to be included by an LSP when signaling a path</td>
</tr>
<tr>
<td>Exclude Grps</td>
<td>The admin groups that are to be avoided by an LSP when signaling a path</td>
</tr>
<tr>
<td>Path Trans</td>
<td>The number of times a path has made a transition between up and down states</td>
</tr>
<tr>
<td>CSPF Queries</td>
<td>The number of requests made by the LSP to the TE database</td>
</tr>
<tr>
<td>Failure Code</td>
<td>The reason code for in-progress MBB failure. A value of none indicates t</td>
</tr>
<tr>
<td>Failure Node</td>
<td>The IP address of the node in the LSP at which the in-progress MBB failed.</td>
</tr>
<tr>
<td>Explicit Hops</td>
<td>The hops that have been specified by the user</td>
</tr>
<tr>
<td>Actual Hops</td>
<td>The hops that the route has taken, either numbered or unnumbered</td>
</tr>
<tr>
<td>Record Label</td>
<td>The label recorded at the specified hop</td>
</tr>
<tr>
<td>Computed Hops</td>
<td>The hops computed and returned from the routing database, either numbered</td>
</tr>
<tr>
<td>LastResignalAttempt</td>
<td>The system up time when the last attempt to resignal this LSP was made</td>
</tr>
<tr>
<td>Last Resignal</td>
<td>The last time the route was resig</td>
</tr>
<tr>
<td>Metric</td>
<td>The value of the metric</td>
</tr>
<tr>
<td>Last MBB</td>
<td>The header for the last make-before-break (MBB) information</td>
</tr>
<tr>
<td>MBB Type</td>
<td>An enumerated integer that specifies the type of make-before-break (MBB)</td>
</tr>
<tr>
<td>MBB State</td>
<td>The state of the most recent invocation of the make-before-break function</td>
</tr>
<tr>
<td>Ended at</td>
<td>The system up time when the last MBB ended</td>
</tr>
</tbody>
</table>
**Table 14**  Show Router MPLS LSP Path Detail Output Fields (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Old Metric</td>
<td>The cost of the traffic engineered path for the LSP prior to MBB</td>
</tr>
<tr>
<td>In Progress MBB</td>
<td>Header for the currently in-progress MBB information</td>
</tr>
<tr>
<td>MBB Type</td>
<td>An enumerated integer that specifies the type of make-before-break (MBB) operation. If none displays, then there is no MBB in progress or no last MBB.</td>
</tr>
<tr>
<td>NextRetryIn</td>
<td>The amount of time remaining, in seconds, before the next attempt is made to retry the in-progress MBB</td>
</tr>
<tr>
<td>Started At</td>
<td>The time the current MBB began</td>
</tr>
<tr>
<td>RetryAttempt</td>
<td>The number of attempts for the MBB in progress</td>
</tr>
<tr>
<td>Failure Code</td>
<td>The reason code for in-progress MBB failure. A value of none indicates that no failure has occurred.</td>
</tr>
<tr>
<td>Failure Node</td>
<td>The IP address of the node in the LSP at which the in-progress MBB failed. If no failure has occurred, this value is none.</td>
</tr>
</tbody>
</table>

**Output Example**

```bash
*A:ALU-48# show router mpls lsp path mbb
```

```
MPLS LSP Path MBB

LSP 1 Path 1

LastResignalAttempt: 2008/04/08 11:42:33.22 PST  CSPF Metric : 0

Last MBB:
MBB Type : Timer-based Resignal  MBB State : Success/Failed
Ended at  : 2008/04/08 11:12:23.76 PST  Old Metric : 3000

In Progress MBB:
MBB Type : Config Change  NextRetryIn: 16 sec
Started at : 2008/04/08 12:01:02.20 PST  RetryAttempt: 3
Failure Code: noCspfRouteToDestination  Failure Node: 10.20.1.1

```

```
LSP 2 Path 1

LastResignalAttempt: 2008/04/08 11:42:33.54 PST  CSPF Metric : 0

Last MBB:
MBB Type : Timer-based Resignal  MBB State : Success/Failed

```

```
LSP 4 Path 1
```

```bash
```
Last Resignal Attempt: 2008/04/08 11:42:34.12 PST  CSPF Metric : 0

In Progress MBB:
MBB Type : Global Revertive  Next Retry In : 10 sec
Started at : 2008/04/08 11:45:02.20 PST  Retry Attempt: 2
Failure Code: noCspfRouteToDestination  Failure Node: 10.20.1.1

Table 15  Show Router MPLS LSP Path MBB Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LastResignalAttempt</td>
<td>The system up time when the last attempt to resignal this LSP was made</td>
</tr>
<tr>
<td>CSPF Metric</td>
<td>The value of the CSPF metric</td>
</tr>
<tr>
<td>Last MBB</td>
<td>Header for the last make-before-break (MBB) information</td>
</tr>
<tr>
<td>MBB Type</td>
<td>An enumerated integer that specifies the type of make-before-break (MBB)</td>
</tr>
<tr>
<td></td>
<td>operation. If none displays, then there is no MBB in progress or no last MBB.</td>
</tr>
<tr>
<td>MBB State</td>
<td>The state of the most recent invocation of the make-before-break functionality</td>
</tr>
<tr>
<td>Ended at</td>
<td>The system up time when the last MBB ended</td>
</tr>
<tr>
<td>Old Metric</td>
<td>The cost of the traffic-engineered path for the LSP path prior to MBB</td>
</tr>
<tr>
<td>In Progress MBB</td>
<td>The header for the currently in-progress MBB information</td>
</tr>
<tr>
<td>MBB Type</td>
<td>An enumerated integer that specifies the type of make-before-break (MBB)</td>
</tr>
<tr>
<td></td>
<td>operation. If none displays, then there is no MBB in progress or no last MBB.</td>
</tr>
<tr>
<td>Next Retry In</td>
<td>The amount of time remaining, in seconds, before the next attempt is made</td>
</tr>
<tr>
<td></td>
<td>to retry the in-progress MBB</td>
</tr>
<tr>
<td>Started At</td>
<td>The time that the current MBB began</td>
</tr>
<tr>
<td>Retry Attempt</td>
<td>The number of attempts for the MBB in progress</td>
</tr>
<tr>
<td>Failure Code</td>
<td>The reason code for in-progress MBB failure. A value of none indicates that</td>
</tr>
<tr>
<td></td>
<td>no failure has occurred.</td>
</tr>
<tr>
<td>Failure Node</td>
<td>The IP address of the node in the LSP path at which the in-progress MBB</td>
</tr>
<tr>
<td></td>
<td>failed. When no failure has occurred, this value is none.</td>
</tr>
</tbody>
</table>
Output Example

A:ALU-48# show router mpls lsp auto-lsp mesh-p2p
===============================================================================
MPLS LSPs (Originating)
===============================================================================
<table>
<thead>
<tr>
<th>LSP Name</th>
<th>Type</th>
<th>Fastfail</th>
<th>Admin State</th>
<th>Oper State</th>
</tr>
</thead>
<tbody>
<tr>
<td>MESH-192.0.2.8-61456</td>
<td>MeshP2P</td>
<td>Yes</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>MESH-192.0.2.9-61457</td>
<td>MeshP2P</td>
<td>Yes</td>
<td>Up</td>
<td>Up</td>
</tr>
</tbody>
</table>
===============================================================================
Auto-LSPs : 2
===============================================================================
A:ALU-48#

Table 16  Show Router MPLS Auto LSP Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP Name</td>
<td>The name of the LSP used in the path</td>
</tr>
<tr>
<td>Type</td>
<td>The type of auto LSP</td>
</tr>
<tr>
<td>FastFail Config</td>
<td>enabled — fast reroute is enabled. In the event of a failure, traffic is immediately rerouted on the precomputed protection LSP, thus minimizing packet loss</td>
</tr>
<tr>
<td></td>
<td>disabled — there is no protection LSP from each node on the primary path</td>
</tr>
<tr>
<td>Admin State</td>
<td>Down — the path is administratively disabled</td>
</tr>
<tr>
<td></td>
<td>Up — the path is administratively enabled</td>
</tr>
<tr>
<td>Oper State</td>
<td>Down — the path is operationally down</td>
</tr>
<tr>
<td></td>
<td>Up — the path is operationally up</td>
</tr>
<tr>
<td>LSPs</td>
<td>The total number of LSPs configured</td>
</tr>
</tbody>
</table>

lsp-template

**Syntax**
lsp-template [template-name] bindings
lsp-template [template-name] [detail]

**Context**
show>router>mpls

**Description**
This command displays MPLS LSP template information.

**Parameters**
template-name — the unique name for the LSP template
bindings — displays any bindings associated with the LSP template
**Output Example**

```
A:ALU-12# show router mpls lsp-template detail
```

```
MPLS LSP Templates (Detail)  
LSP Template : MeshTemplateWithLoosePath

<table>
<thead>
<tr>
<th>Type</th>
<th>MeshP2P</th>
<th>Admin State</th>
<th>Up</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>10.20.1.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Path</td>
<td>LooseHopPathNameW*</td>
<td>Adaptive</td>
<td>Enabled</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>0 Mbps</td>
<td>Hop Limit</td>
<td>18</td>
</tr>
<tr>
<td>CSPF</td>
<td>Enabled</td>
<td>Use TE metric</td>
<td>Disabled</td>
</tr>
<tr>
<td>Propagate Admin Grp</td>
<td>Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Include Groups</td>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td>G0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>G1</td>
<td>G2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>G3</td>
<td>FastReroute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FR Method</td>
<td>Facility</td>
<td>FR Hop Limit</td>
<td>13</td>
</tr>
<tr>
<td>FR Prop Admin Group</td>
<td>Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FR Node Protect</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Record Route</td>
<td>Record</td>
<td>Record Label</td>
<td>Record</td>
</tr>
<tr>
<td>Retry Limit</td>
<td>100</td>
<td>Retry Timer</td>
<td>30 sec</td>
</tr>
<tr>
<td>LSP Count</td>
<td>3</td>
<td>Ref Count</td>
<td>0</td>
</tr>
<tr>
<td>LdpOverRsvp</td>
<td>Disabled</td>
<td>VprnAutoBind</td>
<td>Enabled</td>
</tr>
<tr>
<td>IGP Shortcut</td>
<td>Enabled</td>
<td>BGP Shortcut</td>
<td>Disabled</td>
</tr>
<tr>
<td>IGP LFA</td>
<td>Disabled</td>
<td>IGP Rel Metric</td>
<td>Disabled</td>
</tr>
<tr>
<td>Least Fill</td>
<td>Enabled</td>
<td>Metric</td>
<td>25</td>
</tr>
<tr>
<td>SetupPriority</td>
<td>7</td>
<td>Hold Priority</td>
<td>0</td>
</tr>
<tr>
<td>Egress Stats</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collect Stats</td>
<td>Disabled</td>
<td>Accounting Policy</td>
<td>None</td>
</tr>
<tr>
<td>Class Type</td>
<td>0</td>
<td>Backup Class Type</td>
<td>0</td>
</tr>
<tr>
<td>Main CT Retry Limit</td>
<td>0</td>
<td>BGP Transport Tunn</td>
<td>Enabled</td>
</tr>
<tr>
<td>ADSPEC</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**Table 17**  
Show Router MPLS LSP Template Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of LSP</td>
</tr>
<tr>
<td>Admin State</td>
<td>Down — the path is administratively disabled</td>
</tr>
<tr>
<td></td>
<td>Up — the path is administratively enabled</td>
</tr>
<tr>
<td>From</td>
<td>The IP address of the ingress router for the LSP</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default Path</td>
<td>The value used to order the hops in a path</td>
</tr>
<tr>
<td>Adaptive</td>
<td>Indicates whether the adaptive option is enabled or disabled</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>n/a</td>
</tr>
<tr>
<td>Hop Limit</td>
<td>The maximum number of hops that an LSP can traverse, including the ingress and egress routers</td>
</tr>
<tr>
<td>CSPF</td>
<td>Indicates whether the CSPF option is enabled or disabled</td>
</tr>
<tr>
<td>Use TE metric</td>
<td>Indicates whether the TE metric option is enabled or disabled</td>
</tr>
<tr>
<td>Propagate Admin Grp</td>
<td>Indicates whether the propagate admin group option is enabled or disabled</td>
</tr>
<tr>
<td>Include Groups</td>
<td>The admin groups that are to be included by an LSP when signaling a path</td>
</tr>
<tr>
<td>Exclude Groups</td>
<td>The admin groups that are to be excluded by an LSP when signaling a path</td>
</tr>
<tr>
<td>FastReroute</td>
<td>Indicates whether the Fast Reroute option is enabled or disabled</td>
</tr>
<tr>
<td>FR Method</td>
<td>The type of Fast Reroute (FRR) that is used by the path (always Facility for LSP templates)</td>
</tr>
<tr>
<td>FR Hop Limit</td>
<td>The total number of hops a protection LSP can take before merging back onto the main LSP path</td>
</tr>
<tr>
<td>FR Prop Admin Group</td>
<td>Indicates whether the FRR propagate admin group option is enabled or disabled</td>
</tr>
<tr>
<td>FR Node Protect</td>
<td>Indicates whether FRR has node protection enabled or disabled</td>
</tr>
<tr>
<td>Record Route</td>
<td>Indicates whether the route is being recorded</td>
</tr>
<tr>
<td>Record Label</td>
<td>Indicates whether the label is being recorded</td>
</tr>
<tr>
<td>Retry Limit</td>
<td>The maximum number of retries allowed</td>
</tr>
<tr>
<td>Retry Timer</td>
<td>The time between retry attempts</td>
</tr>
<tr>
<td>LSP Count</td>
<td>The number of LSPs belonging to the LSP template</td>
</tr>
<tr>
<td>Ref Count</td>
<td>n/a</td>
</tr>
<tr>
<td>LdpOverRsvp</td>
<td>n/a</td>
</tr>
</tbody>
</table>
path

Syntax  path [path-name] [lsp-binding]

Context  show>router>mpls

Description  This command displays MPLS paths.

---

**Table 17**  Show Router MPLS LSP Template Fields (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VprnAutoBind</td>
<td>Indicates whether the VPRN auto-bind option is enabled or disabled</td>
</tr>
<tr>
<td>IGP Shortcut</td>
<td>Indicates whether the IGP shortcut option is enabled or disabled</td>
</tr>
<tr>
<td>BGP Shortcut</td>
<td>n/a</td>
</tr>
<tr>
<td>IGP LFA</td>
<td>Indicates whether the IGP LFA option is enabled or disabled</td>
</tr>
<tr>
<td>IGP Rel Metric</td>
<td>Indicates whether the IGP relative metric option is enabled or disabled</td>
</tr>
<tr>
<td>Least Fill</td>
<td>Indicates whether the least fill option is enabled or disabled</td>
</tr>
<tr>
<td>Metric</td>
<td>The TE metric value</td>
</tr>
<tr>
<td>SetupPriority</td>
<td>n/a</td>
</tr>
<tr>
<td>Hold Priority</td>
<td>n/a</td>
</tr>
<tr>
<td>Egress Stats</td>
<td>n/a</td>
</tr>
<tr>
<td>Collect Stats</td>
<td>n/a</td>
</tr>
<tr>
<td>Accounting Policy</td>
<td>n/a</td>
</tr>
<tr>
<td>Class Type</td>
<td>n/a</td>
</tr>
<tr>
<td>Backup Class Type</td>
<td>n/a</td>
</tr>
<tr>
<td>Main CT Retry Limit</td>
<td>n/a</td>
</tr>
<tr>
<td>BGP Transport Tunn</td>
<td>Indicates whether the BGP transport tunnel option is enabled or disabled</td>
</tr>
<tr>
<td>ADSPEC</td>
<td>enabled — the LSP will include advertising data (ADSPEC) objects in RSVP-TE messages</td>
</tr>
<tr>
<td></td>
<td>disabled — the LSP will not include advertising data (ADSPEC) objects in RSVP-TE messages</td>
</tr>
</tbody>
</table>
Parameters

- **path-name** — the unique name label for the LSP path
- **lsp-binding** — displays binding information

Output

The following output is an example of MPLS path information, and Table 18 describes the fields.

**Output Example**

```
A:ALU-12# show router mpls path
===============================================================================
MPLS Path:
===============================================================================
Path Name Adm Hop Index IP Address Strict/Loose
-------------------------------------------------------------------------------
nyc_to_sjc_via_dfw Up 20 100.20.1.4 Strict
30 100.20.1.6 Strict
40 100.20.1.8 Strict
50 100.20.1.10 Strict
nyc_to_sjc_via_den Up 10 100.20.1.5 Strict
20 100.20.1.7 Loose
30 100.20.1.9 Loose
40 100.20.1.11 Loose
50 100.20.1.13 Strict
secondary_path2 Down no hops n/a n/a
-------------------------------------------------------------------------------
Paths : 3
===============================================================================
```

```
A:ALU-12# show router mpls path lsp-binding
===============================================================================
MPLS Path:
===============================================================================
Path Name Opr LSP Name Binding
-------------------------------------------------------------------------------
nyc_to_sjc_via_dfw Up NYC_SJC_customer1 Primary
nyc_to_sjc_via_den Up NYC_SJC_customer1 Standby
secondary_path2 Down NYC_SJC_customer1 Secondary*
-------------------------------------------------------------------------------
Paths : 3
===============================================================================
```

**Table 18** Show Router MPLS Path Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path Name</td>
<td>The unique name label for the LSP path</td>
</tr>
<tr>
<td>Adm</td>
<td>Down — the path is administratively disabled</td>
</tr>
<tr>
<td></td>
<td>Up — the path is administratively enabled</td>
</tr>
</tbody>
</table>
**Table 18**  Show Router MPLS Path Output Fields (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hop Index</td>
<td>The value used to order the hops in a path</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the hop that the LSP should traverse on the way to the egress router</td>
</tr>
<tr>
<td>Strict/Loose</td>
<td>- Strict — the LSP must take a direct path from the previous hop router to the next router</td>
</tr>
<tr>
<td></td>
<td>- Loose — the route taken by the LSP from the previous hop to the next hop can traverse other routers</td>
</tr>
<tr>
<td>Opr</td>
<td>The operational status of the path (up or down)</td>
</tr>
<tr>
<td>LSP Name</td>
<td>The name of the LSP used in the path</td>
</tr>
<tr>
<td>Binding</td>
<td>- Primary — the preferred path for the LSP</td>
</tr>
<tr>
<td></td>
<td>- Secondary — the standby path for the LSP</td>
</tr>
<tr>
<td>Paths</td>
<td>Total number of paths configured</td>
</tr>
</tbody>
</table>

`srlg-group`

**Syntax**  
`srlg-group [group-name]`

**Context**  
show>router>mpls

**Description**  
This command displays MPLS shared risk link groups (SRLGs)

**Parameters**  
`group-name` — specifies the name of the SRLG within a router instance.

**Output**  
The following output is an example of MPLS SRLG group information, and Table 19 describes the fields.

**Output Example**

```
*A:ALU-48>show>router>mpls# srlg-group test2
===============================================================================
MPLS Srlg Groups
===============================================================================
Group Name Group Value Interfaces
-------------------------------------------------------------------------------
test2 2 to-104
-------------------------------------------------------------------------------
No. of Groups: 1
===============================================================================
*A:ALU-48>show>router>mpls#  
```
**static-lsp**

**Syntax**

- static-lsp [lsp-name]
- static-lsp [lsp-type]
- static-lsp count

**Context**

show>router>mpls

**Description**

This command displays MPLS static LSP information.

**Parameters**

- **lsp-name** — name that identifies the LSP. The LSP name can be up to 32 characters long and must be unique.
- **lsp-type** — type that identifies the LSP. The LSP type is one of the keywords **transit** or **terminate**, where **terminate** displays the number of static LSPs that terminate at the router, and **transit** displays the number of static LSPs that transit the router.
- **count** — the number of static LSPs that originate and terminate at the router

**Output**

The following output is an example of MPLS static LSP information, and Table 20 describes the fields.

### Output Example - static-lsp

```
ALU-12# show router mpls static-lsp
MPLS Static LSPs (Originating)
LSP Name ID To Next Hop Out Label Out Port Up/Down Time Adm Opr
---------- ---------- ----------- ----------- ----------- ---------- -------
to131 1 10.9.9.9 10.1.2.2 131 n/a 30d 02:42:53 Up Down

to121 2 10.8.8.8 10.1.3.2 121 n/a 30d 02:42:53 Up Down

static-lsp_- 3 10.9.9.9 10.1.2.2 35 0d 01:39:34 Up Down

LSPs : 3
```

---

**Table 9**  Show Router MPLS SRLG Group Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>The name of the SRLG group within a router instance</td>
</tr>
<tr>
<td>Group Value</td>
<td>The group value associated with this SRLG group</td>
</tr>
<tr>
<td>Interfaces</td>
<td>The interface where the SRLG group is associated</td>
</tr>
<tr>
<td>No. of Groups</td>
<td>The total number of SRLG groups associated with the output</td>
</tr>
</tbody>
</table>
Output Example - static-lsp transit

*A:ALU-2# show router mpls static-lsp transit

MPLS Static LSPs (Transit)

<table>
<thead>
<tr>
<th>In Label</th>
<th>In I/F</th>
<th>Out Label</th>
<th>Out I/F</th>
<th>Next Hop</th>
<th>Adm</th>
<th>Opr</th>
</tr>
</thead>
<tbody>
<tr>
<td>1020</td>
<td>1/1/1</td>
<td>1021</td>
<td>1/1/5</td>
<td>10.10.10.6</td>
<td>Up</td>
<td>Up</td>
</tr>
</tbody>
</table>

LSPs : 1

Output Example - static-lsp terminate

*A:ALU-2# show router mpls static-lsp terminate

MPLS Static LSPs (Terminate)

<table>
<thead>
<tr>
<th>In Label</th>
<th>In Port</th>
<th>Out Label</th>
<th>Out Port</th>
<th>Next Hop</th>
<th>Adm</th>
<th>Opr</th>
</tr>
</thead>
<tbody>
<tr>
<td>131</td>
<td>1/3/1</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>Up</td>
<td>Down</td>
</tr>
<tr>
<td>121</td>
<td>1/2/1</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>Up</td>
<td>Down</td>
</tr>
<tr>
<td>35</td>
<td>1/3/1</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>Up</td>
<td>Down</td>
</tr>
</tbody>
</table>

LSPs : 3

Output Example - static-lsp count

*A:ALU-2# show router mpls static-lsp count

MPLS Static-LSP Count

<table>
<thead>
<tr>
<th>Originate</th>
<th>Transit</th>
<th>Terminate</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

*A:ALU-2# show router mpls static-lsp

Table 20 Show Router MPLS Static LSP Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lsp Name</td>
<td>The name of the LSP used in the path</td>
</tr>
<tr>
<td>To</td>
<td>The system IP address of the egress router for the LSP</td>
</tr>
<tr>
<td>Next Hop</td>
<td>The system IP address of the next hop in the LSP path</td>
</tr>
<tr>
<td>Out Label</td>
<td>The egress label</td>
</tr>
</tbody>
</table>
**status**

**Syntax**

status

**Context**

show>router>mpls

**Description**

This command displays MPLS operation information.

**Output**

The following output is an example of MPLS status information, and Table 21 describes the fields.

**Output Example**

A:ALU-48>show router mpls status
===============================================================================
MPLS Status
===============================================================================
Admin Status : Up Oper Status : Up
Oper Down Reason : n/a Resignal Timer : Disabled
FR Object : Enabled Next Resignal : N/A
Hold Timer : 1 seconds Srlg Frr : Disabled
Srlg Frr Strict : Disabled
Dynamic Bypass : Enabled
LSP Counts | Originate | Transit | Terminate
-------------|-----------|---------|-----------
Static LSPs : 0 0 0
Dynamic LSPs : 0 0 0
Detour LSPs : 0 0 0
===============================================================================

---

**Table 20**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adm</td>
<td>Down — indicates that the path is administratively disabled</td>
</tr>
<tr>
<td></td>
<td>Up — indicates that the path is administratively enabled</td>
</tr>
<tr>
<td>Opr</td>
<td>Down — indicates that the path is operationally down</td>
</tr>
<tr>
<td></td>
<td>Up — indicates that the path is operationally up</td>
</tr>
<tr>
<td>LSPs</td>
<td>The total number of static LSPs</td>
</tr>
<tr>
<td>In Label</td>
<td>The ingress label</td>
</tr>
<tr>
<td>In Port</td>
<td>The ingress port</td>
</tr>
<tr>
<td>Out Port</td>
<td>The egress port</td>
</tr>
<tr>
<td>Up/Down Time</td>
<td>The duration that the LSP is either operationally up or down</td>
</tr>
<tr>
<td>Static-LSP Count</td>
<td>The number of originating, transit, and terminating static LSPs</td>
</tr>
</tbody>
</table>

---

Adm Down — indicates that the path is administratively disabled

Up — indicates that the path is administratively enabled

Opr Down — indicates that the path is operationally down

Up — indicates that the path is operationally up

LSPs The total number of static LSPs

In Label The ingress label

In Port The ingress port

Out Port The egress port

Up/Down Time The duration that the LSP is either operationally up or down

Static-LSP Count The number of originating, transit, and terminating static LSPs
A:ALU-48>config>router>mpls#

### Table 21  
Show Router MPLS Status Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Status</td>
<td>Down — indicates that MPLS is administratively disabled</td>
</tr>
<tr>
<td></td>
<td>Up — indicates that MPLS is administratively enabled</td>
</tr>
<tr>
<td>Oper Status</td>
<td>Down — indicates that MPLS is operationally down</td>
</tr>
<tr>
<td></td>
<td>Up — indicates that MPLS is operationally up</td>
</tr>
<tr>
<td>LSP Counts</td>
<td>Static LSPs — displays the count of static LSPs that originate, transit, and terminate on or through the router</td>
</tr>
<tr>
<td></td>
<td>Dynamic LSPs — displays the count of dynamic LSPs that originate, transit, and terminate on or through the router</td>
</tr>
<tr>
<td></td>
<td>Detour LSPs — displays the count of detour LSPs that originate, transit, and terminate on or through the router</td>
</tr>
<tr>
<td>FR Object</td>
<td>Enabled — specifies that fast reroute object is signaled for the LSP</td>
</tr>
<tr>
<td></td>
<td>Disabled — specifies that fast reroute object is not signaled for the LSP</td>
</tr>
<tr>
<td>Resignal Timer</td>
<td>Enabled — specifies that the resignal timer is enabled for the LSP</td>
</tr>
<tr>
<td></td>
<td>Disabled — specifies that the resignal timer is disabled for the LSP</td>
</tr>
<tr>
<td>Hold Timer</td>
<td>The amount of time that the ingress node holds before programming its data plane and declaring the LSP up to the service module</td>
</tr>
<tr>
<td>Oper Down Reason</td>
<td>The reason that MPLS is operationally down</td>
</tr>
<tr>
<td>Next Resignal</td>
<td>The amount of time until the next resignal for the LSP</td>
</tr>
<tr>
<td>Dynamic Bypass</td>
<td>Indicates whether dynamic bypass is enabled or disabled</td>
</tr>
<tr>
<td>LSP Counts</td>
<td>The number of originate, transit, and terminate LSPs that are static, dynamic, or detour</td>
</tr>
</tbody>
</table>
3.20.2.4 Show Commands (RSVP)

**Note:** The following command outputs are examples only; actual displays may differ depending on supported functionality and user configuration.

interface

**Syntax**

```
interface [ip-int-name | ip-address] statistics [detail]
```

**Context**

```
show>router>rsvp
```

**Description**

This command shows RSVP-TE interface information.

**Parameters**

- **ip-int-name** — identifies the network IP interface. The interface name cannot be in the form of an IP address. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

- **ip-address** — the system or network interface IP address

- **statistics** — the IP address and the number of packets sent and received on an per-interface basis

- **detail** — displays detailed information

**Output**

The following outputs are examples of RSVP-TE interface information:

- RSVP-TE Interface (Output Example, Table 22)
- RSVP-TE Interface Detail (Output Example, Table 23)
- RSVP-TE Interface Statistics (Output Example, Table 24)

**Output Example**

```
A:ALU-12# show router rsvp interface
===============================================================================
RSVP Interfaces
===============================================================================
<table>
<thead>
<tr>
<th>Interface</th>
<th>Total Sessions</th>
<th>Active Sessions</th>
<th>Total BW (Mbps)</th>
<th>Resv BW (Mbps)</th>
<th>Adm Opr</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Up</td>
</tr>
<tr>
<td>ip-10.10.1.1</td>
<td>1</td>
<td>1</td>
<td>100</td>
<td>0</td>
<td>Up</td>
</tr>
<tr>
<td>ip-10.10.2.1</td>
<td>1</td>
<td>1</td>
<td>100</td>
<td>0</td>
<td>Up</td>
</tr>
<tr>
<td>ip-10.10.3.1</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>Up</td>
</tr>
</tbody>
</table>
===============================================================================
Interfaces : 4
===============================================================================
A:ALU-12#
```
### Table 22  Show Router RSVP-TE Interface Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The name of the IP interface</td>
</tr>
<tr>
<td>Total Sessions</td>
<td>The total number of RSVP-TE sessions on this interface. This count includes sessions that are active as well as sessions that have been signaled but a response has not yet been received.</td>
</tr>
<tr>
<td>Active Sessions</td>
<td>The total number of active RSVP-TE sessions on this interface</td>
</tr>
<tr>
<td>Total BW (Mbps)</td>
<td>The amount of bandwidth in megabits per second (Mbps) available to be reserved for the RSVP-TE protocol on the interface</td>
</tr>
<tr>
<td>Resv BW (Mbps)</td>
<td>The amount of bandwidth in megabits per second (Mbps) reserved on this interface. A value of zero (0) indicates that no bandwidth is reserved.</td>
</tr>
<tr>
<td>Adm</td>
<td>Down — the RSVP-TE interface is administratively disabled</td>
</tr>
<tr>
<td></td>
<td>Up — the RSVP-TE interface is administratively enabled</td>
</tr>
<tr>
<td>Opr</td>
<td>Down — the RSVP-TE interface is operationally down</td>
</tr>
<tr>
<td></td>
<td>Up — the RSVP-TE interface is operationally up</td>
</tr>
<tr>
<td>Interfaces</td>
<td>The number of interfaces listed in the display</td>
</tr>
</tbody>
</table>

### Output Example

A: ALU-12# show router rsvp interface "ip-10.10.1.1" detail
----------------------------------
RSVP Interfaces (Detailed): ip-10.10.1.1
----------------------------------
Interface : ip-10.10.1.1
----------------------------------
Interface : ip-10.10.1.1
Port ID : 1/1/1
Admin State : Up  Oper State : Up
Active Sessions : 0  Active Resvs : 0
Total Sessions : 0
Subscription : 10 %  Port Speed : 1000 Mbps
Total BW : 100 Mbps  Aggregate : Disabl
Hello Interval : 3000 ms  Hello Timeouts : 0
Key Type Auth : Disabled
Keychain Auth : Disabled
Auth Rx Seq Num : n/a  Auth Key Id : n/a
Auth Tx Seq Num : n/a  Auth Win Size : n/a
Refresh Reduc. : Disabled  Reliable Deli. : Disabled
Bfd Enabled : No  Graceful Shut. : Disabled
ImplicitNullLabel : Disabled*  GR helper : Disabled
IGP Update
Table 23  Show Router RSVP-TE Interface Detail Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The name of the IP interface</td>
</tr>
<tr>
<td>Port ID</td>
<td>The physical port bound to the interface</td>
</tr>
<tr>
<td>Admin State</td>
<td>Down — the RSVP-TE interface is administratively disabled</td>
</tr>
<tr>
<td></td>
<td>Up — the RSVP-TE interface is administratively enabled</td>
</tr>
<tr>
<td>Oper State</td>
<td>Down — the RSVP-TE interface is operationally down</td>
</tr>
<tr>
<td></td>
<td>Up — the RSVP-TE interface is operationally up</td>
</tr>
<tr>
<td>Active Sessions</td>
<td>The total number of active RSVP-TE sessions on this interface</td>
</tr>
<tr>
<td>Active Resvs</td>
<td>The total number of active RSVP-TE sessions that have reserved bandwidth</td>
</tr>
<tr>
<td>Total Sessions</td>
<td>The total number of RSVP-TE sessions on this interface. This count includes sessions that are active as well as sessions that have been signaled but a response has not yet been received.</td>
</tr>
<tr>
<td>Subscription</td>
<td>The percentage of the link bandwidth that RSVP-TE can use for reservation. When the value is zero (0), no new sessions are permitted on this interface.</td>
</tr>
<tr>
<td>Port Speed</td>
<td>The speed on the interface</td>
</tr>
<tr>
<td>Total BW</td>
<td>The amount of bandwidth in megabits per second (Mbps) available to be reserved for the RSVP-TE protocol on this interface</td>
</tr>
<tr>
<td>Aggregate</td>
<td>Indicates whether aggregate messages are sent. Aggregate messages are used to pack multiple RSVP messages into a single packet to reduce the network overhead. When the value is true, RSVP negotiates with each neighbor and gets consensus before sending aggregate messages.</td>
</tr>
</tbody>
</table>
### Table 23: Show Router RSVP-TE Interface Detail Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello Interval</td>
<td>The length of time, in seconds, between the Hello packets that the router sends on the interface. This value must be the same for all routers attached to a common network. A value of zero (0) indicates that the sending of hello messages is disabled. A value of n/a indicates that the interface is an unnumbered interface.</td>
</tr>
<tr>
<td>Hello Timeouts</td>
<td>The total number of Hello messages that timed out on this RSVP-TE interface. A value of n/a indicates that the interface is an unnumbered interface.</td>
</tr>
<tr>
<td>Auth Rx Seq Num</td>
<td>The received MD5 sequence number</td>
</tr>
<tr>
<td>Auth Key Id</td>
<td>The MD5 key identifier</td>
</tr>
<tr>
<td>Auth Tx Seq Num</td>
<td>The transmitted MD5 sequence number</td>
</tr>
<tr>
<td>Auth Win Size</td>
<td>The MD5 window size</td>
</tr>
<tr>
<td>Refresh Reduc.</td>
<td>Indicates whether refresh reduction capabilities are enabled or disabled</td>
</tr>
<tr>
<td>Reliable Deli.</td>
<td>Indicates whether reliable delivery is enabled or disabled</td>
</tr>
<tr>
<td>Bfd Enabled</td>
<td>Indicates whether BFD is enabled or disabled on the RSVP-TE interface. A value of n/a indicates that BFD is not applicable because the interface is an unnumbered interface.</td>
</tr>
<tr>
<td>Graceful Shut.</td>
<td>Indicates whether graceful shutdown is enabled or disabled</td>
</tr>
<tr>
<td>ImplicitNullLabel</td>
<td>Indicates whether the implicit null label is enabled or disabled</td>
</tr>
<tr>
<td>GR helper</td>
<td>Indicates whether Graceful-Restart Helper is enabled or disabled</td>
</tr>
<tr>
<td><strong>IGP Update</strong></td>
<td></td>
</tr>
<tr>
<td>Up Thresholds (%)</td>
<td>Indicates up threshold levels for the interface</td>
</tr>
<tr>
<td>Down Thresholds (%)</td>
<td>Indicates down threshold levels for the interface</td>
</tr>
<tr>
<td>IGP Update Pending</td>
<td>Indicates whether an IGP update will occur</td>
</tr>
<tr>
<td>Next Update</td>
<td>Indicates when the next IGP update will be, if there is one pending</td>
</tr>
</tbody>
</table>
Output Example

A:ALU-12# show router rsvp interface statistics

===============================================================================
RSVP Interface (statistics)
===============================================================================
Interface system
-------------------------------------------------------------------------------
Interface : Up
Total Packets (Sent) : 0 (Recd.): 0
Bad Packets (Sent) : 0 (Recd.): 0
Paths (Sent) : 0 (Recd.): 0
Path Errors (Sent) : 0 (Recd.): 0
Path Tears (Sent) : 0 (Recd.): 0
Resvs (Sent) : 0 (Recd.): 0
Resv Confirms (Sent) : 0 (Recd.): 0
Resv Errors (Sent) : 0 (Recd.): 0
Resv Tears (Sent) : 0 (Recd.): 0
Refresh Summaries (Sent) : 0 (Recd.): 0
Refresh Acks (Sent) : 0 (Recd.): 0
Bundle Packets (Sent) : 0 (Recd.): 0
Hellos (Sent) : 0 (Recd.): 0
Auth Errors (Sent) : 0 (Recd.): 0
-------------------------------------------------------------------------------

Table 24 Show Router RSVP-TE Interface Statistics Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The name of the IP interface displayed in the header</td>
</tr>
<tr>
<td>Interface (status)</td>
<td>The status of the interface (up or down)</td>
</tr>
<tr>
<td>Sent</td>
<td>The total number of error-free RSVP-TE packets that have been transmitted on the RSVP-TE interface</td>
</tr>
<tr>
<td>Recd</td>
<td>The total number of error-free RSVP-TE packets received on the RSVP-TE interface</td>
</tr>
<tr>
<td>Total Packets</td>
<td>The total number of RSVP-TE packets, including errors, received on the RSVP-TE interface</td>
</tr>
<tr>
<td>Bad Packets</td>
<td>The total number of RSVP-TE packets with errors transmitted on the RSVP-TE interface</td>
</tr>
<tr>
<td>Paths</td>
<td>The total number of RSVP-TE PATH messages received on the RSVP-TE interface</td>
</tr>
<tr>
<td>Path Errors</td>
<td>The total number of RSVP-TE PATH ERROR messages transmitted on the RSVP-TE interface</td>
</tr>
<tr>
<td>Path Tears</td>
<td>The total number of RSVP-TE PATH TEAR messages received on the RSVP-TE interface</td>
</tr>
</tbody>
</table>
**Syntax**
neighbor [ip-address] [detail]

**Context**
show>router>rsvp

**Description**
This command displays RSVP-TE neighbors.

**Parameters**
- **ip-address** — the IP address of the originating router
- **detail** — displays detailed information

**Output**
The following output is an example of RSVP-TE neighbor information, and Table 24 describes the fields.

**Output Example**
*A:ALU-12>show>router>rsvp# neighbor
===============================================================================
RSVP Neighbors
===============================================================================
Legend :

**Table 24**  Show Router RSVP-TE Interface Statistics Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resvs</td>
<td>The total number of RSVP-TE RESV messages received on the RSVP-TE interface</td>
</tr>
<tr>
<td>Resv Confirms</td>
<td>The total number of RSVP-TE RESV CONFIRM messages received on the RSVP-TE interface</td>
</tr>
<tr>
<td>Resv Errors</td>
<td>The total number of RSVP-TE RESV ERROR messages received on the RSVP-TE interface</td>
</tr>
<tr>
<td>Resv Tears</td>
<td>The total number of RSVP-TE RESV TEAR messages received on the RSVP-TE interface</td>
</tr>
<tr>
<td>Refresh Summaries</td>
<td>The total number of RSVP-TE RESV summary refresh messages received on the RSVP-TE interface</td>
</tr>
<tr>
<td>Refresh Acks</td>
<td>The total number of RSVP-TE RESV acknowledgment messages received when refresh reduction is enabled on the RSVP-TE interface</td>
</tr>
<tr>
<td>Bundle Packets</td>
<td>The total number of RSVP-TE RESV bundle packets received on the RSVP-TE interface</td>
</tr>
<tr>
<td>Hellos</td>
<td>The total number of RSVP-TE RESV HELLO REQ messages received on the RSVP-TE interface</td>
</tr>
<tr>
<td>Auth Errors</td>
<td>The number of authentication errors</td>
</tr>
</tbody>
</table>
**Table 25** Show Router RSVP-TE Neighbor Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>The IP address of the RSVP-TE neighbor</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface ID of the RSVP-TE neighbor</td>
</tr>
<tr>
<td>Hello</td>
<td>The status of the Hello message</td>
</tr>
<tr>
<td>Last Oper Change</td>
<td>The time of the last operational change to the connection</td>
</tr>
<tr>
<td>Flags</td>
<td>Any flags associated with the connection to the neighbor</td>
</tr>
</tbody>
</table>

**session**

**Syntax**

```
session [session-type] [from ip-address | to ip-address | lsp-name name] [status {up | down}] [detail]
```

**Context**

`show>router>rsvp`

**Description**

This command shows RSVP-TE session information.

**Parameters**

`session-type` — specifies the session type

**Values**

- originate, transit, terminate, detour, detour-transit, detour-terminate, bypass-tunnel, manual-bypass

`from ip-address` — specifies the IP address of the originating router

`to ip-address` — specifies the IP address of the egress router

`name` — specifies the name of the LSP used in the path

`status up` — specifies to display a session that is operationally up

`status down` — specifies to display a session that is operationally down

`detail` — displays detailed information

**Output**

The following output is an example of RSVP-TE session information, and Table 26 describes the fields.
Output Example

A:ALU-12# show router rsvp session
===============================================================================
RSVP Sessions
===============================================================================
From To Tunnel LSP Name State
ID ID ID
-------------------------------------------------------------------------------
10.20.1.3 10.20.1.1 1 37 C_A_1::C_A_1 Up
10.20.1.3 10.20.1.1 2 38 C_A_2::C_A_2 Up
10.20.1.3 10.20.1.1 3 39 C_A_3::C_A_3 Up
10.20.1.3 10.20.1.1 4 40 C_A_4::C_A_4 Up
10.20.1.1 10.20.1.3 2 40 A_C_2::A_C_2 Up
10.20.1.1 10.20.1.3 3 41 A_C_3::A_C_3 Up
10.20.1.1 10.20.1.3 4 42 A_C_4::A_C_4 Up
10.20.1.1 10.20.1.3 5 43 A_C_5::A_C_5 Up
10.20.1.1 10.20.1.3 6 44 A_C_6::A_C_6 Up
10.20.1.1 10.20.1.3 7 45 A_C_7::A_C_7 Up
10.20.1.1 10.20.1.3 8 46 A_C_8::A_C_8 Up
10.20.1.3 10.20.1.1 5 41 C_A_5::C_A_5 Up
10.20.1.3 10.20.1.1 6 42 C_A_6::C_A_6 Up
10.20.1.3 10.20.1.1 7 43 C_A_7::C_A_7 Up
10.20.1.3 10.20.1.1 8 44 C_A_8::C_A_8 Up
...

Sessions : 65
===============================================================================
A:ALU-12#

A:ALU-12# show router rsvp session lsp-name A_C_2::A_C_2 status up
===============================================================================
RSVP Sessions
===============================================================================
From To Tunnel LSP Name State
ID ID ID
-------------------------------------------------------------------------------
10.20.1.3 10.20.1.1 2 40 A_C_2::A_C_2 Up

Sessions : 1
===============================================================================
A:ALU-12#

Table 26   Show Router RSVP-TE Session Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>The IP address of the originating router</td>
</tr>
<tr>
<td>To</td>
<td>The IP address of the egress router</td>
</tr>
<tr>
<td>Tunnel ID</td>
<td>The ID of the ingress node of the tunnel supporting this RSVP-TE session</td>
</tr>
<tr>
<td>LSP ID</td>
<td>The ID assigned by the agent to this RSVP-TE session</td>
</tr>
</tbody>
</table>
**Table 26** Show Router RSVP-TE Session Output Fields (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The administrative name assigned to the RSVP-TE session by the agent</td>
</tr>
<tr>
<td>State</td>
<td>Down — the operational state of this RSVP-TE session is down</td>
</tr>
<tr>
<td></td>
<td>Up — the operational state of this RSVP-TE session is up</td>
</tr>
</tbody>
</table>

**statistics**

**Syntax**

```plaintext
statistics
```

**Context**

```plaintext
show>router>rsvp
```

**Description**

This command displays global statistics in the RSVP-TE instance.

**Output**

The following output is an example of RSVP-TE statistics information, and Table 27 describes the fields.

**Output Example**

```
A:ALU-12# show router rsvp statistics
=======================================================================
RSVP Global Statistics
=======================================================================
PATH Timeouts : 0
RESV Timeouts : 0
GR Helper PATH Tim*: 0
GR Helper RESV Tim*: 0
=======================================================================
```

**Table 27** Show Router RSVP-TE Statistics Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PATH Timeouts</td>
<td>The total number of PATH timeouts</td>
</tr>
<tr>
<td>RESV Timeouts</td>
<td>The total number of RESV timeouts</td>
</tr>
<tr>
<td>GR Helper PATH Timeouts</td>
<td>The total number of graceful restart helper PATH timeouts</td>
</tr>
<tr>
<td>GR Helper RESV Timeouts</td>
<td>The total number of graceful restart helper RESV timeouts</td>
</tr>
</tbody>
</table>
status

Syntax

status

Context

show>router>rsvp

Description

This command displays RSVP-TE operational status.

Output

The following output is an example of RSVP-TE status information, and Table 28 describes the fields.

Output Example

A:ALU-12# show router rsvp status
===============================================================================
<table>
<thead>
<tr>
<th>RSVP Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Status : Down</td>
</tr>
<tr>
<td>Keep Multiplier : 3</td>
</tr>
<tr>
<td>Message Pacing : Disabled</td>
</tr>
<tr>
<td>Max Packet Burst : 650 msgs</td>
</tr>
<tr>
<td>Rapid Retransmit : 5 hmsec</td>
</tr>
<tr>
<td>Graceful Shutdown : Disabled</td>
</tr>
<tr>
<td>GR Max Recovery : 300 sec</td>
</tr>
<tr>
<td>Implicit Null Label: Disabled</td>
</tr>
<tr>
<td>P2P Merge Point Ab*: Disabled</td>
</tr>
<tr>
<td>DiffServTE AdmModel: Basic</td>
</tr>
<tr>
<td>Percent Link Bw CT0: 100</td>
</tr>
<tr>
<td>Percent Link Bw CT1: 0</td>
</tr>
<tr>
<td>Percent Link Bw CT2: 0</td>
</tr>
<tr>
<td>Percent Link Bw CT3: 0</td>
</tr>
<tr>
<td>TE0 -&gt; Class Type : 0</td>
</tr>
<tr>
<td>TE1 -&gt; Class Type : 0</td>
</tr>
<tr>
<td>TE2 -&gt; Class Type : 0</td>
</tr>
<tr>
<td>TE3 -&gt; Class Type : 0</td>
</tr>
<tr>
<td>TE4 -&gt; Class Type : 0</td>
</tr>
<tr>
<td>TE5 -&gt; Class Type : 0</td>
</tr>
<tr>
<td>TE6 -&gt; Class Type : 0</td>
</tr>
<tr>
<td>TE7 -&gt; Class Type : 0</td>
</tr>
<tr>
<td>IgpThresholdUpdate : Disabled</td>
</tr>
<tr>
<td>Up Thresholds(%) : 0 15 30 45 60 75 80 85 90 95 96 97 98 99 100</td>
</tr>
<tr>
<td>Down Thresholds(%) : 100 99 98 97 96 95 90 85 80 75 60 45 30 15 0</td>
</tr>
<tr>
<td>Update Timer : N/A</td>
</tr>
<tr>
<td>Update on CAC Fail : Disabled</td>
</tr>
</tbody>
</table>
===============================================================================

Table 28

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Status</td>
<td>Down — RSVP-TE is administratively disabled</td>
</tr>
<tr>
<td></td>
<td>Up — RSVP-TE is administratively enabled</td>
</tr>
</tbody>
</table>
### Table 28  Show Router RSVP-TE Status Output Fields  (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oper Status</td>
<td>Down — RSVP-TE is operationally down</td>
</tr>
<tr>
<td></td>
<td>Up — RSVP-TE is operationally up</td>
</tr>
<tr>
<td>Keep Multiplier</td>
<td>The <code>keep-multiplier number</code> used by RSVP-TE to declare that a reservation is down or the neighbor is down</td>
</tr>
<tr>
<td>Refresh Time</td>
<td>The <code>refresh-time interval</code>, in seconds, between the successive PATH and RESV refresh messages</td>
</tr>
<tr>
<td>Message Pacing</td>
<td>Enabled — RSVP-TE messages, specified in the <code>max-burst</code> command, are sent in a configured interval, specified in the <code>period</code> command</td>
</tr>
<tr>
<td></td>
<td>Disabled — message pacing is disabled. RSVP-TE message transmission is not regulated.</td>
</tr>
<tr>
<td>Pacing Period</td>
<td>The time interval, in milliseconds, during which the router can send the number of RSVP-TE messages specified in the <code>max-burst</code> command</td>
</tr>
<tr>
<td>Max Packet Burst</td>
<td>The maximum number of RSVP-TE messages that are sent under normal operating conditions in the period specified</td>
</tr>
<tr>
<td>Refresh Bypass</td>
<td>Enabled — the <code>refresh-reduction-over-bypass</code> command is enabled</td>
</tr>
<tr>
<td></td>
<td>Disabled — the <code>refresh-reduction-over-bypass</code> command is disabled</td>
</tr>
<tr>
<td>Rapid Retransmit</td>
<td>The time interval for the rapid retransmission time, which is used in the retransmission mechanism that handles unacknowledged message_id objects (the units “hmsec” represent hundreds of msec; for example, 5 hmsec represents 500 msec)</td>
</tr>
<tr>
<td>Rapid Retry Limit</td>
<td>The value of the rapid retry limit, which is used in the retransmission mechanism that handles unacknowledged message_id objects</td>
</tr>
<tr>
<td>Graceful Shutdown</td>
<td>Specifies whether graceful shutdown of the RSVP node is enabled</td>
</tr>
</tbody>
</table>
### 3.20.2.5 Clear Commands

#### interface

**Syntax**
```
interface [ip-int-name] [statistics]
```

**Context**
clear>router>mpls

**Description**
This command resets or clears statistics for MPLS interfaces.

**Parameters**
- `ip-int-name` — specifies an existing IP interface. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
- `statistics` — clears only statistics

#### lsp

**Syntax**
```
lsp [lsp-name]
```

**Context**
clear>router>mpls

**Description**
This command resets and restarts an LSP.

**Parameters**
- `lsp-name` — specifies the name of the LSP to clear

#### interface

**Syntax**
```
interface [ip-int-name] [statistics]
```

**Context**
clear>router>rsvp

**Description**
This command resets or clears statistics for an RSVP-TE interface.

**Parameters**
- `ip-int-name` — identifies the IP interface to clear. The interface name cannot be in the form of an IP address. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes
- `statistics` — clears only statistics
statistics

**Syntax**    statistics

**Context**   clear>router>rsvp

**Description**  This command clears global statistics for the RSVP-TE instance; for example, clears *path* and *resv timeout* counters.
### 3.20.2.6 Debug Commands

**mpls**

**Syntax**

