JUNOS® Software

MPLS Applications Configuration Guide

Release 9.3

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Part Number: 530-027191-01, Revision 1

JUNOS® Software MPLS Applications Configuration Guide
Release 9.3

Writing: Albert Statti
Editing: Sonia Saruba
Illustration: Nathaniel Woodward
Cover Design: Edmonds Design

Revision History
10 October 2008—Revision 1

The information in this document is current as of the date listed in the revision history.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. The JUNOS software has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.

c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at http://www.gnu.org/licenses/gpl.html, and a copy of the LGPL at http://www.gnu.org/licenses/lgpl.html.

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous

agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient redigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Abbreviated Table of Contents

		About This Guide	xxxi
Part 1		**Overview**	
	Chapter 1	Traffic Engineering Overview	3
	Chapter 2	Complete MPLS Applications Configuration Mode Statements	9
Part 2		**MPLS**	
	Chapter 3	MPLS Overview	21
	Chapter 4	MPLS Configuration Statements	51
	Chapter 5	MPLS-Signaled LSPs Configuration Guidelines	57
	Chapter 6	DiffServ-Aware Traffic Engineering Configuration Guidelines	113
	Chapter 7	Static and Explicit-Path LSP Configuration Guidelines	135
	Chapter 8	Point-to-Multipoint LSP Configuration Guidelines	143
	Chapter 9	Miscellaneous MPLS Properties Configuration Guidelines	151
	Chapter 10	Summary of MPLS Configuration Statements	175
Part 3		**RSVP**	
	Chapter 11	RSVP Overview	253
	Chapter 12	RSVP Configuration Guidelines	269
	Chapter 13	Summary of RSVP Configuration Statements	297
Part 4		**LDP**	
	Chapter 14	LDP Overview	329
	Chapter 15	LDP Configuration Guidelines	337
	Chapter 16	Summary of LDP Configuration Statements	365
Part 5		**CCC and TCC**	
	Chapter 17	CCC and TCC Overview	393
	Chapter 18	CCC and TCC Configuration Guidelines	397
	Chapter 19	Summary of CCC and TCC Configuration Statements	421
Part 6		**GMPLS**	
	Chapter 20	GMPLS Overview	437

Chapter 21 GMPLS Configuration Guidelines 443
Chapter 22 RSVP LSP Hierarchy Configuration Guidelines 459
Chapter 23 Summary of GMPLS Configuration Statements 465

Part 7 Indexes

Index 485
Index of Statements and Commands 501

Table of Contents

About This Guide xxxi

Objectives xxxi
Audience xxxi
Supported Routing Platforms xxxii
Using the Indexes xxxii
Using the Examples in This Manual xxxii
Merging a Full Example xxxiii
Merging a Snippet xxxiii
Documentation Conventions xxxiv
List of Technical Publications xxxvi
Documentation Feedback xliii
Requesting Technical Support xliii

Part 1 Overview

Chapter 1 Traffic Engineering Overview 3

Components of Traffic Engineering 3
Packet Forwarding Component 4
Packet Forwarding Based on Label Swapping 4
How a Packet Traverses an MPLS Backbone 4
Information Distribution Component 5
Path Selection Component 5
Offline Planning and Analysis 6
Signaling Component 6
Flexible LSP Calculation and Configuration 7

Chapter 2 Complete MPLS Applications Configuration Mode Statements 9

[edit logical-systems] Hierarchy Level 9
[edit protocols connections] Hierarchy Level 10
[edit protocols ldp] Hierarchy Level 11
[edit protocols link-management] Hierarchy Level 12
[edit protocols mpls] Hierarchy Level 12
[edit protocols rsvp] Hierarchy Level 16

Part 2 MPLS

Chapter 3 MPLS Overview 21

MPLS Standards 21
Link-Layer Support 23
MPLS and Traffic Engineering 24
Label Description 25
Special Labels 25
Label Allocation 25
Operations on Labels 27
Routers in an LSP 27
How a Packet Travels Along an LSP 28
Types of LSPs 28
Scope of LSPs 29
Constrained-Path LSP Computation 29
How CSPF Selects a Path 30
Path Selection Tie-Breaking 31
Computing Paths Offline 31
LSPs on an Overloaded Router 31
Fate Sharing 32
IGP Shortcuts 33
Enabling IGP Shortcuts 34
LSPs Qualified in Shortcut Computations 34
IGP Shortcut Applications 35
IGP Shortcuts and Routing Table 35
Router Requirements 36
IGP Shortcuts and VPN Environments 36
Advertising LSPs into IGPs 36
IP and MPLS Packets on Aggregated Interfaces 37
MPLS Applications 38
BGP Destinations 38
IGP and BGP Destinations 39
Selecting a Forwarding LSP Next Hop 40
MPLS and Routing Tables 40
MPLS and Traffic Protection 42
Fast Reroute 43
Fast Reroute Overview 43
Detour Merging Process 45
Detour Computations 46
Fast Reroute Path Optimization 46
Automatic Bandwidth Allocation 47
Point-to-Multipoint LSPs 47
MPLS Load Balancing Based on the IP Header and MPLS Labels 49

Chapter 4 MPLS Configuration Statements 51

MPLS Configuration Statements 51
Minimum MPLS Configuration 55

Chapter 5 MPLS-Signaled LSPs Configuration Guidelines 57

Configuring the Ingress Router for Signaled LSPs 57
Creating a Named Path 58
Examples: Creating a Named Path 59
Configuring Alternate Backup Paths Using Fate Sharing 59
Configuring Fate Sharing 60
Implications for CSPF 61
Example: Configuring Fate Sharing 61
Configuring All Other MPLS Routers for Signaled LSPs 62
Configuring an LSP 62
Configuring the Address of the Egress and Ingress Routers 66
Configuring the Address of the Egress Router 66
Preventing the Addition of Egress Router Addresses to Routing Tables 67
Configuring the Address of the Ingress Router 68
Configuring the Primary and Secondary LSPs 68
Configuring Primary and Secondary Paths for an LSP 68
Configuring the Revert Timer 69
Specifying Path Selection 70
Configuring the Description 71
Configuring Fast Reroute 71
Configuring the Optimization Interval for Fast Reroute Paths 72
Configuring Addresses to Associate with the LSP 73
Configuring Path Connection Retry Information 74
Configuring the LSP Metric 75
Configuring a Dynamic LSP Metric 75
Configuring a Static LSP Metric 75
Configuring CSPF Tie Breaking 76
Configuring Load Balancing for MPLS LSPs 77
Using the First MPLS Label in the Hash Key 77
Using the Second MPLS Label in the Hash Key 77
Using the Third MPLS Label in the Hash Key 78
Using the IP Payload in the Hash Key 78
Using the First Two Labels and the IP Payload in the Hash Key 78
Configuring Load Balancing for MPLS LSPs Without CSPF 79
Disabling Normal TTL Decrementing 79
Configuring MPLS Soft Preemption 80
Configuring Automatic Bandwidth Allocation 81
Configuring MPLS Statistics for Automatic Bandwidth Allocation 82
Configuring Automatic Bandwidth Allocation on an LSP 82
Requesting an Automatic Bandwidth Allocation Adjustment 87
Disabling Constrained-Path LSP Computation 88
Configuring Administrative Groups 89
Configuring the LSP Preference 91
Configuring Path Route Recording 91
Configuring Class of Service for MPLS 91
Class of Service for MPLS Overview 91
Configuring the MPLS CoS Bits 92
Rewriting IEEE 802.1p Packet Headers with the MPLS CoS Value 93

Configuring Adaptive LSPs 94
Configuring Priority and Preemption for LSPs 95
Optimizing Signaled LSPs 96
Configuring the Smart Optimize Timer 97
Configuring the Maximum Path Length 98
Configuring the Path Bandwidth 98
Configuring the Standby State 99
Configuring LSP Hold Time 100
Configuring LDP Tunneling 100
Enabling RSVP 100
Configuring MPLS Exception Monitoring 101
Improving TED Accuracy with RSVP PathErr Messages 101
PathErr Messages 102
Identifying the Problem Link 102
Configuring the Router to Improve TED Accuracy 103
Examples: Configuring Signaled LSPs 103
Example: Constrained-Path LSP, JUNOS Makes All Forwarding Decisions 103
Example: Explicit-Path LSP 104
Example: Constrained-Path LSP, JUNOS Makes Most Forwarding Decisions, Hop Constraints Accounted For 105
Example: Constrained-Path LSP, JUNOS Makes Most Forwarding Decisions, Secondary Path Is Explicit 105
Configuring MPLS over GRE Tunnels 106
Example: Configuring MPLS over GRE Tunnels 107
Configuring IPv6 Tunnels over MPLS 108
IPv6 over MPLS Standards 109
Configuring an IPv4 MPLS Tunnel to Carry IPv6 Traffic 110
Configuring IPv6 on Both Core-Facing and CE Router–Facing Interfaces 110
Configuring MPLS and RSVP Between PE Routers 110
Enabling IPv6 Tunneling in MPLS 111
Configuring Multiprotocol BGP to Carry IPv6 Traffic 111
Configuring ICMP Message Tunneling 112
LSP Attributes for GMPLS 112

Chapter 6 DiffServ-Aware Traffic Engineering Configuration Guidelines 113

DiffServ-Aware Traffic Engineering Standards 114
DiffServ-Aware Traffic Engineering Terminology 114
DiffServ-Aware Traffic Engineering Overview 115
DiffServ-Aware Traffic Engineering Features 115
DiffServ-Aware Traffic Engineered LSPs 116
DiffServ-Aware Traffic Engineered LSPs Overview 116
DiffServ-Aware Traffic Engineered LSPs Operation 116
Multiclass LSPs 117
Multiclass LSP Overview 117
Establishing a Multiclass LSP on the Differentiated Services Domain 118

Configuring DiffServ-Aware Traffic Engineering 118
Configuring the Bandwidth Model 119
Configuring Traffic Engineering Classes 120
Requirements and Limitations for the Traffic Engineering Class Matrix 121
Configuring Class of Service 121
Bandwidth Oversubscription Overview 122
LSP Size Oversubscription 123
Link Size Oversubscription 123
Class Type Oversubscription and Local Oversubscription Multipliers 123
Class Type Bandwidth and the LOM 124
LOM Calculation for the MAM and Extended MAM Bandwidth Models 124
LOM Calculation for the Russian Dolls Bandwidth Model 125
Example: LOM Calculation 125
Configuring the Bandwidth Subscription Percentage for LSPs 126
Bandwidth Subscription Troubleshooting 127
Configuring DiffServ-Aware Traffic Engineering for LSPs 128
Configuring Class of Service for the Interfaces 129
Configuring IGP 129
Configuring a Traffic Engineered LSP 129
Configuring Policing for LSPs 130
Configuring Fast Reroute for Traffic Engineered LSPs 130
Configuring Multiclass LSPs 131
Configuring Class of Service for the Interfaces 131
Configuring the IGP 132
Configuring a Multiclass LSP 132
Configuring Policing for Multiclass LSPs 133
Configuring Fast Reroute for Multiclass LSPs 133

Chapter 7 Static and Explicit-Path LSP Configuration Guidelines 135

Configuring Static LSPs 135
Configuring the Ingress Router for Static LSPs 135
Example: Configuring the Ingress Router 137
Configuring the Intermediate and Egress Routers for Static LSPs 138
Example: Configuring an Intermediate Router 139
Example: Configuring an Egress Router 140
Configuring Static Unicast Routes for Point-to-Multipoint LSPs 140
Configuring Explicit-Path LSPs 142

Chapter 8 Point-to-Multipoint LSP Configuration Guidelines 143

Configuring Primary and Branch LSPs 143
Configuring the Primary Point-to-Multipoint LSP 143
Configuring a Branch LSP for the Point-to-Multipoint LSP 144
Configuring the Branch LSP as a Dynamic Path 144
Configuring the Branch LSP as a Static Path 145
Example: Configuring Point-to-Multipoint LSPs 145
Configuring Link Protection for Point-to-Multipoint LSPs 146

Configuring Graceful Restart for Point-to-Multipoint LSPs 146
Configuring a Multicast RPF Check Policy for Point-to-Multipoint LSPs 147
Example: Multicast RPF Check Policy for Point-to-Multipoint LSPs 148
Configuring Ingress PE Router Redundancy for Point-to-Multipoint LSPs 148
Binding Point-to-Point LSPs to PE Routers and Backup PE Router Groups 149
Ensuring Compatibility with JUNOS 9.1 and Earlier Releases for P2MP LSPs 149

Chapter 9 Miscellaneous MPLS Properties Configuration Guidelines 151

Configuring MPLS to Pop the Label on the Ultimate-Hop Router 151
Configuring Traffic Engineering for LSPs 152
Using RSVP and LDP Routes for Traffic Forwarding 152
Using RSVP and LDP Routes for Forwarding in VPNs 153
Using RSVP and LDP Routes for Forwarding But Not Route Selection 153
Advertising the LSP Metric in Summary LSAs 154
Enabling Interarea Traffic Engineering 154
Enabling Inter-AS Traffic Engineering for LSPs 155
Inter-AS Traffic Engineering Requirements 155
Inter-AS Traffic Engineering Limitations 156
Configuring OSPF Passive TE Mode 157
Configuring MPLS to Gather Statistics 158
Controlling MPLS System Log Messages and SNMP Traps 159
Configuring MPLS Firewall Filters and Policers 160
Configuring MPLS Firewall Filters 160
Examples: Configuring MPLS Firewall Filters 161
Configuring Policers for LSPs 162
LSP Policer Limitations 163
Example: Configuring an LSP Policer 163
Configuring Automatic Policers 164
Configuring Automatic Policers for LSPs 165
Configuring Automatic Policers for DiffServ-Traffic Engineering LSPs 165
Disabling Automatic Policing on an LSP 166
Example: Configuring Automatic Policers for LSPs 166
Writing Different DSCP and EXP Values in MPLS-Tagged IP Packets 167
Configuring MPLS Rewrite Rules 167
Rewriting the EXP Bits of All Three Labels of an Outgoing Packet 167
Rewriting MPLS and IPv4 Packet Headers 168
Configuring BFD for MPLS LSPs 169
Configuring BFD for RSVP LSPs 169
Pinging LSPs 170
Pinging an MPLS LSP 171
Pinging a P2MP LSP 171
Pinging an MPLS LSP Endpoint 171
Pinging a CCC LSP 171
Pinging a Layer 3 VPN 172
LSP Ping and Traceroute Based on RFC 4379 172
Tracing MPLS and LSP Packets and Operations 172