```text
[no] mpls [lsp lsp-name] [sender source-address] [endpoint endpoint-address] [tunnel-id tunnel-id] [lsp-id lsp-id] [interface ip-int-name]
```

**Context**

`debug>router`

**Description**

This command enables and configures debugging for MPLS.

**Parameters**

- `lsp-name` — the name that identifies the LSP. The LSP name can be up to 32 characters long and must be unique.
- `source-address` — specifies the system IP address of the sender
- `endpoint-address` — specifies the far-end system IP address
- `tunnel-id` — specifies the MPLS SDP ID
  - **Values**
    - 0 to 4294967295
- `lsp-id` — specifies the LSP ID
  - **Values**
    - 1 to 65535
- `ip-int-name` — identifies the interface. The interface name cannot be in the form of an IP address. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (», $, spaces, etc.), the entire string must be enclosed within double quotes.

**event**

**Syntax**

```text
[no] event
```

**Context**

`debug>router>mpls`

`debug>router>rsvp`

**Description**

This command enables debugging for specific events.

The `no` form of the command disables the debugging.
all

**Syntax**

all [detail]
no all

**Context**

degue-router>mpls>event
degue-router>rsvp>event

**Description**

This command debugs all events.

The **no** form of the command disables the debugging.

**Parameters**

detail — displays detailed information about all events

frr

**Syntax**

frr [detail]
no frr

**Context**

degue-router>mpls>event

**Description**

This command debugs fast reroute events.

The **no** form of the command disables the debugging.

**Parameters**

detail — displays detailed information about reroute events

iom

**Syntax**

iom [detail]
no iom

**Context**

degue-router>mpls>event

**Description**

This command debugs MPLS IOM events.

The **no** form of the command disables the debugging.

**Parameters**

detail — displays detailed information about MPLS IOM events

lsp-setup

**Syntax**

lsp-setup [detail]
no lsp-setup

**Context**

degue-router>mpls>event
**Description**

This command debugs LSP setup events.

The `no` form of the command disables the debugging.

**Parameters**

detail — displays detailed information about LSP setup events

---

**mbb**

**Syntax**

`mbb [detail]`

`no mbb`

**Context**

debug>router>mpls>event

**Description**

This command debugs the state of the most recent invocation of the make-before-break (MBB) functionality.

The `no` form of the command disables the debugging.

**Parameters**

detail — displays detailed information about MBB events

---

**misc**

**Syntax**

`misc [detail]`

`no misc`

**Context**

debug>router>mpls>event

debug>router>rsvp>event

**Description**

This command debugs miscellaneous events.

The `no` form of the command disables the debugging.

**Parameters**

detail — displays detailed information about miscellaneous events

---

**XC**

**Syntax**

`xc [detail]`

`no xc`

**Context**

debug>router>mpls>event

**Description**

This command debugs cross-connect events.

The `no` form of the command disables the debugging.

**Parameters**

detail — displays detailed information about cross-connect events
**rsvp**

**Syntax**

```
[no] rsvp [lsp lsp-name] [sender sender-address] [endpoint endpoint-address] [tunnel-id tunnel-id] [lsp-id lsp-id] [interface ip-int-name]
```

**Context**

```
debug>router
```

**Description**

This command enables and configures debugging for RSVP.

**Parameters**

- **lsp-name** — name that identifies the LSP. The LSP name can be up to 80 characters long and must be unique.
- **sender-address** — specifies the system IP address of the sender (a.b.c.d)
- **endpoint-address** — specifies the far-end system IP address (a.b.c.d)
- **tunnel-id** — specifies the RSVP-TE tunnel ID
  - **Values**
    - 0 to 4294967295
- **lsp-id** — specifies the LSP ID
  - **Values**
    - 1 to 65535
- **ip-int-name** — identifies the interface. The interface name cannot be in the form of an IP address. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

**auth**

**Syntax**

```
auth
no auth
```

**Context**

```
debug>router>rsvp>event
```

**Description**

This command debugs authentication events.

The **no** form of the command disables the debugging.

**Parameters**

- **detail** — displays detailed information about authentication events

**nbr**

**Syntax**

```
nbr [detail]
no nbr
```

**Context**

```
debug>router>rsvp>event
```

**Description**

This command debugs neighbor events.
The **no** form of the command disables the debugging.

**Parameters**
- `detail` — displays detailed information about neighbor events

### path

**Syntax**
```
path [detail]
no path
```

**Context**
`debug>router>rsvp>event`

**Description**
This command debugs path-related events.

The **no** form of the command disables the debugging.

**Parameters**
- `detail` — displays detailed information about path-related events

### resv

**Syntax**
```
resv [detail]
no resv
```

**Context**
`debug>router>rsvp>event`

**Description**
This command debugs RSVP-TE reservation events.

The **no** form of the command disables the debugging.

**Parameters**
- `detail` — displays detailed information about RSVP-TE reservation events

### rr

**Syntax**
```
rr
no rr
```

**Context**
`debug>router>rsvp>event`

**Description**
This command debugs refresh reduction events.

The **no** form of the command disables the debugging.

**Parameters**
- `detail` — displays detailed information about refresh reduction events
packet

Syntax  
[no] packet

Context  
debug>router>rsvp

Description  
This command enters the context to debug packets.

ack

Syntax  
ack [detail]
no ack

Context  
debug>router>rsvp>packet

Description  
This command debugs ack packets.

The no form of the command disables the debugging.

Parameters  
detail — displays detailed information about RSVP-TE ack packets

all

Syntax  
all [detail]
no all

Context  
debug>router>rsvp>packet

Description  
This command debugs all packets.

The no form of the command disables the debugging.

Parameters  
detail — displays detailed information about all RSVP-TE packets

bundle

Syntax  
bundle [detail]
no bundle

Context  
debug>router>rsvp>packet

Description  
This command debugs bundle packets.

The no form of the command disables the debugging.

Parameters  
detail — displays detailed information about RSVP-TE bundle packets
### hello

**Syntax**
```
hello [detail]
no hello
```

**Context**
debug>router>rsvp>packet

**Description**
This command debugs hello packets.

The `no` form of the command disables the debugging.

**Parameters**
- `detail` — displays detailed information about hello packets

### path

**Syntax**
```
path [detail]
no path
```

**Context**
debug>router>rsvp>packet

**Description**
This command enables debugging for RSVP-TE path packets.

The `no` form of the command disables the debugging.

**Parameters**
- `detail` — displays detailed information about path-related events

### patherr

**Syntax**
```
patherr [detail]
no patherr
```

**Context**
debug>router>rsvp>packet

**Description**
This command debugs path error packets.

The `no` form of the command disables the debugging.

**Parameters**
- `detail` — displays detailed information about path error packets

### path Tear

**Syntax**
```
pathtear [detail]
no pathtear
```

**Context**
debug>router>rsvp>packet

**Description**
This command debugs path tear packets.
The no form of the command disables the debugging.

Parameters

detail — displays detailed information about path tear packets

resv

Syntax
resv [detail]
no resv

Context debug>router>rsvp>packet

Description
This command enables debugging for RSVP-TE RESV packets.

The no form of the command disables the debugging.

Parameters
detail — displays detailed information about RSVP-TE RESV packets

resverr

Syntax
resverr [detail]
no resverr

Context debug>router>rsvp>packet

Description
This command debugs ResvErr packets.

The no form of the command disables the debugging.

Parameters
detail — displays detailed information about ResvErr packets

resvtear

Syntax
resvtear [detail]
no resvtear

Context debug>router>rsvp>packet

Description
This command debugs ResvTear packets.

The no form of the command disables the debugging.

Parameters
detail — displays detailed information about ResvTear packets
srefresh

**Syntax**  
srefresh [detail]  
no srefesh

**Context**  
debug>router>rsvp>packet

**Description**  
This command debugs srefesh packets.

The no form of the command disables the debugging.

**Parameters**  
detail — displays detailed information about RSVP-TE srefesh packets
4 PCEP

This section contains information on the following topics:

- Introduction to the Path Computation Element (PCE) Communication Protocol (PCEP)
- Base Implementation of Path Computation Elements (PCE)
- PCEP Session Establishment and Maintenance
- PCEP Parameters
- PCEP Support for RSVP-TE LSPs
- LSP Path Diversity and Bidirectionality Constraints
- Configuring RSVP-TE LSPs with PCEP Using the CLI
- PCEP Configuration Command Reference
4.1 Introduction to the Path Computation Element (PCE) Communication Protocol (PCEP)

Note: The 7705 SAR operates as a PCE Client (PCC) only, supporting PCC capabilities for RSVP-TE LSPs. References to PCE router operation and SR-TE LSPs apply to the 7750 SR product family and are included for informational purposes only.

The Path Computation Element Communication Protocol (PCEP) is one of several protocols used for communication between a wide area network (WAN) software-defined network (SDN) controller and network elements.

The Nokia WAN SDN Controller is known as the Network Services Platform (NSP). The NSP is a set of applications which are built on a common framework that hosts and integrates them by providing common functions. The applications are developed in a Java environment.

The NSP provides two major functions:

• programmable multi-vendor service provisioning
• network resource control, including resource management at Layer 0 (optical path), Layer 1 (ODU path), Layer 2 (MPLS tunnel), and at the IP flow level

The network discovery and control function implements a common set of standards-based southbound interfaces to the network elements for both topology discovery and tunnel and flow programming. A virtual 7705 SAR (vSAR) applies the southbound interfaces to the network elements and the adaptation layer to the applications. The southbound interfaces include IGP and the Network Functions Manager - Packet (NFM-P) for topology discovery, PCEP for handling path computation requests and LSP state updates with the network elements, and forwarding plane programming protocols such as Openflow, BGP flowspec, and I2RS.

The above NSP functions are provided in a number of modules that can be used together or separately as illustrated in Figure 14.
The two main components of the NSP are:

- **Network Services Director (NSD)**
  
  The NSD is a programmable and multi-vendor service provisioning tool providing a single and simple API to the user and OSS. It implements a service model abstraction and adapts to each vendor-specific service model. It supports provisioning services such as E-Line, E-LAN, E-Tree, Layer 3 VPN, traffic steering, and service chaining.

- **Network Resource Controller (NRC)**
  
  The NRC implements separate modules for computing and managing optimal paths for optical tunnels (NRC-T) and MPLS tunnels (NRC-P), and for computing optimal routing and placement of IP flows (NRC-F). In addition, a resource controller for inter-layer IP and optical path computation and more complex inter-domain MPLS path computation is provided as part of the NRC-X.
The Network Resource Controller - Packet (NRC-P) implements the stateful Path Computation Element (PCE) for packet networks. Figure 15 illustrates the NRC-P architecture and its main components.

**Figure 15** NRC-P Architecture

The NRC-P has the following architecture:

- a single Virtual Machine (VM) handling the Java implementation of an MPLS path computation engine, a TE graph database, and an LSP database
- a plug-in adapter with the Nokia CPROTO interface, providing reliable, TCP-based message delivery between vSAR and Java-VM. The plug-in adapter implements a compact encoding/decoding (codec) function for the message content using Google ProtoBuf. Google ProtoBuf also provides for automatic C++ (vSAR side) and Java (Java-VM side) code generation to process the exchanged message content.
- a single VM running a vSAR image that handles the functions of topology discovery of multiple IGP instances and areas via IGP and NFM-P. For larger network domains, one VM running the vSAR image can be dedicated to a specific function.
The PCE module uses PCEP to communicate with its PCE Clients (PCCs). It also uses PCEP to communicate with other PCEs to coordinate inter-domain path computation. Each router acting as a PCC initiates a PCEP session to the PCE in its domain.

When the user enables PCE control for one or more segment routing (SR) or RSVP-TE LSPs, the PCE owns the path updating and periodic reoptimization of the LSPs. In this case, the PCE acts in an active stateful role. The PCE can also act in a passive stateful role for other LSPs on the router by discovering the LSPs and taking into account their resource consumption when computing the path for the LSPs it has control ownership of.

The following is a high-level description of the PCE and PCC capabilities:

- base PCEP implementation, as per RFC 5440
- active and passive stateful PCE LSP update, as per draft-ietf-pce-stateful-pce
- delegation of LSP control to the PCE
- synchronization of the LSP database with network elements for PCE-controlled LSPs and network element-controlled LSPs
- support for PCC-initiated LSPs, as per draft-ietf-pce-stateful-pce
- support for LSP path diversity across different LERs using extensions to the PCE path profile, as per draft-alvarez-pce-path-profiles
- support for LSP path bidirectionality constraints using extensions to the PCE path profile, as per draft-alvarez-pce-path-profiles
4.2 Base Implementation of Path Computation Elements (PCE)

The base implementation of the PCE uses the PCEP extensions defined in RFC 5440.

The main functions of PCEP are:

- PCEP session establishment, maintenance, and closing
- path computation requests using the PCReq message
- path computation replies using the PCRep message
- notification messages (PCNtf) by which the PCEP speaker can inform its peer about events, such as path request cancellation by the PCC or path computation cancellation by the PCE
- error messages (PCErr) by which the PCEP speaker can inform its peer about errors related to processing requests, message objects, or TLVs

Table 29 lists the base PCEP TLVs, objects, and messages.

<table>
<thead>
<tr>
<th>TLV, Object, or Message</th>
<th>Contained in Object</th>
<th>Contained in Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPEN Object</td>
<td>N/A</td>
<td>OPEN, PCErr</td>
</tr>
<tr>
<td>Request Parameter (RP) Object</td>
<td>N/A</td>
<td>PCReq, PCRep, PCErr, PCNtf</td>
</tr>
<tr>
<td>NO-PATH Object</td>
<td>N/A</td>
<td>PCRep</td>
</tr>
<tr>
<td>END-POINTS Object</td>
<td>N/A</td>
<td>PCReq</td>
</tr>
<tr>
<td>BANDWIDTH Object</td>
<td>N/A</td>
<td>PCReq, PCRep, PCRpt¹</td>
</tr>
<tr>
<td>METRIC Object</td>
<td>N/A</td>
<td>PCReq, PCRep, PCRpt¹</td>
</tr>
<tr>
<td>Explicit Route Object (ERO)</td>
<td>N/A</td>
<td>PCRep</td>
</tr>
<tr>
<td>Reported Route Object (RRO)</td>
<td>N/A</td>
<td>PCReq</td>
</tr>
<tr>
<td>LSPA Object</td>
<td>N/A</td>
<td>PCReq, PCRep, PCRpt¹</td>
</tr>
<tr>
<td>Include Route Object (IRO)</td>
<td>N/A</td>
<td>PCReq, PCRep</td>
</tr>
<tr>
<td>SVEC Object</td>
<td>N/A</td>
<td>PCReq</td>
</tr>
<tr>
<td>NOTIFICATION Object</td>
<td>N/A</td>
<td>PCNtf</td>
</tr>
</tbody>
</table>
The behavior and limitations of the implementation of the objects in Table 29 are as follows.

- The PCE treats all supported objects received in a PCReq message as mandatory, regardless of whether the P-flag in the object’s common header is set (mandatory object) or not (optional object).
- The PCC implementation will always set the B-flag (B=1) in the metric object containing the hop metric value, which means that a bound value must be included in PCReq message. The PCE returns the computed value in the PCRep message with flags set identically to the PCReq message.
- The PCC implementation will always set flags B=0 and C=1 in the metric object for the IGP or TE metric values in the PCReq message. This means that the request is to optimize (minimize) the metric without providing a bound value. The PCE returns the computed value in the PCRep message with flags set identically to the PCReq message.
- The IRO and LOAD-BALANCING objects are not part of the NSP PCE feature. If the PCE receives a PCReq message with one or more of these objects, it will ignore them regardless of the setting of the P-flag, and will process the path computations normally.
- The LSPA, metric, and bandwidth objects are also included in the PCRpt message. The inclusion of these objects in the PCRpt message is proprietary to Nokia.

The following features are not supported on the 7705 SAR:

- PCE discovery using IS-IS, per RFC 5089, and OSPF, per RFC 5088, along with corresponding extensions for discovering stateful PCE, per draft-sivabalapce-disco-stateful
- security of the PCEP session using MD5 or TLS between PCEP peers
- PCEP synchronization optimization as per draft-ietf-pce-stateful-sync-optimizations

**Note:**
1. Nokia proprietary

### Table 29  Base PCEP TLVs, Objects, and Messages (Continued)

<table>
<thead>
<tr>
<th>TLV, Object, or Message</th>
<th>Contained in Object</th>
<th>Contained in Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCEP-ERROR Object</td>
<td>N/A</td>
<td>PCErr</td>
</tr>
<tr>
<td>LOAD-BALANCING Object</td>
<td>N/A</td>
<td>PCReq</td>
</tr>
<tr>
<td>CLOSE Object</td>
<td>N/A</td>
<td>CLOSE</td>
</tr>
</tbody>
</table>
• support of end-to-end secondary backup paths for an LSP. PCE standards do not currently support an LSP container with multiple paths, and the PCE treats each request as a path with a unique PLSP-ID. It is up to the router to tie the two paths together to create 1:1 protection and to request path or SRLG diversity among them when it makes the request to the PCE.

• jitter, latency, and packet loss metrics support as per RFC 7471 and draft-ietf-isis-te-metric-extensions, and their use in the PCE metric object as per draft-ietf-pce-pcep-service-aware
4.3 PCEP Session Establishment and Maintenance

PCEP operates over TCP using destination TCP port 4189. The PCC always initiates the connection. When the user configures the PCEP local address and the peer address on the PCC, the PCC initiates a TCP connection to the PCE. When a connection is established, the PCC and PCE exchange OPEN messages, which initializes the PCEP session and exchanges the session parameters to be negotiated.

The PCC always checks first to determine if the remote PCE address is reachable out-of-band via the management port. If the remote address is not reachable, the PCC will try to reach the remote PCE address in-band. When the session comes up out-of-band, the system IP address is always used; the local address configured by the user is ignored and is only used for an in-band session.

A keepalive mechanism is used as an acknowledgment of the acceptance of the session within the negotiated parameters. It is also used as a maintenance function to detect whether or not the PCEP peer is still alive.

The negotiated parameters include the keepalive timer and the dead timer, and one or more PCEP capabilities such as support of stateful PCE and the LSP Path type.

The PCEP session initialization steps are illustrated in Figure 16.

**Figure 16 PCEP Session Initialization**
If the session to the PCE times out, the router acting as a PCC keeps the last successfully programmed path provided by the PCE until the session to the PCE is re-established. Any subsequent change to the state of an LSP is synchronized at the time the session is re-established.

When a PCEP session to a peer times out or closes, the rate at which the PCEP speaker attempts the establishment of the session is subject to an exponential back-off mechanism.
4.4 PCEP Parameters

The following PCEP parameters are user-configurable on the PCC:

- keepalive timer
  A PCEP speaker must send a keepalive message if no other PCEP message is sent to the peer at the expiry of this timer. This timer is restarted every time a PCEP message is sent or the keepalive message is sent.
  The keepalive mechanism is asymmetric, meaning that each peer can use a different keepalive timer value.
  The range of this timer is 1 to 255 seconds and the default value is 30 seconds.

- dead timer
  This timer tracks the amount of time a PCEP speaker waits after the receipt of the last PCEP message before declaring its peer down.
  The dead timer mechanism is asymmetric, meaning that each PCEP speaker can propose a different dead timer value to its peer to use to detect session timeouts.
  The range of this timer is 1 to 255 seconds and the default value is 120 seconds.

- maximum rate of unknown messages
  When the rate of received unrecognized or unknown messages reaches the configured limit, the PCEP speaker closes the session to the peer.
  The range of this message rate is 1 to 255 messages per minute and the default value is 10 messages per minute.

- session reestablishment and state timeout
  If the PCEP session to the PCE goes down, all delegated PCC-initiated LSPs have their state maintained in the PCC and are not timed out. The PCC continues to try re-establishing the PCEP session. When the PCEP session is re-established, the LSP database is synchronized with the PCE database, and any LSP that went down since the last time the PCEP session was up has its path updated by the PCE.

4.4.1 PCC Configuration

The following PCC parameters can be modified while the PCEP session is operational:

- report-path-constraints
- unknown-message-rate
The following PCC parameters cannot be modified while the PCEP session is operational:

- local-address
- keepalive
- dead-timer
- peer (regardless of shutdown state)

### 4.4.2 Stateful PCE

The main function introduced by stateful PCE over the base PCE implementation is the ability to synchronize the LSP state between the PCC and the PCE. This allows the PCE to have all the required LSP information to perform reoptimization and updating of the LSP paths.

Table 30 describes the TLVs, objects, and messages supported by stateful PCE on the 7705 SAR.

**Table 30  PCEP Stateful PCE Extension TLVs, Objects, and Messages**

<table>
<thead>
<tr>
<th>TLV, Object, or Message</th>
<th>Contained in Object</th>
<th>Contained in Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path Computation State Report (PCRpt)</td>
<td>N/A</td>
<td>New message</td>
</tr>
<tr>
<td>Path Computation Update Request (PCUpd)</td>
<td>N/A</td>
<td>New message</td>
</tr>
<tr>
<td>STATEFUL-PCE-CAPABILITY TLV</td>
<td>OPEN</td>
<td>OPEN</td>
</tr>
<tr>
<td>Stateful Request Parameter (SRP) Object</td>
<td>N/A</td>
<td>PCRpt&lt;sup&gt;1&lt;/sup&gt;, PCErr</td>
</tr>
<tr>
<td>LSP Object</td>
<td>ERO</td>
<td>PCRpt&lt;sup&gt;1&lt;/sup&gt;, PCReq, PCRep</td>
</tr>
<tr>
<td>LSP-IDENTIFIERS TLV</td>
<td>LSP</td>
<td>PCRpt&lt;sup&gt;1&lt;/sup&gt;</td>
</tr>
<tr>
<td>SYMBOLIC-PATH-NAME TLV</td>
<td>LSP, SRP</td>
<td>PCRpt&lt;sup&gt;1&lt;/sup&gt;</td>
</tr>
<tr>
<td>LSP-ERROR-CODE TLV</td>
<td>LSP</td>
<td>PCRpt&lt;sup&gt;1&lt;/sup&gt;</td>
</tr>
<tr>
<td>RSVP-ERROR-SPEC TLV</td>
<td>LSP</td>
<td>PCRpt&lt;sup&gt;1&lt;/sup&gt;</td>
</tr>
</tbody>
</table>

**Note:**

1. Nokia proprietary
The behavior and limitations of the implementation of the TLVs, objects, and messages in Table 30 are as follows.

- The PCC and PCE support all PCEP capability TLVs defined in this document and will always advertise them. If the OPEN object received from a PCEP speaker does not contain one or more of the capabilities, the PCE or PCC will not use them during that specific PCEP session.
- The PCC always includes the LSP object in the PCReq message to make sure that the PCE can correlate the PLSP-ID for this LSP when a subsequent PCRpt message arrives with the delegation bit set. The PCE will, however, still honor a PCReq message without the LSP Object.
- PCE path computation will only consider the bandwidth used by LSPs in its LSP-DB. As a result, there are two situations where PCE path computation will not accurately take into account the bandwidth used in the network:
  - when there are LSPs that are signaled by the routers but are not synchronized with the PCE. The user can enable the reporting of the LSP to the PCE LSP database for each LSP.
  - when the stateful PCE is peering with a third-party stateless PCC, implementing only the original RFC 5440. While the PCE will be able to bring the PCEP session up, the LSP database will not be updated, because stateless PCC does not support the PCRpt message. Therefore, PCE path computation will not accurately take into account the bandwidth used by these LSPs in the network.
- The PCE ignores the R-flag (reoptimize flag) in the PCReq message when acting in passive stateful mode for an LSP and will always return the newly computed path, regardless whether it is link-by-link identical or has the same metric as the current path. The decision whether to initiate the new path in the network belongs to the PCC.
- The synchronization vector (SVEC) object is not supported on the 7705 SAR and the NSP. If the PCE receives a PCReq message with the SVEC object, it will ignore the SVEC object and treat each path computation request in the PCReq message as independent, regardless of the setting of the P-flag in the SVEC object common header.
- When an LSP is delegated to the PCE, there may be no prior state in the NRC-P LSP database for the LSP. This could be due to the PCE not having received a PCReq message for the same PLSP-ID. In order for the PCE to become aware of the original constraints of such an LSP, the following additional procedures are performed. These procedures are proprietary to Nokia.
  - The PCC appends a duplicate of each of the LSPA, metric, and bandwidth objects in the PCRpt message. The only difference between the two objects of the same type is that the P-flag is set in the common header of the duplicate object to indicate a mandatory object for processing by the PCE.
The value of the metric or bandwidth in the duplicate object contains the original constraint value, while the first object contains the operational value. This is applicable to hop metrics in the metric object and bandwidth object only. The 7705 SAR PCC does not support putting a bound value on the IGP or TE metric in the path computation.

The path computation on the PCE uses the first set of objects when updating a path if the PCRpt message contains a single set. If the PCRpt message contains a duplicate set, PCE path computation must use the constraints in the duplicate set.

For interoperability, implementations compliant with PCEP standards should be able to accept the first metric object and ignore the second object without additional error handling. Because there are also bandwidth and LSPA objects, the `no report-path-constraints` command is provided in the PCC on a per-PCEP session basis to disable the inclusion of the duplicate objects. Duplicate objects are included by default.

4.4.3 LSP Initiation

An LSP that is configured on the router is referred to as a PCC-initiated LSP. An LSP that is not configured on the router, but is instead created by the PCE at the request of an application or a service instantiation, is referred to as a PCE-initiated LSP.

The 7705 SAR supports three modes of operation for PCC-initiated LSPs, which are configurable on a per-LSP basis:

**PCC-initiated and PCC-controlled**

When the path of the LSP is computed and updated by the router acting as a PCE Client (PCC), the LSP is referred to as PCC-initiated and PCC-controlled.

A PCC-initiated and PCC-controlled LSP has the following characteristics:

- The LSP can contain strict or loose hops, or a combination of both.
- CSPF is supported for RSVP-TE LSPs. Local path computation takes the form of hop-to-label translation for LSPs.
- LSPs can be reported to synchronize the LSP database of a stateful PCE server using the `pce-report` option. In this case, the PCE acts in passive stateful mode for this LSP. The LSP path cannot be updated by the PCE. The control of the LSP is maintained by the PCC.

**PCC-initiated and PCE-computed**

When the path of the LSP is computed by the PCE at the request of the PCC, it is referred to as PCC-initiated and PCE-computed.

A PCC-initiated and PCE-computed LSP has the following characteristics:
- The **pce-computation** option must be enabled for the LSP so that the PCE can perform path computation at the request of the PCC only. The PCC retains control.

- LSPs can be reported to synchronize the LSP database of a stateful PCE server using the **pce-report** option. In this case, the PCE acts in passive stateful mode for this LSP.

**PCC-initiated and PCE-controlled**

When the path of the LSP is updated by the PCE following a delegation from the PCC, it is referred to as PCC-initiated and PCE-controlled.

A PCC-initiated and PCE-controlled LSP has the following characteristics:

- The **pce-control** option must be enabled for the LSP so that the PCE can perform path updates following a network event without an explicit request from the PCC. The PCC delegates full control.

- The **pce-report** option must be enabled for LSPs that cannot be delegated to the PCE. The PCE acts in active stateful mode for this LSP.

### 4.4.4 PCC-Initiated and PCE-Computed or PCE-Controlled LSPs

The following is the procedure for configuring and programming a PCC-initiated LSP when control is delegated to the PCE.

**Step 1.** The LSP configuration is created on the PE router via CLI or via the OSS/NSP NFM-P.

The configuration dictates which PCE control mode is desired: active (**pce-control** and **pce-report** options enabled) or passive (**pce-computation** enabled and **pce-control** disabled).

**Step 2.** PCC assigns a unique PLSP-ID to the LSP. The PLSP-ID uniquely identifies the LSP on a PCEP session and must remain constant during its lifetime. PCC on the router must keep track of the association of the PLSP-ID to the Tunnel-ID and Path-ID, and use the latter to communicate with MPLS about a specific path of the LSP. PCC also uses the SRP-ID to correlate PCRpt messages for each new path of the LSP.

**Step 3.** The PE router does not validate the entered path. Note however that in the 7705 SAR OS, the PCE supports the computation of a path for an LSP with empty-hops in its path definition. While PCC will include the IRO objects in the PCReq message to PCE, the PCE will ignore them and compute the path with the other constraints except the IRO.
Step 4. The PE router sends a PCReq message to the PCE to request a path for the LSP, and includes the LSP parameters in the METRIC object, the LSPA object, and the BANDWIDTH object. The PE router also includes the LSP object with the assigned PLSP-ID. At this point, the PCC does not delegate the control of the LSP to the PCE.

Step 5. The PCE computes a new path, reserves the bandwidth, and returns the path in a PCRep message with the computed ERO in the ERO object. It also includes the LSP object with the unique PLSP-ID, the METRIC object with any computed metric value, and the BANDWIDTH object.

Note: For the PCE to be able to use the SRLG path diversity and admin-group constraints in the path computation, the user must configure the SRLG and admin-group membership against the MPLS interface and make sure that the traffic-engineering option is enabled in IGP. This causes IGP to flood the link SRLG and admin-group membership in its participating area, and for PCE to learn it in its TE database.

Step 6. The PE router updates the CPM and the data path with the new path. Up to this point, the PCC and PCE are using passive stateful PCE procedures. The next steps will synchronize the LSP database of the PCC and PCE for both PCE-computed and PCE-controlled LSPs. They will also initiate the active PCE stateful procedures for the PCE-controlled LSP only.

Step 7. The PE router sends a PCRpt message to update the PCE with an UP state, and also sends the RRO as confirmation. It now includes the LSP object with the unique PLSP-ID. For a PCE-controlled LSP, the PE router also sets the delegation control flag to delegate control to the PCE. The state of the LSP is now synchronized between the router and the PCE.

Step 8. Following a network event or a reoptimization, the PCE computes a new path for a PCE-controlled LSP and returns it in a PCUpd message with the new ERO. It will include the LSP object with the same unique PLSP-ID assigned by the PCC, as well as the Stateful Request Parameter (SRP) object with a unique SRP-ID-number to track error and state messages specific to this new path.

Step 9. The PE router updates the CPM and the data path with the new path.

Step 10. The PE router sends a PCRpt message to inform the PCE that the older path is deleted. It includes the unique PLSP-ID value in the LSP object and the R (Remove) bit set.

Step 11. The PE router sends a new PCRpt message to update PCE with an UP state, and also sends the RRO to confirm the new path. The state of the LSP is now synchronized between the router and the PCE.
Step 12. If PCE owns the delegation of the LSP and is making a path update, MPLS will initiate the LSP and update the operational value of the changed parameters while the configured administrative values will not change. Both the administrative and operational values are shown in the details of the LSP path in MPLS.

Step 13. If the user makes any configuration change to the PCE-computed or PCE-controlled LSP, MPLS requests that the PCC first revoke delegation in a PCRpt message (PCE-controlled only), and then MPLS and PCC follow the above steps to convey the changed constraint to PCE which will result in the programming of a new path into the data path, the synchronization of the PCC and PCE LSP databases, and the return of delegation to PCE.

The above procedure is followed when the user performs a no shutdown command on a PCE-controlled or PCE-computed LSP. The starting point is an LSP which is administratively down with no active path. For an LSP with an active path, the following items may apply:

a. If the user enabled the pce-computation option on a PCC-controlled LSP with an active path, no action is performed until the next time the router needs a path for the LSP following a network event of a LSP parameter change. At that point, the prior procedure is followed.

b. If the user enabled the pce-control option on a PCC-controlled or PCE-computed LSP with an active path, the PCC will issue a PCRpt message to the PCE with an UP state, as well as the RRO of the active path. It will set the delegation control flag to delegate control to the PCE. The PCE will keep the active path of the LSP and make no updates to it until the next network event or reoptimization. At that point, the prior procedure is followed.
4.5 PCEP Support for RSVP-TE LSPs

This section describes the support of PCC-initiated RSVP-TE LSPs. PCEP support of an RSVP-TE LSP is described in LSP Initiation with the following differences:

- each primary and secondary path is assigned its own unique path LSP-ID (PLSP-ID)
- the PCC indicates to the PCE the state of each path (either up or down) and which path is currently active and carrying traffic (active state)

This section includes the following topics:

- RSVP-TE LSP Configuration for a PCC Router
- Behavior of the LSP Path Update
- Behavior of LSP MBB
- Behavior of Secondary LSP Paths
- PCE Path Profile Support

4.5.1 RSVP-TE LSP Configuration for a PCC Router

The following MPLS-level and LSP-level CLI commands are used to configure RSVP-TE LSPs in a router acting as a PCEP Client (PCC). See MPLS and RSVP-TE Command Reference for command descriptions.

- `config>router>mpls>
  pce-report rsvp-te {enable | disable}`
- `config>router>mpls>lsp>
  path-profile profile-id [path-group group-id]
  pce-computation
  pce-control
  pce-report {enable | disable | inherit}`
- `config>router>mpls>lsp-template
  pce-report {enable | disable | inherit}`

The `cspf` option must be enabled on the LSP before enabling the `pce-computation` or `pce-control` options. An attempt to disable the `cspf` option on an RSVP-TE LSP that has the `pce-computation` or `pce-control` options enabled will be rejected.
If the LSP has disabled PCE reporting, either due to inheritance from the MPLS-level configuration or due to LSP-level configuration, enabling the `pce-control` option for the LSP has no effect. To help troubleshoot this situation, the output of the `show` commands for the LSP displays the operational values of both the `pce-report` and `pce-control` options.

**Note:** The PCE function implemented in the NSP and referred to as the NRC-P, supports only Shared Explicit (SE) style bandwidth management for RSVP-TE LSPs. The PCEP does not support the ability of the PCC to convey this value to the PCE. Therefore, whether the LSP configuration option `rsvp-resv-style` is set to **se** or **ff**, the PCE will always use the SE style in the CSPF computation of the path for a PCE-computed or PCE-controlled RSVP-TE LSP.

A **one-hop-p2p** or a **mesh-p2p** RSVP-TE auto-lsp only supports the `pce-report` command in the LSP template:

```
config>router>mpls>lsp-template>
    pce-report {enable | disable | inherit}
```

The user must first shut down the LSP template before changing the value of the `pce-report` option.

A manual bypass LSP does not support any of the PCE-related commands. Reporting a bypass LSP to the PCE is not required because the bypass LSP does not book bandwidth.

All other MPLS, LSP, and path-level commands are supported, with the exception of the following commands:

- `least-fill`
- `srlg` (on secondary standby path)

For more information on RSVP-TE PCC instantiation modes, see LSP Initialization.

### 4.5.2 Behavior of the LSP Path Update

When the `pce-control` option is enabled, the PCC delegates control of the RSVP-TE LSP to the PCE.

The NRC-P sends a path update using the PCUud message in the following cases:

- a failure event that impacts a link or a node in the path of a PCE-controlled LSP
The operation is performed by the PCC as a Make-Before-Break (MBB) if the LSP remained in the up state due to protection provided by FRR or a secondary path. If the LSP went down, the update brings it into the up state. A PCRpt message is sent by the PCC for each change to the state of the LSP during this process. See Behavior of LSP MBB for more information.

- a topology change that impacts a link in the path of a PCE-controlled LSP
  This topology change can be a change to the IGP metric, the TE metric, admin-group, or SRLG membership of an interface. This update is performed as an MBB by the PCC.
- the user performed a manual resignal of a PCE-controlled RSVP-TE LSP path from the NRC-P
  This update is performed as an MBB by the PCC.
- the user performed a Global Concurrent Optimization (GCO) on a set of PCE-controlled RSVP-TE LSPs from the NRC-P
  This update is performed as an MBB by the PCC.

The procedures for the path update are described in LSP Initiation. However, for an RSVP-TE LSP, the PCUpd message from the PCE contains the interface IP address or system IP address in the computed ERO. The PCC signals the path using the ERO returned by the PCE and, if successful, programs the data path, then sends the PCRpt message with the resulting RRO and hop labels provided by RSVP-TE signaling.

If the signaling of the ERO fails, the ingress LER returns a PCErr message to the PCE with the LSP Error code field of the LSP-ERROR-CODE TLV set to a value of 8 (RSVP signaling error).

If an RSVP-TE LSP has the no adaptive option set, the ingress LER cannot perform an MBB for the LSP. A PCUpd message received from the PCE is then failed by the ingress LER, which returns a PCErr message to the PCE with the LSP Error code field of the LSP-ERROR-CODE TLV set to a value of 8 (RSVP signaling error).

### 4.5.2.1 Path Update with Empty ERO

When the NRC-P reoptimizes the path of a PCE-controlled RSVP-TE LSP, it is possible that a path that satisfies the constraints of the LSP no longer exists. In this case, the NRC-P sends a PCUpd message with an empty ERO, which forces the PCC to bring down the path of the RSVP-TE LSP.

The NRC-P sends a PCUpd message with an empty ERO if any of the following cases are true:
4.5.3 Behavior of LSP MBB

In addition to the MBB support when the PCC receives a path update, as described in Behavior of the LSP Path Update, an RSVP-TE LSP supports the MBB procedure for any parameter configuration change, including the PCEP-related commands when they result in a change to the path of the LSP.

If the user adds or modifies the path-profile command for an RSVP-TE LSP, a config change MBB is only performed if the pce-computation, pce-report, or pce-control options are enabled on the LSP. Otherwise, no action occurs. When pce-computation, pce-report, or pce-control are enabled on the LSP, the path update MBB (tools>perform>router>mpls>update-path) fails, resulting in no operation.

MBB is also supported for the manual ressignal and auto-bandwidth MBB types.

When the LSP goes into an MBB state at the ingress LER, the behavior is dependent on the operating mode of the LSP.

This section contains information on the following LSP MBB procedures:

- PCC-Controlled LSPs
- PCE-Computed LSPs
- PCE-Controlled LSPs

4.5.3.1 PCC-Controlled LSPs

All MBB types are supported for PCC-controlled LSPs. The LSP MBB procedures for a PCC-controlled LSP (pce-computation and pce-control disabled) are as follows.

1. MPLS submits a path request, including the updated path constraints, to the local CSPF.
2. If the local CSPF returns a path, the PCC signals the LSP with the RSVP control plane and moves traffic to the new MBB path. If `pce-report` is enabled for this LSP, the PCC sends a PCRpt message with the delegation bit clear to retain control and containing the RRO and LSP objects, with the LSP-IDENTIFIERS TLV containing the LSP-ID of the new MBB path. The message includes the metric, LSPA, and bandwidth objects where the P-flag is clear, which indicates the operational values of these parameters. Unless the user disables the `report-path-constraints` option under the `pcc` context, the PCC also includes a second set of metric, LSPA, and bandwidth objects with the P-flag set to convey to the PCE the constraints of the path.

3. If the CSPF returns no path or the RSVP-TE signaling of the returned path fails, MPLS puts the LSP into retry mode and sends a request to the local CSPF every `retry-timer` seconds and up to the value of `retry-count`.

4. When `pce-report` is enabled for the LSP and the FRR global revertive MBB is triggered following a bypass LSP activation by a PLR in the network, the PCC issues an updated PCRpt message with the new RRO reflecting the PLR and RRO hops. The PCE releases the bandwidth on the links that are no longer used by the LSP path.

### 4.5.3.2 PCE-Computed LSPs

All MBB types are supported for PCE-computed LSPs. The LSP MBB procedures for a PCE-computed LSP (`pce-computation` enabled and `pce-control` disabled) are as follows.

1. The PCC issues a PCReq for the same PLSP-ID and includes the updated constraints in the metric, LSPA, and bandwidth objects.
   - If the PCE successfully finds a path, it replies with a PCRep message with the ERO.
   - If the PCE does not find a path, it replies with a PCRep message containing the No-Path object.

2. If the PCE returns a path, the PCC signals the LSP with the RSVP control plane and moves traffic to the new MBB path. If `pce-report` is enabled for this LSP, the PCC sends a PCRpt message with the delegation D-bit clear to retain control and containing the RRO and LSP objects, with the LSP-IDENTIFIERS TLV containing the LSP-ID of the new MBB path. The message includes the metric, LSPA, and bandwidth objects where the P-flag is clear, which indicates the operational values of these parameters. Unless the user disables the `report-path-constraints` option under the `pcc` context, the PCC also includes a second set of metric, LSPA, and bandwidth objects with the P-flag set to convey to the PCE the constraints of the path.
3. If the PCE returns no path or the RSVP-TE signaling of the returned path fails, MPLS puts the LSP into retry mode and sends a request to PCE every retry-timer seconds and up to the value of retry-count.

4. When the pce-report is enabled for the LSP and the FRR global revertive MBB is triggered following a bypass LSP activation by a PLR in the network, the PCC issues an updated PCRpt message with the new RRO reflecting the PLR and RRO hops. The PCE releases the bandwidth on the links that are no longer used by the LSP path.

5. If the user changes the RSVP-TE LSP configuration from pce-computation to no pce-computation, MBB procedures are not supported. In this case, the LSP path is torn down and is put into retry mode to compute a new path from the local CSPF on the router to signal the LSP.

4.5.3.3 PCE-Controlled LSPs

The LSP MBB procedures for a PCE-controlled LSP (pce-control enabled) are as follows.

Note: Items 1 through 5 of the following procedure apply to the config change, manual resignal, and auto-bandwidth MBB types. The delayed retry MBB type used with the SRLG on secondary standby LSP feature is not supported with a PCE-controlled LSP. See Behavior of Secondary LSP Paths for information about the SRLG on secondary standby LSP feature.

1. The PCC temporarily removes delegation by sending a PCRpt message for the corresponding path LSP-ID (PLSP-ID) with the delegation D-bit clear.
2. For an LSP with pce-computation disabled, MPLS submits a path request to the local CSPF, which includes the updated path constraints.
3. For an LSP with pce-computation enabled, the PCC issues a PCReq for the same PLSP-ID and includes the updated constraints in the metric, LSPA, or bandwidth objects.
   - If the PCE successfully finds a path, it replies with a PCRep message with the ERO.
   - If the PCE does not find a path, it replies with a PCRep message containing the No-Path object.
4. If the local CSPF or the PCE returns a path, the PCC performs the following actions.
The PCC signals the LSP with the RSVP control plane and moves traffic to the new MBB path. It then sends a PCRpt message with the delegation D-bit set to return delegation and containing the RRO and LSP objects, with the LSP-IDENTIFIERS TLV containing the LSP-ID of the new MBB path. The message includes the metric, LSPA, and bandwidth objects where the P-flag is clear, which indicates the operational values of these parameters. Unless the user disabled the report-path-constraints option under the pcc context, the PCC also includes a second set of metric, LSPA, or bandwidth objects with the P-flag set to convey to the PCE the constraints of the path.

The PCC sends a PathTear message to delete the state of the older path in the network. The PCC then sends a PCRpt message to the PCE with the older path LSP (PLSP-ID) and the remove R-bit set to also have the PCE remove the state of that LSP from its database.

5. If the local CSPF or the PCE returns no path or the RSVP-TE signaling of the returned path fails, the router makes no further requests. That is, there is no retry for the MBB.

The PCC sends a PCErr message to the PCE with the LSP Error code field of the LSP-ERROR-CODE TLV set to a value of 8 (RSVP signaling error) if the MBB failed due to a RSVP-TE signaling error.

The PCC sends a PCRpt message with the delegation D-bit set to return delegation and containing the RRO and LSP objects, with the LSP-IDENTIFIERS TLV containing the LSP-ID of the currently active path. The message includes the metric, LSPA, and bandwidth objects where the P-flag is clear to indicate the operational values of these parameters. Unless the user disabled the report-path-constraints option under the pcc context, the PCC also includes a second set of metric, LSPA, and bandwidth objects with the P-flag set to convey to the PCE the constraints of the path.

6. The ingress LER takes no action in the case of a network event triggered MBB, such as FRR global revertive or TE graceful shutdown.

The ingress PE keeps the information as required and sets the state of MBB to one of the FRR global revertive or TE graceful shutdown MBB values but does not perform the MBB action.

The NRC-P computes a new path for the global revertive MBB due to a failure event. This computation uses the PCUpd message to update the path using the MBB procedure described in Behavior of the LSP Path Update. The activation of a bypass LSP by a point of local repair (PLR) in the network causes the PCC to issue an updated PCRpt message with the new RRO reflecting the PLR and RRO hops. The PCE will release the bandwidth on the links that are no longer used by the LSP path.
− The NRC-P computes a new path for the TE graceful shutdown MBB if the RSVP-TE is using the TE metric, because the TE metric of the link in TE graceful shutdown is set to infinity. This computation uses the PCUpd message to update the path using the MBB procedure described in Behavior of the LSP Path Update.

− The NRC-P does not act on the TE graceful shutdown MBB if the RSVP-TE is using the IGP metric; however, the user can perform a manual resignal of the LSP path from the NRC-P to force a new path computation, which accounts for the newly available bandwidth on the link that caused the MBB event. This computation uses the PCUpd message to update the path using the MBB procedure described in Behavior of the LSP Path Update.

− The user can perform a manual resignal of the LSP path from the ingress LER, which forces an MBB for the path as per the remove-delegation/MBB/return-delegation procedures described in this section.

− If the user performs no pce-control while the LSP still has the state for any of the network event triggered MBBS, the MBB is performed immediately by the PCC as described in the procedures in PCE-Computed LSPs for a PCE-computed LSP and as described in the procedures in PCC-Controlled LSPs for a PCC-controlled LSP.

7. The timer-based manual resignal MBB behaves like the TE graceful shutdown MBB. The user can perform a manual resignal of the LSP path from the ingress LER or from the PCE.

8. The path update MBB (tools>perform>router>mpls>update-path) fails, which results in no operation. This is true in all cases when the RSVP-TE LSP enables the pce-report option.

4.5.4 Behavior of Secondary LSP Paths

Each of the primary, secondary standby, and secondary non-standby paths of the same LSP must use a separate path LSP-ID (PLSP-ID). The PCE function of the NSP, the NRC-P, checks the LSP-IDENTIFIERS TLV in the LSP object and can identify which PLSP-IDs are associated with the same LSP or the same RSVP-TE session. The parameters are the IPv4 Tunnel Sender Address, the Tunnel ID, the Extended Tunnel ID, and the IPv4 Tunnel Endpoint Address. This approach allows the use of all the PCEP procedures for all three types of LSP paths.

The PCC indicates to the PCE the following states for the path in the LSP object: down, up (signaled but not carrying traffic), or active (signaled and carrying traffic).

The PCE tracks active paths and displays them in the NSP GUI. It also provides only the tunnel ID of an active PLSP-ID to a destination prefix when a request is made by a service or a steering application.
The PCE recomputes the paths of all PLSP-IDs that are affected by a network event. The user can select each path separately on the NSP GUI and trigger a manual resignal of one or more paths of the RSVP-TE LSP.

**Note:** Enabling the `srlg` option on a secondary standby path results in no operation. The NRC-P supports link and SRLG disjointness using the PCE path profile. The user can apply the PCE path profile to the primary and secondary paths of the same LSP. See [PCE Path Profile Support](#) for more information.

### 4.5.5 PCE Path Profile Support

The PCE path profile ID and path group ID are configured at the LSP level (`config>router>mpls>lsp<path-profile>`).

The NRC-P can enforce path disjointness and bidirectionality among a pair of forward and a pair of reverse LSP paths. Both pairs of LSP paths must use a unique path group ID along with the same path profile ID.

When the user wants to apply path disjointness and path bidirectionality constraints to RSVP-TE LSP paths, it is important to follow the following guidelines. The user can configure the following sets of LSP paths:

- a set consisting of a pair of forward RSVP-TE LSPs and a pair of reverse RSVP-TE LSPs, each with a single primary or secondary path. The pair of forward LSPs can originate and terminate on different routers. The pair of reverse LSPs must mirror the forward pair. In this case, the path profile ID and the path group ID configured for each LSP must match. Because each LSP has a single path, the bidirectionality constraint applies automatically to the forward and reverse LSPs, which share the same originating node and the same terminating routers.

- a pair consisting of a forward RSVP-TE LSP and a reverse RSVP-TE LSP, each with a primary path and a single secondary path, or each with two secondary paths. Because the two paths of each LSP inherit the same LSP level path profile ID and path group ID configuration, the NRC-P path computation algorithm cannot guarantee that the primary paths in both directions meet the bidirectionality constraint. That is, it is possible that the primary path for the forward LSP shares the same links as the secondary path of the reverse LSP and vice-versa.
4.6 LSP Path Diversity and Bidirectionality Constraints

The PCE path profile defined in draft-alvarez-pce-path-profiles is used to request path diversity or a disjoint for two or more LSPs originating on the same or different PE routers. It is also used to request that paths of two unidirectional LSPs between the same two routers use the same TE links. This is referred to as the bidirectionality constraint.

Path profiles are defined by the user directly on the NRC-P Policy Manager with a number of LSP path constraints, which are metrics with upper bounds specified, and with an objective, which are metrics optimized with no bounds specified. The NRC-P Policy Manager allows the following PCE constraints to be configured within each PCE path profile:

- path diversity, node-disjoint, link-disjoint
- path bidirectionality, symmetric reverse route preferred, symmetric reverse route required
- maximum path IGP metric (cost)
- maximum path TE metric
- maximum hop count

The user can also specify which PCE objective to use to optimize the path of the LSP in the PCE path profile, one of:

- IGP metric (cost)
- TE metric
- hops (span)

The CSPF algorithm will optimize the objective. If a constraint is provided for the same metric, the CSPF algorithm ensures that the selected path achieves a lower or equal value to the bound value specified in the constraint.

For hop-count metrics, if a constraint is sent in a metric object and is also specified in a PCE profile referenced by the LSP, the constraint in the metric object is used.

For IGP and TE metrics, if an objective is sent in a metric object and is also specified in a PCE profile referenced by the LSP, the objective in the path profile is used.

The constraints in the bandwidth object and the LSPA object, specifically the include and exclude admin-group constraints and setup and hold priorities, are not supported in the PCE profile.
In order to indicate the path diversity and bidirectionality constraints to the PCE, the user must configure the profile ID and path group ID of the PCE path that the LSP belongs to. The CLI commands for this are described in Configuring RSVP-TE LSPs with PCEP Using the CLI. The path group ID does not need to be defined in the PCE as part of the path profile configuration and identifies implicitly the set of paths that must have the path diversity constraint applied.

The user can only associate a single path group ID with a specific PCE path profile ID for an LSP. However, the same path group ID can be associated with multiple PCE profile IDs for the same LSP.

The path profiles are inferred using the path ID in the path request by the PCC. When the PE router acting as a PCC wants to request path diversity from a set of other LSPs belonging to a path group ID value, it adds a new PATH-PROFILE object in the PCReq message. The object contains the path profile ID and the path group ID as an extended ID field. In other words, the diversity metric is carried in an opaque way from the PCC to the PCE.

The bidirectionality constraint operates the same way as the diversity constraint. The user can configure a PCE profile with both the path diversity and bidirectionality constraints. The PCE will check if there is an LSP in the reverse direction that belongs to the same path group ID as an originating LSP it is computing the path for, and will enforce the constraint.

In order for the PCE to be aware of the path diversity and bidirectionality constraints for an LSP that is delegated but for which there is no prior state in the NRC-P LSP database, the PATH-PROFILE object is included in the PCRpt message with the P-flag set in the common header to indicate that the object must be processed. This is proprietary to Nokia.

Table 31 describes the new objects and TLVs introduced in the PCE path profile.

### Table 31 PCEP Path Profile Extension Objects and TLVs

<table>
<thead>
<tr>
<th>TLV, Object, or Message</th>
<th>Contained in Object</th>
<th>Contained in Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>PATH-PROFILE-CAPABILITY TLV</td>
<td>OPEN</td>
<td>OPEN</td>
</tr>
<tr>
<td>PATH-PROFILE Object</td>
<td>N/A</td>
<td>PCReq, PCRpt ¹</td>
</tr>
</tbody>
</table>

**Note:**

1. Nokia proprietary
A PATH-PROFILE object can contain multiple TLVs containing each profile ID and extend ID, and should be processed properly. If multiple PATH-PROFILE objects are received, the first object is interpreted and the others are ignored. The PCC and the PCE support all PCEP capability TLVs defined in this chapter and will always advertise them. If the OPEN object received from a PCEP speaker does not contain one or more of the capabilities, the PCE or PCC will not use them during that PCEP session.
4.7 Configuring RSVP-TE LSPs with PCEP Using the CLI

This section provides information about using the CLI to configure and operate RSVP-TE LSPs with PCEP.

The following information describes the detailed configuration of an inter-area RSVP-TE LSP with both a primary path and a secondary path. The network uses IS-IS with the backbone area in Level 2 and the leaf areas in Level 1. Topology discovery is learned by the NRC-P using IGP and the NFM-P.

The LSP uses an admin-group constraint to keep the paths of the secondary and primary links disjoint in the backbone area. The LSP is PCE-controlled but also has `pce-computation` enabled so that the initial path, and any MBB path, is also computed by the PCE.

The NSP and 7705 SAR load versions used to produce this example in this section are:

- NSP: NSP-2.0.3-rel.108
- PCE SROS: TiMOS-B-0.0.W129
- PCC: TiMOS-B-0.0.I4902

This section provides configuration and show commands for the following examples:

- PCEP on the PCE Node and the PCC Node
- MPLS on the PCC Node

4.7.1 PCEP on the PCE Node and the PCC Node

Figure 17 shows a multi-level IS-IS topology in the NSP GUI:
The following example shows the configuration and show command output of the PCEP on the PCE node and the PCC node.

**Note:** The 7705 SAR operates as a PCE Client (PCC) only, supporting PCC capabilities for RSVP-TE LSPs. References to PCE router operation and SR-TE LSPs apply to the 7750 SR product family and are included here for informational purposes only.

*A:* PCE Server 226>config>router>pcep>pce# info

       local-address 138.120.48.226
       no shutdown

*A:* Reno 194>config>router>pcep>pcc# info

       peer 138.120.48.226
       no shutdown
       exit

       no shutdown

*A:* PCE Server 226>config>router>pcep>pce# show router pcep pce status

Path Computation Element Protocol (PCEP) Path Computation Element (PCE) Info

Admin Status : Up  Oper Status : Up
Unknown Msg Limit : 10 msg/min
Keepalive Interval : 30 seconds  DeadTimer Interval : 120 seconds
Capabilities List : stateful-delegate stateful-pce segment-rt-path
Local Address : 138.120.48.226
PCE Overloaded : false

PCEP Path Computation Element (PCE) Peer Info

Peer      Sync State  Oper Keepalive/Oper DeadTimer
138.120.48.190:4189 done 30/120
138.120.48.194:4189 done 30/120
138.120.48.198:4189 done 30/120
138.120.48.199:4189 done 30/120
138.120.48.219:4189 done 30/120
138.120.48.221:4189 done 30/120
138.120.48.224:4189 done 30/120

* A: Reno 194# show router pcep pcc status

Path Computation Element Protocol (PCEP) Path Computation Client (PCC) Info

<table>
<thead>
<tr>
<th>Admin Status</th>
<th>Oper Status</th>
<th>Unknown Msg Limit</th>
<th>Keepalive Interval</th>
<th>DeadTimer Interval</th>
<th>Capabilities List</th>
<th>Address</th>
<th>Report Path Constraints</th>
<th>PCEP Path Computation Client (PCC) Peer Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up</td>
<td>Up</td>
<td>10 msg/min</td>
<td>30 seconds</td>
<td>120 seconds</td>
<td>stateful-delegate stateful-pce segment-rt-path</td>
<td>138.120.48.194</td>
<td>True</td>
<td>Peer Admin State/Oper State Oper Keepalive/Oper DeadTimer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>138.120.48.226 Up/Up 30/120</td>
</tr>
</tbody>
</table>

* A: Reno 194# show router pcep pcc lsp-db

PCEP Path Computation Client (PCC) LSP Update Info

<table>
<thead>
<tr>
<th>PCEP-specific LSP ID</th>
<th>LSP ID</th>
<th>LSP Type</th>
<th>Tunnel ID</th>
<th>Extended Tunnel Id</th>
<th>LSP Name</th>
<th>Source Address</th>
<th>Destination Address</th>
<th>LSP Delegated</th>
<th>Delegate PCE Address</th>
<th>Oper Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>14378</td>
<td>rsvp-p2p</td>
<td>1</td>
<td>38.120.48.194</td>
<td>From Reno to Atlanta RSVP-TE::primary_empty</td>
<td>38.120.48.194</td>
<td>38.120.48.224</td>
<td>True</td>
<td>138.120.48.226</td>
<td>active</td>
</tr>
<tr>
<td>12</td>
<td>14380</td>
<td>rsvp-p2p</td>
<td>1</td>
<td>38.120.48.194</td>
<td>From Reno to Atlanta RSVP-TE::secondary_empty</td>
<td>38.120.48.194</td>
<td>38.120.48.224</td>
<td>True</td>
<td>138.120.48.226</td>
<td>up</td>
</tr>
</tbody>
</table>
4.7.2  MPLS on the PCC Node

Figure 18 shows primary and secondary RSVP-TE LSP paths in the NSP GUI.

**Figure 18**  Primary and Secondary RSVP-TE LSP Paths in the NSP GUI

![Diagram showing primary and secondary RSVP-TE LSP paths](image)

The following example shows the configuration and show command output of the MPLS on the PCC node.

```
*A:Reno 194>config>router>mpls>lsp# info
----------------------------------------------
to 38.120.48.224
  egress-statistics
  shutdown
  exit
cspf
  fast-reroute facility
  no node-protect
  exit
pce-computation
pce-report enable
pce-control
revert-timer 1
primary "primary_empty"
  exclude "top"
  bandwidth 10
  exit
secondary "secondary_empty"
  standby
  exclude "bottom"
  bandwidth 5
  exit
```
no shutdown

* A: Reno 194# show router mpls lsp "From Reno to Atlanta RSVP-TE" path detail

MPLS LSP From Reno to Atlanta RSVP-TE Path (Detail)

Legend:
- @ - Detour Available
- # - Detour In Use
- b - Bandwidth Protected
- n - Node Protected
- s - Soft Preemption
- S - Strict
- L - Loose
- A - ABR

LSP from Reno to Atlanta RSVP-TE Path primary_empty

<table>
<thead>
<tr>
<th>LSP Name</th>
<th>From Reno to Atlanta RSVP-TE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path LSP ID</td>
<td>14382</td>
</tr>
<tr>
<td>From</td>
<td>38.120.48.194</td>
</tr>
<tr>
<td>To</td>
<td>38.120.48.224</td>
</tr>
<tr>
<td>Admin State</td>
<td>Up</td>
</tr>
<tr>
<td>Oper State</td>
<td>Up</td>
</tr>
<tr>
<td>Path Name</td>
<td>primary_empty</td>
</tr>
<tr>
<td>Path Type</td>
<td>Primary</td>
</tr>
<tr>
<td>Path Admin</td>
<td>Up</td>
</tr>
<tr>
<td>Path Oper</td>
<td>Up</td>
</tr>
<tr>
<td>Out Interface</td>
<td>1/1/1</td>
</tr>
<tr>
<td>Out Label</td>
<td>262094</td>
</tr>
<tr>
<td>Path Up Time</td>
<td>0d 00:00:22</td>
</tr>
<tr>
<td>Path Down Time</td>
<td>0d 00:00:00</td>
</tr>
<tr>
<td>Retry Limit</td>
<td>0</td>
</tr>
<tr>
<td>Retry Timer</td>
<td>30 sec</td>
</tr>
<tr>
<td>Retry Attempt</td>
<td>0</td>
</tr>
<tr>
<td>Next Retry In</td>
<td>0 sec</td>
</tr>
<tr>
<td>BFD Template</td>
<td>None</td>
</tr>
<tr>
<td>BFD Ping Interval</td>
<td>60</td>
</tr>
<tr>
<td>BFD Enable</td>
<td>False</td>
</tr>
<tr>
<td>Adspec</td>
<td>Disabled</td>
</tr>
<tr>
<td>Oper Adspec</td>
<td>Disabled</td>
</tr>
<tr>
<td>CSPF</td>
<td>Enabled</td>
</tr>
<tr>
<td>Oper CSPF</td>
<td>Enabled</td>
</tr>
<tr>
<td>Least Fill</td>
<td>Disabled</td>
</tr>
<tr>
<td>Oper LeastFill</td>
<td>Disabled</td>
</tr>
<tr>
<td>FRR</td>
<td>Enabled</td>
</tr>
<tr>
<td>Oper FRR</td>
<td>Enabled</td>
</tr>
<tr>
<td>FRR NodeProtect</td>
<td>Disabled</td>
</tr>
<tr>
<td>Oper FRR NP</td>
<td>Disabled</td>
</tr>
<tr>
<td>FR Hop Limit</td>
<td>16</td>
</tr>
<tr>
<td>Oper FRHopLimit</td>
<td>16</td>
</tr>
<tr>
<td>FR Prop Admin Gr*</td>
<td>Disabled</td>
</tr>
<tr>
<td>Oper FRPropAdmGrp</td>
<td>Disabled</td>
</tr>
<tr>
<td>Propagate Adm Grp</td>
<td>Disabled</td>
</tr>
<tr>
<td>Oper Prop Adm Grp</td>
<td>Disabled</td>
</tr>
<tr>
<td>Inter-area</td>
<td>False</td>
</tr>
<tr>
<td>PCE Updtd ID</td>
<td>0</td>
</tr>
<tr>
<td>PCE Report</td>
<td>Enabled</td>
</tr>
<tr>
<td>Oper PCE Report</td>
<td>Enabled</td>
</tr>
<tr>
<td>PCE Control</td>
<td>Enabled</td>
</tr>
<tr>
<td>Oper PCE Control</td>
<td>Enabled</td>
</tr>
<tr>
<td>PCE Compute</td>
<td>Enabled</td>
</tr>
<tr>
<td>Neg MTU</td>
<td>1496</td>
</tr>
<tr>
<td>Oper MTU</td>
<td>1496</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>10 Mbps</td>
</tr>
<tr>
<td>Oper Bandwidth</td>
<td>10 Mbps</td>
</tr>
<tr>
<td>Hop Limit</td>
<td>255</td>
</tr>
<tr>
<td>Oper HopLimit</td>
<td>255</td>
</tr>
<tr>
<td>Record Route</td>
<td>Record</td>
</tr>
<tr>
<td>Oper Record Route</td>
<td>Record</td>
</tr>
<tr>
<td>Record Label</td>
<td>Record</td>
</tr>
<tr>
<td>Oper Record Label</td>
<td>Record</td>
</tr>
<tr>
<td>Setup Priority</td>
<td>7</td>
</tr>
<tr>
<td>Oper Setup Priority</td>
<td>7</td>
</tr>
<tr>
<td>Hold Priority</td>
<td>0</td>
</tr>
<tr>
<td>Oper Hold Priority</td>
<td>0</td>
</tr>
<tr>
<td>Class Type</td>
<td>0</td>
</tr>
<tr>
<td>Oper CT</td>
<td>0</td>
</tr>
<tr>
<td>Backup CT</td>
<td>None</td>
</tr>
<tr>
<td>MainCT Retry</td>
<td>n/a</td>
</tr>
<tr>
<td>Rem</td>
<td></td>
</tr>
<tr>
<td>MainCT Retry</td>
<td>0</td>
</tr>
<tr>
<td>Limit</td>
<td></td>
</tr>
<tr>
<td>Include Groups</td>
<td>Oper Include Groups</td>
</tr>
<tr>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Exclude Groups</td>
<td>Oper Exclude Groups</td>
</tr>
<tr>
<td>top</td>
<td>top</td>
</tr>
</tbody>
</table>
PCEP

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive</td>
<td>Enabled</td>
</tr>
<tr>
<td>Preference</td>
<td>n/a</td>
</tr>
<tr>
<td>Path Trans</td>
<td>7</td>
</tr>
<tr>
<td>Failure Code</td>
<td>noError</td>
</tr>
<tr>
<td>Failure Node</td>
<td>n/a</td>
</tr>
<tr>
<td>Explicit Hops</td>
<td>No Hops Specified</td>
</tr>
<tr>
<td>Actual Hops</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10.202.5.194 (38.120.48.194) @ Record Label : N/A</td>
</tr>
<tr>
<td></td>
<td>-&gt; 10.202.5.199 (38.120.48.199) @ Record Label : 262094</td>
</tr>
<tr>
<td></td>
<td>-&gt; 38.120.48.185 (38.120.48.185) @ Record Label : 262111</td>
</tr>
<tr>
<td></td>
<td>-&gt; 10.0.5.185 @ Record Label : 262111</td>
</tr>
<tr>
<td></td>
<td>-&gt; 38.120.48.223 (38.120.48.223) @ Record Label : 262121</td>
</tr>
<tr>
<td></td>
<td>-&gt; 10.0.7.223 @ Record Label : 262121</td>
</tr>
<tr>
<td></td>
<td>-&gt; 38.120.48.224 (38.120.48.224) @ Record Label : 262116</td>
</tr>
<tr>
<td></td>
<td>-&gt; 10.101.4.224 @ Record Label : 262116</td>
</tr>
<tr>
<td>Computed Hops</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10.202.5.199 (S)</td>
</tr>
<tr>
<td></td>
<td>-&gt; 10.0.5.185 (S)</td>
</tr>
<tr>
<td></td>
<td>-&gt; 10.0.7.223 (S)</td>
</tr>
<tr>
<td></td>
<td>-&gt; 10.101.4.224 (S)</td>
</tr>
<tr>
<td>Resignal Eligible</td>
<td>False</td>
</tr>
<tr>
<td>Last Resignal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CSPF Metric : 40</td>
</tr>
</tbody>
</table>

---

**LSP From Reno to Atlanta RSVP-TE Path secondary_empty**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP Name</td>
<td>From Reno to Atlanta RSVP-TE</td>
</tr>
<tr>
<td>Path LSP ID</td>
<td>14384</td>
</tr>
<tr>
<td>From</td>
<td>38.120.48.194 To 38.120.48.224</td>
</tr>
<tr>
<td>Admin State</td>
<td>Up</td>
</tr>
<tr>
<td>Path Name</td>
<td>secondary_empty Path Type : Standby</td>
</tr>
<tr>
<td>Path Admin</td>
<td>Up Path Oper : Up</td>
</tr>
<tr>
<td>Out Interface</td>
<td>1/1/1 Out Label : 262091</td>
</tr>
<tr>
<td>Path Up Time</td>
<td>0d 00:00:25 Path Down Time : 0d 00:00:00</td>
</tr>
<tr>
<td>Retry Limit</td>
<td>0 Retry Timer : 30 sec</td>
</tr>
<tr>
<td>Retry Attempt</td>
<td>0 Next Retry In : 0 sec</td>
</tr>
<tr>
<td>BFD Template</td>
<td>None BFD Ping Interval : 60</td>
</tr>
<tr>
<td>BFD Enable</td>
<td>False</td>
</tr>
<tr>
<td>Adspec</td>
<td>Disabled Oper Apspec : Disabled</td>
</tr>
<tr>
<td>CSPF</td>
<td>Enabled Oper CSPF : Enabled</td>
</tr>
<tr>
<td>Least Fill</td>
<td>Disabled Oper LeastFill : Disabled</td>
</tr>
<tr>
<td>Propagate Adm Grp</td>
<td>Disabled Oper Prop Adm Grp : Disabled</td>
</tr>
<tr>
<td>Inter-area</td>
<td>False</td>
</tr>
<tr>
<td>PCE Updt ID</td>
<td>0</td>
</tr>
<tr>
<td>PCE Report</td>
<td>Enabled Oper PCE Report : Enabled</td>
</tr>
<tr>
<td>PCE Control</td>
<td>Enabled Oper PCE Control : Enabled</td>
</tr>
<tr>
<td>PCE Compute</td>
<td>Enabled</td>
</tr>
<tr>
<td>Neg MTU</td>
<td>1496 Oper MTU : 1496</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>5 Mbps Oper Bandwidth : 5 Mbps</td>
</tr>
<tr>
<td>Hop Limit</td>
<td>255 Oper HopLimit : 255</td>
</tr>
<tr>
<td>Record Route</td>
<td>Record Oper Record Route : Record</td>
</tr>
<tr>
<td>Record Label</td>
<td>Record Oper Record Label : Record</td>
</tr>
<tr>
<td>Setup Priority</td>
<td>7 Oper Setup Priority : 7</td>
</tr>
<tr>
<td>Hold Priority</td>
<td>0 Oper Hold Priority : 0</td>
</tr>
<tr>
<td>Class Type</td>
<td>0 Oper CT : 0</td>
</tr>
<tr>
<td>Include Groups</td>
<td>Oper Include Groups :</td>
</tr>
<tr>
<td>None</td>
<td>bottom</td>
</tr>
<tr>
<td>Exclude Groups</td>
<td>Oper Exclude Groups :</td>
</tr>
<tr>
<td></td>
<td>bottom</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Adaptive</td>
<td>Enabled</td>
</tr>
<tr>
<td>Preference</td>
<td>255</td>
</tr>
<tr>
<td>Path Trans</td>
<td>28</td>
</tr>
<tr>
<td>CSPF Queries</td>
<td>10</td>
</tr>
<tr>
<td>Failure Code</td>
<td>noError</td>
</tr>
<tr>
<td>Failure Node</td>
<td>n/a</td>
</tr>
<tr>
<td>Explicit Hops</td>
<td>No Hops Specified</td>
</tr>
<tr>
<td>Actual Hops</td>
<td></td>
</tr>
<tr>
<td>10.202.5.194 (38.120.48.194)</td>
<td>Record Label : N/A</td>
</tr>
<tr>
<td>10.202.5.199 (38.120.48.199)</td>
<td>Record Label : 262091</td>
</tr>
<tr>
<td>10.0.9.198 (38.120.48.198)</td>
<td>Record Label : 262096</td>
</tr>
<tr>
<td>38.120.48.184 (38.120.48.184)</td>
<td>Record Label : 262102</td>
</tr>
<tr>
<td>10.0.2.184</td>
<td></td>
</tr>
<tr>
<td>38.120.48.221 (38.120.48.221)</td>
<td>Record Label : 262119</td>
</tr>
<tr>
<td>10.0.4.221</td>
<td></td>
</tr>
<tr>
<td>38.120.48.223 (38.120.48.223)</td>
<td>Record Label : 262088</td>
</tr>
<tr>
<td>10.0.10.223</td>
<td></td>
</tr>
<tr>
<td>38.120.48.224 (38.120.48.224)</td>
<td>Record Label : 262115</td>
</tr>
<tr>
<td>10.101.4.224</td>
<td></td>
</tr>
<tr>
<td>Computed Hops</td>
<td></td>
</tr>
<tr>
<td>10.202.5.199(S)</td>
<td></td>
</tr>
<tr>
<td>10.0.9.198(S)</td>
<td></td>
</tr>
<tr>
<td>10.0.2.184(S)</td>
<td></td>
</tr>
<tr>
<td>10.0.4.221(S)</td>
<td></td>
</tr>
<tr>
<td>10.0.10.223(S)</td>
<td></td>
</tr>
<tr>
<td>10.101.4.224(S)</td>
<td></td>
</tr>
<tr>
<td>Srlg</td>
<td>Disabled</td>
</tr>
<tr>
<td>Srlg Disjoint</td>
<td>False</td>
</tr>
<tr>
<td>Resignal Eligible</td>
<td>False</td>
</tr>
<tr>
<td>Last Resignal</td>
<td>n/a</td>
</tr>
<tr>
<td>CSPF Metric</td>
<td>60</td>
</tr>
</tbody>
</table>

---
4.8 PCEP Configuration Command Reference

4.8.1 Command Hierarchies

• PCEP Commands
• Show Commands
4.8.1.1 PCEP Commands

```plaintext
config
  — router
    — [no] pcep
    — [no] pcc
      — dead-timer seconds
      — no dead-timer
      — keepalive seconds
      — no keepalive
      — local-address ip-address
      — no local-address
      — [no] peer ip-address
        — [no] shutdown
      — [no] report-path-constraints
      — [no] shutdown
      — unknown-message-rate msg/min
      — no unknown-message-rate
```

4.8.1.2 Show Commands

```plaintext
show
  — router
    — pcep
      — pcc
        — detail
        — lsp-db [lsp-type lsp_type] [delegated-pce ip-address]
        — lsp-db [lsp-type lsp_type] from ip-address [delegated-pce ip-address]
        — lsp-db [lsp-type lsp_type] lsp lsp-name [delegated-pce ip-address]
        — lsp-db [lsp-type lsp_type] to ip-address [tunnel-id [tunnel-id]]
        — lsp-db [lsp-type lsp_type] tunnel-id [tunnel-id]
        — path-request [lsp-type (rsvp-p2p)] [dest ip-address] [detail]
        — peer [ip-address] [detail]
        — status
```
4.8.2 Command Descriptions

- PCEP Commands
- Show Commands
4.8.2.1 PCEP Commands

pcep

Syntax [no] pcep
Context config>router
Description This command enables the Path Computation Element Communication Protocol (PCEP) and enters the context to configure PCEP parameters.

The **no** form of the command disables PCEP.

pcc

Syntax [no] pcc
Context config>router>pcep
Description This command enables the context to configure PCC parameters.

dead-timer

Syntax `dead-timer seconds`
`no dead-timer`
Context config>router>pcep>pcc
Description This command configures the PCEP session dead timer value, which is the amount of time a PCEP speaker will wait after the receipt of the last PCEP message before declaring its peer down.

The dead timer mechanism is asymmetric, meaning that each PCEP speaker can propose a different dead timer value to its peer to use to detect session timeout.

The **no** form of the command returns the dead timer to the default value.

Default 120

Parameters `seconds` — the dead timer value, in seconds

Values 1 to 255
keepalive

**Syntax**

```plaintext
keepalive seconds
no keepalive
```

**Context**

```
config>router>pcep>pcc
```

**Description**

This command configures the PCEP session keepalive value. A PCEP speaker must send a keepalive message if no other PCEP message is sent to the peer at the expiry of this timer. This timer is restarted every time a PCEP message or keepalive message is sent.

The keepalive mechanism is asymmetric, meaning that each peer can use a different keepalive timer value at its end.

The `no` form of the command returns the keepalive timer to the default value.

**Default**

30

**Parameters**

- `seconds` — the keepalive value, in seconds
  
  **Values**
  
  1 to 255

---

local-address

**Syntax**

```plaintext
local-address ip-address
no local-address
```

**Context**

```
config>router>pcep>pcc
```

**Description**

This command configures the local address of the PCEP speaker.

The PCEP protocol operates over TCP using destination TCP port 4189. The PCE client (PCC) always initiates the connection. When the user configures the PCEP local address and the peer address on the PCC, the PCC initiates a TCP connection to the PCE. When the connection is established, the PCC and PCE exchange OPEN messages, which initializes the PCEP session and exchanges the session parameters to be negotiated.

The PCC always checks first to determine if the remote PCE address is reachable out-of-band via the management port. If the remote address is not reachable, the PCC will check if the remote PCE address is reachable in-band. When the session comes up out-of-band, the system IP address is always used. The local address configured by the user is only used for in-band sessions and is otherwise ignored.

The `no` form of the command removes the configured local address of the PCEP speaker.

**Parameters**

- `ip-address` — the IP address of the PCEP speaker to be used for in-band sessions
peer

Syntax  
[no] peer ip-address

Context  
config>router>pcep>pcc

Description  
This command configures the IP address of a peer PCEP speaker. The address is used as the destination address in the PCEP session messages to a PCEP peer.

The no form of the command removes the specified peer PCEP speaker.

Parameters  
ip-address — the IP address of the PCEP peer to be used as the destination address in the PCEP session

Values  
a.b.c.d

report-path-constraints

Syntax  
[no] report-path-constraints

Context  
config>router>pcep>pcc

Description  
This command enables the inclusion of LSP path constraints in the PCE report messages sent from the PCC to a PCE.

In order for the PCE to know about the original constraints for an LSP that is delegated but for which there is no prior state in its LSP database; for example, if no PCReq message was sent for the same PLSP-ID, the following proprietary behavior is observed:

• the PCC appends a duplicate of each of the LSPA, metric, and bandwidth objects in the PCRpt message. The only difference between two objects of the same type is that the P-flag is set in the common header of the duplicate object to indicate that it is a mandatory object for processing by the PCE.
• the value of the metric or bandwidth in the duplicate object contains the original constraint value, while the first object contains the operational value. This is applicable to hop metrics in the metric and bandwidth objects only. The 7705 SAR PCC does not support configuring a boundary on the path computation IGP or TE metrics.
• the path computation on the PCE must use the first set of objects when updating a path if the PCRpt message contained a single set. If the PCRpt message contained a duplicate set, PCE path computation must use the constraints in the duplicate set.

The no form of the command disables the above behavior in case of interoperability issues with third-party PCE implementations.

Default  
report-path-constraints
shutdown

Syntax  [no] shutdown

Context  config>router>pcep>pcc
         config>router>pcep>pcc>peer

Description  This command administratively disables the PCC process.

The following PCC parameters can be modified without shutting down the PCEP session:

• report-path-constraints
• unknown-message-rate

The following PCC parameters can only be modified when the PCEP session is shut down:

• local-address
• keepalive
• dead-timer
• peer

Default  shutdown

unknown-message-rate

Syntax  unknown-message-rate msg/min
         no unknown-message-rate

Context  config>router>pcep>pcc

Description  This command configures the maximum rate of unknown messages that can be received during a PCEP session.

When the rate of received unrecognized or unknown messages reaches the configured limit, the PCEP speaker closes the session to the peer.

The no form of the command returns the unknown message rate to the default value.

Default  10

Parameters  msg/min — the rate of unknown messages, in messages per minute

Values  1 to 255
4.8.2.2 Show Commands

**Note:** The following command outputs are examples only; actual displays may differ depending on supported functionality and user configuration.

detail

**Syntax**

detail

**Context**

show>router>pcep>pcc

**Description**

This command displays PCEP PCC detailed information.

**Output**

The following output is an example of PCEP PCC detailed information, and Table 32 describes the fields.

**Output Example**

*A:Sar18 Dut-B>show>router>pcep# pcc detail
================================================================================
Path Computation Element Protocol (PCEP) Path Computation Client (PCC) Info
================================================================================
Admin Status : Down Oper Status : Down
Unknown Msg Limit : 10 msg/min
Keepalive Interval : 50 seconds DeadTimer Interval : 150 seconds
Capabilities List : stateful-delegate stateful-pce rsvp-path
Address : 10.10.10.10
Report Path Constraints: True
Open Wait Timer : 60 seconds Keep Wait Timer : 60 seconds
Sync Timer : 60 seconds Request Timer : 120 seconds
Connection Timer : 60 seconds Allow Negotiations : False
Max Sessions : 1 Max Unknown Req : 1000
================================================================================
*A:Sar18 Dut-B>show>router>pcep#

**Table 32** Show PCEP PCC Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Status</td>
<td>The administrative status of the PCC</td>
</tr>
<tr>
<td>Oper Status</td>
<td>The operational status of the PCC</td>
</tr>
<tr>
<td>Unknown Msg Limit</td>
<td>The maximum rate of unknown messages that can be received on a PCEP session</td>
</tr>
<tr>
<td>Keepalive Interval</td>
<td>The specified keepalive interval for the PCEP session</td>
</tr>
<tr>
<td>DeadTimer Interval</td>
<td>The specified dead time interval for the PCEP session</td>
</tr>
</tbody>
</table>
Table 32  Show PCEP PCC Output Fields (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capabilities List</td>
<td>The capabilities list for the PCEP session</td>
</tr>
<tr>
<td>Address</td>
<td>The local IP address of the PCEP speaker</td>
</tr>
<tr>
<td>Report Path Constraints</td>
<td>Indicates whether to include LSP path constraints in the PCE report messages sent from the PCC to a PCE</td>
</tr>
<tr>
<td>Open Wait Timer</td>
<td>The value of the open wait timer for the PCEP session</td>
</tr>
<tr>
<td>Keep Wait Timer</td>
<td>The value of the keep wait timer for the PCEP session</td>
</tr>
<tr>
<td>Sync Timer</td>
<td>The value of the synchronization timer for the PCEP session</td>
</tr>
<tr>
<td>Request Timer</td>
<td>The value of the request timer for the PCEP session</td>
</tr>
<tr>
<td>Connection Timer</td>
<td>The value of the keep wait timer for the PCEP session</td>
</tr>
<tr>
<td>Allow Negotiations</td>
<td>Indicates where negotiations between PCEP PCC and PCE are allowed</td>
</tr>
<tr>
<td>Max Sessions</td>
<td>The maximum number of PCEP sessions on the router</td>
</tr>
<tr>
<td>Max Unknown Req</td>
<td>The maximum number of unknown requests for PCEP sessions on the router</td>
</tr>
</tbody>
</table>

lsp-db

Syntax

lsp-db [lsp-type lsp_type] [delegated-pce ip-address]
lsp-db [lsp-type lsp_type] from ip-address [delegated-pce ip-address]
lsp-db [lsp-type lsp_type] lsp lsp-name [delegated-pce ip-address]
lsp-db [lsp-type lsp_type] to ip-address [tunnel-id [tunnel-id]]
lsp-db [lsp-type lsp_type] tunnel-id [tunnel-id]

Context

show>router>pce>pcc

Description

This command displays PCEP PCC LSP information.

Parameters

lsp_type — specifies the type of LSP to display. The only available option is RSVP-TE point-to-point LSPs (rsvp-p2p);
tunnel-id — specifies a tunnel ID

Values 0 to 65535

ip-address — specifies an IPv4 address

Values a.b.c.d

Output

The following output is an example of PCEP PCC LSP information.
Output Example

*A:7705:Dut-C# show router pcep pcc lsp-db
===============================================================================
PCEP Path Computation Client (PCC) LSP Update Info
===============================================================================
PCEP-specific LSP ID: 1
  LSP ID : 21504 LSP Type : rsvp-p2p
  Tunnel ID : 1 Extended Tunnel Id : 10.20.1.3
  LSP Name : test_lsp::fully_loose
  Source Address : 10.20.1.3 Destination Address : 10.20.1.1
  LSP Delegated : True Delegate PCE Address: 138.120.210.36
  Oper Status : active
-------------------------------------------------------------------------------
PCEP-specific LSP ID: 2
  LSP ID : 21510 LSP Type : rsvp-p2p
  Tunnel ID : 1 Extended Tunnel Id : 10.20.1.3
  LSP Name : test_lsp::stdby_fully_loose_2
  Source Address : 10.20.1.3 Destination Address : 10.20.1.1
  LSP Delegated : True Delegate PCE Address: 138.120.210.36
  Oper Status : up
===============================================================================
*A:7705:Dut-C#

path-request

Syntax  path-request [lsp-type {rsvp-p2p}] [dest ip-address] [detail]

Context  show>router>pcep>pcc

Description  This command displays PCEP PCC path request information.

Parameters  lsp-type — specifies the type of LSP to display. The only available option is RSVP-TE point-to-point LSPs.
  
ip-address — specifies the destination IPv4 address to display

Values  a.b.c.d
detail — displays detailed path request information

Output  The following output is an example of PCEP PCC path request information.

Output Example

*A:7705:Dut-C# show router pcep pcc path-request
===============================================================================
PCEP Path Computation Client (PCC) Path Computation Request (PCReq) Info
===============================================================================
  Request ID : 4 Message State : sent-for-compute
  Tunnel ID : 2 Extended Tunnel Id : 10.20.1.3
  LSP ID : 62468 LSP Type : rsvp-p2p
  LSP Name : test_lsp::fully_loose
  Source Address : 10.20.1.3 Destination Address: 10.20.1.1
  SVEC Id : 4 LSP Bandwidth : 0
===============================================================================

A:HE 11012 AAAC TQZZA
peer

**Syntax**

```
peer [ip-address] [detail]
```

**Context**

```
show>router>pcep>pcc
```

**Description**

This command displays PCEP PCC peer information.

**Parameters**

- **ip-address** — specifies a peer IPv4 address to display
  
  **Values**
  
  a.b.c.d

- **detail** — displays detailed peer information

**Output**

The following output is an example of a PCEP PCC peer information, and Table 33 describes the fields.

**Output Example**

```
*A:Sar18 Dut-B>show>router>pcep>pcc# peer detail
```

<table>
<thead>
<tr>
<th></th>
<th>Sent</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC Request Message</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PC Reply Message</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PC Error Message</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PC Notification Message</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PC Keepalive Message</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PC Update Message</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PC Report Message</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Path Report</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Path Request</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

```

```
*A:Sar18 Dut-B>show>router>pcep>pcc#
```

---

### Table 33

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>10.10.10.11</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Down</td>
</tr>
<tr>
<td>Peer Capabilities</td>
<td>(Not Specified)</td>
</tr>
<tr>
<td>Speaker ID</td>
<td>(Undefined)</td>
</tr>
<tr>
<td>Sync State</td>
<td>not-initialized</td>
</tr>
<tr>
<td>Peer Overloaded</td>
<td>False</td>
</tr>
<tr>
<td>Session Establish Time</td>
<td>0d 00:00:00</td>
</tr>
<tr>
<td>Oper Keepalive</td>
<td>N/A</td>
</tr>
<tr>
<td>Oper DeadTimer</td>
<td>N/A</td>
</tr>
<tr>
<td>Session Setup Count</td>
<td>0</td>
</tr>
<tr>
<td>Session Setup Fail Count</td>
<td>0</td>
</tr>
</tbody>
</table>
### Table 33  Show PCEP PCC Peer Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the PCC peer</td>
</tr>
<tr>
<td>Admin Status</td>
<td>The administrative status of the PCC peer</td>
</tr>
<tr>
<td>Oper Status</td>
<td>The operational status of the PCC peer</td>
</tr>
<tr>
<td>Peer Capabilities</td>
<td>The PCEP capabilities of the PCC peer</td>
</tr>
<tr>
<td>Speaker ID</td>
<td>The IP address of the PCC peer speaker</td>
</tr>
<tr>
<td>Sync State</td>
<td>The synchronization state of the</td>
</tr>
<tr>
<td>Peer Overloaded</td>
<td>Indicates whether the PCC peer is overloaded</td>
</tr>
<tr>
<td>Session Establish Time</td>
<td>The length of time since the PCEP session was established</td>
</tr>
<tr>
<td>Oper Keepalive</td>
<td>The operational value for the PCC peer keepalive timer</td>
</tr>
<tr>
<td>Oper DeadTimer</td>
<td>The operational value for the PCC peer dead timer</td>
</tr>
<tr>
<td>Session Setup Count</td>
<td>The number of times that the PCEP session has been set up</td>
</tr>
<tr>
<td>Session Setup Fail Count</td>
<td>The number of times that the PCEP session failed to be set up</td>
</tr>
<tr>
<td>Statistics Information</td>
<td></td>
</tr>
<tr>
<td>PC Request Message</td>
<td>The number of path computation (PC) request messages sent the PCC peer and received from the PCC peer</td>
</tr>
<tr>
<td>PC Reply Message</td>
<td>The number of PC reply messages sent to the PCC peer and received from the PCC peer</td>
</tr>
<tr>
<td>PC Error Message</td>
<td>The number of PC error messages sent to the PCC peer and received from the PCC peer</td>
</tr>
<tr>
<td>PC Notification Message</td>
<td>The number of PC notification messages sent to the PCC peer and received from the PCC peer</td>
</tr>
<tr>
<td>PC Keepalive Message</td>
<td>The number of PC keepalive messages sent to the PCC peer and received from the PCC peer</td>
</tr>
<tr>
<td>PC Update Message</td>
<td>The number of PC update messages sent to the PCC peer and received from the PCC peer</td>
</tr>
<tr>
<td>PC Report Message</td>
<td>The number of PC report messages sent to the PCC peer and received from the PCC peer</td>
</tr>
<tr>
<td>Path Report</td>
<td>The number of path reports sent to the PCC peer and received from the PCC peer</td>
</tr>
</tbody>
</table>
status

Syntax  status
Context  show>router>pcep>pcc
Description  This command displays PCEP PCC status information.
Output  The following output is an example of a PCEP PCC status information, and Table 34 describes the fields.

Output Example

*A:Sar18 Dut-B>show>router>pcep>pcc# status
Path Computation Element Protocol (PCEP) Path Computation Client (PCC) Info
Admin Status : Down Oper Status : Down
Unknown Msg Limit : 10 msg/min
Keepalive Interval : 50 seconds DeadTimer Interval : 150 seconds
Capabilities List : stateful-delegate stateful-pce rsvp-path
Address : 10.10.10.10
Report Path Constraints: True
PCEP Path Computation Client (PCC) Peer Info
Peer Admin State/Oper State Oper Keepalive/Oper DeadTimer
10.10.10.11 Down/Down Not-Applicable/Not-Applicable
*A:Sar18 Dut-B>show>router>pcep>pcc#

Table 33  Show PCEP PCC Peer Output Fields (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path Request</td>
<td>The path requests sent to the PCC peer and received from the PCC peer</td>
</tr>
</tbody>
</table>

Table 34  Show PCEP PCC Status Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Status</td>
<td>The administrative status of the PCC</td>
</tr>
<tr>
<td>Oper Status</td>
<td>The operational status of the PCC</td>
</tr>
<tr>
<td>Unknown Msg Limit</td>
<td>The maximum rate of unknown messages that can be received on a PCEP session</td>
</tr>
<tr>
<td>Keepalive Interval</td>
<td>The specified keepalive interval for the PCEP session</td>
</tr>
</tbody>
</table>
### Show PCEP PCC Status Output Fields (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeadTimer Interval</td>
<td>The specified dead time interval for the PCEP session</td>
</tr>
<tr>
<td>Capabilities List</td>
<td>The capabilities list for the PCEP session</td>
</tr>
<tr>
<td>Address</td>
<td>The local IP address of the PCEP speaker</td>
</tr>
<tr>
<td>Report Path Constraints</td>
<td>Indicates whether to include LSP path constraints in the PCE report messages sent from the PCC to a PCE</td>
</tr>
</tbody>
</table>

**PCEP Path Computation Client (PCC) Peer Info**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer</td>
<td>The IP address of the PCC peer</td>
</tr>
<tr>
<td>Admin State/Oper State</td>
<td>The administrative and operational states of the PCC peer</td>
</tr>
<tr>
<td>Oper Keepalive/Oper DeadTimer</td>
<td>The operational keepalive and dead timer intervals of the PCC peer</td>
</tr>
</tbody>
</table>
5 Label Distribution Protocol

This chapter provides information to enable the Label Distribution Protocol (LDP).

Topics in this chapter include:

- Label Distribution Protocol
- LDP Point-to-Multipoint Support
- Multicast LDP Fast Upstream Switchover
- LDP Process Overview
- Configuration Notes
- Configuring LDP with CLI
- LDP Command Reference
5.1 Label Distribution Protocol

Label Distribution Protocol (LDP) is used to distribute labels in non-traffic-engineered applications. LDP allows routers to establish LSPs through a network by mapping network-layer routing information directly to data link LSPs.

An LSP is defined by the set of labels from the ingress LER to the egress LER. LDP associates a Forwarding Equivalence Class (FEC) with each LSP it creates. A FEC is a collection of common actions associated with a class of packets. When an ingress LER assigns a label to a FEC, it must let other LSRs in the path know about the label. LDP helps to establish the LSP by providing a set of procedures that LSRs can use to distribute labels.

The FEC associated with an LSP specifies which packets are mapped to that LSP. LSPs are extended through a network by each LSR, where each LSR splices incoming labels for the FEC to the outgoing label assigned to the next hop for the FEC.

LDP allows an LSR to request a label from a downstream LSR so it can bind the label to a specific FEC. The downstream LSR responds to the request from the upstream LSR by sending the requested label.

LSRs can distribute a FEC label binding in response to an explicit request from another LSR. This is known as Downstream On Demand (DOD) label distribution. LSRs can also distribute label bindings to LSRs that have not explicitly requested them. This is called Downstream Unsolicited (DU). For LDP on the 7705 SAR, Downstream Unsolicited (DU) mode is implemented.

This section contains the following topics:

- LDP and MPLS
- LDP Architecture
- LDP Subsystem Interrelationships
- Execution Flow
- Label Exchange
- LDP Filters
- Multi-area and Multi-instance Extensions to LDP
- ECMP Support for LDP
- Graceful Restart Helper
- Graceful Handling of Resource Exhaustion
- LDP Support for Unnumbered Interfaces
- LDP Fast Reroute (FRR)
LDP performs dynamic label distribution in MPLS environments. The LDP operation begins with a Hello discovery process network to form an adjacency with an LDP peer in the network. LDP peers are two MPLS routers that use LDP to exchange label/FEC mapping information. An LDP session is created between LDP peers. A single LDP session allows each peer to learn the other's label mappings and to distribute its own label information (LDP is bidirectional), and exchange label binding information.

LDP signaling works with the MPLS label manager to manage the relationships between labels and the corresponding FEC. For service-based FECs, LDP works in tandem with the Service Manager to identify the virtual leased lines (VLLs) and pseudowires (PWs) to signal.

An MPLS label identifies a set of actions that the forwarding plane performs on an incoming packet before discarding it. The FEC is identified through the signaling protocol (in this case LDP), and is allocated a label. The mapping between the label and the FEC is communicated to the forwarding plane. In order for this processing on the packet to occur at high speeds, optimized tables that enable fast access and packet identification are maintained in the forwarding plane.