Chapter 10 **Summary of MPLS Configuration Statements** **175**

adaptive 175
adjust-interval 176
adjust-threshold 176
adjust-threshold-overflow-limit 177
admin-down 177
admin-group 178
    admin-group (for Interfaces) 178
    admin-group (for LSPs) 179
admin-groups 180
advertisement-hold-time 180
allow-fragmentation 181
associate-backup-pe-groups 181
auto-bandwidth 182
auto-policing 183
backup-pe-group 184
bandwidth 185
bandwidth-model 186
bandwidth-percent 187
bfd-liveness-detection 188
class-of-service 189
default-route 190
description 190
diffserv-te 191
disable 192
discard 192
double-push 193
encoding-type 193
exclude 194
    exclude (for Administrative Groups) 194
    exclude (for Fast Reroute) 195
expand-loose-hop 195
explicit-null 196
fast-reroute 196
fate-sharing 197
from 198
gpid 199
hop-limit 200
icmp-tunneling 200
include-all 201
    include-all (for Administrative Groups) 201
    include-all (for Fast Reroute) 202
include-any 203
    include-any (for Administrative Groups) 203
    include-any (for Fast Reroute) 204
install 204
interface 205
ipv6-tunneling 206
label-map 206
label-switched-path 207

ldp-tunneling 209
least-fill 210
link-protection 210
log-updown 211
lsp-attributes 212
maximum-bandwidth 212
metric 213
minimum-bandwidth 213
monitor-bandwidth 214
most-fill 214
mpls 214
mtu-signaling 215
next-hop 215
no-cspf 216
no-decrement-ttl 217
no-exclude 217
no-include-all 217
no-include-any 217
no-install-to-address 218
no-propagate-ttl 218
no-record 219
no-trap 219
oam 220
optimize-aggressive 220
optimize-timer 221
p2mp 222
p2mp-lsp-next-hop 222
path 223
path-mtu 224
policing 224
pop 225
preference 226
primary 227
priority 228
push 229
random 230
record 231
reject 231
retry-limit 232
retry-timer 232
revert-timer 233
rpf-check-policy 234
rsvp-error-hold-time 235
secondary 236
select 237
signal-bandwidth 237
smart-optimize-timer 238
soft-preemption 238
standby 239
static-path 240
statistics 241

swap 242
swap-push 243
switching-type 244
te-class-matrix 245
to 246
traceoptions 247
traffic-engineering 249
triple-push 250

Part 3 RSVP

Chapter 11 RSVP Overview 253

RSVP Standards 254
JUNOS Software RSVP Protocol Implementation 255
RSVP Operation 255
RSVP Operation Overview 255
RSVP Authentication 256
RSVP and IGP Hello Packets and Timers 256
RSVP Message Types 257
Path Messages 257
Resv Messages 257
PathTear Messages 258
ResvTear Messages 258
PathErr Messages 258
ResvErr Messages 258
ResvConfirm Messages 258
RSVP Reservation Styles 259
RSVP Refresh Reduction 259
MTU Signaling in RSVP 260
How the Correct MTU Is Signaled in RSVP 261
Determining an Outgoing MTU Value 262
MTU Signaling in RSVP Limitations 262
Link Protection 263
Fast Reroute, Node Protection, and Link Protection 263
Multiple Bypass LSPs 264
Node Protection 265
RSVP Graceful Restart 266
RSVP Graceful Restart Standard 266
RSVP Graceful Restart Terminology 266
RSVP Graceful Restart Operation 267
Processing the Restart Cap Object 268

Chapter 12 RSVP Configuration Guidelines 269

Minimum RSVP Configuration 271
Configuring RSVP and MPLS 271
Example: Configuring RSVP and MPLS 272

Configuring RSVP Interface Properties 273
Configuring RSVP Refresh Reduction 273
Determining the Refresh Reduction Capability of RSVP Neighbors 275
Configuring the RSVP Hello Interval 276
Configuring RSVP Authentication 276
Configuring the Bandwidth Subscription for Class Types 277
Configuring the RSVP Update Threshold on an Interface 277
Configuring RSVP for Unnumbered Interfaces 278
Configuring Node Protection or Link Protection 278
Configuring Node Protection or Link Protection on an LSP 279
Configuring Link Protection on the Interfaces Used by the LSPs 279
Configuring Bypass LSPs 280
Configuring Administrative Groups for Bypass LSPs 281
Configuring the Bandwidth for Bypass LSPs 282
Configuring the Class of Service for Bypass LSPs 282
Configuring the Hop Limit for Bypass LSPs 283
Configuring the Maximum Number of Bypass LSPs 283
Disabling CSPF for Bypass LSPs 284
Disabling Node Protection for Bypass LSPs 284
Configuring the Optimization Interval for Bypass LSPs 284
Configuring an Explicit Path for Bypass LSPs 285
Configuring the Amount of Bandwidth Subscribed for Bypass LSPs 285
Configuring Priority and Preemption for Bypass LSPs 286
Configuring RSVP Graceful Restart 286
Enabling Graceful Restart on the Router 286
Disabling Graceful Restart for RSVP 287
Disabling RSVP Helper Mode 287
Configuring the Maximum Helper Recovery Time 287
Configuring the Maximum Helper Restart Time 287
Configuring RSVP LSP Load Balancing 287
Configuring RSVP Timers 289
Preempting RSVP Sessions 290
Configuring MTU Signaling in RSVP 290
Enabling MTU Signaling in RSVP 291
Enabling Packet Fragmentation 291
Configuring RSVP to Pop the Label on the Ultimate-Hop Router 291
Disabling Adjacency Down and Neighbor Down Notification in IS-IS and OSPF 292
Enabling Ultimate-Hop Popping on Point-to-Multipoint LSPs 293
Tracing RSVP Protocol Traffic 294
Examples: Tracing RSVP Protocol Traffic 295

Chapter 13 Summary of RSVP Configuration Statements 297

admin-group 297
aggregate 298
authentication-key 299
bandwidth 300

bypass 301
class-of-service 302
disable 303
fast-reroute optimize-timer 304
graceful-deletion-timeout 304
graceful-restart 305
hello-interval 306
hop-limit 306
interface 307
keep-multiplier 308
link-protection 309
    link-protection (MPLS) 309
    link-protection (RSVP) 310
load-balance 311
max-bypasses 312
no-adjacency-down-notification 312
no-aggregate 313
no-cspf 313
no-neighbor-down-notification 313
no-p2mp-sublsp 314
no-reliable 314
node-link-protection 314
optimize-timer 315
path 316
peer-interface 317
preemption 318
priority 319
refresh-time 320
reliable 320
rsvp 321
soft-preemption 321
subscription 322
traceoptions 323
tunnel-services 325
update-threshold 325

Part 4 LDP

Chapter 14 LDP Overview 329

LDP Standards 329
JUNOS Software LDP Protocol Implementation 330
LDP Operation 330
LDP Label Filtering 331
Tunneling LDP LSPs in RSVP LSPs 331
    Tunneling LDP LSPs in RSVP LSPs Overview 331
    Label Operations 331

LDP Message Types 333
Discovery Messages 333
Session Messages 334
Advertisement Messages 334
Notification Messages 334
LDP Graceful Restart 334

Chapter 15 LDP Configuration Guidelines 337

Minimum LDP Configuration 339
Enabling and Disabling LDP 339
Configuring the LDP Hello Interval 339
Configuring the LDP Hold Time 340
Configuring the LDP Keepalive Interval 340
Configuring the LDP Keepalive Timeout 340
Configuring LDP Route Preferences 341
Configuring LDP Graceful Restart 341
Enabling Graceful Restart 341
Disabling LDP Graceful Restart or Helper Mode 342
Configuring Recovery Time and Maximum Recovery Time 342
Configuring LDP Received-Label Filtering 343
Examples: Configuring Received-Label Filtering 344
Configuring LDP Outbound-Label Filtering 345
Examples: Configuring Outbound-Label Filtering 346
Configuring LDP Transport Address Control 347
Configuring the LDP Egress Policy 347
Example: Configuring the LDP Egress Policy 348
Configuring FEC Deaggregation 348
Configuring Policers for LDP FECs 349
Configuring LDP IPv4 FEC Filtering 350
Configuring BFD for LDP LSPs 350
Configuring ECMP-Aware BFD for RSVP LSPs 351
Configuring LDP LSP Traceroute 352
Collecting LDP Statistics 353
LDP Statistics Output 353
Disabling LDP Statistics on the Penultimate-Hop Router 354
LDP Statistics Limitations 355
Tracing LDP Protocol Traffic 355
Tracing LDP Protocol Traffic at the Protocol and Routing Instance Levels 355
Tracing LDP Protocol Traffic Within FEC 356
Examples: Tracing LDP Protocol Traffic 357
Configuring Miscellaneous LDP Properties 358
Configuring LDP to Use the IGP Route Metric 358
Preventing Ingress Routes from Being Added to inet.0 358
Multiple-Instance LDP and Carrier-of-Carriers VPNs 359
Configuring MPLS and LDP to Pop the Label on the Ultimate-Hop Router 359
Enabling LDP over RSVP-Established LSPs 360

Enabling LDP over RSVP-Established LSPs in Heterogeneous Networks 360
Configuring the TCP MD5 Signature for an LDP Session 361
Disabling SNMP Traps for LDP 361
Enabling Strict Targeted Hellos 362
Configuring LDP Synchronization with the IGP 362
Configuring the Label Withdrawal Timer 363
Ignoring the LDP Subnet Check 363

Chapter 16 Summary of LDP Configuration Statements 365

allow-subnet-mismatch 365
authentication-key 366
bfd-liveness-detection 367
deaggregate 368
disable 369
ecmp 370
egress-policy 370
explicit-null 371
export 371
graceful-restart 372
hello-interval 372
helper-disable 373
hold-time 373
ignore-lsp-metrics 374
import 374
interface 375
keepalive-interval 376
keepalive-timeout 376
l2-smart-policy 377
label-withdrawal-delay 377
ldp 378
ldp-synchronization 378
log-updown 379
maximum-neighbor-recovery-time 379
no-deaggregate 380
no-forwarding 380
oam 381
periodic-traceroute 382
policing 383
preference 384
recovery-time 384
session 385
strict-targeted-hellos 385
traceoptions 386
track-igp-metric 388
traffic-statistics 389
transport-address 390

Part 5 CCC and TCC

Chapter 17 CCC and TCC Overview 393

CCC Overview 393
TCC Overview 394
CCC and TCC Graceful Restart 394

Chapter 18 CCC and TCC Configuration Guidelines 397

Configuring CCC 397
Configuring Layer 2 Switching Cross-Connects 397
Defining the Encapsulation for Layer 2 Switching Cross-Connects 398
Defining the CCC Connection for Layer 2 Switching Cross-Connects 402
Configuring MPLS 403
Example: Configuring Layer 2 Switching Cross-Connects 403
Configuring MPLS LSP Tunnel Cross-Connects 405
Defining the CCC Encapsulation for LSP Tunnel Cross-Connects 406
Defining the CCC Connection for LSP Tunnel Cross-Connects 408
Example: Configuring LSP Tunnel Cross-Connects 408
Configuring LSP Stitching Cross-Connects 409
Example: Configuring LSP Stitching Cross-Connects 410
Transmitting Nonstandard BPDUs 411
Configuring TCC 411
Defining the Encapsulation for the Layer 2 Switching TCCs 411
PPP and Cisco HDLC Encapsulation for Layer 2 Switching TCCs 412
ATM Encapsulation for Layer 2 Switching TCCs 412
Frame Relay Encapsulation for Layer 2 Switching TCCs 413
Ethernet Encapsulation for Layer 2 Switching TCCs 413
Ethernet Extended VLAN Encapsulation for Layer 2 Switching TCCs 414
ARP Configuration for Ethernet TCC Encapsulations 415
Defining the Connection for the Layer 2 Switching TCC 415
Configuring MPLS 416
Configuring CCC and TCC Graceful Restart 417
Configuring CCC Switching for Point-to-Multipoint LSPs 417
Configuring the Point-to-Multipoint LSP Switch on the Ingress PE Router 417
Configuring the Point-to-Multipoint LSP Switch on the Egress PE Router 418

Chapter 19 Summary of CCC and TCC Configuration Statements 421

connections 422
encapsulation 423
encapsulation (Logical Interface) 424
encapsulation (Physical Interface) 427
interface-switch 429
lsp-switch 430
p2mp-receive-switch 431
p2mp-transmit-switch 432
remote-interface-switch 433

Part 6 GMPLS

Chapter 20 GMPLS Overview 437

GMPLS Standards 437
Terms and Acronyms 438
Overview 439
GMPLS Operation 440
GMPLS and OSPF 441
GMPLS and CSPF 441
GMPLS Features 441

Chapter 21 GMPLS Configuration Guidelines 443

Configuring LMP 443
Configuring LMP Traffic Engineering Links 444
Configuring the Local IP Address for the Traffic Engineering Link 445
Configuring the Remote IP Address for the Traffic Engineering Link 445
Configuring the Remote ID for the Traffic Engineering Link 445
Configuring LMP Peers 446
Configuring the LMP Peer ID 447
Configuring the Control Channel Interface 447
Configuring the LMP Control Channel Interface for the Peer 447
Configuring the Remote IP Address for the LMP Control Channel 448
Configuring the Hello Message Attributes for the LMP Control Channel 448
Configuring Message Attributes for the LMP Control Channel 449
Configuring the Local Peer to Wait for the Remote Peer 450
Configuring the Traffic Engineering Link for the LMP Peer 450
Disabling the Traffic Engineering Link for the LMP Peer 450

Configuring Peer Interfaces in RSVP and OSPF 451
Configuring Peer Interfaces in RSVP 451
Configuring Peer Interfaces in OSPF 451
Configuring the Hello Interval for Peer Interfaces 452
Configuring MPLS Paths for GMPLS 452
Tracing LMP Traffic 452
Configuring MPLS LSPs for GMPLS 453
Configuring the Encoding Type 454
Configuring the GPID 454
Configuring the Signal Bandwidth Type 455
Configuring GMPLS Bidirectional LSPs 455
Allowing Non-Packet GMPLS LSPs to Establish Paths Through a JUNOS-based Router 455
Gracefully Tearing Down GMPLS LSPs 456
Temporarily Deleting a GMPLS LSP 456
Permanently Deleting a GMPLS LSP 456
Configuring the Graceful Deletion Timeout Interval 457

Chapter 22 RSVP LSP Hierarchy Configuration Guidelines 459

RSVP LSP Hierarchy Standard 459
RSVP LSP Hierarchy Terminology 459
RSVP LSP Hierarchy Overview 460
RSVP LSP Hierarchy 460
Advertising the Forwarding Adjacency with OSPF 460
Configuring the RSVP LSP Hierarchy 460
Configuring an RSVP LSP 461
Configuring a Forwarding Adjacency 461
Configuring the Local IP Address for the Forwarding Adjacency 461
Configuring the Remote IP Address for the Forwarding Adjacency 462
Configuring the LSP for the Forwarding Adjacency 462
Configuring RSVP for a Forwarding Adjacency 462
Advertising a Forwarding Adjacency Using OSPF 463

Chapter 23 Summary of GMPLS Configuration Statements 465

address 465
admin-down 465
control-channel 466
dead-interval 466
disable 467
disable (for GMPLS) 467
disable (for OSPF) 467
hello-dead-interval 468
hello-interval 469
hello-interval (for LMP) 469
hello-interval (for OSPF) 470
interface 470
label-switched-path 471

link-management 471
lmp-control-channel 472
lmp-protocol 472
local-address 473
passive 473
peer 474
peer-interface 475
peer-interface (for OSPF) 475
peer-interface (for RSVP) 475
remote-address 476
remote-address (for LMP Control Channel) 476
remote-address (for LMP Traffic Engineering) 476
remote-id 477
retransmission-interval 477
retransmit-interval 478
retry-limit 478
te-link 479
traceoptions 480
transit-delay 482