When an unlabeled packet ingresses the 7705 SAR, classification policies associate it with a FEC, the appropriate label is imposed on the packet, and then the packet is forwarded. Other actions can also take place on a packet before it is forwarded, including imposing additional labels, other encapsulations, or learning actions. Once all actions associated with the packet are completed, the packet is forwarded.

When a labeled packet ingresses the router, the label or stack of labels indicates the set of actions associated with the FEC for that label or label stack. The actions are performed on the packet and then the packet is forwarded.

The LDP implementation provides support for DU, ordered control, and liberal label retention mode.

For LDP label advertisement, DU mode is supported. To prevent filling the uplink bandwidth with unassigned label information, Ordered Label Distribution Control mode is supported.
A PW/VLL label can be dynamically assigned by targeted LDP operations. Targeted LDP allows the inner labels (that is, the VLL labels) in the MPLS headers to be managed automatically. This makes it easier for operators to manage the VLL connections. There is, however, additional signaling and processing overhead associated with this targeted LDP dynamic label assignment.

5.1.1.1 BFD for T-LDP

BFD is a simple protocol for detecting failures in a network. BFD uses a “hello” mechanism that sends control messages periodically to the far end and receives periodic control messages from the far end. BFD is implemented in asynchronous mode only, meaning that neither end responds to control messages; rather, the messages are sent in the time period configured at each end.

A T-LDP session is a session between either directly or non-directly connected peers and requires that adjacencies be created between two peers. BFD for T-LDP sessions allows support for tracking of failures of nodes that are not directly connected. BFD timers must be configured under the system router interface context before being enabled under T-LDP.

BFD tracking of an LDP session associated with a T-LDP adjacency allows for faster detection of the status of the session by registering the loopback address of the peer as the transport address.

5.1.2 LDP Architecture

LDP comprises a few processes that handle the protocol PDU transmission, timer-related issues, and protocol state machine. The number of processes is kept to a minimum to simplify the architecture and to allow for scalability. Scheduling within each process prevents starvation of any particular LDP session, while buffering alleviates TCP-related congestion issues.

The LDP subsystems and their relationships to other subsystems are illustrated in Figure 19. This illustration shows the interaction of the LDP subsystem with other subsystems, including memory management, label management, service management, SNMP, interface management, and RTM. In addition, debugging capabilities are provided through the logger.
Communication within LDP tasks is typically done by interprocess communication through the event queue, as well as through updates to the various data structures. The following list describes the primary data structures that LDP maintains:

- **FEC/label database** — this database contains all the FEC-to-label mappings, including both sent and received. It also contains both address FECs (prefixes and host addresses) as well as service FECs (L2 VLLs).
- **Timer database** — this database contains all the timers for maintaining sessions and adjacencies
- **Session database** — this database contains all the session and adjacency records, and serves as a repository for the LDP MIB objects

### 5.1.3 LDP Subsystem Interrelationships

*Figure 19* shows the relationships between LDP subsystems and other 7705 SAR subsystems. The following sections describe how the subsystems work to provide services.

#### 5.1.3.1 Memory Manager and LDP

LDP does not use any memory until it is instantiated. It preallocates some amount of fixed memory so that initial startup actions can be performed. Memory allocation for LDP comes out of a pool reserved for LDP that can grow dynamically as needed.

Fragmentation is minimized by allocating memory in large chunks and managing the memory internally to LDP. When LDP is shut down, it releases all memory allocated to it.

#### 5.1.3.2 Label Manager

LDP assumes that the label manager is up and running. LDP will abort initialization if the label manager is not running. The label manager is initialized at system boot-up; hence anything that causes it to fail will likely indicate that the system is not functional. The 7705 SAR uses a label range from 28 672 (28K) to 131 071 (128K-1) to allocate all dynamic labels, including VC labels.
5.1.3.3 LDP Configuration

The 7705 SAR uses a single consistent interface to configure all protocols and services. CLI commands are translated to SNMP requests and are handled through an agent-LDP interface. LDP can be instantiated or deleted through SNMP. Also, targeted LDP sessions can be set up to specific endpoints. Targeted session parameters are configurable.
5.1.3.4 Logger

LDP uses the logger interface to generate debug information relating to session setup and teardown, LDP events, label exchanges, and packet dumps. Per-session tracing can be performed. Refer to the 7705 SAR System Management Guide for logger configuration information.

5.1.3.5 Service Manager

All interaction occurs between LDP and the service manager, since LDP is used primarily to exchange labels for Layer 2 services. In this context, the service manager informs LDP when an LDP session is to be set up or torn down, and when labels are to be exchanged or withdrawn. In turn, LDP informs the service manager of relevant LDP events, such as connection setups and failures, timeouts, and labels signaled or withdrawn.

5.1.4 Execution Flow

LDP activity in the 7705 SAR is limited to service-related signaling. Therefore, the configurable parameters are restricted to system-wide parameters, such as hello and keepalive timeouts.

5.1.4.1 Initialization

MPLS must be enabled when LDP is initialized. LDP makes sure that the various prerequisites are met, such as ensuring that the system IP interface and the label manager are operational, and ensuring that there is memory available. It then allocates a pool of memory to itself and initializes its databases.

5.1.4.2 Session Lifetime

In order for a targeted LDP session to be established, an adjacency has to be created. The LDP extended discovery mechanism requires hello messages to be exchanged between two peers for session establishment. Once the adjacency is established, session setup is attempted.
5.1.4.2.1 Adjacency Establishment

In the 7705 SAR, adjacency management is done through the establishment of a Service Destination Point (SDP) object, which is a service entity in the Nokia service model.

The service model uses logical entities that interact to provide a service. The service model requires the service provider to create and configure four main entities:

- customers
- services
- Service Access Points (SAPs) on local 7705 SAR routers
- SDPs that connect to one or more remote 7705 SAR routers or 77x0 SR routers

An SDP is the network-side termination point for a tunnel to a remote 7705 SAR or 77x0 SR router. An SDP defines a local entity that includes the system IP address of the remote 7705 SAR routers and 77x0 SR routers, and a path type.

Each SDP comprises:

- the SDP ID
- the transport encapsulation type, MPLS
- the far-end system IP address

If the SDP is identified as using LDP signaling, then an LDP extended hello adjacency is attempted.

If another SDP is created to the same remote destination and if LDP signaling is enabled, no further action is taken, since only one adjacency and one LDP session exists between the pair of nodes.

An SDP is a unidirectional object, so a pair of SDPs pointing at each other must be configured in order for an LDP adjacency to be established. Once an adjacency is established, it is maintained through periodic hello messages.

5.1.4.2.2 Session Establishment

When the LDP adjacency is established, the session setup follows as per the LDP specification. Initialization and keepalive messages complete the session setup, followed by address messages to exchange all interface IP addresses. Periodic keepalives or other session messages maintain the session liveness.
Since TCP is back-pressured by the receiver, it is necessary to be able to push that back-pressure all the way into the protocol. Packets that cannot be sent are buffered on the session object and reattempted as the back-pressure eases.

5.1.5 Label Exchange

Label exchange is initiated by the service manager. When an SDP is attached to a service (that is, once the service gets a transport tunnel), a message is sent from the service manager to LDP. This causes a label mapping message to be sent. Additionally, when the SDP binding is removed from the service, the VC label is withdrawn. The peer must send a label release to confirm that the label is not in use.

5.1.5.1 Other Reasons for Label Actions

Label actions can also occur for the following reasons:

- MTU changes — LDP withdraws the previously assigned label and resignals the FEC with the new Maximum Transmission Unit (MTU) in the interface parameter
- clear labels — when a service manager command is issued to clear the labels, the labels are withdrawn and new label mappings are issued
- SDP down — when an SDP goes administratively down, the VC label associated with that SDP for each service is withdrawn
- memory allocation failure — if there is no memory to store a received label, the received label is released
- VC type unsupported — when an unsupported VC type is received, the received label is released

5.1.5.2 Cleanup

LDP closes all sockets, frees all memory, and shuts down all its tasks when it is deleted, so that it uses no memory (0 bytes) when it is not running.
5.1.6 LDP Filters

The 7705 SAR supports both inbound and outbound LDP label binding filtering.

Inbound filtering (import policy) allows the user to configure a policy to control the label bindings an LSR (Label Switch Router) accepts from its peers.

Import policy label bindings can be filtered based on the following:

- neighbor — match on bindings received from the specified peer
- prefix-list — match on bindings with the specified prefix/prefixes

The default import behavior is to accept all FECs received from peers.

Outbound filtering (export policy) allows the user to configure a policy to control the set of LDP label bindings advertised by the LSR (Label Switch Router).

Because the default behavior is to originate label bindings for the system IP address only, when a non-default loopback address is used as the transport address, the 7705 SAR will not advertise the loopback FEC automatically. With LDP export policy, the user is now able to explicitly export the loopback address in order to advertise the loopback address label and allow the node to be reached by other network elements.

Export policy label bindings can be filtered based on the following:

- all — all local subnets by specifying “direct” as the match protocol
- prefix-list — match on bindings with the specified prefix/prefixes

Note: In order for the 7705 SAR to consider a received label to be active, there must be an exact match to the FEC advertised together with the label found in the routing table, or a longest prefix match (if the aggregate-prefix-match option is enabled; see Multi-area and Multi-instance Extensions to LDP). This can be achieved by configuring a static route pointing to the prefix encoded in the FEC.
5.1.7 Multi-area and Multi-instance Extensions to LDP

When a network has two or more IGP areas, or instances, inter-area LSPs are required for MPLS connectivity between the PE devices that are located in the distinct IGP areas. In order to extend LDP across multiple areas of an IGP instance or across multiple IGP instances, the current standard LDP implementation based on RFC 3036, *LDP Specification*, requires that all /32 prefixes of PEs be leaked between the areas or instances. IGP route leaking is the distribution of the PE loopback addresses across area boundaries. An exact match of the prefix in the routing table (RIB) is required to install the prefix binding in the FIB and set up the LSP.

This behavior is the default behavior for the 7705 SAR when it is configured as an Area Border Router (ABR). However, exact prefix matching causes performance issues for the convergence of IGP on routers deployed in networks where the number of PE nodes scales to thousands of nodes. Exact prefix matching requires the RIB and FIB to contain the IP addresses maintained by every LSR in the domain and requires redistribution of a large number of addresses by the ABRs. Security is a potential issue as well, as host routes leaked between areas can be used in DoS and DDoS attacks and spoofing attacks.

To avoid these performance and security issues, the 7705 SAR can be configured for an optional behavior in which LDP installs a prefix binding in the LDP FIB by performing a longest prefix match with an aggregate prefix in the routing table (RIB). This behavior is described in RFC 5283, *LDP Extension for Inter-Area Label Switched Paths*. The LDP prefix binding continues to be advertised on a per-individual /32 prefix basis.

When the longest prefix match option is enabled and an LSR receives a FEC-label binding from an LDP neighbor for a prefix-address FEC element, FEC1, it installs the binding in the LDP FIB if:

- the routing table (RIB) contains an entry that matches FEC1. Matching can either be a longest IP match of the FEC prefix or an exact match.
- the advertising LDP neighbor is the next hop to reach FEC1

When the FEC-label binding has been installed in the LDP FIB, LDP programs an NHLFE entry in the egress data path to forward packets to FEC1. LDP also advertises a new FEC-label binding for FEC1 to all its LDP neighbors.

When a new prefix appears in the RIB, LDP checks the LDP FIB to determine if this prefix is a closer match for any of the installed FEC elements. If a closer match is found, this may mean that the LSR used as the next hop will change; if so, the NHLFE entry for that FEC must be changed.
When a prefix is removed from the RIB, LDP checks the LDP FIB for all FEC elements that matched this prefix to determine if another match exists in the routing table. If another match exists, LDP must use it. This may mean that the LSR used as the next hop will change; if so, the NHLFE entry for that FEC must be changed. If another match does not exist, the LSR removes the FEC binding and sends a label withdraw message to its LDP neighbors.

If the next hop for a routing prefix changes, LDP updates the LDP FIB entry for the FEC elements that matched this prefix. It also updates the NHLFE entry for the FEC elements.

5.1.8 ECMP Support for LDP

Equal-Cost Multipath Protocol (ECMP) support for LDP performs load balancing for services that use LDP-based LSPs as transport tunnels, by having multiple equal-cost outgoing next hops for an IP prefix.

ECMP for LDP load-balances traffic across all equal-cost links based on the output of the hashing algorithm using the allowed inputs, based on the service type. For detailed information, refer to “LAG and ECMP Hashing” in the 7705 SAR Interface Configuration Guide.

There is only one next-hop peer for a network link. To offer protection from a network link or next-hop peer failure, multiple network links can be configured to connect to different next-hop peers, or multiple links to the same peer. For example, an MLPPP link and an Ethernet link can be connected to two peers, or two Ethernet links can be connected to the same peer. ECMP occurs when the cost of each link reaching a target IP prefix is equal.

The 7705 SAR uses a liberal label retention mode, which retains all labels for an IP prefix from all next-hop peers. A 7705 SAR acting as an LSR load-balances the MPLS traffic over multiple links using a hashing algorithm.

The 7705 SAR supports the following optional fields as hash inputs and supports profiles for various combinations:

- hashing algorithms
  - label-only option: hashing is done on the MPLS label stack, up to a maximum of 10 labels (default)
  - label-IP option: hashing is done on the MPLS label stack and the IPv4 source and destination IP address if an IPv4 header is present after the MPLS labels
- Layer 4 header (source or destination UDP or TCP port number) and TEID: hashing is done on the MPLS label stack, the IPv4 source and destination IP address (if present), then on the Layer 4 source and destination UDP or TCP port fields (if present) and the TEID in the GTP header (if present)

- label stack profile options on significance of the bottom-of-stack label (VC label)
  - profile 1: favors better load balancing for pseudowires when the VC label distribution is contiguous (default)
  - profile 2: similar to profile 1 where the VC labels are contiguous, but provides an alternate distribution
  - profile 3: all labels have equal influence in hash key generation

- ingress LAG port at the LSR (default is disabled)
  The **use-ingress-port** option, when enabled, specifies that the ingress port will be used by the hashing algorithm at the LSR. This option should be enabled for ingress LAG ports because packets with the same label stack can arrive on all ports of a LAG interface. In this case, using the ingress port in the hashing algorithm will result in better egress load balancing, especially for pseudowires. The option should be disabled for LDP ECMP so that the ingress port is not used by the hashing algorithm. For ingress LDP ECMP, if the ingress port is used by the hashing algorithm, the hash distribution could be biased, especially for pseudowires.

- system IP address – hashing on the system IP address is enabled and disabled at the system level only

All of the above options can be configured with the lsr-load-balancing command, with the exception of the system IP address, which is configured with the system-ip-load-balancing command.

**Note:** The global IF index is no longer a hash input for LSR ECMP load balancing. It has been replaced with the **use-ingress-port** configurable option in the lsr-load-balancing command. As well, the default treatment of the MPLS label stack has changed to focus on the bottom-of-stack label (VC label). In previous releases, all labels had equal influence.

LSR load balancing can be configured at the system level or interface level. Configuration at the interface level overrides the system-level settings for the specific interface. Configuration must be done on the ingress network interface (that is, the interface on the LDP LSR node that the packet is received on).
Configuration of load balancing at the interface level provides some control to the user; for example, the label-IP option can be disabled on a specific interface if labeled packets received on the interface include non-IP packets that can be confused by the hash routine for IP packets. Disabling the label-IP option can be used in cases where the first nibble of a non-IP packet is a 4, which would result in the packet being hashed incorrectly if the label-IP option was enabled.

If ECMP is not enabled, the label from only one of the next-hop peers is selected and installed in the forwarding plane. In this case, the algorithm used to distribute the traffic flow looks up the route information, and selects the network link with the lowest IP address. If the selected network link or next-hop peer fails, another next-hop peer is selected, and LDP reprograms the forwarding plane to use the label sent by the newly selected peer.

ECMP is supported on all Ethernet ports in network mode, and is also supported on the 4-port OC3/STM1 Clear Channel Adapter card when it is configured for POS (ppp-auto) encapsulation and network mode.

For information on configuring the 7705 SAR for LSR ECMP, refer to the `lsr-load-balancing` and `system-ip-load-balancing` commands in the 7705 SAR Basic System Configuration Guide, “System Information and General Commands” and the `lsr-load-balancing` command in the 7705 SAR Router Configuration Guide, “Router Interface Commands”.

For information on LDP treetrace commands for tracing ECMP paths, refer to the 7705 SAR OAM and Diagnostics Guide.

**Note:** LDP treetrace works best with label-IP hashing (lbl-ip) enabled, rather than label-only (lbl-only) hashing. These options are set with the `lsr-load-balancing` command.

**Note:**

- Because of the built-in timeout to dynamic ARP, the MAC address of the remote peer needs to be renewed periodically. The flow of IP traffic resets the timers back to their maximum values. In the case of LDP ECMP, one link could be used for transporting user MPLS (pseudowire) traffic but the LDP session could possibly be using a different equal-cost link. For LDPs using ECMP and for static LSPs, it is important to ensure that the remote MAC address is learned and does not expire. Configuring static ARP entries or running continuous IP traffic ensures that the remote MAC address is always known. Running BFD for fast detection of Layer 2 faults or running any OAM tools with SAA ensures that the learned MAC addresses do not expire.
- ARP entries are refreshed by static ARP and BFD, SAA, OSPF, IS-IS, or BGP.
- For information on configuring static ARP and running BFD, refer to the 7705 SAR Router Configuration Guide.
5.1.8.1 Label Operations

If an LSR is the ingress router for a given IP prefix, LDP programs a PUSH operation for the prefix in the IOM. This creates an LSP ID to the Next Hop Label Forwarding Entry (NHLFE) mapping (LTN mapping) and an LDP tunnel entry in the forwarding plane. LDP will also inform the Tunnel Table Manager (TTM) about this tunnel. Both the LSP ID to NHLFE (LTN) entry and the tunnel entry will have an NHLFE for the label mapping that the LSR received from each of its next-hop peers.

If the LSR is to behave as a transit router for a given IP prefix, LDP will program a SWAP operation for the prefix in the IOM. This involves creating an Incoming Label Map (ILM) entry in the forwarding plane. The ILM entry might need to map an incoming label to multiple NHLFEs.

If an LSR is an egress router for a given IP prefix, LDP will program a POP entry in the IOM. This too will result in an ILM entry being created in the forwarding plane, but with no NHLFEs.

When unlabeled packets arrive at the ingress LER, the forwarding plane consults the LTN entry and uses a hashing algorithm to map the packet to one of the NHLFEs (PUSH label) and forward the packet to the corresponding next-hop peer. For a labeled packet arriving at a transit or egress LSR, the forwarding plane consults the ILM entry and either uses a hashing algorithm to map it to one of the NHLFEs if they exist (SWAP label) or routes the packet if there are no NHLFEs (POP label).

5.1.9 Graceful Restart Helper

Graceful Restart (GR) is part of the LDP handshake process (that is, the LDP peering session initialization) and needs to be supported by both peers. GR provides a mechanism that allows the peers to cope with a service interruption due to a CSM switchover, which is a period of time when the standby CSM is not capable of synchronizing the states of the LDP sessions and labels being advertised and received.

Graceful Restart Helper (GR-Helper) decouples the data plane from the control plane so that if the control plane is not responding (that is, there is no LDP message exchange between peers), then the data plane can still forward frames based on the last known (advertised) labels.
Because the 7705 SAR supports non-stop services / high-availability for LDP (and MPLS), the full implementation of GR is not needed. However, GR-Helper is implemented on the 7705 SAR to support non-high-availability devices. With GR-Helper, if an LDP peer of the 7705 SAR requests GR during the LDP handshake, the 7705 SAR agrees to it but does not request GR. For the duration of the LDP session, if the 7705 SAR LDP peer fails, the 7705 SAR continues to forward MPLS packets based on the last advertised labels and will not declare the peer dead until the GR timer expires.

5.1.10 Graceful Handling of Resource Exhaustion

Graceful handling of resource exhaustion enhances the behavior of LDP when a data path or a CSM resource required for the resolution of a FEC is exhausted. In prior releases, the entire LDP protocol was shut down, causing all LDP peering sessions to be torn down and therefore impacting all peers. The user was required to fix the issue that caused the FEC scaling to be exceeded, and to restart the LDP session by executing the `no shutdown` CLI command. With graceful handling of resource exhaustion, only the responsible session or sessions are shut down, which impacts only the appropriate peer or peers.

Graceful handling of resources implements a capability by which the LDP interface to the peer, or the targeted peer in the case of a targeted LDP (T-LDP) session, is shut down.

If LDP tries to resolve a FEC over a link or a T-LDP session and runs out of data path or CSM resources, LDP brings down that interface or targeted peer, which brings down the Hello adjacency over that interface to all linked LDP peers or to the targeted peer. The interface is brought down for the LDP context only and is still available to other applications such as IP forwarding and RSVP LSP forwarding.

After taking action to free up resources, the user must manually perform a `no shutdown` command on the interface or the targeted peer to bring it back into operation. This re-establishes the Hello adjacency and resumes the resolution of FECs over the interface or to the targeted peer.
5.1.11 LDP Support for Unnumbered Interfaces

Unnumbered interfaces are point-to-point interfaces that are not explicitly configured with a dedicated IP address and subnet; instead, they borrow (or link to) an IP address from another interface on the system (the system IP address, another loopback interface, or any other numbered interface) and use it as the source IP address for packets originating from the interface. For more information on support for unnumbered interfaces, refer to the 7705 SAR Router Configuration Guide, “Unnumbered Interfaces”.

This feature allows LDP to establish a Hello adjacency and to resolve unicast FECs over unnumbered LDP interfaces.

For example, LSR A and LSR B are the two endpoints of an unnumbered link. These interfaces are identified on each system with their unique link local identifier. The combination router ID and link local identifier uniquely identifies the interface in IS-IS throughout the network.

A borrowed IP address is also assigned to the interface to be used as the source address of IP packets that must originate from the interface. The borrowed IP address defaults to the system interface address, A and B in this example. The borrowed IP interface can be configured to any IP interface by using the following CLI command:

```
config> router>interface>unnumbered {ip-int-name | ip-address}.
```

The `fec-originate` command, which defines how to originate a FEC for egress and non-egress LSRs, includes a parameter to specify the name of the interface that the label for the originated FEC is swapped to. For an unnumbered interface, this parameter is mandatory because an unnumbered interface does not have its own IP address.

When the unnumbered interface is added into LDP, the follow behavior occurs.

**For link LDP (L-LDP) sessions:**

1. The Hello adjacency is brought up using a link Hello packet with the source IP address set to the interface borrowed IP address and a destination IP address set to 224.0.0.2.

2. Hello packets with the same source IP address should be accepted when received over parallel unnumbered interfaces from the same peer LSR ID. The corresponding Hello adjacencies are associated with a single LDP session.

3. The transport address for the TCP connection, which is encoded in the Hello packet, is always set to the LSR ID of the node whether or not the interface option was enabled using the `config>router>ldp>interface-parameters>interface>transport-address` command.
4. The **local-lsr-id** option can be configured on the interface and the value of the LSR ID can be changed to either the local interface or to some other interface name. If the local interface is selected or the provided interface name corresponds to an unnumbered IP interface, the unnumbered interface borrowed IP address is used as the LSR ID. In all cases, the transport address for the LDP session is updated to the new LSR ID value, but the link Hello packets continue to use the interface borrowed IP address as the source IP address.

5. The LSR with the highest transport address, the LSR ID in this case, bootstraps the TCP connection and LDP session.

6. The source and destination IP addresses of LDP packets are the transport addresses, that is, the LDP LSR IDs of the LSRs at the endpoints of the link (A and B in the example).

**For targeted LDP (T-LDP) sessions:**

1. The source and destination addresses of the targeted Hello packet are the LDP LSR IDs of systems A and B.

2. The **local-lsr-id** option can be configured on the interface for the targeted session and the value of the LSR ID can be changed to either the local interface or to some other interface name. If the local interface is selected or the provided interface name corresponds to an unnumbered IP interface, the unnumbered interface borrowed IP address is used as the LSR ID. In all cases, the transport address for the LDP session and the source IP address of the targeted Hello message are updated to the new LSR ID value.

3. The LSR with the highest transport address, the LSR ID in this case, bootstraps the TCP connection and LDP session.

4. The source and destination IP addresses of LDP packets are the transport addresses, that is, the LDP LSR IDs of the LSRs at the endpoints of the link (A and B in the example).
**FEC resolution:**

- LDP advertises/withdraws unnumbered interfaces using the Address/Address-Withdraw message. The borrowed IP address of the interface is used.
- A FEC can be resolved to an unnumbered interface in the same way as it is resolved to a numbered interface. The outgoing interface and next hop are looked up in the RTM cache. The next hop is the router ID and link identifier of the interface at the peer LSR.
- LDP FEC ECMP next hops over a mix of unnumbered and numbered interfaces are supported.
- All LDP FEC types are supported.
- The `fec-originate` command is supported when the next hop is over an unnumbered interface.

All LDP features supported for numbered IP interfaces are supported for unnumbered interfaces, with the following exceptions:

- BFD is not supported on unnumbered IP interfaces
- LDP FRR is not triggered by a BFD session timeout, only by a physical failure or the local interface going down
- unnumbered IP interfaces cannot be added into LDP global and peer prefix policies

The unnumbered interface feature also extends the support of LSP ping and LSP traceroute to test an LDP unicast FEC that is resolved over an unnumbered LDP interface.

### 5.1.12 LDP Fast Reroute (FRR)

LDP Fast Reroute (FRR) provides local protection for an LDP FEC by precalculating and downloading a primary and a backup NHLFE for the FEC to the LDP FIB. The primary NHLFE corresponds to the label of the FEC received from the primary next hop as per the standard LDP resolution of the FEC prefix in the RTM. The backup NHLFE corresponds to the label received for the same FEC from a Loop-Free Alternate (LFA) next hop.

LDP FRR protects against single link or single node failure. SRLG failure protection is not supported.
Without FRR, when a local link or node fails, the router must signal the failure to its neighbors via the IGP providing the routing (OSPF or IS-IS), recalculate primary next-hop NHLFEs for all affected FECs, and update the FIB. Until the new primary next hops are installed in the FIB, any traffic destined for the affected FECs is discarded. This process can take hundreds of milliseconds.

LDP FRR improves convergence in case of a local link or node failure in the network, by using the label-FEC binding received from the LFA next hop to forward traffic for a given prefix as soon as the primary next hop is not available. This means that a router resumes forwarding LDP packets to a destination prefix using the backup path without waiting for the routing convergence. Convergence times should be similar to RSVP-TE FRR, in the tens of milliseconds.

OSPF or IS-IS must perform the Shortest Path First (SPF) calculation of an LFA next hop, as well as the primary next hop, for all prefixes used by LDP to resolve FECs. The IGP also populates both routes in the RTM.

When LDP FRR is enabled and an LFA backup next hop exists for the FEC prefix in the RTM, or for the longest prefix the FEC prefix matches to when the aggregate-prefix-match option is enabled, LDP will program the data path with both a primary NHLFE and a backup NHLFE for each next hop of the FEC.

In order to perform a switchover to the backup NHLFE in the fast path, LDP follows the standard FRR failover procedures, which are also supported for RSVP-TE FRR.

When any of the following events occurs, the backup NHLFE is enabled for each affected FEC next hop:

- an LDP interface goes operationally down or is administratively shut down
  In this case, LDP sends a neighbor/next hop down message to each LDP with which it has an adjacency over the interface.
- an LDP session to a peer goes down because the Hello timer or keepalive timer has expired over an interface
  In this case, LDP sends a neighbor/next hop down message to the affected peer.
- the TCP connection used by a link LDP session to a peer goes down
  In this case, LDP sends a neighbor/next hop down message to the affected peer.

Refer to RFC 5286, Basic Specification for IP Fast Reroute: Loop-Free Alternates, for more information on LFAs.
5.1.12.1 ECMP vs FRR

If ECMP is enabled, which provides multiple primary next hops for a prefix, LDP FRR is not used. That is, the LFA next hops are not populated in the RTM and the ECMP paths are used instead.

5.1.12.2 IGP Shortcuts (RSVP-TE Tunnels)

IGP shortcuts are an MPLS functionality where LSPs are treated like physical links within IGPs; that is, LSPs can be used for next-hop reachability. If an RSVP-TE LSP is used as a shortcut by OSPF or IS-IS, it is included in the SPF calculation as a point-to-point link for both primary and LFA next hops. It can also be advertised to neighbors so that the neighboring nodes can also use the links to reach a destination via the advertised next hop.

IGP shortcuts can be used to simplify remote LFA support and simplify the number of LSPs required in a ring topology.

When both IGP shortcuts and LFA are enabled under OSPF or IS-IS, and LDP FRR is also enabled, the following applies:

- a FEC that is resolved to a direct primary next hop can be backed up by a tunneled LFA next hop
- a FEC that is resolved to a tunneled primary next hop will not have an LFA next hop; it relies on RSVP-TE FRR for protection

5.1.12.3 LDP FRR Configuration

To configure LDP FRR, LFA calculation by the SPF algorithm must first be enabled under the OSPF or IS-IS protocol level with the command:

```
config>router>ospf>loopfree-alternate
```

or

```
config>router>ospf3>loopfree-alternate
```

or

```
config>router>isis>loopfree-alternate
```

Next, LDP must be enabled to use the LFA next hop with the command

```
config>router>ldp>fast-reroute
```
If IGP shortcuts are used, they must be enabled under the OSPF or IS-IS routing protocol. As well, they must be enabled under the MPLS LSP context, using the command `config>router>mpls>lsp>igp-shortcut`.

For information on LFA and IGP shortcut support for OSPF and IS-IS, refer to the 7705 SAR Routing Protocols Guide, “LDP and IP Fast Reroute for OSPF Prefixes” and “LDP and IP Fast Reroute for IS-IS Prefixes”.

Both LDP FRR and IP FRR are supported; for information on IP FRR, refer to the 7705 SAR Router Configuration Guide, “IP Fast Reroute (FRR)”.

### 5.1.13 TCP MD5 Authentication

The operation of a network can be compromised if an unauthorized system is able to form or hijack an LDP session and inject control packets by falsely representing itself as a valid neighbor. This risk can be mitigated by enabling TCP MD5 authentication on one or more of the sessions.

When TCP MD5 authentication is enabled on a session, every TCP segment exchanged with the peer includes a TCP option (19) containing a 16-byte MD5 digest of the segment (more specifically the TCP/IP pseudo-header, TCP header, and TCP data). The MD5 digest is generated and validated using an authentication key that must be known to both sides. If the received digest value is different from the locally computed one, the TCP segment is dropped, thereby protecting the router from a spoofed TCP segment.

The TCP Enhanced Authentication Option, as specified in `draft-bonica-tcpauth-05.txt`, *Authentication for TCP-based Routing and Management Protocols*, is a TCP extension that enhances security for LDP, BGP, and other TCP-based protocols. It extends the MD5 authentication option to include the ability to change keys in an LDP or BGP session seamlessly without tearing down the session, and allows for stronger authentication algorithms to be used. It is intended for applications where secure administrative access to both endpoints of the TCP connection is normally available.

TCP peers can use this extension to authenticate messages passed between one another. This strategy improves upon the practice described in RFC 2385, *Protection of BGP Sessions via the TCP MD5 Signature Option*. Using this new strategy, TCP peers can update authentication keys during the lifetime of a TCP connection. TCP peers can also use stronger authentication algorithms to authenticate routing messages.
TCP enhanced authentication uses keychains that are associated with every protected TCP connection.

Keychains are configured in the config>system>security>keychain context. For more information about configuring keychains, refer to the 7705 SAR System Management Guide, “TCP Enhanced Authentication and Keychain Authentication”.
5.2  LDP Point-to-Multipoint Support

The 7705 SAR supports point-to-multipoint mLDP. This section contains information on the following topics:

- LDP Point-to-Multipoint Configuration
- LDP Point-to-Multipoint Protocol
- Make-Before-Break (MBB)
- ECMP Support

5.2.1  LDP Point-to-Multipoint Configuration

A node running LDP also supports point-to-multipoint LSP setup using LDP. By default, the node advertises the capability to a peer node using the point-to-multipoint capability TLV in LDP initialization message.

The multicast-traffic configuration option (per interface) restricts or allows the use of an interface for LDP multicast traffic forwarding towards a downstream node. The interface configuration option does not restrict or allow the exchange of the point-to-multipoint FEC by way of an established session to the peer on an interface, but only restricts or allows the use of next hops over the interface.

5.2.2  LDP Point-to-Multipoint Protocol

Only a single generic identifier range is defined for signaling a multipoint data tree (MDT) for all client applications. Implementation on the 7705 SAR reserves the range 1 to 8292 for generic point-to-multipoint LSP ID values for static point-to-multipoint LSP on the root node.

5.2.3  Make-Before-Break (MBB)

When a transit or leaf node detects that the upstream node towards the root node of a multicast tree has changed, the node follows the graceful procedure that allows make-before-break transition to the new upstream node. Make-before-break support is optional via the mp-mbb-time command. If the new upstream node does not support MBB procedures, then the downstream node waits for the configured timer to time out before switching over to the new upstream node.
5.2.4 ECMP Support

If multiple ECMP paths exist between two adjacent nodes, then the upstream node of the multicast receiver programs all entries in the forwarding plane. Only one entry is active and it is based on the ECMP hashing algorithm.
5.3 Multicast LDP Fast Upstream Switchover

This feature allows a downstream LSR of a multicast LDP (mLDP) FEC to perform a fast switchover in order to source the traffic from another upstream LSR while IGP and LDP are converging due to a failure of the upstream LSR, where the upstream LSR is the primary next hop of the root LSR for the point-to-multipoint FEC. The feature is enabled through the `mcast-upstream-frr` command.

The feature provides upstream fast reroute (FRR) node protection for mLDP FEC packets. The protection is at the expense of traffic duplication from two different upstream nodes into the node that performs the fast upstream switchover.

The detailed procedures for this feature are described in `draft-pdutta-mpls-mldp-up-redundancy`.

5.3.1 mLDP Fast Upstream Switchover Configuration

To enable the mLDP fast upstream switchover feature, configure the following option in the CLI:

```
config>router>ldp>mcast-upstream-frr
```

When `mcast-upstream-frr` is enabled and LDP is resolving an mLDP FEC received from a downstream LSR, LDP checks for the existence of an ECMP next hop or a loop-free alternate (LFA) next hop to the root LSR node. If LDP finds one, it programs a primary incoming label map (ILM) on the interface corresponding to the primary next hop and a backup ILM on the interface corresponding to the ECMP or LFA next hop. LDP then sends the corresponding labels to both upstream LSR nodes. In normal operation, the primary ILM accepts packets and the backup ILM drops them. If the interface or the upstream LSR of the primary ILM goes down, causing the LDP session to go down, the backup ILM starts accepting packets.

To use the ECMP next hop, configure the `ecmp max-ecmp-routes` value in the system to be at least 2, using the following command:

```
config>router>ecmp max-ecmp-routes
```

To use the LFA next hop, enable LFA using the following commands (as needed):

```
config>router>isis>loopfree-alternate
```

or

```
config>router>ospf>loopfree-alternate
```
Enabling IP FRR or LDP FRR is not strictly required, since LDP only needs to know the location of the alternate next hop to the root LSR in order to send the label mapping message and program the backup ILM during the initial signaling of the tree. That is, enabling the LFA option is sufficient for providing the backup ILM information. However, if unicast IP and LDP prefixes need to be protected, then IP FRR and LDP FRR—and the mLDP fast upstream switchover—can be enabled concurrently using the following commands:

```
config>router>ip-fast-reroute
or
config>router>ldp>fast-reroute
```

An mLDP FRR fast switchover relies on the fast detection of a lost LDP session to the upstream peer to which the primary ILM label had been advertised. To ensure fast detection of a lost LDP session, do the following:

**Step 1.** Enable BFD on all LDP interfaces to upstream LSR nodes. When BFD detects the loss of the last adjacency to the upstream LSR, it brings down the LDP session immediately, which causes the CSM to activate the backup ILM.

**Step 2.** If there is a concurrent T-LDP adjacency to the same upstream LSR node, enable BFD on the T-LDP peer in addition to enabling it on the interface.

**Step 3.** Enable the `ldp-sync-timer` option on all interfaces to the upstream LSR nodes. If an LDP session to the upstream LSR to which the primary ILM is resolved goes down for any reason other than a failure of the interface or the upstream LSR, then routing and LDP go out of synchronization. This means that the backup ILM remains activated until the next time SPF is run by IGP.

By enabling the IGP-LDP synchronization feature, the advertised link metric changes to the maximum value as soon as the LDP session goes down. This, in turn, triggers an SPF, and LDP will likely download a new set of primary and backup ILMs.

### 5.3.2 mLDP Fast Upstream Switchover Behavior

This feature allows a downstream LSR to send a label binding to two upstream LSR nodes, but only accept traffic as follows:

- for normal operation, traffic is accepted from the ILM on the interface to the primary next hop of the root LSR for the point-to-multipoint FEC
- for failure operation, traffic is accepted from the ILM on the interface to the backup next hop
A candidate upstream LSR node must be either an ECMP next hop or an LFA next hop. Either option allows the downstream LSR to perform a fast switchover and to source the traffic from another upstream LSR while IGP is converging due to a failure of the LDP session of the upstream peer, which is the primary next hop of the root LSR for the point-to-multipoint FEC. That is, the candidate upstream LSR node provides upstream FRR node protection for the mLDP FEC packets.

Multicast LDP fast upstream switchover is illustrated in Figure 20. LSR U is the primary next hop for the root LSR R of the point-to-multipoint FEC. LSR U' is an ECMP or LFA backup next hop for the root LSR R of the same point-to-multipoint FEC.

**Figure 20  Multicast LDP Fast Upstream Switchover**

In Figure 20, downstream LSR Z sends a label mapping message to both upstream LSR nodes, and programs the primary ILM on the interface to LSR U and the backup ILM on the interface to LSR U'. The labels for the primary and backup ILMs must be different. Thus LSR Z attracts traffic from both ILMs. However, LSR Z blocks the ILM on the interface to LSR U' and only accepts traffic from the ILM on the interface to LSR U.

If the link to LSR U fails, or LSR U fails, causing the LDP session to LSR U to go down, LSR Z will detect the failure and reverse the ILM blocking state. In addition, LSR Z immediately starts receiving traffic from LSR U' until IGP converges and provides a new primary next hop and a new ECMP or LFA backup next hop, which may or may not be on the interface to LSR U'. When IGP convergence is complete, LSR Z updates the primary and backup ILMs in the datapath.

**Note:** LDP uses the interface of either an ECMP next hop or an LFA next hop to the root LSR prefix, whichever is available, to program the backup ILM. However, ECMP next hop and LFA next hop are mutually exclusive for a given prefix. IGP installs the ECMP next hop in preference to the LFA next hop as a prefix in the routing table manager (RTM).
If one or more ECMP next hops for the root LSR prefix exist, LDP picks the interface for the primary ILM based on the rules of mLDP FEC resolution specified in RFC 6388, *Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*:

1. The candidate upstream LSRs are numbered from lowest to highest IP address.
2. The following hash is performed:
   \[
   H = (CRC32(Opaque\ Value)) \mod\ N
   \]
   where \( N \) is the number of upstream LSRs
   The Opaque Value is the field in the point-to-multipoint FEC element immediately after the Opaque Length field. The Opaque Length indicates the opaque value used in this calculation.
3. The selected upstream LSR \( U \) is the LSR that has the number \( H \).

LDP then picks the interface for the backup ILM using the following new rules:

```plaintext
if (H + 1 < NUM_ECMP) {
    // If the hashed entry is not last in the next hops then pick up the next as backup.
    backup = H + 1;
} else {
    // Wrap around and pick up the first.
    backup = 1;
}
```

In some topologies, it is possible that no ECMP or LFA next hop is found. In this case, LDP programs the primary ILM only.
5.4 LDP Process Overview

Figure 21 displays the process to provision basic LDP parameters.

Figure 21 LDP Configuration and Implementation

START

ENABLE LDP

APPLY IMPORT AND EXPORT POLICIES

CONFIGURE LDP INTERFACE PARAMETERS

CONFIGURE TARGETED SESSION PARAMETERS

CONFIGURE PEER PARAMETERS

TURN UP
5.5 Configuration Notes

Refer to the 7705 SAR Services Guide for information about signaling.

5.5.1 Reference Sources

For information on supported IETF drafts and standards, as well as standard and proprietary MIBs, refer to Standards and Protocol Support.
5.6 Configuring LDP with CLI

This section provides information to configure LDP using the command line interface.

Topics in this section include:

- LDP Configuration Overview
- Basic LDP Configuration
- Common Configuration Tasks
- LDP Configuration Management Tasks
5.7 LDP Configuration Overview

When the 7705 SAR implementation of LDP is instantiated, the protocol is in the no shutdown state. In addition, targeted sessions are then enabled. The default parameters for LDP are set to the documented values for targeted sessions in draft-ietf-mpls-ldp-mib-09.txt.

LDP must be enabled in order for signaling to be used to obtain the ingress and egress labels in frames transmitted and received on the service destination point (SDP). When signaling is off, labels must be manually configured when the SDP is bound to a service.
### 5.8 Basic LDP Configuration

This section provides information to configure LDP and gives configuration examples of common configuration tasks.

The LDP protocol instance is created in the **no shutdown** (enabled) state.

The following example displays the default LDP configuration output.

```
ALU-1>config>router>ldp# info
----------------------------------
| interface-parameters |
| exit                |
| targeted-session    |
| exit                |
----------------------------------
ALU-1>config>router>ldp#
```
5.9 Common Configuration Tasks

This section provides a brief overview of the following common configuration tasks to configure LDP:

- Enabling LDP
- Configuring Graceful Restart Helper Parameters
- Applying Import and Export Policies
- Configuring Interface Parameters
- Specifying Targeted Session Parameters
- Specifying Peer Parameters
- Configuring LDP Support for Multicast VPN (MVPN)
- Enabling LDP Signaling and Services

5.9.1 Enabling LDP

LDP must be enabled in order for the protocol to be active. MPLS must also be enabled. MPLS is enabled in the `config>router>mpls` context.

Use the following CLI syntax to enable LDP on a 7705 SAR router:

**CLI Syntax:**

```
ldp
```

**Example:**

```
config>router# ldp
```

The following example displays the enabled LDP configuration output.

```
ALU-1>config>router# info
----------------------------------------------
#------------------------------------------
edo "LDP Configuration"
#------------------------------------------
   ldp
       interface-parameters
       exit
       targeted-session
       exit
       exit
----------------------------------------------
... 
ALU-1>config>router#
```
5.9.2 Configuring Graceful Restart Helper Parameters

Graceful Restart Helper advertises to its LDP neighbors by carrying the fault tolerant (FT) session TLV in the LDP initialization message, assisting the LDP in preserving its IP forwarding state across the restart. The 7705 SAR recovery is self-contained and relies on information stored internally to self-heal.

Maximum recovery time is the time (in seconds) that the sender of the TLV would like the receiver to wait, after detecting the failure of LDP communication with the sender.

Neighbor liveness time is the time (in seconds) that the LSR is willing to retain its MPLS forwarding state. The time should be long enough to allow the neighboring LSRs to resynchronize all the LSPs in a graceful manner, without creating congestion in the LDP control plane.

Use the following syntax to configure graceful restart parameters:

**CLI Syntax:**
```
config>router>ldp
  [no] graceful-restart
  [no] maximum-recovery-time interval
  [no] neighbor-liveness-time interval
```

**Example:**
```
config>router>ldp
config>router>ldp# graceful-restart
config>router>ldp# maximum-recovery-time 120
config>router>ldp# neighbor-liveness-time 60
config>router>ldp# exit
config>router#
```

The following example displays the import policy configuration output.

```
ALU-1>config>router>ldp>graceful-restart# info
------------------------------
  maximum-recovery-time 120
  neighbor-liveness-time 60
------------------------------
ALU-1>config>router>ldp>graceful-restart#
```
5.9.3 Applying Import and Export Policies

Inbound filtering (import policy) allows a route policy to control the label bindings that an LSR accepts from its peers. An import policy can accept or reject label bindings received from LDP peers. Label bindings can be filtered based on the following:

- neighbor — match on bindings received from the specified peer
- prefix-list — match on bindings with the specified prefix or prefixes

Outbound filtering (export policy) allows a route policy to control the label bindings advertised by the LSR to its peers. Label bindings can be filtered based on the following:

- all — all local subnets by specifying “direct” as the match protocol
- prefix-list — match on bindings with the specified prefix/prefixes

Import or export policies must already exist before they are applied to LDP. Policies are configured in the `config>router>policy-options` context. Refer to the “Route Policies” section in the 7705 SAR Router Configuration Guide for details.

Use the following CLI syntax to apply import or export policies:

**CLI Syntax:**
```
cfg>router>ldp
   import policy-name [policy-name...(up to 5 max)]
   export policy-name [policy-name...(up to 5 max)]
```

**Example:**
```
cfg>router>ldp
cfg>router>ldp# import LDP-import
cfg>router>ldp# export LDP-export
cfg>router>ldp# exit
cfg>router#
```
The following example displays the import and export policy configuration output.

ALU-1>config>router>ldp# info
----------------------------------------------
export "LDP-export"
import "LDP-import"
interface-parameters
exit
targeted-session
exit
----------------------------------------------

5.9.4 Configuring Interface Parameters

Use the following CLI syntax to configure LDP interface parameters:

**CLI Syntax:**
```
config>router# ldp
  interface-parameters
    hello timeout factor
    interface ip-int-name
      hello timeout factor
    keepalive timeout factor
    local-lsr-id {system | interface}
    transport-address {system | interface}
    no shutdown
    keepalive timeout factor
    transport-address {system | interface}
```

**Example:**
```
config>router# ldp
config>router>ldp# interface-parameters
config>router>ldp>if-params# interface to-104
config>router>ldp>if-params>if# hello 15 3
config>router>ldp>if-params>if# local-lsr-id system
config>router>ldp>if-params>if# no shutdown
config>router>ldp>if-params>if# exit
config>router>ldp>if-params# exit
config>router>ldp#
```

The following example displays the LDP interface parameter configuration output.

ALU-1>config>router>ldp# info
----------------------------------------------
import "LDP-import"
interface-parameters
  hello 15 3
  keepalive 30 3
  interface "to-104"
    hello 15 3
    keepalive 30 3
5.9.5 Specifying Targeted Session Parameters

Use the following CLI syntax to specify targeted session parameters:

**CLI Syntax:**
```plaintext
config>router# ldp
targeted-session
    disable-targeted-session
    hello timeout factor
    keepalive timeout factor
    peer ip-address
        bfd-enable
        hello timeout factor
        keepalive timeout factor
        local-lsr-id interface-name
    no shutdown
```

**Example:**
```plaintext
config>router# ldp
cfg-router# targeted-session
cfg-router# targeted-session# bfd-enable
cfg-router# targeted-session# hello 5000 255
cfg-router# targeted-session# keepalive 5000 255
cfg-router# targeted-session# peer 10.10.10.104
cfg-router# targeted-session# peer# hello 2500 100
cfg-router# targeted-session# peer# keepalive 15 3
cfg-router# targeted-session# peer# local-lsr-id to-104
cfg-router# targeted-session# peer# no shutdown
cfg-router# targeted-session# peer# exit
cfg-router# targeted-session# exit
cfg-router# ldp#
```

The following example displays the LDP targeted session configuration output.

```
ALU-1>config>router>ldp# info
```
```plaintext
import "LDP-import"
interface-parameters
    hello 15 3
    keepalive 30 3
    interface "to-104"
```
5.9.6 Specifying Peer Parameters

Use the following CLI syntax to specify LDP peer parameters:

**CLI Syntax:**
```
config>router# ldp
    peer-parameters
        peer ip-address
            auth-keychain name
            authentication-key {authentication-key | hash-key} [hash | hash2]
```

**Example:**
```
config>router# ldp
config>router>ldp# peer-parameters
config>router>ldp>peer-params# peer 10.10.10.104
config>router>ldp>peer-params>peer$ authentication-key testuser
config>router>ldp>peer-params>peer$ exit
```

The following example displays the LDP peer parameters configuration output.
```
ALU-1>config>router>ldp# info
----------------------------------------------
import "LDP-import"
graceful-restart
exit
import "LDP-import"
peer-parameters
    peer 10.10.10.104
        authentication-key "nGjXyHQtGxhByBm.kDeYdzSmFy9KK03" hash2
exit
exit
interface-parameters
    interface "test"
exit
interface "to-104"
```
5.9.7 Configuring LDP Support for Multicast VPN (MVPN)

For LDP support for MVPN, configure the `multicast-traffic`, `mp-mbb-time`, and `mcast-upstream-frr` commands.

The following example displays the LDP MVPN configuration output.

```
*A:SarAx Dut-D>config>router>ldp# info detail
-----------------------------------------------
no aggregate-prefix-match
no export
no fast-reroute
no import
no graceful-restart
mcast-upstream-frr
mp-mbb-time 5
no tunnel-down-damp-time
interface-parameters
hello 15 3
keepalive 30 3
transport-address system
interface "mcast_if"
   no bfd-enable
   no hello
   no keepalive
   no local-lsr-id
   multicast-traffic enable
   no transport-address
   no shutdown
exit
exit
targeted-session
   no disable-targeted-session
   hello 45 3
   keepalive 40 4
exit
no shutdown
```

*A:SarAx Dut-D>config>router>ldp#
```
5.9.8 Enabling LDP Signaling and Services

When LDP is enabled, targeted sessions can be established to create remote adjacencies with nodes that are not directly connected. When service destination points (SDPs) are configured, extended discovery mechanisms enable LDP to send periodic targeted hello messages to the SDP’s far-end point. The exchange of LDP hellos triggers session establishment. The SDP’s signaling default enables tldp. The SDP uses the targeted-session parameters configured in the config>router>ldp>targeted-session context.

The service>sdp>ldp and router>lsp commands are mutually exclusive; you can either specify an LSP or enable an LDP. There cannot be two methods of transport in a single SDP.

To enable LDP on the SDP when an LSP is already specified, the LSP must be removed from the configuration using the no lsp lsp-name command. For further information about configuring SDPs, refer to the 7705 SAR Services Guide.

Use the following CLI syntax to enable LDP on an MPLS SDP:

CLI Syntax: config>service>sdp# ldp signaling {off|tldp}

The following example displays an SDP configuration output with the signaling default tldp enabled.

ALU-1>config-service>sdp# info detail
---------------------------------------------
description "MPLS: to-99"
far-end 10.10.10.99
ldp
signaling tldp
path-mtu 4462
keep-alive
hello-time 10
hold-down-time 10
max-drop-count 3
timeout 5
no message-length
no shutdown
exit
no shutdown
---------------------------------------------
ALU-1>config-service>sdp#
5.10  LDP Configuration Management Tasks

This section discusses the following LDP configuration management tasks:

- Disabling LDP
- Modifying Targeted Session Parameters
- Modifying Interface Parameters

5.10.1  Disabling LDP

The `no ldp` command disables the LDP protocol on the router. All parameters revert to the default settings. LDP must be shut down before it can be disabled.

Use the following CLI syntax to disable LDP:

**CLI Syntax:**

```
no ldp
shutdown
```

**Example:**

```
config>router# ldp
config>router>ldp# shutdown
config>router>ldp# exit
config>router# no ldp
```

5.10.2  Modifying Targeted Session Parameters

You can modify targeted session parameters without shutting down entities. However, for any LDP timers (hello or keepalive timers), the changes do not take effect until a `shutdown/no shutdown` command is performed on the LDP session.

The `no` form of a `targeted-session` parameter command reverts modified values back to the default.
The following example displays the CLI syntax to revert targeted session parameters back to the default values.

**Example:**
```
config>router# ldp
config>router>ldp# targeted-session
config>router>ldp>targeted# no disable-targeted-session
config>router>ldp>targeted# no hello
config>router>ldp>targeted# no keepalive
config>router>ldp>targeted# shutdown
config>router>ldp>targeted# no shutdown
config>router>ldp>targeted# no peer 10.10.10.99
```

The following example displays the default value output.

```
ALU-1>config>router>ldp>targeted# info detail
----------------------------------------------
   no disable-targeted-session
   hello 45 3
   keepalive 40 4
----------------------------------------------
ALU-1>config>router>ldp>targeted#
```

### 5.10.3 Modifying Interface Parameters

You can modify LDP interface parameters without shutting down entities. However, at the global timer configuration level (`ldp>interface-parameters`), the **hello** and **keepalive** parameter modifications do not take effect until a **shutdown/no shutdown** command is performed on the LDP session. At the interface timer configuration level (`ldp>interface-parameters@interface`), any changes to the **keepalive** parameter do not take effect until a **shutdown/no shutdown** command is performed on the LDP session. For all other parameters, the changes take effect immediately.

Individual parameters cannot be deleted. The **no** form of an **interface-parameter** command changes modified values back to the defaults.
The following example displays the CLI syntax to change interface parameters back to the default values.

**Example:**

```plaintext
config>router# ldp
config>router>ldp>interface-parameters
config>router>ldp>if-params# no hello
config>router>ldp>if-params>if# interface to-104
config>router>ldp>if-params>if# no keepalive
config>router>ldp>if-params>if# no transport-address
config>router>ldp>if-params>if# shutdown
config>router>ldp>if-params>if# no shutdown
config>router>ldp>if-params>if# exit
config>router>ldp>if-params>if# exit
config>router>ldp>shutdown
config>router>ldp# no shutdown
```

The following example displays the default value output.

```plaintext
ALU-1>config>router>ldp>if-params# info detail
----------------------------------------------
hello 15 3
keepalive 30 3
no transport-address
----------------------------------------------
ALU-1>config>router>ldp>params#
```
5.11 LDP Command Reference

5.11.1 Command Hierarchies

- LDP Commands
- Show Commands
- Clear Commands
- Debug Commands
5.11.1.1 LDP Commands

```
config
  — router [router-name]
    — [no] idp
      — [no] aggregate-prefix-match
        — prefix-exclude policy-name [policy-name...(up to 5 max)]
        — no prefix-exclude
      — [no] shutdown
    — export policy-name [policy-name...(up to 5 max)]
    — no export
    — [no] fast-reroute
    — fec-originate ip-address/mask [advertised-label in-label] [swap-label out-label] interface interface-name
    — fec-originate ip-address/mask [advertised-label in-label] next-hop ip-address [swap-label out-label]
    — fec-originate ip-address/mask [advertised-label in-label] next-hop ip-address [swap-label out-label] interface interface-name
    — fec-originate ip-address/mask [advertised-label in-label] pop
      — no fec-originate ip-address/mask interface interface-name
      — no fec-originate ip-address/mask next-hop ip-address
      — no fec-originate ip-address/mask next-hop ip-address interface interface-name
      — no fec-originate ip-address/mask pop
    — [no] graceful-restart
      — maximum-recovery-time interval
      — no maximum-recovery-time
      — neighbor-liveness-time interval
      — no neighbor-liveness-time
    — import policy-name [policy-name...(up to 5 max)]
    — no import
    — interface-parameters
      — hello timeout factor
      — no hello
      — [no] interface ip-int-name
        — [no] bfd-enable
        — hello timeout factor
        — no hello
        — keepalive timeout factor
        — no keepalive
        — local-lsr-id {system | interface}
        — no local-lsr-id
        — multicast-traffic {enable | disable}
        — [no] shutdown
        — transport-address {system | interface}
        — no transport-address
      — keepalive timeout factor
      — no keepalive
      — transport-address {system | interface}
      — no transport-address
    — [no] legacy-ipv4-lsr-interop
    — [no] mcast-upstream-frr
    — mp-mbb-time interval
```
— no mp-mbb-time
— peer-parameters
  — [no] peer ip-address
    — auth-keychain name
    — no auth-keychain
    — authentication-key {authentication-key | hash-key} [hash | hash2]
      — no authentication-key
— [no] shutdown
— targeted-session
  — [no] disable-targeted-session
  — hello timeout factor
  — no hello
  — keepalive timeout factor
  — no keepalive
  — [no] peer ip-address
    — [no] bfd-enable
    — hello timeout factor
    — no hello
    — keepalive timeout factor
    — no keepalive
    — local-lsr-id interface-name
    — no local-lsr-id
    — [no] shutdown
    — [no] tunneling
    — [no] lsp lsp-name
— tunnel-down-damp-time seconds
— no tunnel-down-damp-time

5.11.1.2 Show Commands

show
  — router [router-instance]
    — idp
      — auth-keychain [keychain]
      — bindings {fec-type fec-type [detail]} [session ip-addr[:label-space]]
      — bindings label-type start-label [end-label]
      — bindings {prefix ip-prefix/mask [detail]} [session ip-addr[:label-space]]
      — bindings active {prefix ip-prefix/mask}
      — bindings vc-type vc-type [vc-id vc-id [session ip-addr[:label-space]]]
      — bindings service-id service-id [detail]
      — discovery [{peer [ip-address]} | {interface [ip-int-name]}] [state state] [detail]
      — fec-originate [ip-address/mask] [operation-type]
      — fec-originate [operation-type] [ipv4]
      — interface [ip-int-name | ip-address] [detail]
      — parameters
      — peer [ip-address] [detail]
      — peer-parameters peer-ip-address
      — session [ip-addr[:label-space]] [detail] [statistics [packet-type]]
      — status
5.11.1.3 Clear Commands

clear
  — router [router-instance]
    — ldp
      — instance
      — interface ip-int-name [statistics]
      — peer ip-address [statistics]
      — session ip-addr:[label-space] [statistics]
      — statistics

5.11.1.4 Debug Commands

[no] debug
  — router [router-instance]
    — [no] ldp
      — [no] interface interface-name
        — [no] event
          — [no] messages
        — [no] packet
          — hello [detail]
          — no hello
        — [no] peer ip-address
          — [no] event
            — [no] bindings
            — [no] messages
          — [no] packet
            — hello [detail]
            — no hello
            — init [detail]
            — no init
            — [no] keepalive
            — label [detail]
            — no label
5.11.2 Command Descriptions

- Configuration Commands
- Show Commands
- Clear Commands
- Debug Commands
5.11.2.1 Configuration Commands

- Generic Commands
- LDP Global Commands
- Interface Parameters Commands
- Targeted Session Commands
- Peer Parameters Commands
5.11.2.1.1 Generic Commands

shutdown

Syntax  [no] shutdown

Context  config>router>ldp
         config>router>ldp>if-params>interface
         config>router>ldp>targ-session>peer
         config>router>ldp>aggregate-prefix-match

Description  This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they can be deleted.

The **no** form of this command administratively enables an entity.

Unlike other commands and parameters where the default state is not indicated in the configuration file, the **shutdown** and **no shutdown** states are always indicated in system-generated configuration files.

Default  no shutdown
### 5.11.2.1.2 LDP Global Commands

**ldp**

**Syntax**  
```markdown
[no] ldp
```

**Context**  
```markdown
config>router
```

**Description**  
This command enables the context to configure an LDP protocol instance. When an LDP instance is created, the protocol is enabled (in the **no shutdown** state). To suspend the LDP protocol, use the **shutdown** command. Configuration parameters are not affected.

The **no** form of the command deletes the LDP protocol instance, removing all associated configuration parameters. The LDP instance must first be disabled with the **shutdown** command before being deleted.

**Default**  
n/a — LDP must be explicitly enabled

**aggregate-prefix-match**

**Syntax**  
```markdown
[no] aggregate-prefix-match
```

**Context**  
```markdown
config>router>ldp
```

**Description**  
This command enables LDP to use the aggregate prefix match function rather than requiring an exact prefix match.

When this command is enabled and an LSR receives a FEC-label binding from an LDP neighbor for a prefix-address FEC element, FEC1, it will install the binding in the LDP FIB if:

- the routing table (RIB) contains an entry that matches FEC1. Matching can either be a longest IP match of the FEC prefix or an exact match.
- the advertising LDP neighbor is the next hop to reach FEC1

When the FEC-label binding has been installed in the LDP FIB, LDP programs an NHLFE entry in the egress data path to forward packets to FEC1. LDP also advertises a new FEC-label binding for FEC1 to all its LDP neighbors.

When a new prefix appears in the RIB, LDP checks the LDP FIB to determine if this prefix is a closer match for any of the installed FEC elements. If a closer match is found, this may mean that the LSR used as the next hop will change; if so, the NHLFE entry for that FEC must be changed.
When a prefix is removed from the RIB, LDP checks the LDP FIB for all FEC elements that matched this prefix to determine if another match exists in the routing table. If another match exists, LDP must use it. This may mean that the LSR used as the next hop will change; if so, the NHLFE entry for that FEC must be changed. If another match does not exist, the LSR removes the FEC binding and sends a label withdraw message to its LDP neighbors.

If the next hop for a routing prefix changes, LDP updates the LDP FIB entry for the FEC elements that matched this prefix. It also updates the NHLFE entry for the FEC elements.

The no form of this command disables the use of the aggregate prefix match function. LDP then only performs an exact prefix match for FEC elements.

**Default**

no aggregate-prefix-match

### prefix-exclude

**Syntax**

prefix-exclude policy-name [policy-name ...(up to 5 max)]

no prefix-exclude

**Context**

config>router>ldp>aggregate-prefix-match

**Description**

This command specifies the policy name containing the prefixes to be excluded from the aggregate prefix match function. Against each excluded prefix, LDP performs an exact match of a specific FEC element prefix, rather than a longest prefix match of one or more LDP FEC element prefixes, when it receives a FEC-label binding or when a change to the prefix occurs in the routing table.

The no form of this command removes all policies from the configuration; therefore, no prefixes are excluded.

**Default**

no prefix-exclude

**Parameters**

policy-name — specifies the import route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

### export

**Syntax**

export policy-name [policy-name ...(up to 5 max)]

no export

**Context**

config>router>ldp
Label Distribution Protocol

Description
This command specifies export route policies that determine which routes are exported to LDP neighbors. Configuring an export policy allows the LSR (Label Switch Router) to advertise addresses other than the system IP address. Policies are configured in the config>router>policy-options context. Refer to the “Route Policies” section in the 7705 SAR Router Configuration Guide.

If no export policy is specified, non-LDP routes will not be exported from the routing table manager to LDP, and only LDP-learned routes will be exported to LDP neighbors.

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified. The specified names must already be defined.

The no form of the command removes all policies from the configuration.

Default
no export

Parameters
policy-name — specifies the export route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

fast-reroute

Syntax
[no] fast-reroute

Context
config>router>ldp

Description
This command enables LDP Fast Reroute (FRR). LDP FRR provides local protection for an LDP FEC by precalculating and downloading a primary and a backup NHLFE for the FEC to the LDP FIB.

When LDP FRR is enabled and an LFA backup next hop exists for the FEC prefix in the RTM, or for the longest prefix the FEC prefix matches to when the aggregate-prefix-match option is enabled, LDP will program the data path with both a primary NHLFE and a backup NHLFE for each next hop of the FEC.

The backup NHLFE is enabled for each affected FEC next hop when any of the following events occurs:

• an LDP interface goes operationally down or is administratively shut down
• an LDP session to a peer goes down because the Hello timer or keepalive timer has expired over an interface
• the TCP connection used by a link LDP session to a peer goes down

The tunnel-down-damp-time command, when enabled, does not cause the corresponding timer to be activated for a FEC as long as a backup NHLFE is still available.
Because LDP can detect the loss of a neighbor/next hop independently, it is possible that it will switch to the LFA next hop while the IGP (OSPF or IS-IS) is still using the primary next hop. As well, when the interface for the previous primary next hop is restored, the IGP may reconverge before LDP completes the FEC exchange with its neighbor over that interface. This may cause LDP to deprogram the LFA next hop from the FEC and blackhole traffic. In order to avoid this situation, IGP-LDP synchronization should be enabled on the LDP interface with the `config>router>if>ldp-sync-timer` command (refer to the 7705 SAR Router Configuration Guide, “IP Router Command Reference”, for information on configuring the `ldp-sync-timer`).

**Default**
no fast-reroute

### fec-originate

**Syntax**

```
fec-originate ip-address/mask [advertised-label in-label] [swap-label out-label] interface interface-name
```

```
fec-originate ip-address/mask [advertised-label in-label] next-hop ip-address [swap-label out-label]
```

```
fec-originate ip-address/mask [advertised-label in-label] next-hop ip-address [swap-label out-label] interface interface-name
```

```
fec-originate ip-address/mask [advertised-label in-label] pop
```

```
no fec-originate ip-address/mask interface interface-name
```

```
no fec-originate ip-address/mask next-hop ip-address
```

```
no fec-originate ip-address/mask next-hop ip-address interface interface-name
```

```
no fec-originate ip-address/mask pop
```

**Context**

config>router>ldp

**Description**

This command adds a FEC to the LDP prefix database with a specific label operation on the node.

Permitted operations are `swap` to originate a FEC for which the LSR is not egress or `pop` to originate a FEC for which the LSR is egress.

For a swap operation, an incoming label can be swapped with a label in the range of 16 to 1048575. If a `swap-label` is not configured, the default value is 3.

A route-table entry is required for a FEC with a pop operation to be advertised. For a FEC with a swap operation, a route-table entry must exist and the user-configured next hop for the swap operation must match one of the next hops in the route-table entry.

The `next-hop`, `advertised-label`, and `swap-label` parameters are optional. If a `next-hop` is configured but no `swap-label` is specified, the swap occurs with label 3 (implicit null), then the label is popped and the packet is forwarded to the next hop. If the `next-hop` and `swap-label` parameters are configured, a regular swap occurs. If no parameters are specified, a pop and forwarding is performed.

**Default**
no fec-originate
Parameters

- **ip-address/mask** — specifies the IP prefix and prefix length
  
  **Values**
  
  - ip-address: a.b.c.d (host bits must be 0)
  - mask: 0 to 32

- **advertised label** — specifies the label advertised to the upstream peer. If not configured, the label that is advertised should be from the label pool. If the configured static label is not available, the IP prefix is not advertised.

  **Values**
  
  - 32 to 2047

- **in-label** — the LSR to swap the label. If configured, the LSR should swap the label with the configured **out-label**. If not configured, the default action is pop if the next-hop parameter is not defined.

  **Values**
  
  - 32 to 2047

- **out-label** — the number of labels to send to the peer associated with this FEC

  **Values**
  
  - 16 to 1048575

- **interface-name** — specifies the name of the interface that the label for the originated FEC is swapped to. For an unnumbered interface, this parameter is mandatory because there is no address for the next hop. For a numbered interface, it is optional.

- **next-hop ip-address** — specifies the IP address of the next hop

  **Values**
  
  - a.b.c.d

- **pop** — specifies to pop the label and transmit the packet

---

**graceful-restart**

**Syntax**

[no] graceful-restart

**Context**

config>router>ldp

**Description**

This command enables graceful restart helper.

The **no** form of the command disables graceful restart.

**Default**

graceful-restart

---

**maximum-recovery-time**

**Syntax**

maximum-recovery-time interval
no maximum-recovery-time

**Context**

config>router>ldp>graceful-restart

**Description**

This command configures the local maximum recovery time, which is the time (in seconds) that the sender of the TLV would like the receiver to wait, after detecting the failure of LDP communication with the sender.
neighbor-liveness-time

Syntax
neighbor-liveness-time interval
no neighbor-liveness-time

Context config>router>ldp>graceful-restart

Description This command configures the neighbor liveness time, which is the time (in seconds) that the LSR is willing to retain its MPLS forwarding state. The time should be long enough to allow the neighboring LSRs to resynchronize all the LSPs in a graceful manner, without creating congestion in the LDP control plane.

The no form of the command returns the default value.

Default 120

Parameters interval — specifies the maximum length of recovery time, in seconds

Values 15 to 1800

import

Syntax import policy-name [policy-name ...(up to 5 max)]
no import

Context config>router>ldp

Description This command specifies import route policies that determine which routes are accepted from LDP neighbors. Policies are configured in the config>router>policy-options context. Refer to the "Route Policies" section in the 7705 SAR Router Configuration Guide.

If no import policy is specified, LDP accepts all routes from configured LDP neighbors. Import policies can be used to limit or modify the routes accepted and their corresponding parameters and metrics.

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple import commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified. The specified names must already be defined.

The no form of the command removes all policies from the configuration.
Default  

no import

Parameters  
policy-name — specifies the import route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

hello

Syntax  

hello timeout factor
no hello

Context  

cfg-router-ldp-interface-parameters
cfg-router-ldp-if-params-interface
cfg-router-ldp-targeted-session
cfg-router-ldp-targ-session-peer

Description  

This command configures the hold time. This is the time interval to wait before declaring a neighbor down. The factor parameter derives the hello interval.

Hold time is local to the system and is sent in the hello messages to the neighbor. Hold time cannot be less than three times the hello interval. The hold time can be configured globally (applies to all LDP interfaces) or per interface. The most specific value is used.

When an LDP session is being set up, the hold time is negotiated to the lower of the two peers. Once an operational value is agreed upon, the hello factor is used to derive the value of the hello interval.

The no form of the command:

• at the interface-parameters and targeted-session levels, sets the hello timeout and the hello factor to the default values
• at the interface level, sets the hello timeout and the hello factor to the value defined under the interface-parameters level
• at the peer level, sets the hello timeout and the hello factor to the value defined under the targeted-session level

Default  

The default value is dependent upon the CLI context. Table 35 lists the hello timeout factor default values.

Table 35  Hello Timeout Factor Default Values

<table>
<thead>
<tr>
<th>Context</th>
<th>Timeout</th>
<th>Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-router-ldp-interface-parameters</td>
<td>15</td>
<td>3</td>
</tr>
<tr>
<td>config-router-ldp-targeted-session</td>
<td>45</td>
<td>3</td>
</tr>
</tbody>
</table>
Table 35  Hello Timeout Factor Default Values (Continued)

<table>
<thead>
<tr>
<th>Context</th>
<th>Timeout</th>
<th>Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>config&gt;router&gt;ldp&gt;if-params&gt;interface</td>
<td>Inherits values from interface-parameters context</td>
<td></td>
</tr>
<tr>
<td>config&gt;router&gt;ldp&gt;targ-session&gt;peer</td>
<td>Inherits values from targeted-session context</td>
<td></td>
</tr>
</tbody>
</table>

Parameters

timeout — configures the time interval, in seconds, that LDP waits before declaring a neighbor down

Values  1 to 65535

factor — specifies the number of keepalive messages that should be sent on an idle LDP session in the hello timeout interval

Values  1 to 255

keepline

Syntax  keepline timeout factor

no keepline

Context  config>router>ldp>interface-parameters
         config>router>ldp>if-params>interface
         config>router>ldp>targ-session>peer

Description  This command configures the time interval, in seconds, that LDP waits before tearing down the session. The factor parameter derives the keepalive interval.

If no LDP messages are exchanged for the configured time interval, the LDP session is torn down. Keepalive timeout is usually three times the keepalive interval. To maintain the session permanently, regardless of the activity, set the value to zero.

When an LDP session is being set up, the keepalive timeout is negotiated to the lower of the two peers. Once a operational value is agreed upon, the keepline factor is used to derive the value of the keepalive interval.

The no form of the command:

- at the interface-parameters and targeted-session levels, sets the keepline timeout and the keepline factor to the default value
- at the interface level, sets the keepline timeout and the keepline factor to the value defined under the interface-parameters level
- at the peer level, sets the keepline timeout and the keepline factor to the value defined under the targeted-session level
The default value is dependent upon the CLI context. Table 36 lists the keepalive timeout factor default values.

### Table 36  Keepalive Timeout Factor Default Values

<table>
<thead>
<tr>
<th>Context</th>
<th>Timeout</th>
<th>Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>config&gt;router&gt;ldp&gt;interface-parameters</td>
<td>30</td>
<td>3</td>
</tr>
<tr>
<td>config&gt;router&gt;ldp&gt;targeted-session</td>
<td>40</td>
<td>4</td>
</tr>
<tr>
<td>config&gt;router&gt;ldp&gt;if-params&gt;interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>config&gt;router&gt;ldp&gt;targ-session&gt;peer</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Parameters

**timeout** — configures the time interval, expressed in seconds, that LDP waits before tearing down the session

**Values**

1 to 65535

**factor** — specifies the number of keepalive messages, expressed as a decimal integer, that should be sent on an idle LDP session in the keepalive timeout interval

**Values**

1 to 255

---

**legacy-ipv4-lsr-interop**

**Syntax**

[no] legacy-ipv4-lsr-interop

**Context**

config>router>ldp

**Description**

This command allows interoperability with third-party legacy IPv4 LSR implementations that do not comply with RFC 5036 with respect to the processing of Hello TLVs with the U-bit set.

The command is a global LDP configuration that disables the Nokia proprietary Interface Info TLV (0x3E05) in the Hello message sent to the peer. Disabling this Hello TLV also results in the non-generation of the Nokia proprietary Hello Adjacency Status TLV (0x3E06) because the Interface Info TLV is not sent.

---

**mcast-upstream-frr**

**Syntax**

[no] mcast-upstream-frr

**Context**

config>router>ldp

**Description**

This command enables the mLDP fast upstream switchover feature.
When this command is enabled and LDP is resolving an mLDP FEC received from a downstream LSR, it checks whether an ECMP next hop or an LFA next hop to the root LSR node exists. If LDP finds one, it programs a primary ILM on the interface corresponding to the primary next hop and a backup ILM on the interface corresponding to the ECMP or LFA next hop. Then, LDP sends the corresponding labels to both upstream LSR nodes. Under normal operation, the primary ILM accepts packets while the backup ILM drops them. If the interface or the upstream LSR of the primary ILM goes down, causing the LDP session to go down, the backup ILM starts accepting packets.

In order to make use of the ECMP next hop, the user must configure the `ecmp` value in the system to at least “2”, using the following command:

```
config>router>ecmp
```

In order to make use of the LFA next hop, the user must enable LFA using the following commands (as needed):

```
config>router>isis>loopfree-alternate
config>router>ospf>loopfree-alternate
```

Enabling the IP FRR or LDP FRR feature is not strictly required since LDP only needs to know the location of the alternate next hop to the root LSR so it can send the Label Mapping message to program the backup ILM at the initial signaling of the tree. Therefore, enabling the LFA option is sufficient. However, if unicast IP and LDP prefixes need to be protected, then these features and the mLDP fast upstream switchover can be enabled concurrently.

The mLDP FRR fast switchover relies on the fast detection of a loss of an LDP session to the upstream peer to which the primary ILM label had been advertised. It is strongly recommended that the following be performed:

**Step 1.** Enable BFD on all LDP interfaces to upstream LSR nodes. When BFD detects the loss of the last adjacency to the upstream LSR, it will immediately bring down the LDP session, which will cause the CSM to activate the backup ILM.

**Step 2.** If there is a concurrent T-LDP adjacency to the same upstream LSR node, enable BFD on the T-LDP peer in addition to enabling it on the interface.

**Step 3.** Enable the `ldp-sync-timer` option on all interfaces to the upstream LSR nodes. If an LDP session to the upstream LSR to which the primary ILM is resolved goes down for any reason other than a failure of the interface or of the upstream LSR, routing and LDP will go out of synchronization. This means that the backup ILM will remain activated until the next time SPF is run by IGP. By enabling the IGP-LDP synchronization feature, the advertised link metric will be changed to the maximum value as soon as the LDP session goes down. This, in turn, triggers an SPF, and LDP will download a new set of primary and backup ILMs.

The no form of this command disables fast upstream switchover for mLDP FECs.

**Default** no mcast-upstream-frr
mp-mbb-time

Syntax  
mp-mbb-time interval
no mp-mbb-time

Context  
config>router>ldp

Description  
This command configures the maximum time a point-to-multipoint transit or bud node must wait before switching over to the new path if the new node does not send an MBB TLV to inform the transit or bud node of the availability of the data plane.

The no form of the command sets the wait time to the default.

Default: 3 s

Parameters  
interval — specifies the MP MBB wait time

Values  
1 to 10 seconds

tunneling

Syntax  
[no] tunneling

Context  
config>router>ldp>targeted-session>peer

Description  
This command enables LDP over tunnels.

The no form of the command disables tunneling.

Default  
no tunneling

lsp

Syntax  
[no] lsp lsp-name

Context  
config>router>ldp>targeted-session>peer>tunneling

Description  
This command configures an LSP destined for this peer to be used for tunneling an LDP FEC over RSVP-TE. A maximum of four RSVP-TE LSPs can be used for tunneling LDP FECs to the T-LDP peer.

It is not necessary to specify any RSVP-TE LSP in this context unless there is a need to restrict the tunneling to selected LSPs. All RSVP-TE LSPs with a to address matching that of the T-LDP peer are eligible by default. The user can also exclude specific LSP names by using the ldp-over-rsvp exclude command in the config>router>mpls>lsp lsp-name context.

The no form of this command removes the LSP association.
Parameters  

`lsp-name` — specifies the name of the LSP

---

tunnel-down-damp-time

**Syntax**

```
tunnel-down-damp-time seconds
no tunnel-down-damp-time
```

**Context**

`config>router>ldp`

**Description**

This command specifies the time interval, in seconds, that LDP waits before posting a tunnel down event to the Tunnel Table Manager (TTM).

When LDP can no longer resolve a FEC and deactivates it, it deprograms the NHLFE in the data path. It will, however, delay deleting the LDP tunnel entry in the TTM until the `tunnel-down-damp-time` timer expires. This means that users of the LDP tunnel, such as SDPs (for all services) and BGP (for Layer 3 VPNs), will not be notified immediately. Traffic is still blackholed because the NHLFE has been deprogrammed.

If the FEC gets resolved before the `tunnel-down-damp-time` timer expires, LDP programs the IOM with the new NHLFE and posts a tunnel modify event to the TTM, updating the dampened entry in the TTM with the new NHLFE information.

If the FEC does not get resolved and the `tunnel-down-damp-time` timer expires, LDP posts a tunnel down event to the TTM, which deletes the LDP tunnel.

The `no` form of the command resets the damp timer value back to the default value of 3. If the timer value is set to 0, tunnel down events are not dampened but are reported immediately.

**Default**

3

**Parameters**

`seconds` — the time interval that LDP waits before posting a tunnel down event to the TTM

**Values**

0 to 20
5.11.2.1.3 Interface Parameters Commands

interface-parameters

Syntax: interface-parameters
Context: config>router>ldp
Description: This command enables the context to configure LDP interfaces and parameters applied to LDP interfaces.

interface

Syntax: [no] interface ip-int-name
Context: config>router>ldp>interface-parameters
Description: This command enables LDP on the specified IP interface.
The no form of the command deletes the LDP interface and all configuration information associated with the LDP interface.
The LDP interface must be disabled using the shutdown command before it can be deleted.
Parameters: ip-int-name — specifies an existing interface. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

local-lsr-id

Syntax: local-lsr-id {system | interface}
no local-lsr-id
Context: config>router>ldp>if-params>interface
Description: This command enables the use of the address of the link LDP interface as the LSR ID in order to establish an LDP adjacency and session with a directly connected LDP peer.
By default, the LDP session uses the system interface address as the LSR ID unless the LSR ID is explicitly configured. This means that targeted LDP (T-LDP) and interface LDP share a common LDP TCP session and therefore a common LDP label space. The system interface must always be configured on the router or the LDP protocol will not come up on the node.
At initial configuration, the LDP session to the peer remains down while the interface is down. If the user changes the LSR ID while the LDP session is up, LDP immediately tears down the session and attempts to re-establish it using the new LSR ID. If the interface used for the local LSR ID goes down, the LDP session will also go down.
The **interface** option is the recommended setting when static route-LDP synchronization is enabled.

When the **interface** option is selected, the transport connection (TCP) for the link LDP session configured by the **transport-address** command is automatically set to interface. Having both the **local-lsr-id** and transport address set to the local interface creates two TCP sessions to the peer and therefore two different LDP label spaces: one to the interface IP address for link LDP (L-LDP) and one to the system IP address for T-LDP.

The **no** form of the command resets the **local-lsr-id** to the default value.

**Parameters**

- **system** — specifies that the system IP address is used to set up the LDP session between peers
- **interface** — specifies that the IP interface address is used to set up the LDP session between peers

---

**multicast-traffic**

**Syntax**  
```
multicast-traffic {enable | disable}
```

**Context**  
```
config>router>ldp>if-params>interface
```

**Description**  
This command enables or disables multicast traffic forwarding on the interface. The **multicast-traffic** command must be configured on a per-LDP interface basis to enable point-to-multipoint LDP setup on the interface. Point-to-multipoint LDP must be configured as an inclusive or selective provider tunnel per MVPN to dynamically initiate a point-to-multipoint LSP to the leaf PE nodes learned via NG-MVPN auto-discovery signaling. S-PMSI is for efficient data distribution and is optional.

Use the **mldp** command to configure point-to-multipoint LDP for an MVPN. The **mldp** command is found under the **config>service>vprn>mvpn>provider-tunnel>inclusive** or **selective** contexts.

**Default**  
enabled

---

**transport-address**

**Syntax**  
```
transport-address {system | interface}
```

**Context**  
```
config>router>ldp>if-params
```

**Description**  
This command configures the transport address to be used when setting up the LDP TCP sessions. The transport address can be configured globally (applies to all LDP interfaces) or per interface. The most specific value is used.
With the `transport-address` command, you can set up the LDP interface to the connection that can be set to the interface address or the system address. However, there can be an issue of which address to use when there are parallel adjacencies. This address selection situation can also occur when there is a link and a targeted adjacency, since targeted adjacencies request the session to be set up only to the system IP address.

The `transport-address` value should not be `interface` if multiple interfaces exist between two LDP neighbors.

Depending on the first adjacency to be formed, the TCP endpoint is chosen. In other words, if one LDP interface is set up as `transport-address interface` and another as `transport-address system`, then, depending on which adjacency was set up first, the TCP endpoint addresses are determined. After that, because the hello contains the LSR ID, the LDP session can be checked to verify that it is set up and then the adjacency can be matched to the session.

The `no` form of the command:

- at the global level, sets the transport address to the default value
- at the interface level, sets the transport address to the value defined under the global level

<table>
<thead>
<tr>
<th>Default</th>
<th>system</th>
</tr>
</thead>
</table>

**Parameters**

- `interface` — specifies that the IP interface address is used to set up the LDP session between neighbors. The transport address interface cannot be used if multiple interfaces exist between two neighbors, since only one LDP session is set up between two neighbors.

- `system` — specifies that the system IP address is used to set up the LDP session between neighbors
5.11.2.1.4 Targeted Session Commands

targeted-session

Syntax targeted-session
Context config>router>ldp
Description This command configures targeted LDP sessions. Targeted sessions are LDP sessions between non-directly connected peers. Hello messages are sent directly to the peer platform instead of to all the routers on this subnet multicast address.

The discovery messages for an indirect LDP session are addressed to the specified peer and not to the multicast address.

Default n/a

disable-targeted-session

Syntax [no] disable-targeted-session
Context config>router>ldp>targeted-session
Description This command disables support for targeted sessions. Targeted sessions are LDP sessions between non-directly connected peers. The discovery messages for an indirect LDP session are addressed to the specified peer and not to the multicast address.

The no form of the command enables the setup of any targeted sessions.

Default no disable-targeted-session

peer

Syntax [no] peer ip-address
Context config>router>ldp>targeted-session
Description This command configures parameters for an LDP peer.

Default n/a
Parameters ip-address — specifies the LDP peer in dotted-decimal notation
**bfd-enable**

**Syntax**

```plaintext
[no] bfd-enable
```

**Context**

```
config>router>ldp>if-params>interface
config>router>ldp>targeted-session>peer
```

**Description**

This command enables or disables bidirectional forwarding detection (BFD) tracking of the LDP session for the interface or the T-LDP session for the peer.

The **no** form of this command disables BFD tracking.

**Default**

n/a

---

**local-lsr-id**

**Syntax**

```plaintext
local-lsr-id interface-name
no local-lsr-id
```

**Context**

```
config>router>ldp>targeted-session>peer
```

**Description**

This command enables the use of the address of a specific interface as the LSR ID in order to establish a targeted LDP (T-LDP) adjacency and session with one or more non-directly connected LDP peers. The interface can be a regular interface or a loopback interface, including the system interface.

By default, a T-LDP session uses the system interface address as the LSR ID, unless the LSR ID is explicitly configured. This means that T-LDP and interface LDP share a common LDP TCP session and therefore a common LDP label space. The system interface must be always be configured on the router or the LDP protocol will not come up on the node.

At initial configuration, the LDP session to the peers remains down while the interface is down. If the user changes the LSR ID while the LDP session is up, LDP immediately tears down the session and attempts to re-establish it using the new LSR ID. If the interface used for the local LSR ID goes down, the LDP session to all peers using this LSR ID will also go down.

The user-configured LSR ID is used for extended peer discovery to establish the T-LDP hello adjacency. It is also used as the transport address for the LDP TCP session when it is bootstrapped by the T-LDP hello adjacency. The user-configured LSR ID is not used in basic peer discovery to establish a link-level LDP hello adjacency.

The **no** form of the command resets the **local-lsr-id** to the default value, which means that the system interface address is used as the LSR ID.

**Default**

no local-lsr-id
Parameters  

interface-name — specifies the name, up to 32 characters in length, of the network IP interface. An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
5.11.2.1.5 Peer Parameters Commands

**peer-parameters**

**Syntax**  
peer-parameters  
**Context**  
config>router>ldp  
**Description**  
This command enables the context to configure peer specific parameters.

**peer**

**Syntax**  
[no] peer ip-address  
**Context**  
config>router>ldp>peer-parameters  
**Description**  
This command configures parameters for an LDP peer.  
**Default**  
n/a  
**Parameters**  
ip-address — specifies the LDP peer in dotted-decimal notation

**auth-keychain**

**Syntax**  
auth-keychain name  
no auth-keychain  
**Context**  
config>router>ldp>peer-parameters>peer  
**Description**  
This command associates an authentication keychain with LDP. The keychain is a collection of keys used to authenticate LDP messages from remote peers. The keychain allows the rollover of authentication keys during the lifetime of a session and also supports stronger authentication algorithms than clear text and MD5.

The keychain must already be defined in the **config>system>security>keychain** context.

Either the **authentication-key** command or the **auth-keychain** command can be used by LDP, but both cannot be supported at the same time. If both commands are configured, the **auth-keychain** configuration will be applied and the **authentication-key** command will be ignored.

By default, authentication is not enabled.

**Default**  
n/a  
**Parameters**  
name — the name of an existing keychain, up to 32 characters
authentication-key

**Syntax**  
```plaintext
authentication-key {authentication-key | hash-key} [hash | hash2]
```

**no authentication-key**

**Context**  
config>router>ldp>peer-parameters>peer

**Description**  
This command specifies the authentication key to be used between LDP peers before establishing sessions. Authentication uses the MD5 message-based digest.

Either the `authentication-key` command or the `auth-keychain` command can be used by LDP, but both cannot be supported at the same time. If both commands are configured, the `auth-keychain` configuration will be applied and the `authentication-key` command will be ignored.

The **no** form of this command disables authentication.

**Default**  
n/a

**Parameters**

- `authentication-key` — specifies the authentication key. Allowed values are any string up to 16 characters long (unencrypted) composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

- `hash-key` — specifies the hash key. Allowed values are any string up to 33 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

  This is useful when a user must configure the parameter; however, for security purposes, the actual unencrypted key value is not provided.

- `hash` — specifies that the key is entered and stored on the node in encrypted form

- `hash2` — specifies that the key is entered and stored on the node in a more complex encrypted form

**Note:** If neither the `hash` or `hash2` keyword is specified, the key is entered in clear text. However, for security purposes, the key is stored on the node using hash encryption.
5.11.2.2 Show Commands

Note: The following command outputs are examples only; actual displays may differ depending on supported functionality and user configuration.

auth-keychain

Syntax: auth-keychain [keychain]

Context: show>router>ldp

Description: This command displays LDP sessions using a particular authentication keychain.

Parameters:
- keychain — specifies an existing keychain name

Output: The following output is an example of LDP sessions using an authentication keychain, and Table 37 describes the fields.

Output Example

*A:ALU-48# show router ldp auth-keychain
===============================================================================
<table>
<thead>
<tr>
<th>Peer</th>
<th>TTL Sec</th>
<th>Min-TTL</th>
<th>Auth</th>
<th>Auth key chain</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.20.1.3</td>
<td>Disabled</td>
<td>n/a</td>
<td>Enabled</td>
<td>eta_keychain1</td>
</tr>
</tbody>
</table>
===============================================================================
No. of Peers: 1
===============================================================================
*A:ALU-48#

Table 37 LDP Auth-keychain Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer</td>
<td>The IP address of the peer</td>
</tr>
<tr>
<td>TTL Sec</td>
<td>Indicates whether LDP peering session security is enabled or disabled</td>
</tr>
<tr>
<td>Min-TTL</td>
<td>The minimum TTL value for an incoming packet</td>
</tr>
<tr>
<td>Auth</td>
<td>Indicates whether authentication using MD5 message-based digest protocol is enabled or disabled</td>
</tr>
<tr>
<td>Auth key chain</td>
<td>Indicates the authentication keychain associated with the session, if applicable</td>
</tr>
</tbody>
</table>
### bindings

**Syntax**
```
bindings [fec-type fec-type [detail]] [session ip-addr[:label-space]]
bindings label-type start-label [end-label]
bindings (prefix ip-prefix/mask [detail]) [session ip-addr[:label-space]]
bindings active [prefix ip-prefix/mask]
bindings vc-type vc-type [vc-id vc-id [session ip-addr[:label-space]]]
bindings service-id service-id [detail]
```

**Context**
```
show>router>ldp
```

**Description**
This command displays the contents of the label information base.

**Parameters**
- **ip-addr** — specifies the IP address of the next hop
  - **Values**
    - a.b.c.d
- **fec-type** — specifies the forwarding class type
  - **Values**
    - prefixes, services
- **ip-prefix** — specifies the IP prefix in dotted-decimal notation
  - **Values**
    - a.b.c.d (host bits must be 0)
- **mask** — specifies the 32-bit address mask used to indicate the bits of an IP address that are being used for the subnet address
  - **Values**
    - 0 to 32
- **label-space** — specifies the label space identifier that the router is advertising on the interface
  - **Values**
    - 0 to 65535
- **label-type** — specifies the label type to display
  - **Values**
    - ingress-label, egress-label
- **start-label** — specifies a label value to begin the display
  - **Values**
    - 16 to 1048575
- **end-label** — specifies a label value to end the display
  - **Values**
    - 17 to 1048575
- **vc-type** — specifies the VC type to display
  - **Values**
    - atmvcc, atmvpcc, cesopsn, cesopsn-cas, satop-e1, satop-t1, ethernet, ipipe
- **vc-id** — specifies the VC ID to display
  - **Values**
    - 1 to 4294967295
- **service-id** — specifies the service ID number or name to display
  - **Values**
    - 1 to 2147483690 or svc-name
Output

The following output is an example of LDP bindings information, and Table 38 describes the fields. Following the table are output examples for:

- LDP bindings detail
- LDP bindings session
- LDP bindings active

Output Example - show router ldp bindings

A:cpm-a# show router ldp bindings
===============================================================================
LDP LSR ID: 1.1.1.30
===============================================================================
Legend: U - Label In Use, N - Label Not In Use, W - Label Withdrawn
S - Status Signaled Up, D - Status Signaled Down
E - Epipe Service, V - VPLS Service, M - Mirror Service
P - Ipipe Service, WP - Label Withdraw Pending, C - Cpipe Service
BU - Alternate for Fast Re-Route, TLV - (Type, Length: Value), H - Hpipe
===============================================================================
LDP Prefix Bindings
-------------------------------------------------------------------------------
Prefix Peer IngLbl EgrLbl EgrIntf/LspId EgrNextHop
-------------------------------------------------------------------------------
1.1.1.30/32 1.1.1.33 131071U -- -- --
1.1.1.30/32 1.1.1.57 131071U -- -- --
1.1.1.33/32 1.1.1.33 -- 131071 1/2/3:1 10.4.1.33
1.1.1.33/32 1.1.1.57 131061U 131059 -- --
1.1.1.57/32 1.1.1.33 131060U 131067 -- --
1.1.1.57/32 1.1.1.57 -- 131071 LspId 1 --
1.1.1.58/32 1.1.1.33 131059U 131066 -- --
1.1.1.58/32 1.1.1.57 131059N 131070 LspId 1 --
-------------------------------------------------------------------------------
No. of Prefix Bindings: 8
===============================================================================
LDP Service FEC 128 Bindings
-------------------------------------------------------------------------------
Type VCId SvcId SDPId Peer IngLbl EgrLbl EgrIntf/LspId EgrNextHop
-------------------------------------------------------------------------------
E-Eth 100 1 1 1.1.1.57 131069U 131068D 1500 1500
E-Eth 101 2 1 1.1.1.57 -- 131067D 1500 1500
E-Eth 102 3 1 1.1.1.57 131067U 131066 1500 1500
E-Eth 103 4 1 1.1.1.57 131066W 131065 1500 1500
E-Eth 104 5 1 1.1.1.57 131065U -- 1500 0
E-Eth 105 5 1 1.1.1.57 131064U -- 1500 0
E-Eth 106 6 1 1.1.1.57 131063U 131064D 1500 1500
E-Eth 107 7 1 1.1.1.57 131062U -- 1500 0
-------------------------------------------------------------------------------
No. of VC Labels: 8
===============================================================================
LDP Service FEC 129 Bindings
-------------------------------------------------------------------------------
AGI SAI TAII
Type SvcId SDPId Peer IngLbl EgrLbl LMTU RMTU
-------------------------------------------------------------------------------
### Table 38  
**LDP Bindings Output Fields**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legend</td>
<td>U: Label In Use</td>
</tr>
<tr>
<td></td>
<td>N: Label Not In Use</td>
</tr>
<tr>
<td></td>
<td>W: Label Withdrawn</td>
</tr>
<tr>
<td></td>
<td>S: Status Signaled Up</td>
</tr>
<tr>
<td></td>
<td>D: Status Signaled Down</td>
</tr>
<tr>
<td></td>
<td>E: Epipe Service</td>
</tr>
<tr>
<td></td>
<td>V: VPLS Service</td>
</tr>
<tr>
<td></td>
<td>M: Mirror Service</td>
</tr>
<tr>
<td></td>
<td>A: Apipe Service</td>
</tr>
<tr>
<td></td>
<td>F: Fpipe Service</td>
</tr>
<tr>
<td></td>
<td>I: IES Service</td>
</tr>
<tr>
<td></td>
<td>R: VPRN service</td>
</tr>
<tr>
<td></td>
<td>P: Ipipe Service</td>
</tr>
<tr>
<td></td>
<td>WP: Label Withdraw Pending</td>
</tr>
<tr>
<td></td>
<td>BU: Alternate for Fast Re-Route</td>
</tr>
<tr>
<td></td>
<td>TLV: (Type, Length: Value)</td>
</tr>
<tr>
<td></td>
<td>H: Hpipe</td>
</tr>
<tr>
<td>Type</td>
<td>The service type exchanging labels in the SDP.</td>
</tr>
<tr>
<td></td>
<td>The possible types displayed are Epipe, Spoke,</td>
</tr>
<tr>
<td></td>
<td>and Unknown.</td>
</tr>
<tr>
<td>VCId</td>
<td>The value used by each end of an SDP tunnel to</td>
</tr>
<tr>
<td></td>
<td>identify the VC</td>
</tr>
<tr>
<td>SvcID</td>
<td>Identifies the service in the service domain</td>
</tr>
<tr>
<td>SDPId</td>
<td>Identifies the SDP in the service domain</td>
</tr>
<tr>
<td>Peer</td>
<td>The IP address of the peer</td>
</tr>
<tr>
<td>InglLbl</td>
<td>The ingress LDP label</td>
</tr>
<tr>
<td></td>
<td>U — indicates that the label is in use</td>
</tr>
<tr>
<td></td>
<td>R — indicates that the label has been released</td>
</tr>
<tr>
<td>EgrLbl</td>
<td>The egress LDP label</td>
</tr>
<tr>
<td>LMTU</td>
<td>The local MTU value</td>
</tr>
<tr>
<td>RMTU</td>
<td>The remote MTU value</td>
</tr>
<tr>
<td>No. of Prefix Bindings</td>
<td>The total number of LDP bindings on the router</td>
</tr>
<tr>
<td>EgrIntf/Lspld</td>
<td>The egress interface LSP ID</td>
</tr>
<tr>
<td>EgrNextHop</td>
<td>The egress next-hop address, or Unnumbered for</td>
</tr>
<tr>
<td></td>
<td>unnumbered interfaces</td>
</tr>
<tr>
<td>No. of VC Labels</td>
<td>The total number of VC labels</td>
</tr>
<tr>
<td>No. of Service Bindings</td>
<td>The total number of service bindings</td>
</tr>
<tr>
<td>AGI Type</td>
<td>The address group identifier (AGI)</td>
</tr>
</tbody>
</table>
### Table 38 LDP Bindings Output Fields (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAIi Peer</td>
<td>The source attachment individual identifier (SAII)</td>
</tr>
<tr>
<td>TAIi EgrLbl</td>
<td>The target attachment individual identifier (TAII)</td>
</tr>
<tr>
<td>Vc-switching</td>
<td>Not applicable – always indicates no</td>
</tr>
<tr>
<td>Egr. Flags</td>
<td>Specifies the egress flags, if any</td>
</tr>
<tr>
<td>Egr. Ctl Word</td>
<td>Indicates whether egress control words are used</td>
</tr>
<tr>
<td>Egr. Status Bits</td>
<td>Indicates whether egress status bits are supported</td>
</tr>
<tr>
<td>Egr If Name</td>
<td>The egress interface name</td>
</tr>
<tr>
<td>Ing. Flags</td>
<td>Specifies the ingress flags, if any</td>
</tr>
<tr>
<td>Ing. Ctl Word</td>
<td>Indicates whether ingress control words are used</td>
</tr>
<tr>
<td>Ing. Status Bits</td>
<td>Indicates whether ingress status bits are supported</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric of the LSP</td>
</tr>
<tr>
<td>Mtu</td>
<td>The size of the MTU for the global FEC or tunnel to which the LDP binding is applied</td>
</tr>
<tr>
<td>Op</td>
<td>The operation performed on the ingress or egress label in the LDP stack (push or pop)</td>
</tr>
</tbody>
</table>

**Output Example - show router ldp bindings detail**