Part 7 Indexes

Index 485
Index of Statements and Commands 501

List of Figures

Figure 1: Label Encoding 26
Figure 2: Class-of-Service Bits 26
Figure 3: CSPF Computation Process 30
Figure 4: Aggregation Router A Dual-Homed on Core Routers B and C 32
Figure 5: Typical SPF Tree, Sourced from Router A 33
Figure 6: Modified SPF Tree, Using LSP A–D as a Shortcut 33
Figure 7: Modified SPF Tree, Using LSP A–D and LSP A–E as Shortcuts 34
Figure 8: IGP Shortcuts 35
Figure 9: IGP Shortcuts in a Bigger Network 35
Figure 10: SPF Computations with Advertised LSPs 36
Figure 11: MPLS Application Topology 39
Figure 12: How BGP Determines How to Reach Next-Hop Addresses 39
Figure 13: Routing and Forwarding Tables, traffic-engineering bgp 41
Figure 14: Routing and Forwarding Tables, traffic-engineering bgp-igp 42
Figure 15: Detours Established for an LSP Using Fast Reroute 44
Figure 16: Detour After the Link from Router B to Router C Fails 44
Figure 17: Detours Merging into Other Detours 45
Figure 18: Point-to-Multipoint LSPs 48
Figure 19: IPv6 Networks Linked by MPLS IPv4 Tunnels 108
Figure 20: Static MPLS Configuration 137
Figure 21: Link Protection Creating a Bypass LSP for the Protected Interface 263
Figure 22: Node Protection Creating a Next-Next-Hop Bypass LSP 265
Figure 23: Swap and Push When LDP LSPs Are Tunneled Through RSVP LSPs 332
Figure 24: Double Push When LDP LSPs Are Tunneled Through RSVP LSPs 333
Figure 25: TCC Example 394
Figure 26: Remote Interface Switch Connecting Two CE Routers Using CCC 395
Figure 27: Layer 2 Switching Cross-Connect 398
Figure 28: Topology of a Frame Relay Layer 2 Switching Cross-Connect 403
Figure 29: Sample Topology of a VLAN Layer 2 Switching Cross-Connect 404
Figure 30: MPLS LSP Tunnel Cross-Connect 405
Figure 31: Example Topology of MPLS LSP Tunnel Cross-Connect 408
Figure 32: LSP Stitching Cross-Connect 409
Figure 33: Example Topology of LSP Stitching Cross-Connect 410

List of Tables

Table 1: Notice Icons xxxiv
Table 2: Text and Syntax Conventions xxxiv
Table 3: Technical Documentation for Supported Routing Platforms xxxvi
Table 4: JUNOS Software Network Operations Guides xl
Table 5: JUNOS Software with Enhanced Services Documentation xli
Table 6: Additional Books Available Through
http://www.juniper.net/books xlii
Table 7: MPLS CoS Values 93
Table 8: Default Values for the Traffic Engineering Class Matrix 120
Table 9: One-to-One Backup Compared with Facility Backup 264
Table 10: RSVP Refresh Reduction Behavior 273
Table 11: from Operators That Apply to LDP Received-Label Filtering 343
Table 12: to Operators for LDP Outbound-Label Filtering 345

About This Guide

This preface provides the following guidelines for using the *JUNOS® Software MPLS Applications Configuration Guide*:

- Objectives on page xxxi
- Audience on page xxxi
- Supported Routing Platforms on page xxxii
- Using the Indexes on page xxxii
- Using the Examples in This Manual on page xxxii
- Documentation Conventions on page xxxiv
- List of Technical Publications on page xxxvi
- Documentation Feedback on page xliii
- Requesting Technical Support on page xliii

Objectives

This guide provides an overview of the MPLS applications functions of the JUNOS software and describes how to configure MPLS applications on the router.

NOTE: This guide documents Release 9.3 of the JUNOS software. For additional information about the JUNOS software—either corrections to or information that might have been omitted from this guide—see the software release notes at http://www.juniper.net/.

Audience

This guide is designed for network administrators who are configuring and monitoring a Juniper Networks M-series, MX-series, T-series, EX-series, or J-series routing platform.

To use this guide, you need a broad understanding of networks in general, the Internet in particular, networking principles, and network configuration. You must also be familiar with one or more of the following Internet routing protocols:

- Border Gateway Protocol (BGP)
- Distance Vector Multicast Routing Protocol (DVMRP)
- Intermediate System-to-Intermediate System (IS-IS)

- Internet Control Message Protocol (ICMP) router discovery
- Internet Group Management Protocol (IGMP)
- Multiprotocol Label Switching (MPLS)
- Open Shortest Path First (OSPF)
- Protocol-Independent Multicast (PIM)
- Resource Reservation Protocol (RSVP)
- Routing Information Protocol (RIP)
- Simple Network Management Protocol (SNMP)

Personnel operating the equipment must be trained and competent; must not conduct themselves in a careless, willfully negligent, or hostile manner; and must abide by the instructions provided by the documentation.

Supported Routing Platforms

For the features described in this manual, the JUNOS software currently supports the following routing platforms:

- J-series
- M-series
- MX-series
- T-series
- EX-series

Using the Indexes

This reference contains two indexes: a complete index that includes topic entries, and an index of statements and commands only.

In the index of statements and commands, an entry refers to a statement summary section only. In the complete index, the entry for a configuration statement or command contains at least two parts:

- The primary entry refers to the statement summary section.
- The secondary entry, *usage guidelines,* refers to the section in a configuration guidelines chapter that describes how to use the statement or command.

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the load merge or the load merge relative command. These commands cause the software to merge the incoming configuration into the current candidate configuration. If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the load merge command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the load merge relative command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file ex-script.conf. Copy the ex-script.conf file to the /var/tmp directory on your routing platform.

   ```
   system {
       scripts {
           commit {
               file ex-script.xsl;
           }
       }
   }
   interfaces {
       fxp0 {
           disable;
           unit 0 {
               family inet {
                   address 10.0.0.1/24;
               }
           }
       }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the load merge configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file ex-script-snippet.conf. Copy the ex-script-snippet.conf file to the /var/tmp directory on your routing platform.

   ```
   commit {
   ```

```
file ex-script-snippet.xsl; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the load merge relative configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the load command, see the *JUNOS CLI User Guide*.

Documentation Conventions

Table 1 on page xxxiv defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xxxiv defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> **configure**

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host> show chassis alarms` `No alarms currently active`
Italic text like this	■ Introduces important new terms. ■ Identifies book names. ■ Identifies RFC and Internet draft titles.	■ A policy *term* is a named structure that defines match conditions and actions. ■ *JUNOS System Basics Configuration Guide* ■ RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Plain text like this	Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components.	■ To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. ■ The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	stub <default-metric *metric*>;
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast | multicast (*string1* | *string2* | *string3*)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [*community-ids*]

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	■ In the Logical Interfaces box, select **All Interfaces**. ■ To cancel the configuration, click **Cancel**.

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select **Protocols > Ospf**.

List of Technical Publications

Table 3 on page xxxvi lists the software and hardware guides and release notes for Juniper Networks J-series, M-series, MX-series, and T-series routing platforms and describes the contents of each document. Table 4 on page xl lists the books included in the *Network Operations Guide* series. Table 5 on page xli lists the manuals and release notes supporting JUNOS software with enhanced services. All documents are available at http://www.juniper.net/techpubs/.

Table 6 on page xlii lists additional books on Juniper Networks solutions that you can order through your bookstore. A complete list of such books is available at http://www.juniper.net/books.

Table 3: Technical Documentation for Supported Routing Platforms

Book	Description
JUNOS Software for Supported Routing Platforms	
Access Privilege	Explains how to configure access privileges in user classes by using permission flags and regular expressions. Lists the permission flags along with their associated command-line interface (CLI) operational mode commands and configuration statements.
Class of Service	Provides an overview of the class-of-service (CoS) functions of the JUNOS software and describes how to configure CoS features, including configuring multiple forwarding classes for transmitting packets, defining which packets are placed into each output queue, scheduling the transmission service level for each queue, and managing congestion through the random early detection (RED) algorithm.
CLI User Guide	Describes how to use the JUNOS command-line interface (CLI) to configure, monitor, and manage Juniper Networks routing platforms. This material was formerly covered in the *JUNOS System Basics Configuration Guide*.
Feature Guide	Provides a detailed explanation and configuration examples for several of the most complex features in the JUNOS software.
High Availability	Provides an overview of hardware and software resources that ensure a high level of continuous routing platform operation and describes how to configure high availability (HA) features such as nonstop active routing (NSR) and graceful Routing Engine switchover (GRES).
MPLS Applications	Provides an overview of traffic engineering concepts and describes how to configure traffic engineering protocols.

Table 3: Technical Documentation for Supported Routing Platforms *(continued)*

Book	Description
Multicast Protocols	Provides an overview of multicast concepts and describes how to configure multicast routing protocols.
Multiplay Solutions	Describes how you can deploy IPTV and voice over IP (VoIP) services in your network.
MX-series Layer 2 Configuration Guide	Provides an overview of the Layer 2 functions of the MX-series routers, including configuring bridging domains, MAC address and VLAN learning and forwarding, and spanning-tree protocols. It also details the routing instance types used by Layer 2 applications. All of this material was formerly covered in the *JUNOS Routing Protocols Configuration Guide*.
MX-series Layer 2 Solutions Guide	Describes common configuration scenarios for the Layer 2 features supported on the MX-series routers, including basic bridged VLANs with normalized VLAN tags, aggregated Ethernet links, bridge domains, Multiple Spanning Tree Protocol (MSTP), and integrated routing and bridging (IRB).
Network Interfaces	Provides an overview of the network interface functions of the JUNOS software and describes how to configure the network interfaces on the routing platform.
Network Management	Provides an overview of network management concepts and describes how to configure various network management features, such as SNMP and accounting options.
Policy Framework	Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, and forwarding options.
Protected System Domain	Provides an overview of the JCS 1200 platform and the concept of Protected System Domains (PSDs). The JCS 1200 platform, which contains up to six redundant pairs of Routing Engines running JUNOS software, is connected to a T320 router or to a T640 or T1600 routing node. To configure a PSD, you assign any number of Flexible PIC concentrators (FPCs) in the T-series routing platform to a pair of Routing Engines on the JCS 1200 platform. Each PSD has the same capabilities and functionality as a physical router, with its own control plane, forwarding plane, and administration.
Routing Protocols	Provides an overview of routing concepts and describes how to configure routing instances, and unicast routing protocols.
Secure Configuration Guide for Common Criteria and JUNOS-FIPS	Provides an overview of secure Common Criteria and JUNOS-FIPS protocols for the JUNOS software and describes how to install and configure secure Common Criteria and JUNOS-FIPS on a routing platform.
Services Interfaces	Provides an overview of the services interfaces functions of the JUNOS software and describes how to configure the services interfaces on the router.
Software Installation and Upgrade Guide	Describes the JUNOS software components and packaging and explains how to initially configure, reinstall, and upgrade the JUNOS system software. This material was formerly covered in the *JUNOS System Basics Configuration Guide*.

Table 3: Technical Documentation for Supported Routing Platforms *(continued)*

Book	Description
Subscriber Access	Provides an overview of the subscriber access features of the JUNOS software and describes how to configure subscriber access support on the router, including dynamic profiles, class of service, AAA, and access methods.
System Basics	Describes Juniper Networks routing platforms and explains how to configure basic system parameters, supported protocols and software processes, authentication, and a variety of utilities for managing your router on the network.
VPNs	Provides an overview and describes how to configure Layer 2 and Layer 3 virtual private networks (VPNs), virtual private LAN service (VPLS), and Layer 2 circuits. Provides configuration examples.
JUNOS References	
Hierarchy and RFC Reference	Describes the JUNOS configuration mode commands. Provides a hierarchy reference that displays each level of a configuration hierarchy, and includes all possible configuration statements that can be used at that level. This material was formerly covered in the *JUNOS System Basics Configuration Guide*.
Interfaces Command Reference	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot interfaces.
Routing Protocols and Policies Command Reference	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot routing policies and protocols, including firewall filters.
System Basics and Services Command Reference	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot system basics, including commands for real-time monitoring and route (or path) tracing, system software management, and chassis management. Also describes commands for monitoring and troubleshooting services such as class of service (CoS), IP Security (IPsec), stateful firewalls, flow collection, and flow monitoring.
System Log Messages Reference	Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message.
J-Web User Guide	
J-Web Interface User Guide	Describes how to use the J-Web graphical user interface (GUI) to configure, monitor, and manage Juniper Networks routing platforms.
JUNOS API and Scripting Documentation	
JUNOScript API Guide	Describes how to use the JUNOScript application programming interface (API) to monitor and configure Juniper Networks routing platforms.
JUNOS XML API Configuration Reference	Provides reference pages for the configuration tag elements in the JUNOS XML API.

Table 3: Technical Documentation for Supported Routing Platforms *(continued)*

Book	Description
JUNOS XML API Operational Reference	Provides reference pages for the operational tag elements in the JUNOS XML API.
NETCONF API Guide	Describes how to use the NETCONF API to monitor and configure Juniper Networks routing platforms.
JUNOS Configuration and Diagnostic Automation Guide	Describes how to use the commit script and self-diagnosis features of the JUNOS software. This guide explains how to enforce custom configuration rules defined in scripts, how to use commit script macros to provide simplified aliases for frequently used configuration statements, and how to configure diagnostic event policies.
Hardware Documentation	
Hardware Guide	Describes how to install, maintain, and troubleshoot routing platforms and components. Each platform has its own hardware guide.
PIC Guide	Describes the routing platform's Physical Interface Cards (PICs). Each platform has its own PIC guide.
DPC Guide	Describes the Dense Port Concentrators (DPCs) for all MX-series routers.
JUNOScope Documentation	
JUNOScope Software User Guide	Describes the JUNOScope software graphical user interface (GUI), how to install and administer the software, and how to use the software to manage routing platform configuration files and monitor routing platform operations.
Advanced Insight Solutions (AIS) Documentation	
Advanced Insight Solutions Guide	Describes the Advanced Insight Manager (AIM) application, which provides a gateway between JUNOS devices and Juniper Support Systems (JSS) for case management and intelligence updates. Explains how to run AI-Scripts on Juniper Networks devices.
J-series Routing Platform Documentation	
Getting Started Guide	Provides an overview, basic instructions, and specifications for J-series routing platforms. The guide explains how to prepare your site for installation, unpack and install the router and its components, install licenses, and establish basic connectivity. Use the *Getting Started Guide* for your router model.
Basic LAN and WAN Access Configuration Guide	Explains how to configure the interfaces on J-series Services Routers for basic IP routing with standard routing protocols, ISDN backup, and digital subscriber line (DSL) connections.
Advanced WAN Access Configuration Guide	Explains how to configure J-series Services Routers in virtual private networks (VPNs) and multicast networks, configure data link switching (DLSw) services, and apply routing techniques such as policies, stateless and stateful firewall filters, IP Security (IPsec) tunnels, and class-of-service (CoS) classification for safer, more efficient routing.