```
A:cpm-a# show router ldp bindings detail
===============================================================================
LDP LSR ID: 10.20.1.3
Legend: U - Label In Use, N - Label Not In Use, W - Label Withdrawn
S - Status Signaled Up, D - Status Signaled Down
E - Epipe Service, V - VPLS Service, M - Mirror Service
P - Ipipe Service, WP - Label Withdraw Pending, C - Cpipe Service
BU - Alternate For Fast Re-Route, TLV - (Type, Length: Value), H - Hpipe
===============================================================================
LDP Prefix Bindings
===============================================================================
Prefix : 10.20.1.3/32
Ing Lbl : 131070U Peer : 10.20.1.5
Egr Lbl : --
Egr Int/LspId : --
EgrNextHop : --
Egr. Flags : None Ing. Flags : None
Prefix : 10.20.1.5/32
```
### MPLS Guide

#### Label Distribution Protocol

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ing Lbl</td>
<td>Egr Lbl</td>
<td>Peer</td>
</tr>
<tr>
<td>--</td>
<td>131070</td>
<td>10.20.1.5</td>
</tr>
<tr>
<td>Egr Int/LspId</td>
<td>aps-1</td>
<td></td>
</tr>
<tr>
<td>EgrNextHop</td>
<td>3.5.1.2</td>
<td></td>
</tr>
<tr>
<td>Egr Flags</td>
<td>None</td>
<td>Ing. Flags : None</td>
</tr>
<tr>
<td>Egr If Name</td>
<td>ip-3.5.1.1</td>
<td></td>
</tr>
<tr>
<td>Metric</td>
<td>10</td>
<td>Mtu : 1570</td>
</tr>
</tbody>
</table>

**Prefix** : 10.20.1.5/32

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ing Lbl</td>
<td>Egr Lbl</td>
<td>Peer</td>
</tr>
<tr>
<td>--</td>
<td>131070</td>
<td>10.20.1.5</td>
</tr>
<tr>
<td>Egr Int/LspId</td>
<td>aps-2</td>
<td></td>
</tr>
<tr>
<td>EgrNextHop</td>
<td>3.5.2.2</td>
<td></td>
</tr>
<tr>
<td>Egr Flags</td>
<td>None</td>
<td>Ing. Flags : None</td>
</tr>
<tr>
<td>Egr If Name</td>
<td>ip-3.5.2.1</td>
<td></td>
</tr>
<tr>
<td>Metric</td>
<td>10</td>
<td>Mtu : 1570</td>
</tr>
</tbody>
</table>

**Prefix** : 10.20.1.5/32

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ing Lbl</td>
<td>Egr Lbl</td>
<td>Peer</td>
</tr>
<tr>
<td>--</td>
<td>131070</td>
<td>10.20.1.5</td>
</tr>
<tr>
<td>Egr Int/LspId</td>
<td>aps-3</td>
<td></td>
</tr>
<tr>
<td>EgrNextHop</td>
<td>3.5.3.2</td>
<td></td>
</tr>
<tr>
<td>Egr Flags</td>
<td>None</td>
<td>Ing. Flags : None</td>
</tr>
<tr>
<td>Egr If Name</td>
<td>ip-3.5.3.1</td>
<td></td>
</tr>
<tr>
<td>Metric</td>
<td>10</td>
<td>Mtu : 1570</td>
</tr>
</tbody>
</table>

** Prefix Bindings:** 4

### LDP Service Bindings

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>E-Eth</td>
<td>VcId</td>
<td>100</td>
</tr>
<tr>
<td>SvcId</td>
<td>1</td>
<td>SdpId</td>
<td>1</td>
</tr>
<tr>
<td>Peer Address</td>
<td>1.1.1.57</td>
<td>Vc-switching : No</td>
<td></td>
</tr>
<tr>
<td>LMTU</td>
<td>1500</td>
<td>RMTU</td>
<td>1500</td>
</tr>
<tr>
<td>Egr Lbl</td>
<td>131068D</td>
<td>Egr. Ctl Word : No</td>
<td></td>
</tr>
<tr>
<td>Egr Flags</td>
<td>None</td>
<td>Egr. Status Bits : Supported (0x16)</td>
<td></td>
</tr>
<tr>
<td>Ing Lbl</td>
<td>131069U</td>
<td>Ing. Ctl Word : No</td>
<td></td>
</tr>
<tr>
<td>Ing Flags</td>
<td>None</td>
<td>Ing. Status Bits : Supported (0x0)</td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>E-Eth</td>
<td>VcId</td>
<td>101</td>
</tr>
<tr>
<td>SvcId</td>
<td>2</td>
<td>SdpId</td>
<td>1</td>
</tr>
<tr>
<td>Peer Address</td>
<td>1.1.1.57</td>
<td>Vc-switching : No</td>
<td></td>
</tr>
<tr>
<td>LMTU</td>
<td>1500</td>
<td>RMTU</td>
<td>1500</td>
</tr>
<tr>
<td>Egr Lbl</td>
<td>131067D</td>
<td>Egr. Ctl Word : Yes</td>
<td></td>
</tr>
<tr>
<td>Egr Flags</td>
<td>None</td>
<td>Egr. Status Bits : Supported (0x16)</td>
<td></td>
</tr>
<tr>
<td>Ing Lbl</td>
<td>--</td>
<td>Ing. Ctl Word : No</td>
<td></td>
</tr>
<tr>
<td>Ing Flags</td>
<td>Released</td>
<td>Ing. Status Bits : N/A</td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>E-Eth</td>
<td>VcId</td>
<td>102</td>
</tr>
<tr>
<td>SvcId</td>
<td>3</td>
<td>SdpId</td>
<td>1</td>
</tr>
<tr>
<td>Peer Address</td>
<td>1.1.1.57</td>
<td>Vc-switching : No</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>------</td>
<td>--------------</td>
<td>-------</td>
</tr>
<tr>
<td>E-Eth</td>
<td>103</td>
<td>No</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>104</td>
<td>Yes 1:105</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>105</td>
<td>Yes 1:104</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>106</td>
<td>No</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>107</td>
<td>No</td>
<td>8</td>
</tr>
</tbody>
</table>

No. of VC Labels: 8
A:cpm-a#
### Output Example - show router ldp bindings session

```
ALU-12# show router ldp bindings session 10.10.10.104

Legend: U - Label In Use, R - Label Released
```

#### LDP Prefix Bindings

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Peer</th>
<th>IngLbl</th>
<th>EgrLbl</th>
<th>EgrIntf</th>
<th>EgrNextHop</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No Matching Entries Found

#### LDP Service FEC 128 Bindings

<table>
<thead>
<tr>
<th>Type</th>
<th>VCId</th>
<th>SvcId</th>
<th>SDPId</th>
<th>Peer</th>
<th>IngLbl</th>
<th>EgrLbl</th>
<th>LMTU</th>
<th>RMTU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ukwn</td>
<td>222</td>
<td>Ukwn</td>
<td>Ukwn</td>
<td>10.10.10.104</td>
<td>--</td>
<td>131071</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VPLS</td>
<td>700</td>
<td>700</td>
<td>2</td>
<td>10.10.10.104</td>
<td>131071U</td>
<td>131070</td>
<td>1514</td>
<td>0</td>
</tr>
</tbody>
</table>

No. of Service Bindings: 2

#### LDP Service FEC 129 Bindings

<table>
<thead>
<tr>
<th>AGI</th>
<th>SAI</th>
<th>TAII</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No Matching Entries Found

---

### Output Example - show router ldp bindings active

```
ALU-12# show router ldp bindings active

Legend: (S) - Static  (M) - Multi-homed Secondary Support  (B) - BGP Next Hop (BU) - Alternate Next-hop for Fast Re-Route
```

#### LDP Prefix Bindings (Active)

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Op</th>
<th>IngLbl</th>
<th>EgrLbl</th>
<th>EgrIntf/LspId</th>
<th>EgrNextHop</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.20.1.1/32</td>
<td>Pop</td>
<td>131071</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>10.20.1.2/32</td>
<td>Push</td>
<td>--</td>
<td>131071</td>
<td>1/1/1</td>
<td>10.10.1.2</td>
</tr>
<tr>
<td>10.20.1.2/32</td>
<td>Swap</td>
<td>131070</td>
<td>131071</td>
<td>1/1/1</td>
<td>10.10.1.2</td>
</tr>
<tr>
<td>10.20.1.2/32</td>
<td>Push</td>
<td>--</td>
<td>262141BU</td>
<td>1/1/2</td>
<td>10.10.2.3</td>
</tr>
<tr>
<td>10.20.1.2/32</td>
<td>Swap</td>
<td>131070</td>
<td>262141BU</td>
<td>1/1/2</td>
<td>10.10.2.3</td>
</tr>
<tr>
<td>10.20.1.3/32</td>
<td>Push</td>
<td>--</td>
<td>131069BU</td>
<td>1/1/1</td>
<td>10.10.1.2</td>
</tr>
<tr>
<td>10.20.1.3/32</td>
<td>Swap</td>
<td>131069</td>
<td>131069BU</td>
<td>1/1/1</td>
<td>10.10.1.2</td>
</tr>
<tr>
<td>10.20.1.3/32</td>
<td>Push</td>
<td>--</td>
<td>262143</td>
<td>1/1/2</td>
<td>10.10.2.3</td>
</tr>
<tr>
<td>10.20.1.3/32</td>
<td>Swap</td>
<td>131069</td>
<td>262143</td>
<td>1/1/2</td>
<td>10.10.2.3</td>
</tr>
<tr>
<td>10.20.1.4/32</td>
<td>Push</td>
<td>--</td>
<td>131068</td>
<td>1/1/1</td>
<td>10.10.1.2</td>
</tr>
<tr>
<td>10.20.1.4/32</td>
<td>Swap</td>
<td>131068</td>
<td>131068</td>
<td>1/1/1</td>
<td>10.10.1.2</td>
</tr>
<tr>
<td>10.20.1.4/32</td>
<td>Push</td>
<td>--</td>
<td>262140BU</td>
<td>1/1/2</td>
<td>10.10.2.3</td>
</tr>
<tr>
<td>10.20.1.4/32</td>
<td>Swap</td>
<td>131068</td>
<td>262140BU</td>
<td>1/1/2</td>
<td>10.10.2.3</td>
</tr>
</tbody>
</table>
### LDP Prefix Bindings (Active)

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Op</th>
<th>IngrLbl</th>
<th>EgrLbl</th>
<th>EgrIntf/LspId</th>
<th>EgrNextHop</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.20.1.1/32</td>
<td>Push --</td>
<td>262143</td>
<td>1/1/1 Unnumbered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.2/32</td>
<td>Swap 262138</td>
<td>262143</td>
<td>1/1/1 Unnumbered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.3/32</td>
<td>Push --</td>
<td>262143</td>
<td>1/1/1 Unnumbered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.4/32</td>
<td>Swap 262139</td>
<td>262143</td>
<td>1/1/2 Unnumbered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.5/32</td>
<td>Push --</td>
<td>262143</td>
<td>2/1/2 Unnumbered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.6/32</td>
<td>Swap 262142</td>
<td>262143</td>
<td>2/1/2 Unnumbered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.7/32</td>
<td>Push --</td>
<td>262143</td>
<td>2/1/2 Unnumbered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.8/32</td>
<td>Swap 262144</td>
<td>262143</td>
<td>2/1/2 Unnumbered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.9/32</td>
<td>Push --</td>
<td>262143</td>
<td>2/1/2 Unnumbered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.10/32</td>
<td>Swap 262145</td>
<td>262143</td>
<td>2/1/2 Unnumbered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.11/32</td>
<td>Push --</td>
<td>262143</td>
<td>2/1/2 Unnumbered</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.12/32</td>
<td>Swap 262146</td>
<td>262143</td>
<td>2/1/2 Unnumbered</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No. of Prefix Bindings: 21

### Output Example - show router ldp bindings active (on unnumbered interfaces)

ALU-12# show router ldp bindings active

**Legend:**
- (S) - Static
- (M) - Multi-homed Secondary Support
- (B) - BGP Next Hop
- (BU) - Alternate Next-hop for Fast Re-Route

### Syntax
```
discovery [peer [ip-address]] | [interface [ip-int-name]]] [state state] [detail]
```

### Context
```
show>router>ldp
```

### Description
This command displays the status of the interfaces participating in LDP discovery.

### Parameters
- `ip-address` — specifies the IP address of the peer
- `ip-int-name` — specifies an existing interface. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
- `state` — specifies the current operational state of the adjacency
- `detail` — displays detailed information
Output

The following outputs are examples of LDP discovery information, and Table 39 describes the fields.

Output Example - show router ldp discovery

ALU-12# show router ldp discovery
-----------------------------------------------------------------------------------------------
LDP Hello Adjacencies
-----------------------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Local Addr</th>
<th>Peer Addr</th>
<th>AdjType</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>10.10.10.103</td>
<td>10.10.10.93</td>
<td>Targ</td>
<td>Trying</td>
</tr>
<tr>
<td>N/A</td>
<td>10.10.10.103</td>
<td>10.10.10.104</td>
<td>Targ</td>
<td>Estab</td>
</tr>
<tr>
<td>to-104</td>
<td>10.0.0.103</td>
<td>224.0.0.2</td>
<td>Link</td>
<td>Trying</td>
</tr>
</tbody>
</table>
-----------------------------------------------------------------------------------------------
No. of Hello Adjacencies: 3
-----------------------------------------------------------------------------------------------
ALU-12#

Output Example - show router ldp discovery detail

ALU-12# show router ldp discovery detail
-----------------------------------------------------------------------------------------------
LDP Hello Adjacencies (Detail)
-----------------------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Peer</th>
<th>Local Address : 10.10.10.103</th>
<th>Peer Address : 10.10.10.93</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adjacency Type</td>
<td>Targeted</td>
<td>State : Trying</td>
</tr>
<tr>
<td>Up Time</td>
<td>0d 18:26:36</td>
<td>Hold Time Remaining: 38</td>
</tr>
<tr>
<td>Hello Msg Recv</td>
<td>76616920</td>
<td>Hello Msg Sent : 466580812</td>
</tr>
<tr>
<td>Remote Cfg Seq No</td>
<td>159</td>
<td>Remote IP Address : 10.10.10.104</td>
</tr>
<tr>
<td>Local Cfg Seq No</td>
<td>1674451</td>
<td>Local IP Address : 0.224.173.172</td>
</tr>
</tbody>
</table>
-----------------------------------------------------------------------------------------------
| Peer 10.10.10.104 |
| Local Address : 10.10.10.103 | Peer Address : 10.10.10.104 |
| Adjacency Type  : Targeted | State : Established |
| Up Time         : 0d 18:26:36 | Hold Time Remaining: 38     |
| Hello Msg Recv  : 76616920 | Hello Msg Sent : 466580812  |
| Remote Cfg Seq No | 159                  | Remote IP Address : 10.10.10.104 |
| Local Cfg Seq No | 1674451                      | Local IP Address : 0.224.173.172 |
-----------------------------------------------------------------------------------------------
Interface "to-104"
-----------------------------------------------------------------------------------------------
| Local Address : 10.0.0.103 | Peer Address : 224.0.0.2 |
| Adjacency Type  : Link    | State : Trying           |
-----------------------------------------------------------------------------------------------
ALU-12#

Table 39 LDP Discovery Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>The name of the interface</td>
</tr>
<tr>
<td>Local Addr</td>
<td>The IP address of the originating (local) router</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Peer Addr</td>
<td>The IP address of the peer</td>
</tr>
<tr>
<td>Adj Type</td>
<td>The adjacency type between the LDP peer and LDP session</td>
</tr>
<tr>
<td>State</td>
<td>Established — indicates that the adjacency is established</td>
</tr>
<tr>
<td></td>
<td>Trying — indicates that the adjacency is not yet established</td>
</tr>
<tr>
<td>No. of Hello Adjacencies</td>
<td>The total number of hello adjacencies discovered</td>
</tr>
<tr>
<td>Up Time</td>
<td>The amount of time the adjacency has been enabled</td>
</tr>
<tr>
<td>Hold-Time Remaining</td>
<td>The time left before a neighbor is declared to be down</td>
</tr>
<tr>
<td>Hello Mesg Recv</td>
<td>The number of Hello messages received for this adjacency</td>
</tr>
<tr>
<td>Hello Mesg Sent</td>
<td>The number of Hello messages that have been sent for this adjacency</td>
</tr>
<tr>
<td>Remote Cfg Seq No</td>
<td>The configuration sequence number that was in the Hello message received when this adjacency started up. This configuration sequence number changes when there is a change of configuration.</td>
</tr>
<tr>
<td>Remote IP Address</td>
<td>The IP address used on the remote end for the LDP session</td>
</tr>
<tr>
<td>Local Cfg Seq No</td>
<td>The configuration sequence number that was used in the Hello message sent when this adjacency started up. This configuration sequence number changes when there is a change of configuration.</td>
</tr>
<tr>
<td>Local IP Address</td>
<td>The IP address used locally for the LDP session</td>
</tr>
</tbody>
</table>
**fec-originate**

**Syntax**
```
fec-originate [ip-address/mask] [operation-type]
fec-originate [operation-type] [ipv4]
```

**Context**
```
show>router>ldp
```

**Description**
This command displays LDP static prefix FECs.

**Parameters**
- `ip-address/mask` — specifies the IP prefix and prefix length
  
  **Values**
  - `ipv4-address` a.b.c.d (host bits must be 0)
  - `mask` 0 to 32

- `operation-type` — specifies the operation type to display
  
  **Values**
  - `pop | swap`

**Output**
The following output is an example of FEC originate information, and Table 40 describes the fields.

**Output Example**
```
*A:ALU-12# show router ldp fec-originate
```
```
Prefix NHType NextHop IngLabel EgrLabel OperIngLabel
-------------------------------------------------------------------------------
24.1.0.0/16    Pop    n/a    --    --    0
24.1.0.1/32    Pop    n/a    --    --    0
24.1.0.2/32    Pop    n/a    --    --    0
24.1.0.3/32    Pop    n/a    --    --    0
24.1.0.4/32    Pop    n/a    --    --    0
24.1.0.5/32    Pop    n/a    --    --    0
24.1.0.6/32    Pop    n/a    --    --    0
24.1.0.7/32    Pop    n/a    --    --    0
24.1.0.8/32    Pop    n/a    --    --    0
24.1.0.9/32    Pop    n/a    --    --    0
...  24.251.0.0/16    Pop    n/a    --    --    0
24.252.0.0/16    Pop    n/a    --    --    0
24.253.0.0/16    Pop    n/a    --    --    0
24.254.0.0/16    Pop    n/a    --    --    0
-------------------------------------------------------------------------------
No. of FECs: 508
```
```
*A:ALU-12#*
```
### Table 40  FEC-Originate Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix</td>
<td>The static prefix FEC</td>
</tr>
<tr>
<td>NHType</td>
<td>The type of next hop for this entry:</td>
</tr>
<tr>
<td></td>
<td>Unknown: the next-hop type has not been set</td>
</tr>
<tr>
<td></td>
<td>IP Addr: the next hop is an IP address</td>
</tr>
<tr>
<td></td>
<td>Pop: there is no next hop; label is popped and packet routed</td>
</tr>
<tr>
<td></td>
<td>Unnumbered: the next hop is an unnumbered interface</td>
</tr>
<tr>
<td>Next Hop</td>
<td>The IP address of the next hop, or Unnumbered for unnumbered interfaces</td>
</tr>
<tr>
<td>IngLabel</td>
<td>The label that is advertised to the upstream peer. If this variable is set</td>
</tr>
<tr>
<td></td>
<td>to the default value of 4294967295, the ingress label will be dynamically</td>
</tr>
<tr>
<td></td>
<td>assigned by the label manager.</td>
</tr>
<tr>
<td>EgrLabel</td>
<td>The egress label associated with this next-hop entry. The LSR will swap the</td>
</tr>
<tr>
<td></td>
<td>incoming label with the configured egress label. If this egress label has a</td>
</tr>
<tr>
<td></td>
<td>value of 4294967295, the LSR will pop the incoming label.</td>
</tr>
<tr>
<td>OperIngLabel</td>
<td>The actual or operational value of the label that was advertised to the</td>
</tr>
<tr>
<td></td>
<td>upstream peer</td>
</tr>
</tbody>
</table>

### interface

**Syntax**  
`interface [ip-int-name | ip-address] [detail]`

**Context**  
`show>router>ldp`

**Description**  
This command displays configuration information about LDP interfaces.

**Parameters**  
- `ip-int-name` — specifies an existing interface. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
- `ip-address` — identifies the LDP neighbor by IP address
- `detail` — displays detailed information

**Output**  
The following output is an example of LDP interface information, and Table 41 describes the fields.
### Output Example

A:ALU-12# show router ldp interface

```
===============================================================================
LDP Interfaces
===============================================================================
Interface          Adm  Opr  Hello  Hold  KA     KA   Factor  Time  Factor  Timeout Address
-------------------------------------------------------------------------------
i2_1/1              Up    Up  3       15     3     30      System

No. of Interfaces: 1
```

A:ALU-12#

A:ALU-12>show>router>ldp# interface detail

```
===============================================================================
LDP Interfaces (Detail)
===============================================================================
Interface "back"
-------------------------------------------------------------------------------
Admin State       : Up      Oper State      : Down
Oper Down Reason  : interfaceDown
Hold Time         : 1000    Hello Factor : 15
Keepalive Timeout : 1000    Keepalive Factor : 15
Transport Addr    : System  Last Modified : 08/08/2007 09:50:15
Active Adjacencies : 0      Tunneling   : Disabled
Lsp Name          : None

-------------------------------------------------------------------------------
```

A:ALU-12>show>router>ldp#

### Table 41 LDP Interface Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface associated with the LDP instance</td>
</tr>
<tr>
<td>Adm</td>
<td>Up — indicates that the LDP is administratively enabled</td>
</tr>
<tr>
<td></td>
<td>Down — indicates that the LDP is administratively disabled</td>
</tr>
<tr>
<td>Opr</td>
<td>Up — indicates that the LDP is operationally enabled</td>
</tr>
<tr>
<td></td>
<td>Down — indicates that the LDP is operationally disabled</td>
</tr>
<tr>
<td>Hello Factor</td>
<td>The value by which the hello timeout should be divided to give the hello time; that is, the time interval, in seconds, between LDP Hello messages. LDP uses hello messages to discover neighbors and to detect loss of connectivity with its neighbors.</td>
</tr>
</tbody>
</table>
parameters

Syntax parameters

Context show>router>ldp

Description This command displays configuration information about LDP parameters.

Output The following output is an example of LDP parameters information, and Table 42 describes the fields.

Output Example

A:ALU-12# show router ldp parameters
========================================================================
LDP Parameters (LSR ID 10.10.10.103)
========================================================================
Graceful Restart Parameters

Table 41 LDP Interface Output Fields (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hold Time</td>
<td>The time interval, in seconds, that LDP waits before declaring a neighbor to be down. Hold time (also known as Hello time) is local to the system and is sent in the hello messages to a neighbor.</td>
</tr>
<tr>
<td>KA Factor</td>
<td>The value by which the keepalive timeout should be divided to give the keepalive time; that is, the time interval, in seconds, between LDP keepalive messages. LDP keepalive messages are sent to keep the LDP session from timing out when no other LDP traffic is being sent between the neighbors.</td>
</tr>
<tr>
<td>KA Timeout</td>
<td>The time interval, in seconds, that LDP waits before tearing down a session. If no LDP messages are exchanged during this time interval, the LDP session is torn down. Generally the value is configured to be three times the keepalive time (the time interval between successive LDP keepalive messages).</td>
</tr>
<tr>
<td>Transport Address</td>
<td>The transport address entity</td>
</tr>
<tr>
<td>No. of Interfaces</td>
<td>The total number of LDP interfaces</td>
</tr>
<tr>
<td>Oper Down Reason</td>
<td>The reason for the LSP being in the down state</td>
</tr>
<tr>
<td>Active Adjacencies</td>
<td>The number of active adjacencies</td>
</tr>
<tr>
<td>Last Modified</td>
<td>The time of the last modification to the LDP interface</td>
</tr>
<tr>
<td>Lsp Name</td>
<td>The LSP name</td>
</tr>
</tbody>
</table>
### LDP Parameters Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Graceful Restart Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>Nbor Liveness Time</td>
<td>The neighbor liveness time</td>
</tr>
<tr>
<td>Max Recovery Time</td>
<td>The local maximum recovery time</td>
</tr>
<tr>
<td><strong>Interface Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>Keepalive Timeout</td>
<td>The time interval, in seconds, that LDP waits before tearing down a session. If no LDP messages are exchanged during this time interval, the LDP session is torn down. Generally the value is configured to be three times the keepalive time (the time interval between successive LDP keepalive messages).</td>
</tr>
<tr>
<td>Keepalive Factor</td>
<td>The value by which the keepalive timeout should be divided to give the keepalive time; that is, the time interval, in seconds, between LDP keepalive messages. LDP keepalive messages are sent to keep the LDP session from timing out when no other LDP traffic is being sent between the neighbors.</td>
</tr>
<tr>
<td>Hold Time</td>
<td>The time interval, in seconds, that LDP waits before declaring a neighbor to be down. Hold time (also known as Hello time) is local to the system and is sent in the hello messages to a neighbor.</td>
</tr>
<tr>
<td>Hello Factor</td>
<td>The value by which the hello timeout should be divided to give the hello time; that is, the time interval, in seconds, between LDP Hello messages. LDP uses hello messages to discover neighbors and to detect loss of connectivity with its neighbors.</td>
</tr>
</tbody>
</table>
### Table 42  LDP Parameters Output Fields (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Propagate Policy</td>
<td>Specifies whether the LSR should generate FECs and which FECs it should generate.</td>
</tr>
<tr>
<td></td>
<td>system — indicates that the LDP will distribute label bindings only for the router’s system IP address</td>
</tr>
<tr>
<td></td>
<td>interface — indicates that the LDP will distribute label bindings for all LDP interfaces</td>
</tr>
<tr>
<td></td>
<td>all — indicates that the LDP will distribute label bindings for all prefixes in the routing table</td>
</tr>
<tr>
<td></td>
<td>none — indicates that the LDP will not distribute any label bindings</td>
</tr>
<tr>
<td>Transport Address</td>
<td>interface — the interface IP address is used to set up the LDP session between neighbors. If multiple interfaces exist between two neighbors, the interface mode cannot be used since only one LDP session is actually set up between the two neighbors.</td>
</tr>
<tr>
<td></td>
<td>system — the system IP address is used to set up the LDP session between neighbors</td>
</tr>
<tr>
<td>Label-Distribution</td>
<td>The label distribution method</td>
</tr>
<tr>
<td>Label-Retention</td>
<td>liberal — all advertised label mappings are retained whether they are from a valid next hop or not. When the label distribution value is downstream unsolicited, a router may receive label bindings for the same destination for all its neighbors. Labels for the non-next-hops for the FECs are retained in the software but not used. When a network topology change occurs where a non-next-hop becomes a true next hop, the label received earlier is then used.</td>
</tr>
<tr>
<td></td>
<td>conservative — advertised label mappings are retained only if they will be used to forward packets; for example if the label came from a valid next hop. Label bindings received from non-next-hops for each FEC are discarded.</td>
</tr>
<tr>
<td>Control Mode</td>
<td>ordered — label bindings are not distributed in response to a label request until a label binding has been received from the next hop for the destination</td>
</tr>
<tr>
<td></td>
<td>independent — label bindings are distributed immediately in response to a label request even if a label binding has not yet been received from the next hop for the destination</td>
</tr>
</tbody>
</table>
peer

Syntax peer [ip-address] [detail]

Context show>router>ldp

Description This command displays configuration information about LDP peers.

Parameters ip-address — specifies the IP address of the LDP peer
detail — displays detailed information

Output The following output is an example of LDP peer information, and Table 43 describes the fields.

<table>
<thead>
<tr>
<th>Table 42 LDP Parameters Output Fields (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Label</strong></td>
</tr>
<tr>
<td>Route Preference</td>
</tr>
<tr>
<td>Targeted Session Parameters</td>
</tr>
<tr>
<td>Keepalive Timeout</td>
</tr>
<tr>
<td>Keepalive Factor</td>
</tr>
<tr>
<td>Hold Time</td>
</tr>
<tr>
<td>Hello Factor</td>
</tr>
</tbody>
</table>
| Passive Mode | True — indicates that LDP responds only when it gets a connect request from a peer and will not attempt to actively connect to its neighbors

False — indicates that LDP actively tries to connect to its peers |

Targeted Sessions

Enabled — indicates that targeted sessions are enabled

Disabled — indicates that targeted sessions are disabled |
Output Example

A:ALU-12# show router ldp peer
===============================================================================
LDP Peers
===============================================================================
Peer | Admin | Oper | Hello Factor | Hold Time | KA Factor | KA Timeout | Mode | Created
--- | --- | --- | --- | --- | --- | --- | --- | ---
10.10.10.93 | Up | Up | 3 | 45 | 4 | 40 | Disabled | Yes
10.10.10.104 | Up | Up | 3 | 45 | 4 | 40 | Disabled | Yes
---
No. of Peers: 2
===============================================================================
A:ALU-12#

A:ALU-12# show router ldp peer detail
===============================================================================
LDP Peers (Detail)
===============================================================================
Peer 1.2.3.4
---
Admin State : Up Oper State : Down
Hold Time : 45 Hello Factor : 3
Keepalive Timeout : 40 Keepalive Factor : 4
Passive Mode : Disabled Last Modified : 05/01/2008 21:44:17
Active Adjacencies : 0 Auto Created : No
Tunneling : None Lsp Name : None
---
A:ALU-12#

Table 43 LDP Peer Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer</td>
<td>The IP address of the peer</td>
</tr>
<tr>
<td>Adm</td>
<td><strong>Up</strong> — indicates that LDP is administratively enabled <strong>Down</strong> — indicates that LDP is administratively disabled</td>
</tr>
<tr>
<td>Opr</td>
<td><strong>Up</strong> — indicates that LDP is operationally enabled <strong>Down</strong> — indicates that LDP is operationally disabled</td>
</tr>
<tr>
<td>Hello Factor</td>
<td>The value by which the hello timeout should be divided to give the hello time; that is, the time interval, in seconds, between LDP Hello messages. LDP uses hello messages to discover neighbors and to detect loss of connectivity with its neighbors.</td>
</tr>
</tbody>
</table>
Table 43  LDP Peer Output Fields  (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hold Time</td>
<td>The time interval, in seconds, that LDP waits before declaring a neighbor to be down. Hold time (also known as Hello time) is local to the system and is sent in the hello messages to a neighbor.</td>
</tr>
<tr>
<td>KA Factor</td>
<td>The value by which the keepalive timeout should be divided to give the keepalive time; that is, the time interval, in seconds, between LDP keepalive messages. LDP keepalive messages are sent to keep the LDP session from timing out when no other LDP traffic is being sent between the neighbors.</td>
</tr>
<tr>
<td>KA Timeout</td>
<td>The time interval, in seconds, that LDP waits before tearing down a session. If no LDP messages are exchanged during this time interval, the LDP session is torn down. Generally the value is configured to be three times the keepalive time (the time interval between successive LDP keepalive messages).</td>
</tr>
<tr>
<td>Passive Mode</td>
<td>The mode used to set up LDP sessions. This value is only applicable to targeted sessions and not to LDP interfaces. This mode is always set to False. True — indicates that LDP responds only when it gets a connect request from a peer and will not attempt to actively connect to its neighbors. False — indicates that LDP actively tries to connect to its peers.</td>
</tr>
<tr>
<td>Auto Create</td>
<td>Specifies whether a targeted peer was automatically created through a Service Manager. For an LDP interface, this value is always false.</td>
</tr>
<tr>
<td>No. of Peers</td>
<td>The total number of LDP peers</td>
</tr>
<tr>
<td>LSP</td>
<td>The LSP name</td>
</tr>
</tbody>
</table>

peer-parameters

**Syntax**  peer-parameters peer-ip-address

**Context**  show>router>ldp

**Description**  This command displays LDP peer information.

**Parameters**  peer-ip-address — specifies the peer IP address

**Output**  The following output is an example of LDP peer-parameters information, and Table 44 describes the fields.
**Output Example**

```plaintext
A:ALU-214># show router ldp peer-parameters
===============================================================================
<table>
<thead>
<tr>
<th>Peer</th>
<th>TTL Sec</th>
<th>Min-TTL</th>
<th>Auth</th>
<th>Auth key chain</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.104</td>
<td>Disabled</td>
<td>n/a</td>
<td>Enabled</td>
<td>n/a</td>
</tr>
<tr>
<td>No. of Peers: 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
===============================================================================
A:ALU-214>#
```

**Table 44**  
**LDP Peer-Parameter Output Fields**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer</td>
<td>The IP address of the peer</td>
</tr>
<tr>
<td>TTL Sec</td>
<td>Indicates whether LDP peering session security is enabled or disabled</td>
</tr>
<tr>
<td>Min-TTL</td>
<td>The minimum TTL value for an incoming packet</td>
</tr>
<tr>
<td>Authentication</td>
<td>Indicates whether authentication using MD5 message-based digest protocol is enabled or disabled</td>
</tr>
<tr>
<td>Auth key chain</td>
<td>Indicates the authentication keychain associated with the session, if applicable</td>
</tr>
</tbody>
</table>

**session**

**Syntax**  
`session [ip-addr [:label-space]] [detail | statistics [packet-type]]`

**Context**  
`show>router>ldp`

**Description**  
This command displays configuration information about LDP sessions.

**Parameters**
- `ip-addr` — specifies the IP address of the LDP peer
- `label-space` — specifies the label space identifier that the router is advertising on the interface

**Values**
- 0 to 65535

- `detail` — displays detailed information
- `packet-type` — specifies the packet type

**Values**
- hello, keepalive, init, label, notification, address

**Output**

The following output is an example of LDP session information, and Table 45 describes the fields.
Output Example

ALU-12# show router ldp session
===============================================================================
LDP Sessions
===============================================================================
Peer LDP Id       Adj Type      State       Msg Sent   Msg Recv   Up Time
-------------------------------------------------------------------------------
10.10.10.104:0    Targeted      Established  13943      13947      0d 21:12:41
-------------------------------------------------------------------------------
No. of Sessions: 1
===============================================================================
ALU-12#
A:cpm-a# show router ldp session detail
===============================================================================
LDP Sessions (Detail)
===============================================================================
Session with Peer 1.1.1.33:0
-------------------------------------------------------------------------------
Adjacency Type : Link   State : Established
Up Time : 0d 00:03:51
Max PDU Length : 4096   KA/Hold Time Remaining: 26
Link Adjacencies : 1    Targeted Adjacencies : 0
Local Address : 1.1.1.30 Peer Address : 1.1.1.33
Local TCP Port : 646    Peer TCP Port : 50232
Local KA Timeout : 30   Peer KA Timeout : 30
Mesg Sent : 89          Mesg Recv : 126
FECs Sent : 3           FECs Recv : 3
GR State : Not Capable  Nbr Liveness Time : 0 Max Recovery Time : 0
Number of Restart : 0   Last Restart Time : Never
Advertise : Address
-------------------------------------------------------------------------------
Session with Peer 1.1.1.57:0
-------------------------------------------------------------------------------
Adjacency Type : Targeted  State : Established
Up Time : 0d 00:03:49
Max PDU Length : 4096     KA/Hold Time Remaining: 36
Link Adjacencies : 0      Targeted Adjacencies : 1
Local Address : 1.1.1.30   Peer Address : 1.1.1.57
Local TCP Port : 646      Peer TCP Port : 49574
Local KA Timeout : 40     Peer KA Timeout : 40
Mesg Sent : 55            Mesg Recv : 61
FECs Sent : 11            FECs Recv : 8
GR State : Not Capable    Nbr Liveness Time : 0 Max Recovery Time : 0
Number of Restart : 0     Last Restart Time : Never
Advertise : Address/Servi*
===============================================================================
A:cpm-a#
**status**

**Syntax**

```
status
```

**Context**

```
show>router>ldp
```

**Description**

This command displays LDP status information.

**Output**

The following output is an example of LDP status information, and Table 46 describes the fields.

**Output Example**

```
*A:csasim2>show>router>ldp# status

===============================================================================
LDP Status for LSR ID 10.10.10.32
===============================================================================
Admin State : Up Oper State : Up
Created at : 05/01/2008 16:12:07 Up Time : 3d 23:31:22
Oper Down Reason : n/a Oper Down Events : 0
Last Change : 05/02/2008 16:49:01 Tunn Down Damp Time : 3 sec
Import Policies : 
               test-policy1 None
Active Adjacencies : 0 Active Sessions : 0
Active Interfaces : 0 Inactive Interfaces : 1
Active Peers : 0 Inactive Peers : 0
Addr FECs Sent : 0 Addr FECs Recv : 0
Serv FECs Sent : 0 Serv FECs Recv : 0
```

---

**Table 45**  LDP Session Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer LDP Id</td>
<td>The IP address of the LDP peer</td>
</tr>
<tr>
<td>Adj Type</td>
<td>The adjacency type between the LDP peer and LDP session that is targeted</td>
</tr>
<tr>
<td></td>
<td>Link — specifies that this adjacency is a result of a Link Hello</td>
</tr>
<tr>
<td></td>
<td>Targeted — specifies that this adjacency is a result of a Targeted Hello</td>
</tr>
<tr>
<td>State</td>
<td>Established — the adjacency is established</td>
</tr>
<tr>
<td></td>
<td>Trying — the adjacency is not yet established</td>
</tr>
<tr>
<td>Msg Sent</td>
<td>The number of messages sent</td>
</tr>
<tr>
<td>Msg Rcvd</td>
<td>The number of messages received</td>
</tr>
<tr>
<td>Up Time</td>
<td>The amount of time the adjacency has been enabled</td>
</tr>
</tbody>
</table>
### Attempted Sessions: 0
No Hello Err: 0  Param Adv Err: 0
Max PDU Err: 0  Label Range Err: 0
Bad LDP Id Err: 0  Bad PDU Len Err: 0
Bad Msg Len Err: 0  Bad TLV Len Err: 0
Malformed TLV Err: 0  Keepalive Expired Err: 0
Shutdown Notif Sent: 0  Shutdown Notif Recv: 0

---

*A:csasim2>show>router>ldp#

---

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State</td>
<td>Up — indicates that LDP is administratively enabled</td>
</tr>
<tr>
<td></td>
<td>Down — indicates that LDP is administratively disabled</td>
</tr>
<tr>
<td>Oper State</td>
<td>Up — indicates that LDP is operationally enabled</td>
</tr>
<tr>
<td></td>
<td>Down — indicates that LDP is operationally disabled</td>
</tr>
<tr>
<td>Created at</td>
<td>The date and time that the LDP instance was created</td>
</tr>
<tr>
<td>Up Time</td>
<td>The time, in hundredths of seconds, that the LDP instance has been</td>
</tr>
<tr>
<td></td>
<td>operationally up</td>
</tr>
<tr>
<td>Oper Down Time</td>
<td>The time, in hundredths of seconds, that the LDP instance has been</td>
</tr>
<tr>
<td></td>
<td>operationally down</td>
</tr>
<tr>
<td>Oper Down Events</td>
<td>The number of times the LDP instance has gone operationally down</td>
</tr>
<tr>
<td></td>
<td>since the instance was created</td>
</tr>
<tr>
<td>Last Change</td>
<td>The date and time that the LDP instance was last modified</td>
</tr>
<tr>
<td>Import Policies</td>
<td>The import policy associated with the LDP instance</td>
</tr>
<tr>
<td>Active Adjacencies</td>
<td>The number of active adjacencies (established sessions) associated with</td>
</tr>
<tr>
<td></td>
<td>the LDP instance</td>
</tr>
<tr>
<td>Active Sessions</td>
<td>The number of active sessions (session in some form of creation)</td>
</tr>
<tr>
<td></td>
<td>associated with the LDP instance</td>
</tr>
<tr>
<td>Active Interfaces</td>
<td>The number of active (operationally up) interfaces associated with</td>
</tr>
<tr>
<td></td>
<td>the LDP instance</td>
</tr>
<tr>
<td>Inactive Interfaces</td>
<td>The number of inactive (operationally down) interfaces associated with</td>
</tr>
<tr>
<td></td>
<td>the LDP instance</td>
</tr>
<tr>
<td>Active Peers</td>
<td>The number of active LDP peers</td>
</tr>
<tr>
<td>Inactive Peers</td>
<td>The number of inactive LDP peers</td>
</tr>
<tr>
<td>Addr FECs Sent</td>
<td>The number of labels that have been sent to the peer associated with this</td>
</tr>
<tr>
<td></td>
<td>FEC</td>
</tr>
</tbody>
</table>
### Table 46  LDP Status Output Fields (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addr FECs Recv</td>
<td>The number of labels that have been received from the peer associated with this FEC</td>
</tr>
<tr>
<td>Serv FECs Sent</td>
<td>The number of labels that have been sent to the peer associated with this FEC</td>
</tr>
<tr>
<td>Serv FECs Recv</td>
<td>The number of labels that have been received from the peer associated with this FEC</td>
</tr>
<tr>
<td>Attempted Sessions</td>
<td>The total number of attempted sessions for this LDP instance</td>
</tr>
<tr>
<td>No Hello Err</td>
<td>The total number of “Session Rejected” or “No Hello Error” notification messages sent or received by this LDP instance</td>
</tr>
<tr>
<td>Param Adv Err</td>
<td>The total number of “Session Rejected” or “Parameters Advertisement Mode Error” notification messages sent or received by this LDP instance</td>
</tr>
<tr>
<td>Max PDU Err</td>
<td>The total number of “Session Rejected” or “Parameters Max PDU Length Error” notification messages sent or received by this LDP instance</td>
</tr>
<tr>
<td>Label Range Err</td>
<td>The total number of “Session Rejected” or “Parameters Label Range Error” notification messages sent or received by this LDP instance</td>
</tr>
<tr>
<td>Bad LDP Id Err</td>
<td>The number of bad LDP identifier fatal errors detected for sessions associated with this LDP instance</td>
</tr>
<tr>
<td>Bad PDU Len Err</td>
<td>The number of bad PDU length fatal errors detected for sessions associated with this LDP instance</td>
</tr>
<tr>
<td>Bad Mesg Len Err</td>
<td>The number of bad message length fatal errors detected for sessions associated with this LDP instance</td>
</tr>
<tr>
<td>Bad TLV Len Err</td>
<td>The number of bad TLV length fatal errors detected for sessions associated with this LDP instance</td>
</tr>
<tr>
<td>Malformed TLV Err</td>
<td>The number of malformed TLV value fatal errors detected for sessions associated with this LDP instance</td>
</tr>
<tr>
<td>Keepalive Expired Err</td>
<td>The number of session keepalive timer expired errors detected for sessions associated with this LDP instance</td>
</tr>
<tr>
<td>Shutdown Notif Sent</td>
<td>The number of shutdown notifications sent related to sessions associated with this LDP instance</td>
</tr>
<tr>
<td>Shutdown Notif Recv</td>
<td>The number of shutdown notifications received related to sessions associated with this LDP instance</td>
</tr>
</tbody>
</table>
5.11.2.3 Clear Commands

instance

Syntax instance
Context clear>router>ldp
Description This command resets the LDP instance.

interface

Syntax interface ip-int-name [statistics]
Context clear>router>ldp
Description This command restarts or clears statistics for LDP interfaces.
Parameters ip-int-name — specifies an existing interface. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
statistics — clears only the statistics for an interface

peer

Syntax peer ip-address [statistics]
Context clear>router>ldp
Description This command restarts or clears statistics for LDP targeted peers.
Parameters ip-address — specifies a targeted peer
statistics — clears only the statistics for a targeted peer

session

Syntax session ip-addr [:label-space] [statistics]
Context clear>router>ldp
Description This command restarts or clears statistics for LDP sessions.
Parameters

- **ip-addr** — specifies the IP address of the LDP peer
- **label-space** — specifies the label space identifier that the router is advertising on the interface

**Values**

- **0 to 65535**

- **statistics** — clears only the statistics for a session

---

**statistics**

**Syntax**

`statistics`

**Context**

`clear>router>ldp`

**Description**

This command clears LDP instance statistics.
5.11.2.4 Debug Commands

The following output shows debug LDP configurations discussed in this section.