Table 3: Technical Documentation for Supported Routing Platforms *(continued)*

Book	Description
Administration Guide	Shows how to manage users and operations, monitor network performance, upgrade software, and diagnose common problems on J-series Services Routers.
Release Notes	
JUNOS Release Notes	Summarize new features and known problems for a particular software release, provide corrections and updates to published JUNOS, JUNOScript, and NETCONF manuals, provide information that might have been omitted from the manuals, and describe upgrade and downgrade procedures.
Hardware Release Notes	Describe the available documentation for the routing platform and summarize known problems with the hardware and accompanying software. Each platform has its own release notes.
JUNOScope Release Notes	Contain corrections and updates to the published JUNOScope manual, provide information that might have been omitted from the manual, and describe upgrade and downgrade procedures.
AIS Release Notes	Summarize AIS new features and guidelines, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide initial setup, upgrade, and downgrade procedures.
AIS AI-Scripts Release Notes	Summarize AI-Scripts new features, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide instructions for automatic and manual installation, including deleting and rolling back.
J-series Services Router Release Notes	Briefly describe Services Router features, identify known hardware problems, and provide upgrade and downgrade instructions.

Table 4: JUNOS Software Network Operations Guides

Book	Description
Baseline	Describes the most basic tasks for running a network using Juniper Networks products. Tasks include upgrading and reinstalling JUNOS software, gathering basic system management information, verifying your network topology, and searching log messages.
Interfaces	Describes tasks for monitoring interfaces. Tasks include using loopback testing and locating alarms.
MPLS	Describes tasks for configuring, monitoring, and troubleshooting an example MPLS network. Tasks include verifying the correct configuration of the MPLS and RSVP protocols, displaying the status and statistics of MPLS running on all routing platforms in the network, and using the layered MPLS troubleshooting model to investigate problems with an MPLS network.

Table 4: JUNOS Software Network Operations Guides *(continued)*

Book	Description
MPLS Log Reference	Describes MPLS status and error messages that appear in the output of the show mpls lsp extensive command. The guide also describes how and when to configure Constrained Shortest Path First (CSPF) and RSVP trace options, and how to examine a CSPF or RSVP failure in a sample network.
MPLS Fast Reroute	Describes operational information helpful in monitoring and troubleshooting an MPLS network configured with fast reroute (FRR) and load balancing.
Hardware	Describes tasks for monitoring M-series and T-series routing platforms.

To configure and operate a J-series Services Router running JUNOS software with enhanced services, you must also use the configuration statements and operational mode commands documented in JUNOS configuration guides and command references. To configure and operate a WX Integrated Services Module, you must also use WX documentation.

Table 5: JUNOS Software with Enhanced Services Documentation

Book	Description
All Platforms	
JUNOS Software Interfaces and Routing Configuration Guide	Explains how to configure J-series interfaces for basic IP routing with standard routing protocols, ISDN service, firewall filters (access control lists), and class-of-service (CoS) traffic classification.
JUNOS Software Security Configuration Guide	Explains how to configure and manage security services such as stateful firewall policies, IP Security (IPsec) virtual private networks (VPNs), firewall screens, Network Address Translation (NAT), Public Key Cryptography, and Application Layer Gateways (ALGs).
JUNOS Software Administration Guide	Shows how to monitor J-series devices and routing operations, firewall and security services, system alarms and events, and network performance. This guide also shows how to administer user authentication and access, upgrade software, and diagnose common problems.
JUNOS Software CLI Reference	Provides the complete JUNOS software with enhanced services configuration hierarchy and describes the configuration statements and operational mode commands not documented in the standard JUNOS manuals.
J-series Only	
JUNOS Software with Enhanced Services Design and Implementation Guide	Provides guidelines and examples for designing and implementing IPsec VPNs), firewalls, and routing on J-series Services Routers running JUNOS software with enhanced services.

Table 5: JUNOS Software with Enhanced Services Documentation *(continued)*

Book	Description
JUNOS Software with Enhanced Services Quick Start	Explains how to quickly set up a J-series Services Router. This document contains router declarations of conformity.
JUNOS Software with Enhanced Services J-series Services Router Hardware Guide	Provides an overview, basic instructions, and specifications for J-series Services Routers. This guide explains how to prepare a site, unpack and install the router, replace router hardware, and establish basic router connectivity. This guide contains hardware descriptions and specifications.
JUNOS Software with Enhanced Services Migration Guide	Provides instructions for migrating an SSG device running ScreenOS software or a J-series Services Router running the JUNOS software to JUNOS software with enhanced services.
WXC Integrated Services Module Installation and Configuration Guide	Explains how to install and initially configure a WXC Integrated Services Module in a J-series Services Router for application acceleration.
JUNOS Software with Enhanced Services Release Notes	Summarizes new features and known problems for a particular release of JUNOS software with enhanced services on J-series Services Routers, including J-Web interface features and problems. The release notes also contain corrections and updates to the manuals and software upgrade and downgrade instructions for JUNOS software with enhanced services.

Table 6: Additional Books Available Through http://www.juniper.net/books

Book	Description
Interdomain Multicast Routing	Provides background and in-depth analysis of multicast routing using Protocol Independent Multicast sparse mode (PIM SM) and Multicast Source Discovery Protocol (MSDP); details any-source and source-specific multicast delivery models; explores multiprotocol BGP (MBGP) and multicast IS-IS; explains Internet Gateway Management Protocol (IGMP) versions 1, 2, and 3; lists packet formats for IGMP, PIM, and MSDP; and provides a complete glossary of multicast terms.
JUNOS Cookbook	Provides detailed examples of common JUNOS software configuration tasks, such as basic router configuration and file management, security and access control, logging, routing policy, firewalls, routing protocols, MPLS, and VPNs.
MPLS-Enabled Applications	Provides an overview of Multiprotocol Label Switching (MPLS) applications (such as Layer 3 virtual private networks [VPNs], Layer 2 VPNs, virtual private LAN service [VPLS], and pseudowires), explains how to apply MPLS, examines the scaling requirements of equipment at different points in the network, and covers the following topics: point-to-multipoint label switched paths (LSPs), DiffServ-aware traffic engineering, class of service, interdomain traffic engineering, path computation, route target filtering, multicast support for Layer 3 VPNs, and management and troubleshooting of MPLS networks.
OSPF and IS-IS: Choosing an IGP for Large-Scale Networks	Explores the full range of characteristics and capabilities for the two major link-state routing protocols: Open Shortest Path First (OSPF) and IS-IS. Explains architecture, packet types, and addressing; demonstrates how to improve scalability; shows how to design large-scale networks for maximum security and reliability; details protocol extensions for MPLS-based traffic engineering, IPv6, and multitopology routing; and covers troubleshooting for OSPF and IS-IS networks.

Table 6: Additional Books Available Through http://www.juniper.net/books *(continued)*

Book	Description
Routing Policy and Protocols for Multivendor IP Networks	Provides a brief history of the Internet, explains IP addressing and routing (Routing Information Protocol [RIP], OSPF, IS-IS, and Border Gateway Protocol [BGP]), explores ISP peering and routing policies, and displays configurations for both Juniper Networks and other vendors' routers.
The Complete IS-IS Protocol	Provides the insight and practical solutions necessary to understand the IS-IS protocol and how it works by using a multivendor, real-world approach.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version (not required for *Network Operations Guides [NOGs])*

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at http://www.juniper.net/customers/support/downloads/710059.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/

- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool located at https://tools.juniper.net/SerialNumberEntitlementSearch/.

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/ .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at http://www.juniper.net/support/requesting-support.html.

Part 1
Overview

- Traffic Engineering Overview on page 3
- Complete MPLS Applications Configuration Mode Statements on page 9

Chapter 1

Traffic Engineering Overview

The task of mapping traffic flows onto an existing physical topology is called *traffic engineering*. Traffic engineering provides the ability to move traffic flow away from the shortest path selected by the interior gateway protocol (IGP) and onto a potentially less congested physical path across a network.

Traffic engineering provides the capabilities to do the following:

- Route primary paths around known bottlenecks or points of congestion in the network.
- Provide precise control over how traffic is rerouted when the primary path is faced with single or multiple failures.
- Provide more efficient use of available aggregate bandwidth and long-haul fiber by ensuring that subsets of the network do not become overutilized while other subsets of the network along potential alternate paths are underutilized.
- Maximize operational efficiency.
- Enhance the traffic-oriented performance characteristics of the network by minimizing packet loss, minimizing prolonged periods of congestion, and maximizing throughput.
- Enhance statistically bound performance characteristics of the network (such as loss ratio, delay variation, and transfer delay) required to support a multiservices Internet.

This chapter discusses the following topics:

- Components of Traffic Engineering on page 3
- Flexible LSP Calculation and Configuration on page 7

Components of Traffic Engineering

In the JUNOS software, traffic engineering is implemented with Multiprotocol Label Switching (MPLS) and the Resource Reservation Protocol (RSVP). Traffic engineering is composed of four functional components:

- Packet Forwarding Component on page 4
- Information Distribution Component on page 5
- Path Selection Component on page 5
- Signaling Component on page 6

Packet Forwarding Component

The packet forwarding component of the JUNOS traffic engineering architecture is MPLS, which is responsible for directing a flow of IP packets along a predetermined path across a network. This path is called a *label-switched path (LSP)*. LSPs are simplex; that is, the traffic flows in one direction from the head-end (ingress) router to a tail-end (egress) router. Duplex traffic requires two LSPs: one LSP to carry traffic in each direction. An LSP is created by the concatenation of one or more label-switched hops, allowing a packet to be forwarded from one router to another across the MPLS domain.

When an ingress router receives an IP packet, it adds an MPLS header to the packet and forwards it to the next router in the LSP. The labeled packet is forwarded along the LSP by each router until it reaches the tail end of the LSP, the egress router. At this point the MPLS header is removed, and the packet is forwarded based on Layer 3 information such as the IP destination address. The value of this scheme is that the physical path of the LSP is not limited to what the IGP would choose as the shortest path to reach the destination IP address.

This section discusses the following topics:

- Packet Forwarding Based on Label Swapping on page 4
- How a Packet Traverses an MPLS Backbone on page 4

Packet Forwarding Based on Label Swapping

The packet forwarding process at each router is based on the concept of label swapping. This concept is similar to what occurs at each Asynchronous Transfer Mode (ATM) switch in a permanent virtual circuit (PVC). Each MPLS packet carries a 4-byte encapsulation header that contains a 20-bit, fixed-length label field. When a packet containing a label arrives at a router, the router examines the label and copies it as an index to its MPLS forwarding table. Each entry in the forwarding table contains an interface-inbound label pair mapped to a set of forwarding information that is applied to all packets arriving on the specific interface with the same inbound label.

How a Packet Traverses an MPLS Backbone

This section describes how an IP packet is processed as it traverses an MPLS backbone network.

At the entry edge of the MPLS backbone, the IP header is examined by the ingress router. Based on this analysis, the packet is classified, assigned a label, encapsulated in an MPLS header, and forwarded toward the next hop in the LSP. MPLS provides a high degree of flexibility in the way that an IP packet can be assigned to an LSP. For example, in the JUNOS traffic engineering implementation, all packets arriving at the ingress router that are destined to exit the MPLS domain at the same egress router are forwarded along the same LSP.

Once the packet begins to traverse the LSP, each router uses the label to make the forwarding decision. The MPLS forwarding decision is made independently of the original IP header: the incoming interface and label are used as lookup keys into the MPLS forwarding table. The old label is replaced with a new label, and the packet is

forwarded to the next hop along the LSP. This process is repeated at each router in the LSP until the packet reaches the egress router.

When the packet arrives at the egress router, the label is removed and the packet exits the MPLS domain. The packet is then forwarded based on the destination IP address contained in the packet's original IP header according to the traditional shortest path calculated by the IP routing protocol.

Information Distribution Component

Traffic engineering requires detailed knowledge about the network topology as well as dynamic information about network loading. To implement the information distribution component, simple extensions to the IGPs are defined. Link attributes are included as part of each router's link-state advertisement. IS-IS extensions include the definition of new type length values (TLVs), whereas Open Shortest Path First (OSPF) extensions are implemented with opaque link-state advertisements (LSAs). The standard flooding algorithm used by the link-state IGPs ensures that link attributes are distributed to all routers in the routing domain. Some of the traffic engineering extensions to be added to the IGP link-state advertisement include maximum link bandwidth, maximum reserved link bandwidth, current bandwidth reservation, and link coloring.

Each router maintains network link attributes and topology information in a specialized traffic engineering database (TED). The TED is used exclusively for calculating explicit paths for the placement of LSPs across the physical topology. A separate database is maintained so that the subsequent traffic engineering computation is independent of the IGP and the IGP's link-state database. Meanwhile, the IGP continues its operation without modification, performing the traditional shortest-path calculation based on information contained in the router's link-state database.

Path Selection Component

After network link attributes and topology information are flooded by the IGP and placed in the TED, each ingress router uses the TED to calculate the paths for its own set of LSPs across the routing domain. The path for each LSP can be represented by either a strict or loose explicit route. An explicit route is a preconfigured sequence of routers that should be part of the physical path of the LSP. If the ingress router specifies all the routers in the LSP, the LSP is said to be identified by a strict explicit route. If the ingress router specifies only some of the routers in the LSP, the LSP is described as a loose explicit route. Support for strict and loose explicit routes allows the path selection process to be given broad latitude whenever possible, but to be constrained when necessary.

The ingress router determines the physical path for each LSP by applying a Constrained Shortest Path First (CSPF) algorithm to the information in the TED. CSPF is a shortest-path-first algorithm that has been modified to take into account specific restrictions when the shortest path across the network is calculated. Input into the CSPF algorithm includes:

- Topology link-state information learned from the IGP and maintained in the TED

- Attributes associated with the state of network resources (such as total link bandwidth, reserved link bandwidth, available link bandwidth, and link color) that are carried by IGP extensions and stored in the TED
- Administrative attributes required to support traffic traversing the proposed LSP (such as bandwidth requirements, maximum hop count, and administrative policy requirements) that are obtained from user configuration

As CSPF considers each candidate node and link for a new LSP, it either accepts or rejects a specific path component based on resource availability or whether selecting the component violates user policy constraints. The output of the CSPF calculation is an explicit route consisting of a sequence of router addresses that provides the shortest path through the network that meets the constraints. This explicit route is then passed to the signaling component, which establishes the forwarding state in the routers along the LSP.

Offline Planning and Analysis

Despite the reduced management effort resulting from online path calculation, an offline planning and analysis tool is still required to optimize traffic engineering globally. Online calculation takes resource constraints into account and calculates one LSP at a time. The challenge with this approach is that it is not deterministic. The order in which LSPs are calculated plays a critical role in determining each LSP's physical path across the network. LSPs that are calculated early in the process have more resources available to them than LSPs calculated later in the process because previously calculated LSPs consume network resources. If the order in which the LSPs are calculated is changed, the resulting set of physical paths for the LSPs also can change.

An offline planning and analysis tool simultaneously examines each link's resource constraints and the requirements of each LSP. Although the offline approach can take several hours to complete, it performs global calculations, compares the results of each calculation, and then selects the best solution for the network as a whole. The output of the offline calculation is a set of LSPs that optimizes utilization of network resources. After the offline calculation is completed, the LSPs can be established in any order because each is installed according to the rules for the globally optimized solution.

Signaling Component

An LSP is not known to be workable until it is actually established by the signaling component. The signaling component, which is responsible for establishing LSP state and distributing labels, relies on a number of extensions to RSVP:

- The Explicit Route object allows an RSVP path message to traverse an explicit sequence of routers that is independent of conventional shortest-path IP routing. The explicit route can be either strict or loose.
- The Label Request object permits the RSVP path message to request that intermediate routers provide a label binding for the LSP that it is establishing.
- The Label object allows RSVP to support the distribution of labels without changing its existing mechanisms. Because the RSVP Resv message follows the reverse

path of the RSVP path message, the Label object supports the distribution of labels from downstream nodes to upstream nodes.

Flexible LSP Calculation and Configuration

Traffic engineering involves mapping traffic flow onto a physical topology. You can determine the paths online using constraint-based routing. Regardless of how the physical path is calculated, the forwarding state is installed across the network through RSVP.

The JUNOS software supports the following ways to route and configure an LSP:

- You can calculate the full path for the LSP offline and individually configure each router in the LSP with the necessary static forwarding state. This is analogous to the way some Internet service providers (ISPs) configure their IP-over-ATM cores.
- You can calculate the full path for the LSP offline and statically configure the ingress router with the full path. The ingress router then uses RSVP as a dynamic signaling protocol to install a forwarding state in each router along the LSP.
- You can rely on constraint-based routing to perform dynamic online LSP calculation. You configure the constraints for each LSP; then the network itself determines the path that best meets those constraints. Specifically, the ingress router calculates the entire LSP based on the constraints and then initiates signaling across the network.
- You can calculate a partial path for an LSP offline and statically configure the ingress router with a subset of the routers in the path; then you can permit online calculation to determine the complete path.

  For example, consider a topology that includes two east-west paths across the United States: one in the north through Chicago and one in the south through Dallas. If you want to establish an LSP between a router in New York and one in San Francisco, you can configure the partial path for the LSP to include a single loose-routed hop of a router in Dallas. The result is an LSP routed along the southern path. The ingress router uses CSPF to compute the complete path and RSVP to install the forwarding state along the LSP.
- You can configure the ingress router with no constraints whatsoever. In this case, normal IGP shortest-path routing is used to determine the path of the LSP. This configuration does not provide any value in terms of traffic engineering. However, it is easy and might be useful in situations when services such as virtual private networks (VPNs) are needed.

In all these cases, you can specify any number of LSPs as backups for the primary LSP, thus allowing you to combine more than one configuration approach. For example, you might explicitly compute the primary path offline, set the secondary path to be constraint-based, and have the tertiary path be unconstrained. If a circuit on which the primary LSP is routed fails, the ingress router notices the outage from error notifications received from a downstream router or by the expiration of RSVP soft-state information. Then the router dynamically forwards traffic to a hot-standby LSP or calls on RSVP to create a forwarding state for a new backup LSP.

Chapter 2

Complete MPLS Applications Configuration Mode Statements

This chapter shows the complete configuration statement hierarchy for the Multiprotocol Label Switching (MPLS) applications configuration statements, listing all possible configuration statements and showing their level in the configuration hierarchy. When you are configuring the JUNOS software, your current hierarchy level is shown in the banner on the line preceding the user@host# prompt.

For a complete list of the JUNOS configuration statements, see the *JUNOS Hierarchy and RFC Reference*.

This chapter is organized as follows:

- [edit logical-systems] Hierarchy Level on page 9
- [edit protocols connections] Hierarchy Level on page 10
- [edit protocols ldp] Hierarchy Level on page 11
- [edit protocols link-management] Hierarchy Level on page 12
- [edit protocols mpls] Hierarchy Level on page 12
- [edit protocols rsvp] Hierarchy Level on page 16

[edit logical-systems] Hierarchy Level

The following MPLS protocol statements can be configured at the [edit logical-systems] hierarchy level. This is not a comprehensive list of statements available for logical routers. Only the statements that are also documented in this manual are listed here. For more information about logical routers, see the *JUNOS Routing Protocols Configuration Guide*.

NOTE: Beginning with JUNOS software Release 9.3, the logical router feature has been renamed logical system.

All configuration statements, operational commands, show command outputs, error messages, log messages, and SNMP MIB objects that contain the string logical-router or logical-routers have been changed to logical-system and logical-systems, respectively.

```
logical-systems {
   logical-system-name {
      protocols {
         connections {
            connections-configuration;
         }
         ldp {
            ldp-configuration;
         }
         link-management {
            link-management-configuration;
         }
         mpls {
            mpls-configuration;
         }
         rsvp {
            rsvp-configuration;
         }
      }
   }
}
```

[edit protocols connections] Hierarchy Level

The following statements can also be configured at the [edit logical-systems *logical-system-name*] hierarchy level:

```
protocols {
   connections {
      interface-switch connection-name {
         interface first-interface-name.unit-number;
         interface second-interface-name.unit-number;
      }
      lsp-switch connection-name {
         transmit-lsp label-switched-path;
         receive-lsp label-switched-path;
      }
      p2mp-receive-switch {
         output-interface interface-name.unit-number;
         receive-p2mp-lsp receiving-point-to-multipoint-lsp;
      }
      p2mp-transmit-switch {
         input-interface input-interface-name.unit-number;
         transmit-p2mp-lsp transmitting-point-to-multipoint-lsp;
      }
      remote-interface-switch connection-name {
         interface interface-name.unit-number;
         transmit-lsp label-switched-path;
         receive-lsp label-switched-path;
      }
   }
}
```

[edit protocols ldp] Hierarchy Level

The following statements can also be configured at the [edit logical-systems *logical-system-name*] hierarchy level:

```
protocols {
    ldp {
        (deaggregate | no-deaggregate);
        egress-policy [ policy-names ];
        explicit-null;
        export [ policy-names ];
        graceful-restart {
            disable;
            helper-disable;
            maximum-neighbor-recovery-time seconds;
            recovery-time seconds;
        }
        import [ policy-names];
        interface (interface-name | all) {
            disable;
            hello-interval seconds;
            hold-time seconds;
            transport-address (interface | router-id);
        }
        keepalive-interval seconds;
        keepalive-timeout seconds;
        log-updown {
            trap disable;
        }
        no-forwarding;
        policing {
            fec fec-address {
                ingress-traffic filter-name;
                transit-traffic filter-name;
            }
        }
        preference preference;
        session address {
            authentication-key md5-authentication-key;
        }
        strict-targeted-hellos;
        traceoptions {
            file filename <replace> <size size> <files number> <no-stamp>
                <world-readable | no-world-readable>;
            flag flag <flag-modifier> <disable>;
        }
        track-igp-metric;
        traffic-statistics {
            file filename <replace> <size size> <files number> <no-stamp>
                <world-readable | no-world-readable>;
            interval interval;
            no-penultimate-hop;
        }
        transport-address (address | interface | router-id);
    }
```

```
}
```

[edit protocols link-management] Hierarchy Level

The following statements can also be configured at the [edit logical-systems *logical-system-name*] hierarchy level:

```
protocols {
   link-management {
      peer peer-name {
         address address;
         control-channel [ control-channel-interfaces ];
         te-link [te-link-names];
      }
      te-link te-link-name {
         disable;
         interface interface-name {
            disable;
            local-address address;
            remote-address address;
            remote-id id-number;
         }
         label-switched-path label-switched-path-name;
         local-address address;
         remote-address address;
         remote-id id-number;
      }
      traceoptions {
         file filename <files number> <no-stamp> <replace> <size size>
            <world-readable | no-world-readable>;
         flag flag <flag-modifier> <disable>;
      }
   }
}
```

[edit protocols mpls] Hierarchy Level

The following statements can also be configured at the [edit logical-systems *logical-system-name*] hierarchy level:

```
protocols {
   mpls {
      disable;
      admin-group {
         exclude [ group-names];
         include-all [ group-names];
         include-any [ group-names];
      }
      admin-groups {
         group-name group-value;
      }
      advertisement-hold-time seconds;
      auto-policing {
         class all (drop | loss-priority-high | loss-priority-low);
```

```
    class ctnumber (drop | loss-priority-high | loss-priority-low);
}
bandwidth bps {
    ct0 bps;
    ct1 bps;
    ct2 bps;
    ct3 bps;
}
class-of-service cos-value;
diffserv-te {
    bandwidth-model {
        extended-mam;
        mam;
        rdm;
    }
    te-class-matrix {
        tenumber {
            priority priority;
            traffic-class ctnumber priority priority;
        }
    }
}
explicit-null;
hop-limit number;
icmp-tunneling;
interface (interface-name | all) {
    disable;
    admin-group [group-names];
    label-map (default-route | in-label-name) {
        class-of-service cos-value;
        next-hop (address| interface-name | address/interface-name) | (discard | reject);
        (pop | swap out-label);
        preference preference;
        swap-push swap-label push-label;
    }
}
ipv6-tunneling;
label-switched-path lsp-name{
    disable;
    adaptive;
    admin-down;
    admin-group {
        exclude [ group-names ];
        include-all;
        include-any [ group-names ];
    }
    auto-bandwidth {
        adjust-interval seconds;
        adjust-threshold percent;
        maximum-bandwidth bps;
        minimum-bandwidth bps;
        monitor-bandwidth;
    }
    bandwidth bps {
        ct0 bps;
        ct1 bps;
```

```
    ct2 bps;
    ct3 bps;
}
class-of-service cos-value;
description text;
fast-reroute {
    (bandwidth bps | bandwidth-percent percent);
    (exclude [ group-names ] | no-exclude);
    hop-limit number;
    (include-all [ group-names ] | no-include-all);
    (include-any [ group-names ] | no-include-any);
}
from address;
hop-limit number;
install {
    destination-prefix/prefix-length <active>;
}
ldp-tunneling;
link-protection;
lsp-attributes {
    encoding-type (ethernet | packet | pdh | sonet-sdh);
    gpid (ethernet | hdlc | ipv4 | ppp);
    signal-bandwidth type;
    switching-type (fiber | lambda | psc-1 | tdm);
}
metric number;
no-cspf;
no-decrement-ttl;
node-link-protection;
optimize-timer seconds;
p2mp path-name;
policing {
    filter filter-name;
    no-automatic-policing;
}
preference preference;
primary path-name {
    adaptive;
    admin-group {
        exclude [ group-names ];
        include-all [ group-names ];
        include-any [ group-names ];
    }
    bandwidth bps {
        ct0 bps;
        ct1 bps;
        ct2 bps;
        ct3 bps;
    }
    class-of-service cos-value;
    hop-limit number;
    no-cspf;
    no-decrement-ttl;
    optimize-timer seconds;
    preference preference;
    priority setup-priority reservation-priority;
```

```
            (record | no-record);
            select (manual | unconditional);
        }
        standby;
    }
    priority setup-priority reservation-priority;
    (random | least-fill | most-fill);
    (record | no-record);
    retry-limit number;
    retry-timer seconds;
    revert-timer seconds;
    secondary path-name {
        adaptive;
        admin-group {
            exclude [ group-names ];
            include-all [ group-names ];
            include-any [ group-names ];
        }
        bandwidth bps {
            ct0 bps;
            ct1 bps;
            ct2 bps;
            ct3 bps;
        }
        class-of-service cos-value;
        hop-limit number;
        no-cspf;
        no-decrement-ttl;
        optimize-timer seconds;
        preference preference;
        priority setup-priority reservation-priority;
        (record | no-record);
        select (manual | unconditional);
        standby;
    }
    soft-preemption {
        cleanup-timer seconds;
    }
    standby;
    to address;
    traceoptions {
        file filename <replace> <size size> <files number> <no-stamp>
            <world-readable | no-world-readable>;
        flag flag <flag-modifier> <disable>;
    }
}
log-updown {
    no-trap {
        mpls-lsp-traps;
        rfc3812–traps;
    }
    (syslog | no-syslog);
    trap;
    trap-path-down;
    trap-path-up;
}
```

```
    no-cspf;
    no-decrement-ttl;
    no-propagate-ttl;
    optimize-aggressive;
    optimize-timer seconds;
    path path-name {
      (address | hostname) <strict | loose>;
    }
    path-mtu {
      allow-fragmentation;
      rsvp {
        mtu-signaling;
      }
    }
    preference preference;
    priority setup-priority reservation-priority;
    (record | no-record );
    revert-timer seconds;
    rsvp-error-hold-time seconds;
    smart-optimize-timer seconds;
    standby;
    static-path inet {
      prefix {
        class-of-service cos-value;
        double-push bottom-label top-label;
        next-hop (address | interface-name | address/interface-name);
        preference preference;
        push out-label;
        triple-push bottom-label middle-label top-label;
      }
    }
    statistics {
      auto-bandwidth;
      file filename <size size> <files number> <no-stamp> <replace>
        <world-readable | no-world-readable>;
      interval seconds;
    }
    traceoptions {
      file filename <replace> <size size> <files number> <no-stamp>
        <world-readable | no-world-readable>;
      flag flag;
    }
    traffic-engineering (bgp | bgp-igp | bgp-igp-both-ribs | mpls-forwarding);
}
```

[edit protocols rsvp] Hierarchy Level

The following statements can also be configured at the [edit logical-systems *logical-system-name*] hierarchy level:

```
  protocols {
    rsvp {
      disable;
      fast-reroute optimize-timer seconds;
      graceful-deletion-timeout seconds;
```

```
graceful-restart {
    disable;
    helper-disable;
    maximum-helper-recovery-time seconds;
    maximum-helper-restart-time seconds;
}
interface interface-name {
    disable;
    (aggregate | no-aggregate);
    authentication-key key;
    bandwidth bps;
    hello-interval seconds;
    link-protection {
        disable;
        admin-group {
            exclude group-names;
            include-all group-names;
            include-any group-names;
        }
        bandwidth bandwidth;
        bypass bypass-name {
            bandwidth bps {
                ct0 bps;
                ct1 bps;
                ct2 bps;
                ct3 bps;
            }
            hop-limit number;
            no-cspf;
            path address <strict | loose>;
            priority setup-priority reservation-priority;
            to address;
        }
        class-of-service cos-value;
        hop-limit number;
        max-bypasses number;
        no-cspf;
        no-node-protection;
        optimize-timer seconds;
        path address <strict | loose>;
        priority setup-priority reservation-priority;
        subscription percentage {
            ct0 percentage;
            ct1 percentage;
            ct2 percentage;
            ct3 percentage;
        }
    }
    (reliable | no-reliable);
    subscription percentage {
        ct0 percentage;
        ct1 percentage;
        ct2 percentage;
        ct3 percentage;
    }
```

```
            update-threshold percentage;
        }
        keep-multiplier number;
        load-balance {
            bandwidth;
        }
        peer-interface peer-interface-name {
            (aggregate | no-aggregate);
            authentication-key key;
            disable;
            hello-interval seconds;
            (reliable | no-reliable);
        }
        preemption {
            (aggressive | disabled | normal);
            soft-preemption {
                cleanup-timer seconds;
            }
        }
        refresh-time seconds;
        traceoptions {
            file filename <replace> <size size> <files number> <no-stamp>
                <world-readable | no-world-readable>;
            flag flag <flag-modifier> <disable>;
        }
        tunnel-services {
            devices device-names;
        }
    }
}
```

Part 2
MPLS

- MPLS Overview on page 21
- MPLS Configuration Statements on page 51
- MPLS-Signaled LSPs Configuration Guidelines on page 57
- DiffServ-Aware Traffic Engineering Configuration Guidelines on page 113
- Static and Explicit-Path LSP Configuration Guidelines on page 135
- Point-to-Multipoint LSP Configuration Guidelines on page 143
- Miscellaneous MPLS Properties Configuration Guidelines on page 151
- Summary of MPLS Configuration Statements on page 175

Chapter 3

MPLS Overview

Multiprotocol Label Switching (MPLS) provides a mechanism for engineering network traffic patterns that is independent of routing tables. MPLS assigns short labels to network packets that describe how to forward them through the network. MPLS is independent of any routing protocol and can be used for unicast packets.