```
ALU-12# debug router ldp peer 10.10.10.104
ALU-12>debug>router>ldp# show debug ldp
debug
    router "Base"
    ldp peer 10.10.10.104
    event
        bindings
        messages
        exit
        packet
        hello
        init
        keepalive
        label
        exit
        exit
    exit
exit
ALU-12>debug>router>ldp#
```

**ldp**

**Syntax**  
[no] ldp

**Context**  
debug>router

**Description**  
This command configures LDP debugging.

**interface**

**Syntax**  
[no] interface interface-name

**Context**  
debug>router>ldp

**Description**  
This command configures debugging for a specific LDP interface.

**Parameters**  
interface-name — specifies an existing interface
peer

Syntax  
[no] peer ip-address

Context  
debug>router>ldp

Description  
This command configures debugging for a specific LDP peer.

Parameters  
ip-address — specifies the LDP peer to debug

event

Syntax  
[no] event

Context  
debug>router>ldp>interface
debug>router>ldp>peer

Description  
This command configures debugging for specific LDP events.

bindings

Syntax  
[no] bindings

Context  
debug>router>ldp>peer>event

Description  
This command displays debugging information about addresses and label bindings learned from LDP peers for LDP bindings.

The no form of the command disables the debugging output.

messages

Syntax  
[no] messages

Context  
debug>router>ldp>if>event
debug>router>ldp>peer>event

Description  
This command displays specific information (for example, message type, source, and destination) regarding LDP messages sent to and received from LDP peers.

The no form of the command disables debugging output for LDP messages.
packet

**Syntax**  
[no] packet

**Context**  
debug>router>ldp>interface  
debug>router>ldp>peer

**Description**  
This command enables debugging for specific LDP packets.  
The no form of the command disables the debugging output.

---

hello

**Syntax**  
hello [detail]

no hello

**Context**  
debug>router>ldp>if>packet  
debug>router>ldp>peer>packet

**Description**  
This command enables debugging for sent and received LDP Hello packets.  
The no form of the command disables the debugging output.

**Parameters**  
detail — displays detailed information

---

init

**Syntax**  
init [detail]

no init

**Context**  
debug>router>ldp>peer>packet

**Description**  
This command enables debugging for LDP Init packets. The detail option displays detailed information on the type length value (TLV) included in mac-flush packets.  
The no form of the command disables the debugging output.

**Parameters**  
detail — displays detailed information
### keepalive

**Syntax**

```plaintext
[no] keepalive
```

**Context**

`debug>router>ldp>peer>packet`

**Description**

This command enables debugging for LDP keepalive packets.

The `no` form of the command disables the debugging output.

### label

**Syntax**

```plaintext
label [detail]