In the traditional Level 3 forwarding paradigm, as a packet travels from one router to the next, an independent forwarding decision is made at each hop. The IP network layer header is analyzed, and the next hop is chosen based on this analysis and on the information in the routing table. In an MPLS environment, the analysis of the packet header is performed just once, when a packet enters the MPLS cloud. The packet is then assigned to a stream, which is identified by a *label*, which is a short (20-bit), fixed-length value at the front of the packet. Labels are used as lookup indexes for the label forwarding table. For each label, this table stores forwarding information. You can associate additional information with a label—such as class-of-service (CoS) values—that can be used to prioritize packet forwarding.

This chapter discusses the following topics:

- MPLS Standards on page 21
- Link-Layer Support on page 23
- MPLS and Traffic Engineering on page 24
- IP and MPLS Packets on Aggregated Interfaces on page 37
- MPLS Applications on page 38
- MPLS and Routing Tables on page 40
- MPLS and Traffic Protection on page 42
- Automatic Bandwidth Allocation on page 47
- Point-to-Multipoint LSPs on page 47
- MPLS Load Balancing Based on the IP Header and MPLS Labels on page 49

MPLS Standards

The JUNOS software supports the following RFCs and Internet drafts related to MPLS:

- RFC 2547, *BGP/MPLS VPNs*
- RFC 2702, *Requirements for Traffic Engineering Over MPLS*
- RFC 2858, *Multiprotocol Extensions for BGP-4*

- RFC 3063, *MPLS Loop Prevention Mechanism*
- RFC 3031, *Multiprotocol Label Switching Architecture* (provides a good overview of MPLS)
- RFC 3032, *MPLS Label Stack Encoding*
- RFC 3140, *Per Hop Behavior Identification Codes*
- RFC 3208, *PGM Reliable Transport Protocol Specification* (only the network element)
- RFC 3270, *Multi-Protocol Label Switching (MPLS) Support of Differentiated Services* (E-LSPs only)
- RFC 3443, *Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks*
- RFC 3469, *Framework for Multi-Protocol Label Switching (MPLS)-based Recovery*
- RFC 3478, *Graceful Restart Mechanism for LDP*
- RFC 3564, *Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering*
- RFC 4124, *Protocol Extensions for Support of Differentiated-Service-aware MPLS Traffic Engineering*
- RFC 4125, *Maximum Allocation Bandwidth Constraints Model for Diff-Serv-aware MPLS Traffic Engineering*
- RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diff-Serv-aware MPLS Traffic Engineering*
- RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*. The JUNOS software supports the traceroute functionality, but only on transit routers.
- Internet draft draft-ietf-bfd-mpls-02.txt, *BFD for MPLS LSPs*
- Internet draft draft-ietf-l3vpn-rfc2547bis-04.txt, *BGP/MPLS IP VPNs*
- Internet draft draft-ietf-mpls-icmp-02.txt, *ICMP Extensions for Multiprotocol Label Switching* (expires February 2001)
- Internet draft draft-ietf-mpls-rsvp-lsp-fastreroute-03.txt, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels* (except node protection in facility backup)
- Internet draft draft-ietf-mpls-icmp-01.txt, *ICMP Extensions for Multiprotocol Label Switching*
- Internet draft draft-ietf-mpls-label-encaps-07.txt, *MPLS Label Stack Encoding*
- Internet draft draft-ietf-mpls-p2mp-requirement-02.txt, *Requirements for Point to Multipoint Extensions to RSVP-TE* (no expiration; revised January 2004)
- Internet draft draft-ietf-mpls-soft-preemption-02.txt, *MPLS Traffic Engineering Soft Preemption* (no expiration; revised March 2004)
- Internet draft draft-ietf-ppvpn-rfc2547bis-03.txt, *BGP/MPLS VPNs*
- Internet draft draft-martini-l2circuit-encap-mpls-07.txt, *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*

The JUNOS software has the following exceptions:

- A packet with a sequence number of 0 is treated as out of sequence.
- Any packet which does not have the next incremental sequence number is considered out of sequence.
- When out-of-sequence packets arrive, the expected sequence number for the neighbor is set to the sequence number in the Layer 2 circuit control word.
- Internet draft draft-martini-l2circuit-trans-mpls-14.txt, *Transport of Layer 2 Frames Over MPLS*
- Internet draft draft-raggarwa-mpls-p2mp-te-02.txt (except non-adjacent signaling for branch LSPs, make-before-break and fast reroute, and LSP hierarchy using P2P LSPs), *Establishing Point to Multipoint MPLS TE LSPs* (no expiration; revised January 2004)

The following documents provide information about traffic engineering:

- RFC 2702, *Requirements for Traffic Engineering Over MPLS*
- RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*
- Internet draft draft-ietf-isis-traffic-04.txt, *IS-IS Extensions for Traffic Engineering* (expires February 2002)
- Internet draft draft-katz-yeung-ospf-traffic-06.txt, *Traffic Engineering Extensions to OSPF* (expires April 2002)
- Internet draft draft-ietf-mpls-rsvp-te-p2mp-01.txt, *Extensions to RSVP-TE for Point to Multipoint TE LSPs* (expires June 2005)

To access Internet RFCs and drafts, go to the IETF Web site at http://www.ietf.org.

The JUNOS software supports a proprietary Management Information Base (MIB) for MPLS objects; see the *JUNOS Network Management Configuration Guide* for more information.

Link-Layer Support

MPLS supports the following link-layer protocols, which are all supported in the JUNOS MPLS implementation:

- Point-to-Point Protocol (PPP)—Protocol ID 0x0281, Network Control Protocol (NCP) protocol ID 0x8281.
- Ethernet/Cisco High-level Data Link Control (HDLC)—Ethernet type 0x8847.
- Asynchronous Transfer Mode (ATM)—Subnetwork attachment point encoded (SNAP-encoded) Ethernet type 0x8847. Support is included for both point-to-point mode or nonbroadcast multiaccess (NBMA) mode. Support is not included for encoding MPLS labels as part of ATM virtual path identifier/virtual circuit identifier (VPI/VCI).

- Frame Relay—SNAP-encoded, Ethernet type 0x8847. Support is not included for encoding MPLS labels as part of Frame Relay data-link connection identifier (DLCI).
- Generic routing encapsulation (GRE) tunnel—Ethernet type 0x8847.

MPLS and Traffic Engineering

Traffic engineering allows you to control the path that data packets follow, bypassing the standard routing model, which uses routing tables. Traffic engineering moves flows from congested links to alternate links that would not be selected by the automatically computed destination-based shortest path. With traffic engineering, you can:

- Make more efficient use of expensive long-haul fibers.
- Control how traffic is rerouted in the face of single or multiple failures.
- Classify critical and regular traffic on a per-path basis.

The core of the traffic engineering design is based on building label-switched paths (LSPs) among routers. An LSP is connection-oriented, like a virtual circuit in Frame Relay or ATM. LSPs are not reliable: Packets entering an LSP do not have delivery guarantees, although preferential treatment is possible. LSPs also are similar to unidirectional tunnels in that packets entering a path are encapsulated in an envelope and switched across the entire path without being touched by intermediate nodes. LSPs provide fine-grained control over how packets are forwarded in a network. To provide reliability, an LSP can use a set of primary and secondary paths.

LSPs can be configured for Border Gateway Protocol (BGP) traffic only (traffic whose destination is outside of an autonomous system [AS]). In this case, traffic within the AS is not affected by the presence of LSPs. LSPs can also be configured for both BGP and interior gateway protocol (IGP) traffic; therefore, both intra-AS and inter-AS traffic is affected by the LSPs.

This section discusses the following topics:

- Label Description on page 25
- Label Allocation on page 25
- Routers in an LSP on page 27
- How a Packet Travels Along an LSP on page 28
- Types of LSPs on page 28
- Scope of LSPs on page 29
- Constrained-Path LSP Computation on page 29
- LSPs on an Overloaded Router on page 31
- Fate Sharing on page 32
- IGP Shortcuts on page 33
- Advertising LSPs into IGPs on page 36

Label Description

Packets traveling along an LSP are identified by a label—a 20-bit, unsigned integer in the range 0 through 1,048,575. Labels 0 through 999,999 are for internal use. Labels 1,000,000 through 1,048,575 are unassigned by the JUNOS software and are available for static LSPs. When you configure static LSPs, you can use only this range of labels.

Special Labels

Some of the reserved labels (in the 0 through 15 range) have well-defined meanings. For more complete details, see RFC 3032, *MPLS Label Stack Encoding*.

- 0, IPv4 Explicit Null label—This value is legal only when it is the sole label entry (no label stacking). It indicates that the label must be popped upon receipt. Forwarding continues based on the IP version 4 (IPv4) packet.
- 1, Router Alert label—When a packet is received with a top label value of 1, it is delivered to the local software module for processing.
- 2, IPv6 Explicit Null label—This value is legal only when it is the sole label entry (no label stacking). It indicates that the label must be popped on receipt. Forwarding continues based on the IP version 6 (IPv6) packet.
- 3, Implicit Null label—This label is used in the control protocol (Label Distribution Protocol [LDP] or Resource Reservation Protocol [RSVP]) only to request label popping by the downstream router. It never actually appears in the encapsulation. Labels with a value of 3 should not be used in the data packet as real labels. No payload type (IPv4 or IPv6) is implied with this label.
- 4 through 15—Unassigned.

Special labels are commonly used between the egress and penultimate routers of an LSP. If the LSP is configured to carry IPv4 packets only, the egress router might signal the penultimate router to use 0 as a final-hop label. If the LSP is configured to carry IPv6 packets only, the egress router might signal the penultimate router to use 2 as a final-hop label.

The egress router might simply signal the penultimate router to use 3 as the final label, which is a request to perform penultimate-hop label popping. The egress router will not process a labeled packet; rather, it receives the payload (IPv4, IPv6, or others) directly, reducing one MPLS lookup at egress.

For label-stacked packets, the egress router receives an MPLS label packet with its top label already popped by the penultimate router. The egress router cannot receive label-stacked packets that use label 0 or 2. It typically requests label 3 from the penultimate router.

Label Allocation

In the JUNOS software, label values are allocated per router. The display output shows only the label (for example, 01024). Labels for multicast packets are independent of those for unicast packets. Currently, the JUNOS software does not support multicast labels.

Labels are assigned by downstream routers relative to the flow of packets. A router receiving labeled packets (the next-hop router) is responsible for assigning incoming labels. A received packet containing a label that is unrecognized (unassigned) is dropped. For unrecognized labels, the router does not attempt to unwrap the label to analyze the network layer header, nor does it generate an Internet Control Message Protocol (ICMP) destination unreachable message.

A packet can carry a number of labels, organized as a last-in, first-out stack. This is referred to as a *label stack*. At a particular router, the decision about how to forward a labeled packet is based exclusively on the label at the top of the stack.

Figure 1 on page 26 shows the encoding of a single label. The encoding appears after data link layer headers, but before any network layer header.

Figure 1: Label Encoding

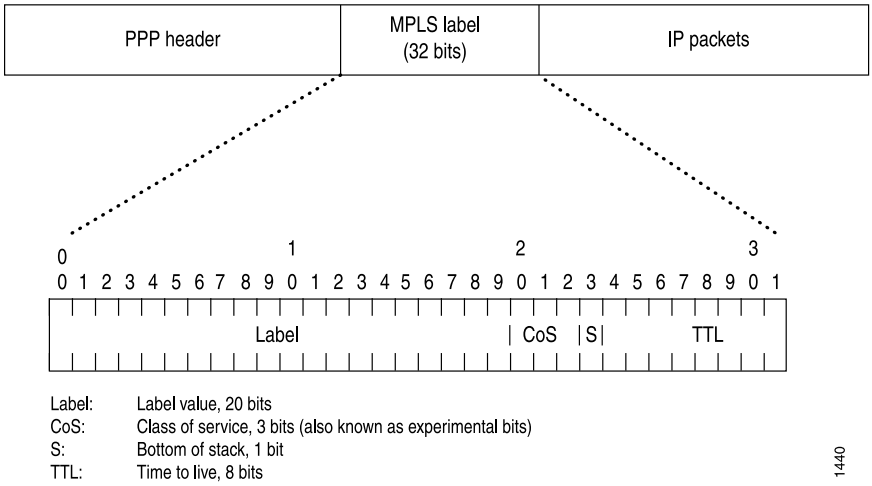
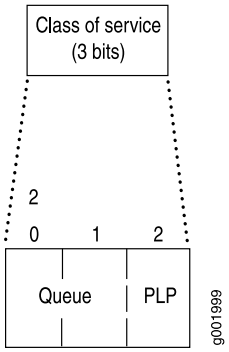


Figure 2 on page 26 illustrates the purpose of the class-of-service bits (also known as the EXP or experimental bits). Bits 20 and 21 specify the queue number. Bit 22 is the packet loss priority (PLP) bit used to specify the random early detection (RED) drop profile. For more information about class of service and the class-of-service bits, see “Configuring Class of Service for MPLS” on page 91.

Figure 2: Class-of-Service Bits



Operations on Labels

The router supports the following label operations:

- Push—Add a new label to the top of the packet. For IPv4 packets, the new label is the first label. The TTL and S bits are derived from the IP packet header. The MPLS CoS is derived from the queue number. If the push operation is performed on an existing MPLS packet, you will have a packet with two or more labels. This is called label stacking. The top label must have its S bit set to 0, and might derive CoS and time to live (TTL) from lower levels. The new top label in a label stack always initializes its TTL to 255, regardless of the TTL value of lower labels.
- Pop—Remove the label from the beginning of the packet. Once the label is removed, the TTL is copied from the label into the IP packet header, and the underlying IP packet is forwarded as a native IP packet. In the case of multiple labels in a packet (label stacking), removal of the top label yields another MPLS packet. The new top label might derive CoS and TTL from a previous top label. The popped TTL value from the previous top label is not written back to the new top label.
- Swap—Replace the label at the top of the label stack with a new label. The S and CoS bits are copied from the previous label, and the TTL value is copied and decremented (unless the no-decrement-ttl or no-propagate-ttl statement is configured). A transit router supports a label stack of any depth.
- Multiple Push—Add multiple labels (up to three) on top of existing packets. This operation is equivalent to pushing multiple times.
- Swap and Push—Replace the existing top of the label stack with a new label, and then push another new label on top.

Routers in an LSP

Each router in an LSP performs one of the following functions:

- Ingress router—The router at the beginning of an LSP. This router encapsulates IP packets with an MPLS Layer 2 frame and forwards it to the next router in the path. Each LSP can have only one ingress router.
- Egress router—The router at the end of an LSP. This router removes the MPLS encapsulation, thus transforming it from an MPLS packet to an IP packet, and forwards the packet to its final destination using information in the IP forwarding table. Each LSP can have only one egress router. The ingress and egress routers in an LSP cannot be the same router.
- Transit router—Any intermediate router in the LSP between the ingress and egress routers. A transit router forwards received MPLS packets to the next router in the MPLS path. An LSP can contain zero or more transit routers, up to a maximum of 253 transit routers in a single LSP.

A single router can be part of multiple LSPs. It can be the ingress or egress router for one or more LSPs, and it also can be a transit router in one or more LSPs. The functions that each router supports depend on your network design.

How a Packet Travels Along an LSP

When an IP packet enters an LSP, the ingress router examines the packet and assigns it a label based on its destination, placing the label in the packet's header. The label transforms the packet from one that is forwarded based on its IP routing information to one that is forwarded based on information associated with the label.

The packet is then forwarded to the next router in the LSP. This router and all subsequent routers in the LSP do not examine any of the IP routing information in the labeled packet. Rather, they use the label to look up information in their label forwarding table. They then replace the old label with a new label and forward the packet to the next router in the path.

When the packet reaches the egress router, the label is removed, and the packet again becomes a native IP packet and is again forwarded based on its IP routing information.

Types of LSPs

There are three types of LSPs:

- Static LSPs—For static paths, you must manually assign labels on all routers involved (ingress, transit, and egress). No signaling protocol is needed. This procedure is similar to configuring static routes on individual routers. Like static routes, there is no error reporting, liveliness detection, or statistics reporting.
- LDP-signaled LSPs—See "LDP Overview" on page 329.
- RSVP-signaled LSPs—For signaled paths, RSVP is used to set up the path and dynamically assign labels. (RSVP signaling messages are used to set up signaled paths.) You configure only the ingress router. The transit and egress routers accept signaling information from the ingress router, and they set up and maintain the LSP cooperatively. Any errors encountered while establishing an LSP are reported to the ingress router for diagnostics. For signaled LSPs to work, a version of RSVP that supports tunnel extensions must be enabled on all routers.

There are two types of RSVP-signaled LSPs:

- Explicit-path LSPs—All intermediate hops of the LSP are manually configured. The intermediate hops can be strict, loose, or any combination of the two. Explicit path LSPs provide you with complete control over how the path is set up. They are similar to static LSPs but require much less configuration.
- Constrained-path LSPs—The intermediate hops of the LSP are automatically computed by the software. The computation takes into account information provided by the topology information from the IS-IS or Open Shortest Path First (OSPF) link-state routing protocol, the current network resource utilization determined by RSVP, and the resource requirements and constraints of the LSP. For signaled constrained-path LSPs to work, either the IS-IS or OSPF protocol and the IS-IS or OSPF traffic engineering extensions must be enabled on all routers.

Scope of LSPs

For constrained-path LSPs, the LSP computation is confined to one IGP domain, and cannot cross any AS boundary. This prevents an AS from extending its IGP into another AS.

Explicit-path LSPs, however, can cross as many AS boundaries as necessary. Because intermediate hops are manually specified, the LSP does not depend on the IGP topology or a local forwarding table.

Constrained-Path LSP Computation

The Constrained Shortest Path First (CSPF) algorithm is an advanced form of the shortest-path-first (SPF) algorithm used in OSPF and IS-IS route computations. CSPF is used in computing paths for LSPs that are subject to multiple constraints. When computing paths for LSPs, CSPF considers not only the topology of the network, but also the attributes of the LSP and the links, and it attempts to minimize congestion by intelligently balancing the network load.

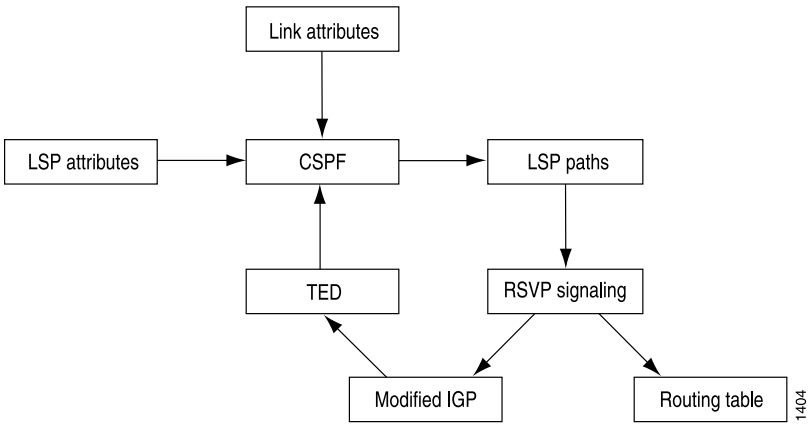
The constraints that CSPF considers include:

- LSP attributes
  - Administrative groups (that is, link color requirements)
  - Bandwidth requirements
  - Explicit route (strict or loose)
  - Hop limitations
  - Priority (setup and hold)
- Link attributes
  - Administrative groups (that is, link colors assigned to the link)
  - Reservable bandwidth of the links (static bandwidth minus the currently reserved bandwidth)

The data that CSPF considers comes from the following sources:

- Traffic engineering database (TED)—Provides CSPF with up-to-date topology information, the current reservable bandwidth of links, and the link colors. For the CSPF algorithm to perform its computations, a link-state IGP (such as OSPF or IS-IS) with special extensions is needed. For CSPF to be effective, the link-state IGP on all routers must support the special extensions. While building the topology database, the extended IGP must take into consideration the current LSPs and must flood the route information everywhere. Because changes in the reserved link bandwidth and link color cause database updates, an extended IGP tends to flood more frequently than a normal IGP. See Figure 3 on page 30 for a diagram of the relationships between these components.
- Currently active LSPs—Includes all the LSPs that should originate from the router and their current operational status (up, down, or timeout).

Figure 3: CSPF Computation Process



This section discusses the following topics:

- How CSPF Selects a Path on page 30
- Path Selection Tie-Breaking on page 31
- Computing Paths Offline on page 31

How CSPF Selects a Path

To select a path, CSPF follows these steps:

1. Computes LSPs one at a time, beginning with the highest priority LSP (the one with the lowest setup priority value). Among LSPs of equal priority, CSPF starts with those that have the highest bandwidth requirement.
2. Prunes the TED of all the links that are not full duplex and do not have sufficient reservable bandwidth.
3. If the LSP configuration includes the include statement, prunes all links that do not share any included colors.
4. If the LSP configuration includes the exclude statement, prunes all links that contain excluded colors. If the link does not have a color, it is accepted.
5. Finds the shortest path toward the LSP's egress router, taking into account explicit-path constraints. For example, if the path must pass through Router A, two separate SPFs are computed, one from the ingress router to Router A, the other from Router A to the egress router.
6. If several paths have equal cost, chooses the one whose last-hop address is the same as the LSP's destination.
7. If several equal-cost paths remain, selects the one with the fewest number of hops.
8. If several equal-cost paths remain, applies the CSPF load-balancing rule configured on the LSP (least fill, most fill, or random).

Path Selection Tie-Breaking

If more than one path is available after the rules from the previous section have been applied, a tie-breaking rule is applied to choose the path for the LSP. There are three tie-breaking rules:

- Random—One of the remaining paths is picked at random. This rule tends to place an equal number of LSPs on each link, regardless of the available bandwidth ratio.
- Least fill—The path with the largest minimum available bandwidth ratio is preferred. This rule tries to equalize the reservation on each link.
- Most fill—The path with the smallest minimum available bandwidth ratio is preferred. This rule tries to fill a link before moving on to alternative links.

The rule used depends on the configuration. Random is the default rule.

For the other rules, the following definitions are needed:

- Reservable bandwidth = bandwidth of link x subscription factor of link
- Available bandwidth = reservable bandwidth – (sum of the bandwidths of the LSPs traversing the link)
- Available bandwidth ratio = available bandwidth/reservable bandwidth
- Minimum available bandwidth ratio (for a path) = the smallest available bandwidth ratio of the links in a path

Computing Paths Offline

The JUNOS software provides online, real-time CSPF computation only; each router performs CSPF calculations independent of the other routers in the network. These calculations are based on currently available topology information—information that is usually recent, but not completely accurate. LSP placements are locally optimized, based on current network status.

To optimize links globally across the network, you can use an offline tool to perform the CSPF calculations and determine the paths for the LSPs. You can create such a tool yourself, or you can modify an existing network design tool to perform these calculations. You should run the tool periodically (daily or weekly) and download the results into the router. An offline tool should take the following into account when performing the optimized calculations:

- All the LSP's requirements
- All link attributes
- Complete network topology

LSPs on an Overloaded Router

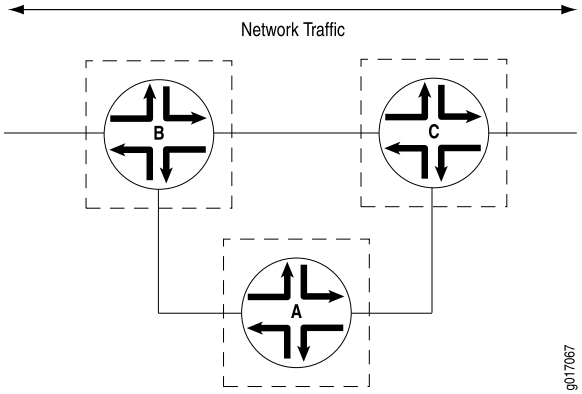
An overloaded router is a router running IS-IS with its overload bit set in its IS-IS configuration. In this case, an MPLS LSP specifically refers to an RSVP- or LDP-signaled LSP. In the case of RSVP, it applies to both CSPF and non-CSPF LSPs.

You cannot establish transit LSPs through an overloaded router. However, you can configure ingress and egress LSPs through an overloaded router.

NOTE: When you set the overload bit on an IS-IS router, all LSPs transiting through it are recomputed and rerouted away from it. If the recomputation fails, no additional attempt to reconfigure the LSP is made, and the affected LSPs are disconnected.

An example of when you might want to establish transit LSPs through an overloaded router is illustrated in Figure 4 on page 32, which shows an aggregation router (Router A) dual-homed on two core routers (Router B and Router C). You want to include the aggregation router in the LSP mesh, but transit LSPs should not pass through it, because it is a less capable router with relatively low-bandwidth uplinks to the core. Certain failure and rerouting scenarios could make it impossible for the aggregation router to establish some of its LSPs. Consequently, you run the router in a steady state with the overload bit set, but you are still able to establish ingress and egress LSPs through it.

Figure 4: Aggregation Router A Dual-Homed on Core Routers B and C



Fate Sharing

Fate sharing allows you to create a database of information that CSPF uses to compute one or more backup paths to use in case the primary path becomes unstable. The database describes the relationships between elements of the network, such as routers and links. You can specify one or more elements within a group.

Through fate sharing, you can configure backup paths that minimize the number of shared links and fiber paths with the primary paths as much as possible, to ensure that if a fiber is cut, the minimum amount of data is lost and a path still exists to the destination.

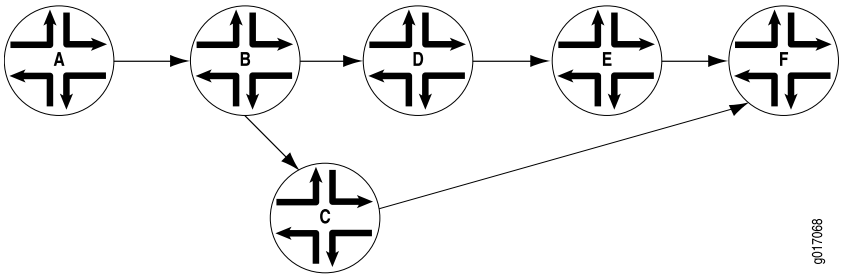
For a backup path to work optimally, it must not share links or physical fiber paths with the primary path, ensuring that a single point of failure will not affect the primary and backup paths simultaneously. For more information about fate sharing, see the *JUNOS Routing Protocols Configuration Guide*.

IGP Shortcuts

Link-state protocols, such as OSPF and IS-IS, use the SPF algorithm to compute the shortest-path tree to all nodes in the network. The results of such computations can be represented by the destination node, next-hop address, and output interface, where the output interface is a physical interface. LSPs can be used to augment the SPF algorithm, for the purposes of resolving BGP next hops. On the node performing the calculations, LSPs appear to be logical interfaces directly connected to remote nodes in the network. If you configure the IGP to treat LSPs the same as a physical interface and use the LSPs as a potential output interface, the SPF computation results are represented by the destination node and output LSP, effectively using the LSP as a shortcut through the network to the destination.

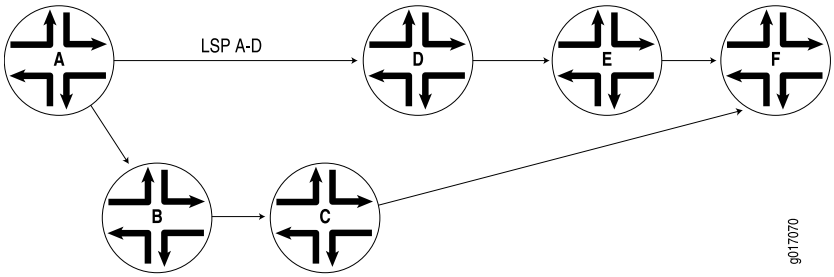
As an illustration, begin with a typical SPF tree (see Figure 5 on page 33).

Figure 5: Typical SPF Tree, Sourced from Router A



If an LSP connects Router A to Router D and if IGP shortcuts are enabled on Router A, you might have the SPF tree shown in Figure 6 on page 33.

Figure 6: Modified SPF Tree, Using LSP A–D as a Shortcut



Note that Router D is now reachable through LSP A–D. When computing the shortest path to reach Router D, Router A has two choices:

- Use IGP path A–B–D.
- Use LSP A–D.

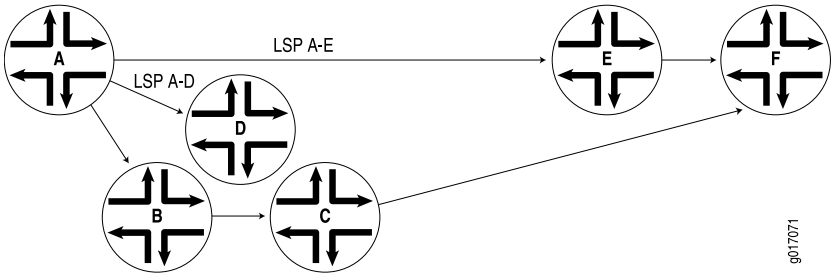
Router A decides between the two choices by comparing the IGP metrics for path A–B–D with the LSP metrics for LSP A–D. If the IGP metric is lower, path A–B–D is chosen (Figure 5 on page 33). If the LSP metric is lower, LSP A–D is used

(Figure 6 on page 33). If both metrics are equal, LSP A–D is chosen because LSP paths are preferred over IGP paths.

Note that Routers E and F are also reachable through LSP A–D, because they are downstream from Router D in the SPF tree.

Assuming that another LSP connects Router A to Router E, you might have the SPF tree shown in Figure 7 on page 34.

Figure 7: Modified SPF Tree, Using LSP A–D and LSP A–E as Shortcuts



This section discusses the following topics:

- Enabling IGP Shortcuts on page 34
- LSPs Qualified in Shortcut Computations on page 34
- IGP Shortcut Applications on page 35
- IGP Shortcuts and Routing Table on page 35
- Router Requirements on page 36
- IGP Shortcuts and VPN Environments on page 36

Enabling IGP Shortcuts

IGP shortcuts are supported for both IS-IS and OSPF. A link-state protocol is required for IGP shortcuts. Shortcuts are disabled by default. For information about enabling IGP shortcuts for IS-IS and OSPF, see the *JUNOS Routing Protocols Configuration Guide*. You can enable IGP shortcuts on a per-router basis; you do not need to enable shortcuts globally. A router's shortcut computation does not depend on another router performing similar computations, and shortcuts performed by other routers are irrelevant.