no label
```

**Context**

`debug>router>ldp neighbor>packet`

**Description**

This command enables debugging for LDP label packets.

The `no` form of the command disables the debugging output.

**Parameters**

`detail` — displays detailed information
## 6 List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>2G</td>
<td>second generation wireless telephone technology</td>
</tr>
<tr>
<td>3DES</td>
<td>triple DES (data encryption standard)</td>
</tr>
<tr>
<td>3G</td>
<td>third generation mobile telephone technology</td>
</tr>
<tr>
<td>6VPE</td>
<td>IPv6 on Virtual Private Edge Router</td>
</tr>
<tr>
<td>7705 SAR</td>
<td>7705 Service Aggregation Router</td>
</tr>
<tr>
<td>7750 SR</td>
<td>7750 Service Router</td>
</tr>
<tr>
<td>9500 MPR</td>
<td>9500 microwave packet radio</td>
</tr>
<tr>
<td>ABR</td>
<td>area border router</td>
</tr>
<tr>
<td></td>
<td>available bit rate</td>
</tr>
<tr>
<td>AC</td>
<td>alternating current attachment circuit</td>
</tr>
<tr>
<td>ACK</td>
<td>acknowledge</td>
</tr>
<tr>
<td>ACL</td>
<td>access control list</td>
</tr>
<tr>
<td>ACR</td>
<td>adaptive clock recovery</td>
</tr>
<tr>
<td>AD</td>
<td>auto-discovery</td>
</tr>
<tr>
<td>ADM</td>
<td>add/drop multiplexer</td>
</tr>
<tr>
<td>ADP</td>
<td>automatic discovery protocol</td>
</tr>
<tr>
<td>AES</td>
<td>advanced encryption standard</td>
</tr>
<tr>
<td>AFI</td>
<td>authority and format identifier</td>
</tr>
<tr>
<td>AIS</td>
<td>alarm indication signal</td>
</tr>
<tr>
<td>ALG</td>
<td>application level gateway</td>
</tr>
<tr>
<td>ANSI</td>
<td>American National Standards Institute</td>
</tr>
<tr>
<td>Apipe</td>
<td>ATM VLL</td>
</tr>
<tr>
<td>APS</td>
<td>automatic protection switching</td>
</tr>
<tr>
<td>ARP</td>
<td>address resolution protocol</td>
</tr>
<tr>
<td>A/S</td>
<td>active/standby</td>
</tr>
</tbody>
</table>
### Table 47  Acronyms (Continued)

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS</td>
<td>autonomous system</td>
</tr>
<tr>
<td>ASAP</td>
<td>any service, any port</td>
</tr>
<tr>
<td>ASBR</td>
<td>autonomous system boundary router</td>
</tr>
<tr>
<td>ASM</td>
<td>any-source multicast autonomous system message</td>
</tr>
<tr>
<td>ASN</td>
<td>autonomous system number</td>
</tr>
<tr>
<td>ATM</td>
<td>asynchronous transfer mode</td>
</tr>
<tr>
<td>ATM PVC</td>
<td>ATM permanent virtual circuit</td>
</tr>
<tr>
<td>B3ZS</td>
<td>bipolar with three-zero substitution</td>
</tr>
<tr>
<td>Batt A</td>
<td>battery A</td>
</tr>
<tr>
<td>B-bit</td>
<td>beginning bit (first packet of a fragment)</td>
</tr>
<tr>
<td>Bc</td>
<td>committed burst size</td>
</tr>
<tr>
<td>Be</td>
<td>excess burst size</td>
</tr>
<tr>
<td>BECN</td>
<td>backward explicit congestion notification</td>
</tr>
<tr>
<td>Bellcore</td>
<td>Bell Communications Research</td>
</tr>
<tr>
<td>BFD</td>
<td>bidirectional forwarding detection</td>
</tr>
<tr>
<td>BGP</td>
<td>border gateway protocol</td>
</tr>
<tr>
<td>BITS</td>
<td>building integrated timing supply</td>
</tr>
<tr>
<td>BMCA</td>
<td>best master clock algorithm</td>
</tr>
</tbody>
</table>
| BMU     | broadcast, multicast, and unknown traffic  
|         | Traffic that is not unicast. Any nature of multipoint traffic:  
|         | • broadcast (that is, all 1s as the destination IP to represent all destinations within the subnet)  
|         | • multicast (that is, traffic typically identified by the destination address, uses special destination address); for IP, the destination must be 224.0.0.0 to 239.255.255.255  
|         | • unknown (that is, the destination is typically a valid unicast address but the destination port/interface is not yet known; therefore, traffic needs to be forwarded to all destinations; unknown traffic is treated as broadcast) |
| BNM     | bandwidth notification message |
### Table 47: Acronyms (Continued)

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOF</td>
<td>boot options file</td>
</tr>
<tr>
<td>BoS</td>
<td>bottom of stack</td>
</tr>
<tr>
<td>BPDU</td>
<td>bridge protocol data unit</td>
</tr>
<tr>
<td>BRAS</td>
<td>Broadband Remote Access Server</td>
</tr>
<tr>
<td>BSC</td>
<td>Base Station Controller</td>
</tr>
<tr>
<td>BSM</td>
<td>bootstrap message</td>
</tr>
<tr>
<td>BSR</td>
<td>bootstrap router</td>
</tr>
<tr>
<td>BSTA</td>
<td>Broadband Service Termination Architecture</td>
</tr>
<tr>
<td>BTS</td>
<td>base transceiver station</td>
</tr>
<tr>
<td>CA</td>
<td>certificate authority</td>
</tr>
<tr>
<td>CAS</td>
<td>channel associated signaling</td>
</tr>
<tr>
<td>CBN</td>
<td>common bonding networks</td>
</tr>
<tr>
<td>CBS</td>
<td>committed buffer space</td>
</tr>
<tr>
<td>CC</td>
<td>continuity check</td>
</tr>
<tr>
<td></td>
<td>control channel</td>
</tr>
<tr>
<td>CCM</td>
<td>continuity check message</td>
</tr>
<tr>
<td>CCTV</td>
<td>closed-circuit television</td>
</tr>
<tr>
<td>CE</td>
<td>circuit emulation</td>
</tr>
<tr>
<td></td>
<td>customer edge</td>
</tr>
<tr>
<td>CEM</td>
<td>circuit emulation</td>
</tr>
<tr>
<td>CES</td>
<td>circuit emulation services</td>
</tr>
<tr>
<td>CESoPSN</td>
<td>circuit emulation services over packet switched network</td>
</tr>
<tr>
<td>CFM</td>
<td>connectivity fault management</td>
</tr>
<tr>
<td>cHDLC</td>
<td>Cisco high-level data link control protocol</td>
</tr>
<tr>
<td>CIDR</td>
<td>classless inter-domain routing</td>
</tr>
<tr>
<td>CIR</td>
<td>committed information rate</td>
</tr>
<tr>
<td>CLI</td>
<td>command line interface</td>
</tr>
<tr>
<td>CLP</td>
<td>cell loss priority</td>
</tr>
</tbody>
</table>
### Table 47  Acronyms (Continued)

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMP</td>
<td>certificate management protocol</td>
</tr>
<tr>
<td>C-multicast</td>
<td>customer multicast</td>
</tr>
<tr>
<td>CoS</td>
<td>class of service</td>
</tr>
<tr>
<td>CPE</td>
<td>customer premises equipment</td>
</tr>
<tr>
<td>Cpipe</td>
<td>circuit emulation (or TDM) VLL</td>
</tr>
<tr>
<td>CPM</td>
<td>Control and Processing Module (CPM is used instead of CSM when referring to CSM filtering to align with CLI syntax used with other SR products). CSM management ports are referred to as CPM management ports in the CLI.</td>
</tr>
<tr>
<td>CPROTO</td>
<td>C prototype</td>
</tr>
<tr>
<td>CPU</td>
<td>central processing unit</td>
</tr>
<tr>
<td>C/R</td>
<td>command/response</td>
</tr>
<tr>
<td>CRC</td>
<td>cyclic redundancy check</td>
</tr>
<tr>
<td>CRC-32</td>
<td>32-bit cyclic redundancy check</td>
</tr>
<tr>
<td>CRL</td>
<td>certificate revocation list</td>
</tr>
<tr>
<td>CRON</td>
<td>a time-based scheduling service (from chronos = time)</td>
</tr>
<tr>
<td>CRP</td>
<td>candidate RP</td>
</tr>
<tr>
<td>CSM</td>
<td>Control and Switching Module</td>
</tr>
<tr>
<td>CSNP</td>
<td>complete sequence number PDU</td>
</tr>
<tr>
<td>CSPF</td>
<td>constrained shortest path first</td>
</tr>
<tr>
<td>C-TAG</td>
<td>customer VLAN tag</td>
</tr>
<tr>
<td>CV</td>
<td>connection verification</td>
</tr>
<tr>
<td>CV</td>
<td>customer VLAN (tag)</td>
</tr>
<tr>
<td>CW</td>
<td>control word</td>
</tr>
<tr>
<td>CWDM</td>
<td>coarse wavelength-division multiplexing</td>
</tr>
<tr>
<td>DA/FAN</td>
<td>distribution automation and field area network</td>
</tr>
<tr>
<td>DC</td>
<td>direct current</td>
</tr>
<tr>
<td>DC-C</td>
<td>DC return - common</td>
</tr>
<tr>
<td>DCE</td>
<td>data communications equipment</td>
</tr>
</tbody>
</table>
### Table 47  Acronyms (Continued)

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC-I</td>
<td>DC return - isolated</td>
</tr>
<tr>
<td>DCO</td>
<td>digitally controlled oscillator</td>
</tr>
<tr>
<td>DCR</td>
<td>differential clock recovery</td>
</tr>
<tr>
<td>DDoS</td>
<td>distributed DoS</td>
</tr>
<tr>
<td>DE</td>
<td>discard eligibility</td>
</tr>
<tr>
<td>DER</td>
<td>distinguished encoding rules</td>
</tr>
<tr>
<td>DES</td>
<td>data encryption standard</td>
</tr>
<tr>
<td>DF</td>
<td>do not fragment</td>
</tr>
<tr>
<td>DH</td>
<td>Diffie-Hellman</td>
</tr>
<tr>
<td>DHB</td>
<td>decimal, hexadecimal, or binary</td>
</tr>
<tr>
<td>DHCP</td>
<td>dynamic host configuration protocol</td>
</tr>
<tr>
<td>DHCPv6</td>
<td>dynamic host configuration protocol for IPv6</td>
</tr>
<tr>
<td>DIS</td>
<td>designated intermediate system</td>
</tr>
<tr>
<td>DLCI</td>
<td>data link connection identifier</td>
</tr>
<tr>
<td>DLCMI</td>
<td>data link connection management interface</td>
</tr>
<tr>
<td>DM</td>
<td>delay measurement</td>
</tr>
<tr>
<td>DNS</td>
<td>domain name server</td>
</tr>
<tr>
<td>DNU</td>
<td>do not use</td>
</tr>
<tr>
<td>DoS</td>
<td>denial of service</td>
</tr>
<tr>
<td>dot1p</td>
<td>IEEE 802.1p bits, in Ethernet or VLAN ingress packet headers, used to map traffic to up to eight forwarding classes</td>
</tr>
<tr>
<td>dot1q</td>
<td>IEEE 802.1q encapsulation for Ethernet interfaces</td>
</tr>
<tr>
<td>DPD</td>
<td>dead peer detection</td>
</tr>
<tr>
<td>DPI</td>
<td>deep packet inspection</td>
</tr>
<tr>
<td>DPLL</td>
<td>digital phase locked loop</td>
</tr>
<tr>
<td>DR</td>
<td>designated router</td>
</tr>
<tr>
<td>DSA</td>
<td>digital signal algorithm</td>
</tr>
<tr>
<td>DSCP</td>
<td>differentiated services code point</td>
</tr>
<tr>
<td>Acronym</td>
<td>Expansion</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>DSL</td>
<td>digital subscriber line</td>
</tr>
<tr>
<td>DSLAM</td>
<td>digital subscriber line access multiplexer</td>
</tr>
<tr>
<td>DTE</td>
<td>data termination equipment</td>
</tr>
<tr>
<td>DU</td>
<td>downstream unsolicited</td>
</tr>
<tr>
<td>DUID</td>
<td>DHCP unique identifier</td>
</tr>
<tr>
<td>DUS</td>
<td>do not use for synchronization</td>
</tr>
<tr>
<td>DV</td>
<td>delay variation</td>
</tr>
<tr>
<td>DVMRP</td>
<td>distance vector multicast routing protocol</td>
</tr>
<tr>
<td>e911</td>
<td>enhanced 911 service</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>EAPOL</td>
<td>EAP over LAN</td>
</tr>
<tr>
<td>E-bit</td>
<td>ending bit (last packet of a fragment)</td>
</tr>
<tr>
<td>E-BSR</td>
<td>elected BSR</td>
</tr>
<tr>
<td>ECMP</td>
<td>equal cost multipath</td>
</tr>
<tr>
<td>EE</td>
<td>end entity</td>
</tr>
<tr>
<td>EFM</td>
<td>Ethernet in the first mile</td>
</tr>
<tr>
<td>EGP</td>
<td>exterior gateway protocol</td>
</tr>
<tr>
<td>EIA/TIA-232</td>
<td>Electronic Industries Alliance/Telecommunications Industry Association Standard 232 (also known as RS-232)</td>
</tr>
<tr>
<td>EIR</td>
<td>excess information rate</td>
</tr>
<tr>
<td>EJBCA</td>
<td>Enterprise Java Bean Certificate Authority</td>
</tr>
<tr>
<td>EL</td>
<td>entropy label</td>
</tr>
<tr>
<td>eLER</td>
<td>egress label edge router</td>
</tr>
<tr>
<td>ELI</td>
<td>entropy label indicator</td>
</tr>
<tr>
<td>E&amp;M</td>
<td>ear and mouth</td>
</tr>
<tr>
<td></td>
<td>earth and magneto</td>
</tr>
<tr>
<td></td>
<td>exchange and multiplexer</td>
</tr>
<tr>
<td>eMBMS</td>
<td>evolved MBMS</td>
</tr>
</tbody>
</table>
### Table 47  Acronyms (Continued)

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>EOP</td>
<td>end of packet</td>
</tr>
<tr>
<td>EPC</td>
<td>evolved packet core</td>
</tr>
<tr>
<td>EPD</td>
<td>early packet discard</td>
</tr>
<tr>
<td>Epipe</td>
<td>Ethernet VLL</td>
</tr>
<tr>
<td>EPL</td>
<td>Ethernet private line</td>
</tr>
<tr>
<td>EPON</td>
<td>Ethernet Passive Optical Network</td>
</tr>
<tr>
<td>EPS</td>
<td>equipment protection switching</td>
</tr>
<tr>
<td>ERO</td>
<td>explicit route object</td>
</tr>
<tr>
<td>ESD</td>
<td>electrostatic discharge</td>
</tr>
<tr>
<td>ESMC</td>
<td>Ethernet synchronization message channel</td>
</tr>
<tr>
<td>ESN</td>
<td>extended sequence number</td>
</tr>
<tr>
<td>ESP</td>
<td>encapsulating security payload</td>
</tr>
<tr>
<td>ETE</td>
<td>end-to-end</td>
</tr>
<tr>
<td>ETH-BN</td>
<td>Ethernet bandwidth notification</td>
</tr>
<tr>
<td>ETH-CFM</td>
<td>Ethernet connectivity fault management (IEEE 802.1ag)</td>
</tr>
<tr>
<td>EVC</td>
<td>Ethernet virtual connection</td>
</tr>
<tr>
<td>EVDO</td>
<td>evolution - data optimized</td>
</tr>
<tr>
<td>EVPL</td>
<td>Ethernet virtual private link</td>
</tr>
<tr>
<td>EXP bits</td>
<td>experimental bits (currently known as TC)</td>
</tr>
<tr>
<td>FC</td>
<td>forwarding class</td>
</tr>
<tr>
<td>FCS</td>
<td>frame check sequence</td>
</tr>
<tr>
<td>FD</td>
<td>frequency diversity</td>
</tr>
<tr>
<td>FDB</td>
<td>forwarding database</td>
</tr>
<tr>
<td>FDL</td>
<td>facilities data link</td>
</tr>
<tr>
<td>FEAC</td>
<td>far-end alarm and control</td>
</tr>
<tr>
<td>FEC</td>
<td>forwarding equivalence class</td>
</tr>
<tr>
<td>FECN</td>
<td>forward explicit congestion notification</td>
</tr>
<tr>
<td>Acronym</td>
<td>Expansion</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>FeGW</td>
<td>far-end gateway</td>
</tr>
<tr>
<td>FEP</td>
<td>front-end processor</td>
</tr>
<tr>
<td>FF</td>
<td>fixed filter</td>
</tr>
<tr>
<td>FFD</td>
<td>fast fault detection</td>
</tr>
<tr>
<td>FIB</td>
<td>forwarding information base</td>
</tr>
<tr>
<td>FIFO</td>
<td>first in, first out</td>
</tr>
<tr>
<td>FIPS-140-2</td>
<td>Federal Information Processing Standard publication 140-2</td>
</tr>
<tr>
<td>FNG</td>
<td>fault notification generator</td>
</tr>
<tr>
<td>FOM</td>
<td>figure of merit</td>
</tr>
<tr>
<td>Fpipe</td>
<td>frame relay VLL</td>
</tr>
<tr>
<td>FQDN</td>
<td>fully qualified domain name</td>
</tr>
<tr>
<td>FR</td>
<td>frame relay</td>
</tr>
<tr>
<td>FRG</td>
<td>fragmentation bit</td>
</tr>
<tr>
<td>FRR</td>
<td>fast reroute</td>
</tr>
<tr>
<td>FTN</td>
<td>FEC-to-NHLFE</td>
</tr>
<tr>
<td>FTP</td>
<td>file transfer protocol</td>
</tr>
<tr>
<td>FXO</td>
<td>foreign exchange office</td>
</tr>
<tr>
<td>FXS</td>
<td>foreign exchange subscriber</td>
</tr>
<tr>
<td>GFP</td>
<td>generic framing procedure</td>
</tr>
<tr>
<td>GigE</td>
<td>Gigabit Ethernet</td>
</tr>
<tr>
<td>GLONASS</td>
<td>Global Navigation Satellite System (Russia)</td>
</tr>
<tr>
<td>GNSS</td>
<td>global navigation satellite system (generic)</td>
</tr>
<tr>
<td>GPON</td>
<td>Gigabit Passive Optical Network</td>
</tr>
<tr>
<td>GPRS</td>
<td>general packet radio service</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GRE</td>
<td>generic routing encapsulation</td>
</tr>
<tr>
<td>GRT</td>
<td>global routing table</td>
</tr>
<tr>
<td>Acronym</td>
<td>Expansion</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile Communications (2G)</td>
</tr>
<tr>
<td>GTP-U</td>
<td>GPRS tunneling protocol user plane</td>
</tr>
<tr>
<td>HA</td>
<td>high availability</td>
</tr>
<tr>
<td>HCM</td>
<td>high capacity multiplexing</td>
</tr>
<tr>
<td>HDB3</td>
<td>high density bipolar of order 3</td>
</tr>
<tr>
<td>HDLC</td>
<td>high-level data link control protocol</td>
</tr>
<tr>
<td>HEC</td>
<td>header error control</td>
</tr>
<tr>
<td>HMAC</td>
<td>hash message authentication code</td>
</tr>
<tr>
<td>Hpipe</td>
<td>HDLC VLL</td>
</tr>
<tr>
<td>H-QoS</td>
<td>hierarchical quality of service</td>
</tr>
<tr>
<td>HSB</td>
<td>hot standby</td>
</tr>
<tr>
<td>HSDPA</td>
<td>high-speed downlink packet access</td>
</tr>
<tr>
<td>HSPA</td>
<td>high-speed packet access</td>
</tr>
<tr>
<td>HVPLS</td>
<td>hierarchical virtual private line service</td>
</tr>
<tr>
<td>IANA</td>
<td>internet assigned numbers authority</td>
</tr>
<tr>
<td>IBN</td>
<td>isolated bonding networks</td>
</tr>
<tr>
<td>ICB</td>
<td>inter-chassis backup</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet control message protocol</td>
</tr>
<tr>
<td>ICMPv6</td>
<td>Internet control message protocol for IPv6</td>
</tr>
<tr>
<td>ICP</td>
<td>IMA control protocol cells</td>
</tr>
<tr>
<td>IDS</td>
<td>intrusion detection system</td>
</tr>
<tr>
<td>IDU</td>
<td>indoor unit</td>
</tr>
<tr>
<td>IED</td>
<td>intelligent end device</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IEEE 1588v2</td>
<td>Institute of Electrical and Electronics Engineers standard 1588-2008</td>
</tr>
<tr>
<td>IES</td>
<td>Internet Enhanced Service</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>Acronym</td>
<td>Expansion</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>IGMP</td>
<td>Internet group management protocol</td>
</tr>
<tr>
<td>IGP</td>
<td>interior gateway protocol</td>
</tr>
<tr>
<td>IID</td>
<td>instance ID</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet key exchange</td>
</tr>
<tr>
<td>iLER</td>
<td>ingress label edge router</td>
</tr>
<tr>
<td>ILM</td>
<td>incoming label map</td>
</tr>
<tr>
<td>IMA</td>
<td>inverse multiplexing over ATM</td>
</tr>
<tr>
<td>INVARP</td>
<td>inverse address resolution protocol</td>
</tr>
<tr>
<td>IOM</td>
<td>input/output module</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPCP</td>
<td>Internet Protocol Control Protocol</td>
</tr>
<tr>
<td>IPiP</td>
<td>IP in IP</td>
</tr>
<tr>
<td>Ipipe</td>
<td>IP interworking VLL</td>
</tr>
<tr>
<td>I-PMSI</td>
<td>inclusive PMSI</td>
</tr>
<tr>
<td>IPoATM</td>
<td>IP over ATM</td>
</tr>
<tr>
<td>IPS</td>
<td>intrusion prevention system</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol security</td>
</tr>
<tr>
<td>ISA</td>
<td>integrated services adapter</td>
</tr>
<tr>
<td>ISAKMP</td>
<td>Internet security association and key management protocol</td>
</tr>
<tr>
<td>IS-IS</td>
<td>Intermediate System-to-Intermediate System</td>
</tr>
<tr>
<td>IS-IS-TE</td>
<td>IS-IS-traffic engineering (extensions)</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>IW</td>
<td>interworking</td>
</tr>
<tr>
<td>JP</td>
<td>join prune</td>
</tr>
<tr>
<td>KG</td>
<td>key group</td>
</tr>
<tr>
<td>LB</td>
<td>loopback</td>
</tr>
<tr>
<td>lbf-in</td>
<td>pound force inch</td>
</tr>
<tr>
<td>Acronym</td>
<td>Expansion</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>LBM</td>
<td>loopback message</td>
</tr>
<tr>
<td>LBO</td>
<td>line buildout</td>
</tr>
<tr>
<td>LBR</td>
<td>loopback reply</td>
</tr>
<tr>
<td>LCP</td>
<td>link control protocol</td>
</tr>
<tr>
<td>LDP</td>
<td>label distribution protocol</td>
</tr>
<tr>
<td>LER</td>
<td>label edge router</td>
</tr>
<tr>
<td>LFA</td>
<td>loop-free alternate</td>
</tr>
<tr>
<td>LFIB</td>
<td>label forwarding information base</td>
</tr>
<tr>
<td>LIB</td>
<td>label information base</td>
</tr>
<tr>
<td>LLDP</td>
<td>link layer discovery protocol</td>
</tr>
<tr>
<td>LLDPDU</td>
<td>link layer discovery protocol data unit</td>
</tr>
<tr>
<td>LLF</td>
<td>link loss forwarding</td>
</tr>
<tr>
<td>LLID</td>
<td>loopback location ID</td>
</tr>
<tr>
<td>LM</td>
<td>loss measurement</td>
</tr>
<tr>
<td>LMI</td>
<td>local management interface</td>
</tr>
<tr>
<td>LOS</td>
<td>line-of-sight loss of signal</td>
</tr>
<tr>
<td>LSA</td>
<td>link-state advertisement</td>
</tr>
<tr>
<td>LSDB</td>
<td>link-state database</td>
</tr>
<tr>
<td>LSP</td>
<td>label switched path link-state PDU (for IS-IS)</td>
</tr>
<tr>
<td>LSPA</td>
<td>LSP attributes</td>
</tr>
<tr>
<td>LSR</td>
<td>label switch router link-state request</td>
</tr>
<tr>
<td>LSU</td>
<td>link-state update</td>
</tr>
<tr>
<td>LT</td>
<td>linktrace</td>
</tr>
<tr>
<td>LTE</td>
<td>long term evolution line termination equipment</td>
</tr>
<tr>
<td>LTM</td>
<td>linktrace message</td>
</tr>
<tr>
<td>Acronym</td>
<td>Expansion</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>LTN</td>
<td>LSP ID to NHLFE</td>
</tr>
<tr>
<td>LTR</td>
<td>link trace reply</td>
</tr>
<tr>
<td>MA</td>
<td>maintenance association</td>
</tr>
<tr>
<td>MAC</td>
<td>media access control</td>
</tr>
<tr>
<td>MA-ID</td>
<td>maintenance association identifier</td>
</tr>
<tr>
<td>MBB</td>
<td>make-before-break</td>
</tr>
<tr>
<td>MBGP</td>
<td>multicast BGP</td>
</tr>
<tr>
<td></td>
<td>multiprotocol BGP</td>
</tr>
<tr>
<td></td>
<td>multiprotocol extensions for BGP</td>
</tr>
<tr>
<td>MBMS</td>
<td>multimedia broadcast multicast service</td>
</tr>
<tr>
<td>MBS</td>
<td>maximum buffer space</td>
</tr>
<tr>
<td></td>
<td>maximum burst size</td>
</tr>
<tr>
<td></td>
<td>media buffer space</td>
</tr>
<tr>
<td>MBSP</td>
<td>mobile backhaul service provider</td>
</tr>
<tr>
<td>MCAC</td>
<td>multicast connection admission control</td>
</tr>
<tr>
<td>MC-APS</td>
<td>multi-chassis automatic protection switching</td>
</tr>
<tr>
<td>MC-MLPPP</td>
<td>multi-class multilink point-to-point protocol</td>
</tr>
<tr>
<td>MCS</td>
<td>multicast server</td>
</tr>
<tr>
<td></td>
<td>multi-chassis synchronization</td>
</tr>
<tr>
<td>MCT</td>
<td>MPT craft terminal</td>
</tr>
<tr>
<td>MD</td>
<td>maintenance domain</td>
</tr>
<tr>
<td>MD5</td>
<td>message digest version 5 (algorithm)</td>
</tr>
<tr>
<td>MDA</td>
<td>media dependent adapter</td>
</tr>
<tr>
<td>MDDDB</td>
<td>multidrop data bridge</td>
</tr>
<tr>
<td>MDL</td>
<td>maintenance data link</td>
</tr>
<tr>
<td>MDT</td>
<td>multicast distribution tree</td>
</tr>
<tr>
<td>ME</td>
<td>maintenance entity</td>
</tr>
<tr>
<td>MED</td>
<td>multi-exit discriminator</td>
</tr>
<tr>
<td>MEF</td>
<td>Metro Ethernet Forum</td>
</tr>
<tr>
<td>Acronym</td>
<td>Expansion</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>MEG</td>
<td>maintenance entity group</td>
</tr>
<tr>
<td>MEG-ID</td>
<td>maintenance entity group identifier</td>
</tr>
<tr>
<td>MEN</td>
<td>Metro Ethernet network</td>
</tr>
<tr>
<td>MEP</td>
<td>maintenance association end point</td>
</tr>
<tr>
<td>MFC</td>
<td>multi-field classification</td>
</tr>
<tr>
<td>MHF</td>
<td>MIP half function</td>
</tr>
<tr>
<td>MIB</td>
<td>management information base</td>
</tr>
<tr>
<td>MI-IS-IS</td>
<td>multi-instance IS-IS</td>
</tr>
<tr>
<td>MIR</td>
<td>minimum information rate</td>
</tr>
<tr>
<td>MLD</td>
<td>multicast listener discovery</td>
</tr>
<tr>
<td>mLDP</td>
<td>multicast LDP</td>
</tr>
<tr>
<td>MLPPP</td>
<td>multilink point-to-point protocol</td>
</tr>
<tr>
<td>mLSP</td>
<td>multicast LSP</td>
</tr>
<tr>
<td>MoFRR</td>
<td>multicast-only fast reroute</td>
</tr>
<tr>
<td>MP</td>
<td>merge point</td>
</tr>
<tr>
<td>MP-BGP</td>
<td>multilink protocol</td>
</tr>
<tr>
<td>MPLS</td>
<td>multipoint</td>
</tr>
<tr>
<td>MPLSCP</td>
<td>multipoint</td>
</tr>
<tr>
<td>MPP</td>
<td>MPT protection protocol</td>
</tr>
<tr>
<td>MPR</td>
<td>see 9500 MPR</td>
</tr>
<tr>
<td>MPR-e</td>
<td>microwave packet radio-standalone mode</td>
</tr>
<tr>
<td>MPT</td>
<td>microwave packet transport</td>
</tr>
<tr>
<td>MPT-HC V2/9558HC</td>
<td>microwave packet transport, high capacity version 2</td>
</tr>
<tr>
<td>MPT-HLC</td>
<td>microwave packet transport, high-capacity long-haul cubic (ANSI)</td>
</tr>
<tr>
<td>MPT-HQAM</td>
<td>microwave packet transport, high capacity (MPT-HC-QAM) or extended power (MPT-XP-QAM) with 512/1024 QAM</td>
</tr>
<tr>
<td>Acronym</td>
<td>Expansion</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>MPT-MC</td>
<td>microwave packet transport, medium capacity</td>
</tr>
<tr>
<td>MPT-XP</td>
<td>microwave packet transport, high capacity (very high power version of MPT-HC V2/9558HC)</td>
</tr>
<tr>
<td>MRAI</td>
<td>minimum route advertisement interval</td>
</tr>
<tr>
<td>MRRU</td>
<td>maximum received reconstructed unit</td>
</tr>
<tr>
<td>MRU</td>
<td>maximum receive unit</td>
</tr>
<tr>
<td>MSDP</td>
<td>Multicast Source Discovery Protocol</td>
</tr>
<tr>
<td>MSDU</td>
<td>MAC Service Data Unit</td>
</tr>
<tr>
<td>MSO</td>
<td>multi-system operator</td>
</tr>
<tr>
<td>MS-PW</td>
<td>multi-segment pseudowire</td>
</tr>
<tr>
<td>MSS</td>
<td>maximum segment size</td>
</tr>
<tr>
<td>MTIE</td>
<td>maximum time interval error</td>
</tr>
<tr>
<td>MTSO</td>
<td>mobile trunk switching office</td>
</tr>
<tr>
<td>MTU</td>
<td>maximum transmission unit</td>
</tr>
<tr>
<td>M-VPLS</td>
<td>management virtual private line service</td>
</tr>
<tr>
<td>MVPN</td>
<td>multicast VPN</td>
</tr>
<tr>
<td>MVR</td>
<td>multicast VPLS registration</td>
</tr>
<tr>
<td>MW</td>
<td>microwave</td>
</tr>
<tr>
<td>MWA</td>
<td>microwave awareness</td>
</tr>
<tr>
<td>N·m</td>
<td>newton meter</td>
</tr>
<tr>
<td>NAT</td>
<td>network address translation</td>
</tr>
<tr>
<td>NAT-T</td>
<td>network address translation traversal</td>
</tr>
<tr>
<td>NBMA</td>
<td>non-broadcast multiple access (network)</td>
</tr>
<tr>
<td>ND</td>
<td>neighbor discovery</td>
</tr>
<tr>
<td>NE</td>
<td>network element</td>
</tr>
<tr>
<td>NET</td>
<td>network entity title</td>
</tr>
<tr>
<td>NFM-P</td>
<td>Network Functions Manager - Packet (formerly 5620 SAM)</td>
</tr>
<tr>
<td>Acronym</td>
<td>Expansion</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NGE</td>
<td>network group encryption</td>
</tr>
<tr>
<td>NG-MVPN</td>
<td>next generation MVPN</td>
</tr>
<tr>
<td>NH</td>
<td>next hop</td>
</tr>
<tr>
<td>NHLFE</td>
<td>next hop label forwarding entry</td>
</tr>
<tr>
<td>NHOP</td>
<td>next-hop</td>
</tr>
<tr>
<td>NLOS</td>
<td>non-line-of-sight</td>
</tr>
<tr>
<td>NLPID</td>
<td>network level protocol identifier</td>
</tr>
<tr>
<td>NLRI</td>
<td>network layer reachability information</td>
</tr>
<tr>
<td>NNHOP</td>
<td>next next-hop</td>
</tr>
<tr>
<td>NNI</td>
<td>network-to-network interface</td>
</tr>
<tr>
<td>Node B</td>
<td>similar to BTS but used in 3G networks — term is used in UMTS (3G systems) while BTS is used in GSM (2G systems)</td>
</tr>
<tr>
<td>NRC-F</td>
<td>Network Resource Controller - Flow</td>
</tr>
<tr>
<td>NRC-P</td>
<td>Network Resource Controller - Packet</td>
</tr>
<tr>
<td>NRC-T</td>
<td>Network Resource Controller - Transport</td>
</tr>
<tr>
<td>NRC-X</td>
<td>Network Resource Controller - Cross Domain</td>
</tr>
<tr>
<td>NSAP</td>
<td>network service access point</td>
</tr>
<tr>
<td>NSD</td>
<td>Network Services Director</td>
</tr>
<tr>
<td>NSP</td>
<td>native service processing</td>
</tr>
<tr>
<td></td>
<td>Network Services Platform</td>
</tr>
<tr>
<td>NSSA</td>
<td>not-so-stubby area</td>
</tr>
<tr>
<td>NTP</td>
<td>network time protocol</td>
</tr>
<tr>
<td>NTR</td>
<td>network timing reference</td>
</tr>
<tr>
<td>OADM</td>
<td>optical add/drop multiplexer</td>
</tr>
<tr>
<td>OAM</td>
<td>operations, administration, and maintenance</td>
</tr>
<tr>
<td>OAMPDU</td>
<td>OAM protocol data units</td>
</tr>
<tr>
<td>OC3</td>
<td>optical carrier level 3</td>
</tr>
<tr>
<td>OCSP</td>
<td>online certificate status protocol</td>
</tr>
<tr>
<td>Acronym</td>
<td>Expansion</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>ODU</td>
<td>outdoor unit</td>
</tr>
<tr>
<td>OIF</td>
<td>outgoing interface</td>
</tr>
<tr>
<td>OLT</td>
<td>optical line termination</td>
</tr>
<tr>
<td>OMC</td>
<td>optical management console</td>
</tr>
<tr>
<td>ONT</td>
<td>optical network terminal</td>
</tr>
<tr>
<td>OOB</td>
<td>out-of-band</td>
</tr>
<tr>
<td>OPX</td>
<td>off premises extension</td>
</tr>
<tr>
<td>ORF</td>
<td>outbound route filtering</td>
</tr>
<tr>
<td>OS</td>
<td>operating system</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection (reference model)</td>
</tr>
<tr>
<td>OSI/INLP</td>
<td>OSI Network Layer Control Protocol</td>
</tr>
<tr>
<td>OSPF</td>
<td>open shortest path first</td>
</tr>
<tr>
<td>OSPF-TE</td>
<td>OSPF-traffic engineering (extensions)</td>
</tr>
<tr>
<td>OSS</td>
<td>operations support system</td>
</tr>
<tr>
<td>OSSP</td>
<td>organization specific slow protocol</td>
</tr>
<tr>
<td>OTP</td>
<td>one time password</td>
</tr>
<tr>
<td>OWAMP</td>
<td>one-way active measurement protocol</td>
</tr>
<tr>
<td>P2MP</td>
<td>point to multipoint</td>
</tr>
<tr>
<td>PADI</td>
<td>PPPoE active discovery initiation</td>
</tr>
<tr>
<td>PADR</td>
<td>PPPoE active discovery request</td>
</tr>
<tr>
<td>PAE</td>
<td>port authentication entities</td>
</tr>
<tr>
<td>PBO</td>
<td>packet byte offset</td>
</tr>
<tr>
<td>PBR</td>
<td>policy-based routing</td>
</tr>
<tr>
<td>PBX</td>
<td>private branch exchange</td>
</tr>
<tr>
<td>PCC</td>
<td>Path Computation Element Client</td>
</tr>
<tr>
<td>PCE</td>
<td>Path Computation Element</td>
</tr>
<tr>
<td>PCEP</td>
<td>Path Computation Element Protocol</td>
</tr>
<tr>
<td>Acronym</td>
<td>Expansion</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>PCM</td>
<td>pulse code modulation</td>
</tr>
<tr>
<td>PCP</td>
<td>priority code point</td>
</tr>
<tr>
<td>PCR</td>
<td>proprietary clock recovery</td>
</tr>
<tr>
<td>PDU</td>
<td>power distribution unit protocol data units</td>
</tr>
<tr>
<td>PDV</td>
<td>packet delay variation</td>
</tr>
<tr>
<td>PDVT</td>
<td>packet delay variation tolerance</td>
</tr>
<tr>
<td>PE</td>
<td>provider edge router</td>
</tr>
<tr>
<td>PEAPv0</td>
<td>protected extensible authentication protocol version 0</td>
</tr>
<tr>
<td>PEM</td>
<td>privacy enhanced mail</td>
</tr>
<tr>
<td>PFoE</td>
<td>power feed over Ethernet</td>
</tr>
<tr>
<td>PFS</td>
<td>perfect forward secrecy</td>
</tr>
<tr>
<td>PHB</td>
<td>per-hop behavior</td>
</tr>
<tr>
<td>PHY</td>
<td>physical layer</td>
</tr>
<tr>
<td>PIC</td>
<td>prefix independent convergence</td>
</tr>
<tr>
<td>PID</td>
<td>protocol ID</td>
</tr>
<tr>
<td>PIM SSM</td>
<td>protocol independent multicast—source-specific multicast</td>
</tr>
<tr>
<td>PIR</td>
<td>peak information rate</td>
</tr>
<tr>
<td>PKCS</td>
<td>public key cryptography standards</td>
</tr>
<tr>
<td>PKI</td>
<td>public key infrastructure</td>
</tr>
<tr>
<td>PLAR</td>
<td>private line automatic ringdown</td>
</tr>
<tr>
<td>PLCP</td>
<td>Physical Layer Convergence Protocol</td>
</tr>
<tr>
<td>PLR</td>
<td>point of local repair</td>
</tr>
<tr>
<td>PLSP</td>
<td>path LSP</td>
</tr>
<tr>
<td>PMSI</td>
<td>P-multicast service interface</td>
</tr>
<tr>
<td>P-multicast</td>
<td>provider multicast</td>
</tr>
<tr>
<td>PoE</td>
<td>power over Ethernet</td>
</tr>
<tr>
<td>PoE+</td>
<td>power over Ethernet plus</td>
</tr>
<tr>
<td>Acronym</td>
<td>Expansion</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>PoP</td>
<td>point of presence</td>
</tr>
<tr>
<td>POS</td>
<td>packet over SONET</td>
</tr>
<tr>
<td>PPP</td>
<td>point-to-point protocol</td>
</tr>
<tr>
<td>PPPoE</td>
<td>point-to-point protocol over Ethernet</td>
</tr>
<tr>
<td>PPS</td>
<td>pulses per second</td>
</tr>
<tr>
<td>PRC</td>
<td>primary reference clock</td>
</tr>
<tr>
<td>PRS</td>
<td>primary reference source</td>
</tr>
<tr>
<td>PRTC</td>
<td>primary reference time clock</td>
</tr>
<tr>
<td>PSE</td>
<td>power sourcing equipment</td>
</tr>
<tr>
<td>PSK</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>PSN</td>
<td>packet switched network</td>
</tr>
<tr>
<td>PSNP</td>
<td>partial sequence number PDU</td>
</tr>
<tr>
<td>PTM</td>
<td>packet transfer mode</td>
</tr>
<tr>
<td>PTP</td>
<td>performance transparency protocol precision time protocol</td>
</tr>
<tr>
<td>PuTTY</td>
<td>an open-source terminal emulator, serial console, and network file transfer application</td>
</tr>
<tr>
<td>PVC</td>
<td>permanent virtual circuit</td>
</tr>
<tr>
<td>PVCC</td>
<td>permanent virtual channel connection</td>
</tr>
<tr>
<td>PW</td>
<td>pseudowire</td>
</tr>
<tr>
<td>PWE</td>
<td>pseudowire emulation</td>
</tr>
<tr>
<td>PWE3</td>
<td>pseudowire emulation edge-to-edge</td>
</tr>
<tr>
<td>Q.922</td>
<td>ITU-T Q-series Specification 922</td>
</tr>
<tr>
<td>QL</td>
<td>quality level</td>
</tr>
<tr>
<td>QoS</td>
<td>quality of service</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial In User Service</td>
</tr>
<tr>
<td>RAN</td>
<td>Radio Access Network</td>
</tr>
<tr>
<td>RBS</td>
<td>robbed bit signaling</td>
</tr>
<tr>
<td>Acronym</td>
<td>Expansion</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>RD</td>
<td>route distinguisher</td>
</tr>
<tr>
<td>RDI</td>
<td>remote defect indication</td>
</tr>
<tr>
<td>RED</td>
<td>random early discard</td>
</tr>
<tr>
<td>RESV</td>
<td>reservation</td>
</tr>
<tr>
<td>RIB</td>
<td>routing information base</td>
</tr>
<tr>
<td>RIP</td>
<td>routing information protocol</td>
</tr>
<tr>
<td>RJ-45</td>
<td>registered jack 45</td>
</tr>
<tr>
<td>RMON</td>
<td>remote network monitoring</td>
</tr>
<tr>
<td>RNC</td>
<td>Radio Network Controller</td>
</tr>
<tr>
<td>RP</td>
<td>rendezvous point</td>
</tr>
<tr>
<td>RPF RTM</td>
<td>reverse path forwarding RTM</td>
</tr>
<tr>
<td>RPS</td>
<td>radio protection switching</td>
</tr>
<tr>
<td>RPT</td>
<td>rendezvous-point tree</td>
</tr>
<tr>
<td>RR</td>
<td>route reflector</td>
</tr>
<tr>
<td>RRO</td>
<td>record route object</td>
</tr>
<tr>
<td>RS-232</td>
<td>Recommended Standard 232 (also known as EIA/TIA-232)</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir, and Adleman (authors of the RSA encryption algorithm)</td>
</tr>
<tr>
<td>RSHG</td>
<td>residential split horizon group</td>
</tr>
<tr>
<td>RSTP</td>
<td>rapid spanning tree protocol</td>
</tr>
<tr>
<td>RSVP-TE</td>
<td>resource reservation protocol - traffic engineering</td>
</tr>
<tr>
<td>RT</td>
<td>receive/transmit</td>
</tr>
<tr>
<td>RTC</td>
<td>route target constraint</td>
</tr>
<tr>
<td>RTM</td>
<td>routing table manager</td>
</tr>
<tr>
<td>RTN</td>
<td>battery return</td>
</tr>
<tr>
<td>RTP</td>
<td>real-time protocol</td>
</tr>
<tr>
<td>R&amp;TTE</td>
<td>Radio and Telecommunications Terminal Equipment</td>
</tr>
<tr>
<td>RTU</td>
<td>remote terminal unit</td>
</tr>
</tbody>
</table>
### Table 47  Acronyms  (Continued)

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>RU</td>
<td>rack unit</td>
</tr>
<tr>
<td>r-VPLS</td>
<td>routed virtual private LAN service</td>
</tr>
<tr>
<td>SA</td>
<td>security association source-active</td>
</tr>
<tr>
<td>SAA</td>
<td>service assurance agent</td>
</tr>
<tr>
<td>SAFI</td>
<td>subsequent address family identifier</td>
</tr>
<tr>
<td>SAP</td>
<td>service access point</td>
</tr>
<tr>
<td>SAR-8</td>
<td>7705 Service Aggregation Router – 8-slot chassis</td>
</tr>
<tr>
<td>SAR-18</td>
<td>7705 Service Aggregation Router – 18-slot chassis</td>
</tr>
<tr>
<td>SAR-A</td>
<td>7705 Service Aggregation Router – two variants:</td>
</tr>
<tr>
<td></td>
<td>• passively cooled chassis with 12 Ethernet ports and 8 T1/E1 ports</td>
</tr>
<tr>
<td></td>
<td>• passively cooled chassis with 12 Ethernet ports and no T1/E1 ports</td>
</tr>
<tr>
<td>SAR-Ax</td>
<td>7705 Service Aggregation Router:</td>
</tr>
<tr>
<td></td>
<td>• passively cooled</td>
</tr>
<tr>
<td></td>
<td>• DC-powered with a dual-feed DC input that can be connected to a +24/-48/-60 VDC power source</td>
</tr>
<tr>
<td></td>
<td>• equipped with 12 Ethernet ports (ports 1 to 4 are XOR ports and 5 to 12 are 100/1000 Ethernet SFP ports)</td>
</tr>
<tr>
<td></td>
<td>• equipped with a factory-installed GPS receiver and GNSS RF faceplate connector</td>
</tr>
<tr>
<td>SAR-H</td>
<td>7705 Service Aggregation Router – temperature- and EMC-hardened to the following specifications: IEEE 1613 and IEC 61850-3</td>
</tr>
<tr>
<td>SAR-Hc</td>
<td>7705 Service Aggregation Router – compact version of 7705 SAR-H</td>
</tr>
</tbody>
</table>
SAR-M 7705 Service Aggregation Router – four variants:
• actively cooled chassis with 16 T1/E1 ports, 7 Ethernet ports, and 1 hot-insertable module slot
• actively cooled chassis with 0 T1/E1 ports, 7 Ethernet ports, and 1 hot-insertable module slot
• passively cooled chassis with 16 T1/E1 ports, 7 Ethernet ports, and 0 module slots
• passively cooled chassis with 0 T1/E1 ports, 7 Ethernet ports, and 0 module slots

SAR-O 7705 Service Aggregation Router passive CWDM device – three variants:
• 2-wavelength CWDM dual-fiber
• 4-wavelength CWDM dual-fiber
• 8-wavelength CWDM single-fiber
Each variant has different models that are used to add and drop different wavelengths

SAR-W 7705 Service Aggregation Router – passively cooled, universal AC and DC powered unit, equipped with five Gigabit Ethernet ports (three SFP ports and two RJ-45 Power over Ethernet (PoE) ports)
SAR-Wx 7705 Service Aggregation Router – passively cooled, universal AC powered unit; there are six variants:
• a unit that is equipped with an AC power input connector, five Gigabit Ethernet data ports (three SFP ports and two RJ-45 Ethernet ports), and an RJ-45 alarm input connector
• a unit that is equipped with an AC power input connector, five Gigabit Ethernet data ports (three SFP ports and two RJ-45 Ethernet ports), a GPS receiver, and an RJ-45 alarm input connector
• a unit that is equipped with an AC power input connector, five Gigabit Ethernet data ports (three SFP ports, one RJ-45 Ethernet port, and one RJ-45 PoE+ port), and an RJ-45 alarm input connector
• a unit that is equipped with an AC power input connector, five Gigabit Ethernet data ports (three SFP ports, one RJ-45 Ethernet port, and one RJ-45 PoE+ port), a GPS receiver, and an RJ-45 alarm input connector
• a unit that is equipped with an AC power input connector, four Gigabit Ethernet data ports (three SFP ports and one RJ-45 port), one RJ-45 4-pair xDSL port, and an RJ-45 alarm input connector
• a unit that is equipped with an AC power input connector, four Gigabit Ethernet data ports (three SFP ports and one RJ-45 port), one RJ-45 4-pair xDSL port, a GPS receiver, and an RJ-45 alarm input connector

SAR-X 7705 Service Aggregation Router – fan-cooled, rack-mountable, IP20 design, available in two variants:
• AC-powered variant with a single-feed AC input that can be connected to a 100 to 240 VAC, 50/60 Hz power source
• DC-powered variant with a dual-feed DC input that can be connected to a +24/-48/-60 VDC power source

SAToP structure-agnostic TDM over packet
SCADA surveillance, control and data acquisition
SC-APS single-chassis automatic protection switching
SCP secure copy
SCTP Stream Control Transmission Protocol

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAR-Wx</td>
<td>7705 Service Aggregation Router – passively cooled, universal AC powered unit; there are six variants:</td>
</tr>
<tr>
<td></td>
<td>• a unit that is equipped with an AC power input connector, five Gigabit Ethernet data ports (three SFP ports and two RJ-45 Ethernet ports), and an RJ-45 alarm input connector</td>
</tr>
<tr>
<td></td>
<td>• a unit that is equipped with an AC power input connector, five Gigabit Ethernet data ports (three SFP ports and two RJ-45 Ethernet ports), a GPS receiver, and an RJ-45 alarm input connector</td>
</tr>
<tr>
<td></td>
<td>• a unit that is equipped with an AC power input connector, five Gigabit Ethernet data ports (three SFP ports, one RJ-45 Ethernet port, and one RJ-45 PoE+ port), and an RJ-45 alarm input connector</td>
</tr>
<tr>
<td></td>
<td>• a unit that is equipped with an AC power input connector, five Gigabit Ethernet data ports (three SFP ports, one RJ-45 Ethernet port, and one RJ-45 PoE+ port), a GPS receiver, and an RJ-45 alarm input connector</td>
</tr>
<tr>
<td></td>
<td>• a unit that is equipped with an AC power input connector, four Gigabit Ethernet data ports (three SFP ports and one RJ-45 port), one RJ-45 4-pair xDSL port, and an RJ-45 alarm input connector</td>
</tr>
<tr>
<td></td>
<td>• a unit that is equipped with an AC power input connector, four Gigabit Ethernet data ports (three SFP ports and one RJ-45 port), one RJ-45 4-pair xDSL port, a GPS receiver, and an RJ-45 alarm input connector</td>
</tr>
<tr>
<td>SAR-X</td>
<td>7705 Service Aggregation Router – fan-cooled, rack-mountable, IP20 design, available in two variants:</td>
</tr>
<tr>
<td></td>
<td>• AC-powered variant with a single-feed AC input that can be connected to a 100 to 240 VAC, 50/60 Hz power source</td>
</tr>
<tr>
<td></td>
<td>• DC-powered variant with a dual-feed DC input that can be connected to a +24/-48/-60 VDC power source</td>
</tr>
<tr>
<td>SAToP</td>
<td>structure-agnostic TDM over packet</td>
</tr>
<tr>
<td>SCADA</td>
<td>surveillance, control and data acquisition</td>
</tr>
<tr>
<td>SC-APS</td>
<td>single-chassis automatic protection switching</td>
</tr>
<tr>
<td>SCP</td>
<td>secure copy</td>
</tr>
<tr>
<td>SCTP</td>
<td>Stream Control Transmission Protocol</td>
</tr>
</tbody>
</table>
### Table 47 Acronyms (Continued)

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expansion</th>
</tr>
</thead>
</table>
| SD      | signal degrade  
space diversity |
<p>| SDH     | synchronous digital hierarchy |
| SDI     | serial data interface |
| SDN     | software defined network |
| SDP     | service destination point |
| SE      | shared explicit |
| SeGW    | secure gateway |
| SETS    | synchronous equipment timing source |
| SF      | signal fail |
| SFP     | small form-factor pluggable (transceiver) |
| SFTP    | SSH file transfer protocol |
| (S,G)   | (source, group) |
| SGT     | self-generated traffic |
| SHA-1   | secure hash algorithm |
| SHG     | split horizon group |
| SIR     | sustained information rate |
| SLA     | Service Level Agreement |
| SLARP   | serial line address resolution protocol |
| SLID    | subscriber location identifier of a GPON module |
| SLM     | synthetic loss measurement |
| SNMP    | Simple Network Management Protocol |
| SNPA    | subnetwork point of attachment |
| SNR     | signal to noise ratio |
| SNTP    | simple network time protocol |
| SONET   | synchronous optical networking |
| S-PE    | switching provider edge router |
| SPF     | shortest path first |</p>
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPI</td>
<td>security parameter index</td>
</tr>
<tr>
<td>S-PMSI</td>
<td>selective PMSI</td>
</tr>
<tr>
<td>SPT</td>
<td>shortest path tree</td>
</tr>
<tr>
<td>SR</td>
<td>service router (includes 7710 SR, 7750 SR)</td>
</tr>
<tr>
<td>SRLG</td>
<td>shared risk link group</td>
</tr>
<tr>
<td>SRP</td>
<td>stateful request parameter</td>
</tr>
<tr>
<td>SRRP</td>
<td>subscriber routed redundancy protocol</td>
</tr>
<tr>
<td>SSH</td>
<td>secure shell</td>
</tr>
<tr>
<td>SSM</td>
<td>source-specific multicast synchronization status messaging</td>
</tr>
<tr>
<td>SSU</td>
<td>system synchronization unit</td>
</tr>
<tr>
<td>S-TAG</td>
<td>service VLAN tag</td>
</tr>
<tr>
<td>STM1</td>
<td>synchronous transport module, level 1</td>
</tr>
<tr>
<td>STP</td>
<td>spanning tree protocol</td>
</tr>
<tr>
<td>SVC</td>
<td>switched virtual circuit</td>
</tr>
<tr>
<td>SVEC</td>
<td>synchronization vector</td>
</tr>
<tr>
<td>SYN</td>
<td>synchronize</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Terminal Access Controller Access-Control System Plus</td>
</tr>
<tr>
<td>TC</td>
<td>traffic class (formerly known as EXP bits)</td>
</tr>
<tr>
<td>TCP</td>
<td>transmission control protocol</td>
</tr>
<tr>
<td>TDA</td>
<td>transmit diversity antenna</td>
</tr>
<tr>
<td>TDEV</td>
<td>time deviation</td>
</tr>
<tr>
<td>TDM</td>
<td>time division multiplexing</td>
</tr>
<tr>
<td>TE</td>
<td>traffic engineering</td>
</tr>
<tr>
<td>TEDB</td>
<td>traffic engineering database</td>
</tr>
<tr>
<td>TEID</td>
<td>tunnel endpoint identifier</td>
</tr>
<tr>
<td>TFTP</td>
<td>trivial file transfer protocol</td>
</tr>
<tr>
<td>T-LDP</td>
<td>targeted LDP</td>
</tr>
</tbody>
</table>
### Table 47 Acronyms (Continued)

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS</td>
<td>transport layer security</td>
</tr>
<tr>
<td>TLV</td>
<td>type length value</td>
</tr>
<tr>
<td>TM</td>
<td>traffic management</td>
</tr>
<tr>
<td>ToD</td>
<td>time of day</td>
</tr>
<tr>
<td>ToS</td>
<td>type of service</td>
</tr>
<tr>
<td>T-PE</td>
<td>terminating provider edge router</td>
</tr>
<tr>
<td>TPID</td>
<td>tag protocol identifier</td>
</tr>
<tr>
<td>TPIF</td>
<td>IEEE C37.94 teleprotection interface</td>
</tr>
<tr>
<td>TPMR</td>
<td>two-port MAC relay</td>
</tr>
<tr>
<td>TPS</td>
<td>transmission protection switching</td>
</tr>
<tr>
<td>TRAIM</td>
<td>time-receiver autonomous integrity monitoring</td>
</tr>
<tr>
<td>TSoP</td>
<td>Transparent SDH/SONET over Packet</td>
</tr>
<tr>
<td>TTL</td>
<td>time to live</td>
</tr>
<tr>
<td>TTLS</td>
<td>tunneled transport layer security</td>
</tr>
<tr>
<td>TTM</td>
<td>tunnel table manager</td>
</tr>
<tr>
<td>TWAMP</td>
<td>two-way active measurement protocol</td>
</tr>
<tr>
<td>U-APS</td>
<td>unidirectional automatic protection switching</td>
</tr>
<tr>
<td>UBR</td>
<td>unspecified bit rate</td>
</tr>
<tr>
<td>UDP</td>
<td>user datagram protocol</td>
</tr>
<tr>
<td>UFD</td>
<td>unidirectional forwarding detection</td>
</tr>
<tr>
<td>UMH</td>
<td>upstream multicast hop</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications System (3G)</td>
</tr>
<tr>
<td>UNI</td>
<td>user-to-network interface</td>
</tr>
<tr>
<td>uRPF</td>
<td>unicast reverse path forwarding</td>
</tr>
<tr>
<td>V.11</td>
<td>ITU-T V-series Recommendation 11</td>
</tr>
<tr>
<td>V.24</td>
<td>ITU-T V-series Recommendation 24</td>
</tr>
<tr>
<td>V.35</td>
<td>ITU-T V-series Recommendation 35</td>
</tr>
<tr>
<td>Acronym</td>
<td>Expansion</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>VC</td>
<td>virtual circuit</td>
</tr>
<tr>
<td>VCB</td>
<td>voice conference bridge</td>
</tr>
<tr>
<td>VCC</td>
<td>virtual channel connection</td>
</tr>
<tr>
<td>VCCV</td>
<td>virtual circuit connectivity verification</td>
</tr>
<tr>
<td>VCI</td>
<td>virtual circuit identifier</td>
</tr>
<tr>
<td>VID</td>
<td>VLAN ID</td>
</tr>
<tr>
<td>VLAN</td>
<td>virtual LAN</td>
</tr>
<tr>
<td>VLL</td>
<td>virtual leased line</td>
</tr>
<tr>
<td>VM</td>
<td>virtual machine</td>
</tr>
<tr>
<td>VoIP</td>
<td>voice over IP</td>
</tr>
<tr>
<td>Vp</td>
<td>peak voltage</td>
</tr>
<tr>
<td>VP</td>
<td>virtual path</td>
</tr>
<tr>
<td>VPC</td>
<td>virtual path connection</td>
</tr>
<tr>
<td>VPI</td>
<td>virtual path identifier</td>
</tr>
<tr>
<td>VPLS</td>
<td>virtual private LAN service</td>
</tr>
<tr>
<td>VPN</td>
<td>virtual private network</td>
</tr>
<tr>
<td>VPRN</td>
<td>virtual private routed network</td>
</tr>
<tr>
<td>VRF</td>
<td>virtual routing and forwarding table</td>
</tr>
<tr>
<td>VRRP</td>
<td>virtual router redundancy protocol</td>
</tr>
<tr>
<td>VSE</td>
<td>vendor-specific extension</td>
</tr>
<tr>
<td>VSO</td>
<td>vendor-specific option</td>
</tr>
<tr>
<td>VT</td>
<td>virtual trunk</td>
</tr>
<tr>
<td>WCDMA</td>
<td>wideband code division multiple access (transmission protocol used in UMTS networks)</td>
</tr>
<tr>
<td>WRED</td>
<td>weighted random early discard</td>
</tr>
<tr>
<td>WTR</td>
<td>wait to restore</td>
</tr>
<tr>
<td>X.21</td>
<td>ITU-T X-series Recommendation 21</td>
</tr>
<tr>
<td>XOR</td>
<td>exclusive-OR</td>
</tr>
<tr>
<td>Acronym</td>
<td>Expansion</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------</td>
</tr>
<tr>
<td>XRO</td>
<td>exclude route object</td>
</tr>
</tbody>
</table>
7 Standards and Protocol Support

This chapter lists the 7705 SAR compliance with EMC, environmental, and safety standards, telecom standards, and supported protocols:

- EMC Industrial Standards Compliance
- EMC Regulatory and Customer Standards Compliance
- Environmental Standards Compliance
- Safety Standards Compliance
- Telecom Interface Compliance
- Directives, Regional Approvals and Certifications Compliance
- Security Standards
- Telecom Standards
- Protocol Support
- Proprietary MIBs
### Table 48  EMC Industrial Standards Compliance

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE Std C37.90</td>
<td>IEEE Standard for relays and relay systems associated with Electric Power Apparatus</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>IEEE Std C37.90.1</td>
<td>Surge Withstand Capability (SWC) Tests</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>IEEE Std C37.90.2</td>
<td>Withstand Capability of Relay Systems to Radiated Electromagnetic Interference from Transceivers</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>IEEE Std C37.90.3</td>
<td>IEEE Standard Electrostatic Discharge Tests for Protective Relays</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>EN 50121-4</td>
<td>Electromagnetic Compatibility – Part 4: Emission and Immunity of the Signalling and Telecommunications Apparatus</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>IEC 62236-4</td>
<td>Electromagnetic Compatibility – Part 4: Emission and Immunity of the Signalling and Telecommunications Apparatus</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>IEC 61000-6-2</td>
<td>Generic standards – Immunity for industrial environments</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>IEC 61000-6-4</td>
<td>Generic standards – Emissions standard for industrial environments</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>IEC 61000-6-5</td>
<td>Generic standards – immunity for equipment used in power station and substation environment</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>IEC 61850-3</td>
<td>Communication networks and systems for power utility automation - Part 3: General requirements</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>IEC/AS 60870.2.1</td>
<td>Telecontrol equipment and systems. Operating conditions. Power supply and electromagnetic compatibility</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
</tbody>
</table>

**Note:** The symbols ✓ and ✓ indicate compliance with the standard.
Notes:
1. Performance Class 1
2. Performance Class 1 (Class 2 with Optics interfaces only)
3. Performance Class 2
4. Zone A; Performance Class 1
5. Zone A; Performance Class 1 (Class 2 with Optics interfaces only)
6. Zone B; Performance Class 1
7. Zone A; Performance Class 2
8. With the exception of DC surges

Table 49  EMC Regulatory and Customer Standards Compliance

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
<th>SAR-X</th>
<th>SAR-A</th>
<th>SAR-Ax</th>
<th>SAR-M</th>
<th>SAR-8</th>
<th>SAR-18</th>
<th>SAR-H</th>
<th>SAR-Hc</th>
<th>SAR-W</th>
<th>SAR-Wx</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 61000-4-2</td>
<td>Electrostatic discharge immunity test</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IEC 61000-4-3</td>
<td>Radiated electromagnetic field immunity test</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IEC 61000-4-4</td>
<td>Electrical fast transient/burst immunity test</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IEC 61000-4-5</td>
<td>Surge immunity test</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IEC 61000-4-6</td>
<td>Immunity to conducted disturbances</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IEC 61000-4-8</td>
<td>Power frequency magnetic field immunity test</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IEC 61000-4-9</td>
<td>Pulse Magnetic field immunity test</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IEC 61000-4-10</td>
<td>Damped Oscillatory Magnetic Field</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IEC 61000-4-11</td>
<td>Voltage dips, short interruptions and voltage variations immunity tests</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IEC 61000-4-12</td>
<td>Oscillatory wave immunity test</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IEC 61000-4-16</td>
<td>Conducted immunity 0 Hz - 150 kHz</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IEC 61000-4-17</td>
<td>Ripple on d.c. input power port immunity test</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IEC 61000-4-18</td>
<td>Damped oscillatory wave immunity test</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IEC 61000-4-29</td>
<td>Voltage dips, short interruptions and voltage variations on d.c. input power port immunity tests</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IEC 61000-3-2</td>
<td>Limits for harmonic current emissions (equipment input current &lt;16A per phase)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
### Table 49: EMC Regulatory and Customer Standards Compliance (Continued)

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 61000-3-3</td>
<td>Limits for voltage fluctuations and flicker in low-voltage supply systems for equipment with rated current &lt;16A</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>ITU-T K.20 (DC Ports)</td>
<td>Resistibility of telecommunication equipment installed in a telecommunications centre to overvoltages and overcurrents</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>ETSI 300 132-2</td>
<td>Power supply interface at the input to telecommunications and datacom (ICT) equipment; Part 2: Operated by -48 V direct current (dc)</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>ETSI 300 132-3</td>
<td>Power supply interface at the input to telecommunications equipment; Part 3: Operated by rectified current source, alternating current source or direct current source up to 400V</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>EN 300 386</td>
<td>Telecommunication network equipment; ElectroMagnetic Compatibility (EMC)</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>ES 201 468</td>
<td>Electromagnetic compatibility and Radio spectrum Matters (ERM); Additional ElectroMagnetic Compatibility (EMC) requirements and resistibility requirements for telecommunications equipment for enhanced availability of service in specific applications</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>EN 55024</td>
<td>Information technology equipment - Immunity characteristics - Limits and methods of measurements</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Telcordia GR-1089-CORE</td>
<td>EMC and Electrical Safety - Generic Criteria for Network Telecommunications Equipment</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>AS/NZS CISPR 22</td>
<td>Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>FCC Part 15, Subpart B</td>
<td>Radio Frequency devices- Unintentional Radiators (Radiated &amp; Conducted Emissions)</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>ICES-003</td>
<td>Information Technology Equipment (ITE) — Limits and methods of measurement</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
</tbody>
</table>

Table 49: EMC Regulatory and Customer Standards Compliance (Continued)
### Table 49  EMC Regulatory and Customer Standards Compliance (Continued)

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>SAR-X 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAR-A 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAR-Ax 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAR-M 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAR-8 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAR-18 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAR-H 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAR-Hc 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAR-W 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAR-Wx 3</td>
</tr>
<tr>
<td>EN 55022</td>
<td>Information technology equipment. Radio disturbance characteristics. Limits and methods of measurement</td>
<td>✓ 2 ✓ 2 ✓ 2 ✓ 2 ✓ 2 ✓ 2 ✓ 3 ✓ 3</td>
</tr>
<tr>
<td>EN 55032</td>
<td>Electromagnetic compatibility of multimedia equipment – Emission requirements</td>
<td>✓ 2 ✓ 2 ✓ 2 ✓ 2 ✓ 2 ✓ 2 ✓ 2 ✓ 2</td>
</tr>
<tr>
<td>CISPR 22</td>
<td>Information technology equipment. Radio disturbance characteristics. Limits and methods of measurement</td>
<td>✓ 2 ✓ 2 ✓ 2 ✓ 2 ✓ 2 ✓ 2 ✓ 3 ✓ 3</td>
</tr>
<tr>
<td>CISPR 32</td>
<td>Electromagnetic compatibility of multimedia equipment – Emission requirements</td>
<td>✓ 2 ✓ 2 ✓ 2 ✓ 2 ✓ 2 ✓ 2 ✓ 2 ✓ 2</td>
</tr>
<tr>
<td>GS7 EMC</td>
<td>Electromagnetic Standard Compatibility (BT standard)</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>KC Notice Emission (KN22) and Immunity (KN24) (South Korea)</td>
<td>EMS standard: NRRA notice</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>KC Notice Emission (KN32) and Immunity (KN35) (South Korea)</td>
<td>EMS standard: NRRA notice</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
</tbody>
</table>

**Notes:**

1. With external AC/DC power supply
2. Class A
3. Class B
### Table 50  Environmental Standards Compliance

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 1613:2009 + A1:2011</td>
<td>Environmental and Testing Requirements for Communications Networking Devices</td>
<td>✓ 1 ✓ 1 ✓ 1 ✓ 1 ✓ ✓</td>
</tr>
<tr>
<td>IEC 61850-3</td>
<td>Communication networks and systems for power utility automation - Part 3: General requirements</td>
<td>✓ 2 ✓ 2 ✓ 2 ✓ 2 ✓ 2 ✓ 2</td>
</tr>
<tr>
<td>IEC 60068-2-1</td>
<td>Environmental testing – Part 2-1: Tests – Test A: Cold</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>IEC 60068-2-2</td>
<td>Environmental testing - Part 2-2: Tests - Test B: Dry heat</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>IEC 60068-2-30</td>
<td>Environmental testing - Part 2: Tests. Test Db and guidance: Damp heat, cyclic (12 + 12-hour cycle)</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>IEC 60255-21-2</td>
<td>Electrical relays - Part 21: Vibration, shock, bump and seismic tests on measuring relays and protection equipment - Section Two: Shock and bump tests</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>ETSI 300 753 Class 3.2</td>
<td>Acoustic noise emitted by telecommunications equipment</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>Telcordia GR-63-CORE</td>
<td>NEBS Requirements: Physical Protection</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>ETSI EN 300 019-2-1 v2.1.2, Class 1.2</td>
<td>Specification of environmental tests; Storage</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>ETSI EN 300 019-2-2 V2.1.2, class 2.3</td>
<td>Specification of environmental tests; Transportation</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>ETSI EN 300 019-2-3 V2.2.2, class 3.2</td>
<td>Specification of environmental tests; Stationary use at weatherprotected locations</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>ETSI EN 300 019-2-4 v2.2.2 class T4.1</td>
<td>Specification of environmental tests; Stationary use at non-weatherprotected locations</td>
<td>✓ ✓</td>
</tr>
<tr>
<td>Telcordia GR-3108-CORE</td>
<td>Generic Requirements for Network Equipment in the Outside Plant (OSP)</td>
<td>✓ 3 ✓ 3 ✓ 3 ✓ 3 ✓ 3 ✓ 4 ✓ 4</td>
</tr>
<tr>
<td>Telcordia GR-950-CORE</td>
<td>Generic Requirements for ONU Closures and ONU Systems</td>
<td>✓ ✓</td>
</tr>
</tbody>
</table>
### Table 50  Environmental Standards Compliance (Continued)

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>&quot;GR-3108 Class 3 Section 6.2</strong> IEC 60068-2-52 - Severity 3 MIL-STD-810G Method 509.5 EN 60721-3-3 Class 3C4 EN 60068-2-11: Salt Mist EN 50155 Class ST4**</td>
<td>Conformal Coating &lt;sup&gt;5&lt;/sup&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Platform</th>
<th>SAR-X</th>
<th>SAR-A</th>
<th>SAR-Ax</th>
<th>SAR-M</th>
<th>SAR-8</th>
<th>SAR-18</th>
<th>SAR-H</th>
<th>SAR-Hc</th>
<th>SAR-W</th>
<th>SAR-Wx</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>
<td></td>
</tr>
</tbody>
</table>

### Notes:
1. Forced air system; uses fans
2. Normal environmental conditions as per IEC 61850-3 ed.2
3. Class 2
4. Class 4
5. Conformal coating is available as an orderable option

### Table 51  Safety Standards Compliance

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>UL/CSA 60950-1</td>
<td>Information technology equipment - Safety - Part 1: General requirements</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

| IEC/EN 60950-1 | Information technology equipment - Safety - Part 1: General requirements |
| ✓        | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     |

| UL/CSA 62368-1 | Audio/video, information and communication technology equipment - Part 1: Safety requirements |
| ✓        | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     |

| IEC/EN 62368-1 | Audio/video, information and communication technology equipment - Part 1: Safety requirements |
| ✓        | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     |

| AS/NZS 60950-1 | Information technology equipment - Safety - Part 1: General requirements |
| ✓        | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     |
### Table 51  
**Safety Standards Compliance (Continued)**

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
<th>Platform</th>
</tr>
</thead>
</table>
| IEC/EN 60825-1 and 2      | Safety of laser products - Part 1: Equipment classification and requirements  
                          | Part 2: Safety of optical fibre communication systems (OFCS)          | ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ |
| UL/CSA 60950-22           | Information Technology Equipment - Safety - Part 22: Equipment to be Installed Outdoors | ✓ ✓ |
| CSA–C22.2 No.94           | Special Purpose Enclosures                                           | ✓ ✓ |
| UL50                      | Enclosures for Electrical Equipment, Non-Environmental Consideration | ✓ ✓ |
| IEC/EN 60950-22           | Information technology equipment. Equipment to be installed Outdoors. | ✓ ✓ |
| IEC 60529                 | Degrees of Protection Provided by Enclosures (IP Code)               | ✓ 1 ✓ 2 ✓ 1 ✓ 1 ✓ 1 ✓ 2 ✓ 2 ✓ 3 ✓ 3 |

**Notes:**

1. IP20
2. IP40
3. IP65
### Table 52  Telecom Interface Compliance

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
<th>SAR-X</th>
<th>SAR-A</th>
<th>SAR-Ax</th>
<th>SAR-M</th>
<th>SAR-8</th>
<th>SAR-18</th>
<th>SAR-H</th>
<th>SAR-Hc</th>
<th>SAR-W</th>
<th>SAR-Wx</th>
</tr>
</thead>
<tbody>
<tr>
<td>IC CS-03 Issue 9</td>
<td>Compliance Specification for Terminal Equipment, Terminal Systems, Network Protection Devices, Connection Arrangements and Hearing Aids Compatibility</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACTA TIA-968-B</td>
<td>Telecommunications - Telephone Terminal Equipment - Technical Requirements for Connection of Terminal Equipment to the Telephone Network</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AS/ACIF S016 (Australia)</td>
<td>Requirements for Customer Equipment for connection to hierarchical digital interfaces</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATIS-06000403</td>
<td>Network and Customer Installation Interfaces- DS1 Electrical Interfaces</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ANSI/TIA/EIA-422-B (RS422)</td>
<td>Electrical Characteristics for balanced voltage digital interfaces circuits</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU-T G.825</td>
<td>The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU-T G.703</td>
<td>Physical/electrical characteristics of hierarchical digital interfaces</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU-T G.712 (E&amp;M)</td>
<td>Transmission performance characteristics of pulse code modulation channels</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU-T G.957</td>
<td>Optical interfaces for equipments and systems relating to the synchronous digital hierarchy</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU-T V.24 (RS232)</td>
<td>List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU-T V.28 (V35)</td>
<td>Electrical characteristics for unbalanced double-current interchange circuits</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITU-T V.36 (V35)</td>
<td>Modems for synchronous data transmission using 60-108 kHz group band circuits</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 52  Telecom Interface Compliance (Continued)

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITU-T V.11 / X.27 (RS-422)</td>
<td>Electrical characteristics for balanced double current interchange circuits operating at data signalling rates up to 10 Mbit/s</td>
<td>✓ ✓</td>
</tr>
<tr>
<td>ITU-T X.21 (RS-422)</td>
<td>Interface between Data Terminal Equipment and Data Circuit-terminating Equipment for synchronous operation on public data networks</td>
<td>✓ ✓</td>
</tr>
<tr>
<td>IEEE 802.3at (POE)</td>
<td>Data Terminal Equipment Power via the Media Dependent Interfaces Enhancements</td>
<td>✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
</tbody>
</table>

### Table 53  Directives, Regional Approvals and Certifications Compliance

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU Directive 2012/19/ EU (WEEE)</td>
<td>Waste Electrical and Electronic Equipment (WEEE)</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>EU Directive 2011/65/ EU (RoHS2)</td>
<td>Restriction of the use of certain Hazardous Substances in Electrical and Electronic Equipment (Recast)</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>CE Mark</td>
<td></td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>CRoHS Logo; Ministry of Information Industry order No.39</td>
<td></td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>China (MII NAL) Network Access License</td>
<td></td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
</tbody>
</table>

---

412 3HE 11012 AAAC TQZZA Edition: 01
<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>South Korea (KC Mark)</td>
<td></td>
<td>SAR-X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAR-A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAR-Ax</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAR-M</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAR-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAR-18</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAR-H</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAR-Hc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAR-W</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAR-Wx</td>
</tr>
<tr>
<td>Australia (RCM Mark)</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Japan (VCCI Mark)</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>NEBS Level 3</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>TL9000 certified</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>ISO 14001 certified</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>ISO 9001:2008 certified</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
Security Standards

FIPS 140-2—Federal Information Processing Standard publication 140-2, Security Requirements for Cryptographic Modules

Telecom Standards

ANSI/TIA/EIA-232-C—Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange

IEEE 802.1ad—IEEE Standard for Local and Metropolitan Area Networks---Virtual Bridged Local Area Networks

IEEE 802.1ag—Service Layer OAM

IEEE 802.1p/q—VLAN Tagging

IEEE 802.3—10BaseT

IEEE 802.3ab—1000BaseT

IEEE 802.3ah—Ethernet OAM

IEEE 802.3u—100BaseTX

IEEE 802.3x —Flow Control

IEEE 802.3z—1000BaseSX/LX

IEEE 802.3-2008—Revised base standard

IEEE 802.1AX-2008—Link Aggregation Task Force (transferred from IEEE 802.3ad)

IEEE C37.94-2002—N Times 64 Kilobit Per Second Optical Fiber Interfaces Between Teleprotection and Multiplexer Equipment

ITU-T G.704—Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels

ITU-T G.707—Network node interface for the Synchronous Digital Hierarchy (SDH)

ITU-T G.984.1—Gigabit-capable passive optical networks (GPON): general characteristics

ITU-T Y.1564—Ethernet service activation test methodology

ITU-T Y.1731—OAM functions and mechanisms for Ethernet-based networks

Protocol Support

ATM

AF-PHY-0086.001—Inverse Multiplexing for ATM (IMA)


GR-1113-CORE—Bellcore, Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1, July 1994

GR-1248-CORE—Generic Requirements for Operations of ATM Network Elements (NEs). Issue 3 June 1996
ITU-T Recommendation I.432.1—B-ISDN user-network interface - Physical layer specification: General characteristics
ITU-T Recommendation I.610—B-ISDN Operation and Maintenance Principles and Functions version 11/95
RFC 2514—Definitions of Textual Conventions and OBJECT_IDENTITIES for ATM Management, February 1999
RFC 2515—Definition of Managed Objects for ATM Management, February 1999
RFC 2684—Multiprotocol Encapsulation over ATM Adaptation Layer 5

BFD
draft-ietf-bfd-mib-00.txt—Bidirectional Forwarding Detection Management Information Base
draft-ietf-bfd-base-o5.txt—Bidirectional Forwarding Detection
draft-ietf-bfd-v4v6-1hop-06.txt—BFD IPv4 and IPv6 (Single Hop)
draft-ietf-bfd-multihop-06.txt—BFD for Multi-hop Paths

BGP
RFC 1397—BGP Default Route Advertisement
RFC 1997—BGP Communities Attribute
RFC 2385—Protection of BGP Sessions via the TCP MD5 Signature Option
RFC 2439—BGP Route Flap Dampening
RFC 2547bis—BGP/MPLS VPNs
RFC 2918—Route Refresh Capability for BGP-4
RFC 3107—Carrying Label Information in BGP-4
RFC 3392—Capabilities Advertisement with BGP-4
RFC 4271—BGP-4 (previously RFC 1771)
RFC 4360—BGP Extended Communities Attribute
RFC 4364—BGP/MPLS IP Virtual Private Networks (VPNs) (previously RFC 2574bis BGP/MPLS VPNs)
RFC 4456—BGP Route Reflection: Alternative to Full-mesh IBGP (previously RFC 1966 and RFC 2796)
RFC 4486—Subcodes for BGP Cease Notification Message
RFC 4684—Constrained Route Distribution for Border Gateway Protocol/ MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)
RFC 4724—Graceful Restart Mechanism for BGP - GR Helper
RFC 4760—Multi-protocol Extensions for BGP (previously RFC 2858)
RFC 4893—BGP Support for Four-octet AS Number Space
RFC 6513—Multicast in MPLS/BGP IP VPNs
RFC 6514—BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs
draft-ietf-idr-add-paths-04.txt—Advertisement of Multiple Paths in BGP
draft-ietf-idr-add-paths-guidelines-00.txt—Best Practices for Advertisement of
Multiple Paths in BGP

**DHCP/DHCPv6**
RFC 1534—Interoperation between DHCP and BOOTP
RFC 2131—Dynamic Host Configuration Protocol (REV)
RFC 2132—DHCP Options and BOOTP Vendor Extensions
RFC 3046—DHCP Relay Agent Information Option (Option 82)
RFC 3315—Dynamic Host Configuration Protocol for IPv6
RFC 3736—Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6

**Differentiated Services**
RFC 2474—Definition of the DS Field in the IPv4 and IPv6 Headers
RFC 2597—Assured Forwarding PHB Group
RFC 2598—An Expedited Forwarding PHB
RFC 3140—Per-Hop Behavior Identification Codes

**Digital Data Network Management**
V.35
RS-232 (also known as EIA/TIA-232)
X.21

**DSL Modules**
IEEE 802.2 LLC/SNAP bridged encapsulation while operating in ATM bonded mode
standards compliance
ITU-T G.991.2 Appendix F and G—Support for up to 5696 Kb/s per pair
ITU-T G.992.1 (ADSL)
ITU-T G.992.3 (G.dmt.bis), Annex A, B, J, M
ITU-T G.992.3 Annex K.2 (ADSL2)
ITU-T G.992.5, Annex A, B, J, M
ITU-T G.992.5 Annex K (ADSL2+)
ITU-T G.993.2 Amendment 1—Seamless Rate Adaptation
ITU-T G.993.2 Annex A and Annex B—xDSL Standards Compliance (ADSL2/2+ and
VDSL2)
ITU-T G.993.2 Annex K.3—Supported Transport Protocol Specific Transmission
Convergence functions
ITU G.994.1 (2/07) Amendment 1 and 2—G.hs Handshake
ITU-T G.998.2—SHDSL 4-pair EFM bonding
ITU-T G.998.4 G.inp—Physical layer retransmission
ITU-T Y.1564 Ethernet service activation test methodology
TR-060—SHDSL rate and reach
TR112 (U-R2 Deutsche Telekom AG) Version 7.0 and report of Self-Test-Result (ATU-T Register#3)

**ECMP**
RFC 2992—Analysis of an Equal-Cost Multi-Path Algorithm

**Frame Relay**
ANSI T1.617 Annex D—Signalling Specification For Frame Relay Bearer Service
ITU-T Q.922 Annex A—Digital Subscriber Signalling System No. 1 (DSS1) data link layer - ISDN data link specification for frame mode bearer services
FRF.1.2—PVC User-to-Network Interface (UNI) Implementation Agreement
FRF.12—Frame Relay Fragmentation Implementation Agreement
RFC 2427—Multiprotocol Interconnect over Frame Relay

**GRE**
RFC 2784—Generic Routing Encapsulation (GRE)

**IPSec**
ITU-T X.690 (2002)—ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
PKCS #12 Personal Information Exchange Syntax Standard
RFC 2315—PKCS #7: Cryptographic Message Syntax
RFC 2401—Security Architecture for the Internet Protocol
RFC 2409—The Internet Key Exchange (IKE)
RFC 2986—PKCS #10: Certification Request Syntax Specification
RFC 3706—A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
RFC 3947—Negotiation of NAT-Traversal in the IKE
RFC 3948—UDP Encapsulation of IPsec ESP Packets
RFC 4303—IP Encapsulating Security Payload (ESP)
RFC 4210—Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)
RFC 4211—Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)
RFC 4945—The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX
Standards and Protocol Support

RFC 5280—Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 5996—Internet Key Exchange Protocol Version 2 (IKEv2)

IPv6
RFC 2460—Internet Protocol, Version 6 (IPv6) Specification
RFC 2462—IPv6 Stateless Address Autoconfiguration
RFC 2464—Transmission of IPv6 Packets over Ethernet Networks
RFC 3587—IPv6 Global Unicast Address Format
RFC 3595—Textual Conventions for IPv6 Flow Label
RFC 4007—IPv6 Scoped Address Architecture
RFC 4193—Unique Local IPv6 Unicast Addresses
RFC 4291—IPv6 Addressing Architecture
RFC 4443—Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification
RFC 4649—DHCPv6 Relay Agent Remote-ID Option
RFC 4861—Neighbor Discovery for IP version 6 (IPv6)
RFC 5095—Deprecation of Type 0 Routing Headers in IPv6
RFC 5952—A Recommendation for IPv6 Address Text Representation

IS-IS
RFC 1142—OSI IS-IS Intra-domain Routing Protocol (ISO 10589)
RFC 1195—Use of OSI IS-IS for routing in TCP/IP & dual environments
RFC 2763—Dynamic Hostname Exchange for IS-IS
RFC 2966—Domain-wide Prefix Distribution with Two-Level IS-IS
RFC 2973—IS-IS Mesh Groups
RFC 3373—Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
RFC 3719—Recommendations for Interoperable Networks using IS-IS
RFC 3787—Recommendations for Interoperable IP Networks
RFC 4205 for Shared Risk Link Group (SRLG) TLV
RFC 5304—IS-IS Cryptographic Authentication
RFC 5308—Routing IPv6 with IS-IS
RFC 5309—Point-to-Point Operation over LAN in Link State Routing Protocols
RFC 5310—IS-IS Generic Cryptographic Authentication
LDP
RFC 5036—LDP Specification
RFC 5283—LDP Extension for Inter-Area Label Switched Paths
RFC 5443—LDP IGP Synchronization
RFC 6388—Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths
RFC 6512—Using Multipoint LDP When the Backbone Has No Route to the Root
draft-pdutta-mpls-mldp-up-redundancy-00.txt—Upstream LSR Redundancy for Multi-point LDP Tunnels

LDP and IP FRR
RFC 5286—Basic Specification for IP Fast Reroute: Loop-Free Alternates

MPLS
RFC 3031—MPLS Architecture
RFC 3032—MPLS Label Stack Encoding
RFC 3815—Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)
RFC 6790—The Use of Entropy Labels in MPLS Forwarding

MPLS – OAM
RFC 4379—Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
RFC 6424—Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels

Multicast
RFC 3956—Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address
RFC 4610—Anycast-RP Using Protocol Independent Multicast (PIM), which is similar to RFC 3446—Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)
RFC 6514—BGP Encodings and Procedures for Multicast in MPLS/IP VPNs
cisco-ipmulticast/pim-autorp-spec—Auto-RP: Automatic discovery of Group-to-RP mappings for IP multicast, which is similar to RFC 5059—Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)
draft-ietf-l2vpn-vpls-pim-snooping-07—Protocol Independent Multicast (PIM) over Virtual Private LAN Service (VPLS)
draft-ietf-mboned-msdp-deploy-nn.txt—Multicast Source Discovery Protocol (MSDP) Deployment Scenarios
Network Management
IANA-IFType-MIB
ITU-T X.721—Information technology- OSI-Structure of Management Information
ITU-T X.734—Information technology- OSI-Systems Management: Event Report Management Function
M.3100/3120—Equipment and Connection Models
RFC 1157—SNMPv1
RFC 1850—OSPF-MIB
RFC 1907—SNMPv2-MIB
RFC 2011—IP-MIB
RFC 2012—TCP-MIB
RFC 2013—UDP-MIB
RFC 2030—Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
RFC 2096—IP-FORWARD-MIB
RFC 2138—RADIUS
RFC 2206—RSVP-MIB
RFC 2571—SNMP-FRAMEWORKMIB
RFC 2572—SNMP-MPD-MIB
RFC 2573—SNMP-TARGET-&-NOTIFICATION-MIB
RFC 2574—SNMP-USER-BASED-SMMIB
RFC 2575—SNMP-VIEW-BASED ACM-MIB
RFC 2576—SNMP-COMMUNITY-MIB
RFC 2588—SONET-MIB
RFC 2665—EtherLike-MIB
RFC 2819—RMON-MIB
RFC 2863—IF-MIB
RFC 2864—INVERTED-STACK-MIB
RFC 3014—NOTIFICATION-LOG MIB
RFC 3164—The BSD Syslog Protocol
RFC 3273—HCRMON-MIB
RFC 3412—Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413—Simple Network Management Protocol (SNMP) Applications
RFC 3414—User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3418—SNMP MIB
draft-ietf-disman-alarm-mib-04.txt
draft-ietf-mpls-ldp-mib-07.txt
draft-ietf-ospf-mib-update-04.txt
draft-ietf-mpls-lsr-mib-06.txt
draft-ietf-mpls-te-mib-04.txt
TMF 509/613—Network Connectivity Model

**OSPF**
RFC 1765—OSPF Database Overflow
RFC 2328—OSPF Version 2
RFC 2370—Opaque LSA Support
RFC 2740—OSPF for IPv6
RFC 3101—OSPF NSSA Option
RFC 3137—OSPF Stub Router Advertisement
RFC 3509—Alternative Implementations of OSPF Area Border Routers
RFC 3623—Graceful OSPF Restart (support for Helper mode)
RFC 3630—Traffic Engineering (TE) Extensions to OSPF
RFC 4203 for Shared Risk Link Group (SRLG) sub-TLV
RFC 4577—OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs) (support for basic OSPF at PE-CE links)

**OSPFv3**
RFC 4552—Authentication/Confidentiality for OSPFv3

**PPP**
RFC 1332—PPP Internet Protocol Control Protocol (IPCP)
RFC 1570—PPP LCP Extensions
RFC 1619—PPP over SONET/SDH
RFC 1661—The Point-to-Point Protocol (PPP)
RFC 1662—PPP in HDLC-like Framing
RFC 1989—PPP Link Quality Monitoring
RFC 1990—The PPP Multilink Protocol (MP)
RFC 2686—The Multi-Class Extension to Multi-Link PPP

**Pseudowires**
Metro Ethernet Forum—Implementation Agreement for the Emulation of PDH Circuits over Metro Ethernet Networks
RFC 3550—RTP: A Transport Protocol for Real-Time Applications
RFC 3985—Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture
RFC 4385—Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN
RFC 4446—IANA Allocation for PWE3
RFC 4447—Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)
RFC 4448—Encapsulation Methods for Transport of Ethernet over MPLS Networks
RFC 4553—Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
RFC 4717—Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks
RFC 4618—Encapsulation Methods for Transport of PPP/High-Level Data Link Control (HDLC) over MPLS Networks
RFC 4619—Encapsulation Methods for Transport of Frame Relay over Multiprotocol Label Switching (MPLS) Networks
RFC 4816—Pseudowire Emulation Edge-to-Edge (PWE3) Asynchronous Transfer Mode (ATM) Transparent Cell Transport Service
RFC 5085—Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires
RFC 5086—Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)
draft-ietf-pwe3-redundancy-02.txt—Pseudowire (PW) Redundancy

RIP
RFC 1058—Routing Information Protocol
RFC 2453—RIP Version 2

RADIUS
RFC 2865—Remote Authentication Dial In User Service
RFC 2866—RADIUS Accounting

RSVP-TE and FRR
RFC 2430—A Provider Architecture for DiffServ & TE
RFC 2961—RSVP Refresh Overhead Reduction Extensions
RFC 2702—Requirements for Traffic Engineering over MPLS
RFC 2747—RSVP Cryptographic Authentication
RFC 3097—RSVP Cryptographic Authentication - Updated Message Type Value
RFC 3209—Extensions to RSVP for LSP Tunnels
RFC 3210—Applicability Statement for Extensions to RSVP for LSP Tunnels
RFC 3477—Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)
RFC 4090—Fast Reroute Extensions to RSVP-TE for LSP Tunnels
RFC 5440—Path Computation Element (PCE) Communication Protocol (PCEP)
draft-ietf-pce-stateful-pce—PCEP Extensions for Stateful PCE
draft-ietf-pce-segment-routing—PCEP Extensions for Segment Routing
draft-alvarez-pce-path-profiles—PCE Path Profiles

SONET/SDH
ITU-T Recommendation G.841—Telecommunication Standardization Section of ITU, Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum1 issued in July 2002

SSH
draft-ietf-secsh-architecture.txt—SSH Protocol Architecture
draft-ietf-secsh-userauth.txt—SSH Authentication Protocol
draft-ietf-secsh-transport.txt—SSH Transport Layer Protocol
draft-ietf-secsh-connection.txt—SSH Connection Protocol
draft-ietf-secsh-newmodes.txt—SSH Transport Layer Encryption Modes

Synchronization
G.781—Synchronization layer functions, 2001/09/17
G.803—Architecture of transport networks based on the synchronous digital hierarchy (SDH)
G.813—Timing characteristics of SDH equipment slave clocks (SEC)
G.823—The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy, 2003/03/16
G.824—The control of jitter and wander within digital networks which are based on the 1544 kbit/s hierarchy, 2003/03/16
G.8261—Timing and synchronization aspects in packet networks
G.8262—Timing characteristics of synchronous Ethernet equipment slave clock
GR 1244 CORE—Clocks for the Synchronized Network: Common Generic Criteria
ITU-T G.8264—Telecommunication Standardization Section of ITU, Distribution of timing information through packet networks, issued 10/2008
ITU-T G.8265.1—Telecommunication Standardization Section of ITU, Precision time protocol telecom profile for frequency synchronization, issued 10/2010
ITU-T G.8275.1—Telecommunication Standardization Section of ITU, Precision time protocol telecom profile for phase/time synchronization with full timing support from the network, issued 07/2014


TACACS+
IETF draft-grant-tacacs-02.txt—The TACACS+ Protocol

TCP/IP
RFC 768—User Datagram Protocol
RFC 791—Internet Protocol
RFC 792—Internet Control Message Protocol
RFC 793—Transmission Control Protocol
RFC 826—Ethernet Address Resolution Protocol
RFC 854—Telnet Protocol Specification
RFC 1350—The TFTP Protocol (Rev. 2)
RFC 1812—Requirements for IPv4 Routers

TWAMP
RFC 5357—A Two-Way Active Measurement Protocol (TWAMP)

VPLS
RFC 4762—Virtual Private LAN Services Using LDP

VRRP
RFC 2787—Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC 3768 Virtual Router Redundancy Protocol
RFC 5798 Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6

Proprietary MIBs
TIMETRA-ATM-MIB.mib
TIMETRA-CAPABILITY-7705-V1.mib
TIMETRA-CHASSIS-MIB.mib
TIMETRA-CLEAR-MIB.mib
TIMETRA-FILTER-MIB.mib
TIMETRA-GLOBAL-MIB.mib
TIMETRA-LAG-MIB.mib
TIMETRA-LDP-MIB.mib
TIMETRA-LOG-MIB.mib
TIMETRA-MPLS-MIB.mib
TIMETRA-OAM-TEST-MIB.mib
TIMETRA-PORT-MIB.mib
TIMETRA-PPP-MIB.mib
TIMETRA-QOS-MIB.mib
TIMETRA-ROUTE-POLICY-MIB.mib
TIMETRA-RSVP-MIB.mib
TIMETRA-SAP-MIB.mib
TIMETRA-SDP-MIB.mib
TIMETRA-SECURITY-MIB.mib
TIMETRA-SERV-MIB.mib
TIMETRA-SYSTEM-MIB.mib
TIMETRA-TC-MIB.mib
TIMETRA-VRRP-MIB.mib
Customer Document and Product Support

Customer documentation
Customer Documentation Welcome Page

Technical Support
Product Support Portal

Documentation feedback
Customer Documentation Feedback