LSPs Qualified in Shortcut Computations

Not all LSPs are used in IGP shortcuts. Only those LSPs whose egress point (using the to statement) matches the router ID of the egress node are considered. Other LSPs, whose egress point matches the egress node interface address, are ignored in IGP shortcuts.

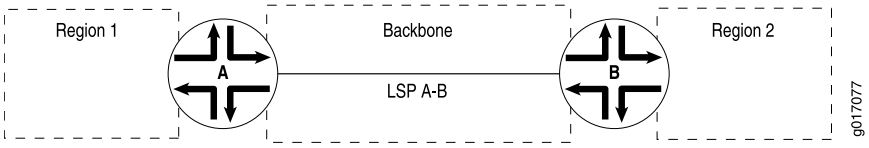
There are exceptions, however. If an LSP has an alias egress point (using the install statement) and it matches certain router IDs, it is included in the shortcut computation as well. If multiple equal metric LSPs destined to the same router ID exist, traffic can load-share among them.

IGP Shortcut Applications

You can use shortcuts to engineer traffic traveling toward destination nodes that do not support MPLS LSPs. For example, in Figure 7 on page 34, traffic traveling toward Router F enters LSP A–E. You can control traffic between Router A and Router F by manipulating LSP A–E; you do not need to explicitly set up an LSP between Router A and Router F.

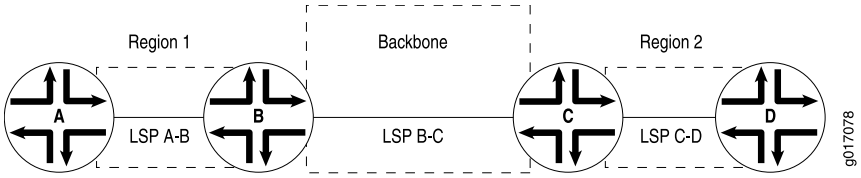
In Figure 8 on page 35, all traffic from Region 1 to Region 2 traverses LSP A–B if IGP shortcuts are enabled on the ingress router (Router A), permitting aggregation of interregional traffic into one LSP. To perform traffic engineering on the interregional traffic, you have to manipulate LSP A-B only, which avoids creating n2 LSPs from all routers in Region 1 to all routers in Region 2 and allows efficient resource controls on the backbone network.

Figure 8: IGP Shortcuts



Shortcuts allow you to deploy LSPs into a network in an incremental, hierarchical fashion. In Figure 9 on page 35, each region can choose to implement traffic engineering LSPs independently, without requiring cooperation from other regions. Each region can choose to deploy intraregion LSPs to fit the region's bandwidth needs, at the pace appropriate for the region.

Figure 9: IGP Shortcuts in a Bigger Network



When intraregion LSPs are in place, interregional traffic automatically traverses the intraregion LSPs as needed, eliminating the need for a full mesh of LSPs between edge routers. For example, traffic from Router A to Router D traverses LSPs A–B, B–C, and C–D.

IGP Shortcuts and Routing Table

IGP typically performs two independent computations. The first is performed without considering any LSP. The result of the computation is stored in the inet.0 table. This step is no different from traditional SPF computations and is always performed even if IGP shortcut is disabled.

The second computation is performed considering only LSPs as a logical interface. Each LSP's egress router is considered. The list of destinations whose shortest path traverses the egress router (established during the first computation) is placed in the

inet.3 routing table. These destinations are given the egress router of the LSP as a next hop, enabling BGP on the local router to use these LSPs to access BGP next hops beyond the egress router. Normally, BGP can use only LSPs that terminate at the BGP next hop. Note that BGP is the only protocol that uses the inet.3 routing table. Other protocols will not route traffic through these LSPs.

If traffic engineering for IGP and BGP is enabled (see "IGP and BGP Destinations" on page 39), IGP moves all routes in inet.3 into inet.0, merging all routes while emptying the inet.3 table. The number of routes in inet.0 will be exactly the same as before. Route next-hops can traverse a physical interface, an LSP, or the combination of the two if the metrics are equal.

Router Requirements

IGP shortcuts are enabled on a per-node basis. You do not need to coordinate with other nodes.

IGP Shortcuts and VPN Environments

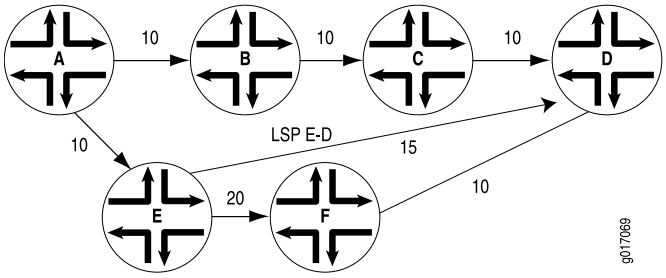
IGP shortcuts (configured under the [protocols mpls traffic-engineering bgp-igp] hierarchy level and under the [protocols ospf traffic-engineering shortcuts] hierarchy level) do not work in VPN environments. IGP shortcuts move routes in the inet.3 routing table to the inet.0 routing table. Virtual private network (VPN) IBGP (which belongs to family inet-vpn) relies on next hops that are in the inet.3 table, so IGP shortcuts are incompatible with VPNs.

Advertising LSPs into IGPs

You can configure your IGP to treat an LSP as a link. IGP shortcuts allow only the ingress router of an LSP to use the LSP in its SPF computation. However, other routers on the network do not know of the existence of that LSP, so they cannot use it. This can lead to suboptimal traffic engineering. In addition, only BGP can use an IGP shortcut to an LSP. When you advertise an LSP as a link into the IGP, all traffic can traverse it, and all routers know about it.

As an example, consider the network shown in Figure 10 on page 36.

Figure 10: SPF Computations with Advertised LSPs



Assume that Router A is computing a path to Router D. The link between Router E and Router F has a metric of 20; all other links have a metric of 10. Here, the path

chosen by Router A is A–B–C–D, which has a metric of 30, instead of A–E–F–D, which has a metric of 40.

If Router E has an LSP to Router D with a metric of 15, you want traffic from Router A to Router D to use the path A–E–D, which has a metric of 25, instead of the path A–B–C–D. However, because Router A does not know about the LSP between Router E and Router D, it cannot route traffic through this path.

For all routers on the network to know about the LSP between Router E and Router D, you need to advertise it. This advertisement announces the LSP as a unidirectional, point-to-point link in the link-state database, and all routers can compute paths using the LSP. The link-state database maintains information about the AS topology and contains information about the router's local state (for example, the router's usable interfaces and reachable neighbors). In Figure 10 on page 36, Router A will see the link from Router E to Router D and route traffic along this lower-metric path.

Because an LSP is announced as a unidirectional link, you might need to configure a reverse LSP (one that starts at the egress router and ends at the ingress router) so that the SPF bidirectionality check succeeds. As a step in the SPF computation, IS-IS considers a link from Router E to Router D. Before IS-IS uses any link, it verifies that there is a link from Router D to Router E (there is bidirectional connectivity between router E and D). Otherwise, the SPF computation will not use an announced LSP.

When an LSP is advertised to the IGP, the advertising router uses the LSP as the forwarding path for regular routes after installing them in the inet.0 routing table. All packets traversing the router could be forwarded through the LSP. Conversely, IGP shortcuts are used only to forward packets that are following BGP routes.

NOTE: Do not configure IGP shortcuts and advertise LSPs to the IGP at the same time.

IP and MPLS Packets on Aggregated Interfaces

You can send IP and MPLS packets over aggregated interfaces. To the IP or MPLS session, there is a single LSP composed of the aggregated interfaces. Packets sent to an LSP that is part of an aggregated interface are redistributed over the aggregated member interfaces.

Sending IP and MPLS packets over aggregated interfaces has the following benefits:

- Bandwidth aggregation—You can increase the number of MPLS packet flows sent over each connection. In MPLS, a set of packets sharing the same label is considered a part of the same flow.
- Link redundancy—If a link or a line card failure affects an aggregate member link, the traffic flowing across that link is immediately forwarded across one of the remaining links.

JUNOS supports aggregated SONET and Ethernet interfaces.

Note that the JUNOS implementation of IP and MPLS over aggregated interfaces (aggregated Ethernet devices only) complies with IEEE 802.3ad.

For information about how to configure aggregated Ethernet or aggregated SONET interfaces, see the *JUNOS Network Interfaces Configuration Guide*.

MPLS Applications

In the JUNOS software implementation of MPLS, establishing an LSP installs on the ingress router a host route (a 32-bit mask) toward the egress router. The address of the host route is the destination address of the LSP. By default, the route has a preference value of 7, a value that is higher than all routes except direct interface and static routes. The 32-bit mask ensures that the route is more specific (that is, a longer match) than all other subnet routes. The host routes can be used to traffic-engineer BGP destinations only, or both IGP and BGP destinations.

This section discusses the following topics:

- BGP Destinations on page 38
- IGP and BGP Destinations on page 39
- Selecting a Forwarding LSP Next Hop on page 40

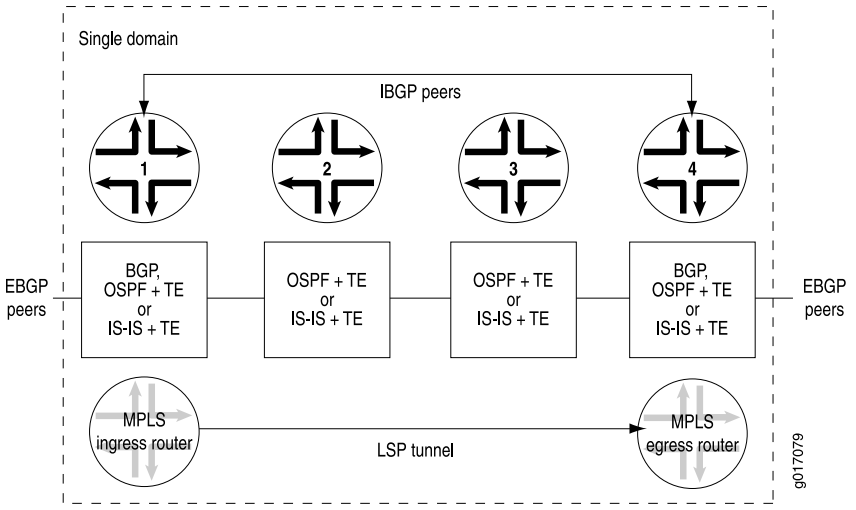
BGP Destinations

You can configure MPLS to control the paths that traffic takes to destinations outside an AS.

Both internal BGP (IBGP) and external BGP (EBGP) take advantage of the LSP host routes without requiring extra configuration. BGP compares the BGP next-hop address with the LSP host route. If a match is found, the packets for the BGP route are label-switched over the LSP. If multiple BGP routes share the same next-hop address, all the BGP routes are mapped to the same LSP route, regardless of which BGP peer the routes are learned from. If the BGP next-hop address does not match an LSP host route, BGP routes continue to be forwarded based on the IGP routes within the routing domain. In general, when both an LSP route and an IGP route exist for the same BGP next-hop address, the one with the lowest preference is chosen.

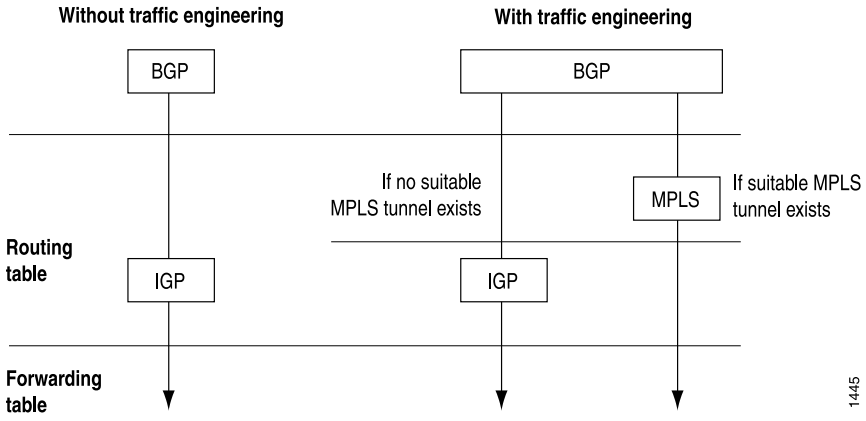
Figure 11 on page 39 shows an MPLS topology that illustrates how MPLS and LSPs work. This topology consists of a single domain with four routers. The two routers at the edges of the domain, Router 1 and Router 4, are running EBGP to communicate with peers outside the domain and IBGP to communicate between themselves. For intradomain communication, all four routers are running an IGP. Finally, an LSP tunnel exists from Router 1 to Router 4.

Figure 11: MPLS Application Topology



When BGP on Router 1 receives prefixes from Router 4, it must determine how to reach a BGP next-hop address. Typically, when traffic engineering is not enabled, BGP uses IGP routes to determine how to reach next-hop addresses. (See the left side of Figure 12 on page 39.) However, when traffic engineering is enabled, if the BGP next-hop matches the LSP tunnel endpoint (that is, the MPLS egress router), those prefixes enter the LSP tunnel. (To track these prefixes, look at the Active Route field in the show mpls lsp command output or at the output of the show route label-switched-path *path-name* command.) If the BGP next hop does not match an LSP tunnel endpoint, those prefixes are sent following the IGP's shortest path. (See Figure 12 on page 39.)

Figure 12: How BGP Determines How to Reach Next-Hop Addresses



IGP and BGP Destinations

You can configure MPLS to control the paths that traffic takes to destinations within an AS.

When traffic engineering is for BGP destinations only, the MPLS host routes are installed in the inet.3 routing table (see Figure 13 on page 41), separate from the routes learned from other routing protocols. Not all inet.3 routes are downloaded into the forwarding table. Packets directly addressed to the egress router do not follow the LSP, which prevents routes learned from LSPs from overriding routes learned from IGPs or other sources.

Traffic within a domain, including BGP control traffic between BGP peers, is not affected by LSPs. MPLS affects interdomain traffic only; that is, it affects only those BGP prefixes that are learned from an external domain. MPLS does not disrupt intradomain traffic, so IS-IS or OSPF routes remain undisturbed. If you issue a ping or traceroute command to any destination within the domain, the ping or traceroute packets follow the IGP path. However, if you issue a ping or traceroute command from Router 1 in Figure 11 on page 39 (the LSP ingress router) to a destination outside of the domain, the packets use the LSP tunnel.

When traffic engineering for IGP and BGP destinations is enabled, the MPLS host routes are installed in the inet.0 table (see Figure 14 on page 42) and downloaded into the forwarding table. Any traffic destined to the egress router could enter the LSP. In effect, it moves all the routes in inet.3 into inet.0, causing the inet.3 table to be emptied.

RSVP packets automatically avoid all MPLS LSPs, including those established by RSVP or LDP. This prevents placing one RSVP session into another LSP, or in other words, nesting one LSP into another.

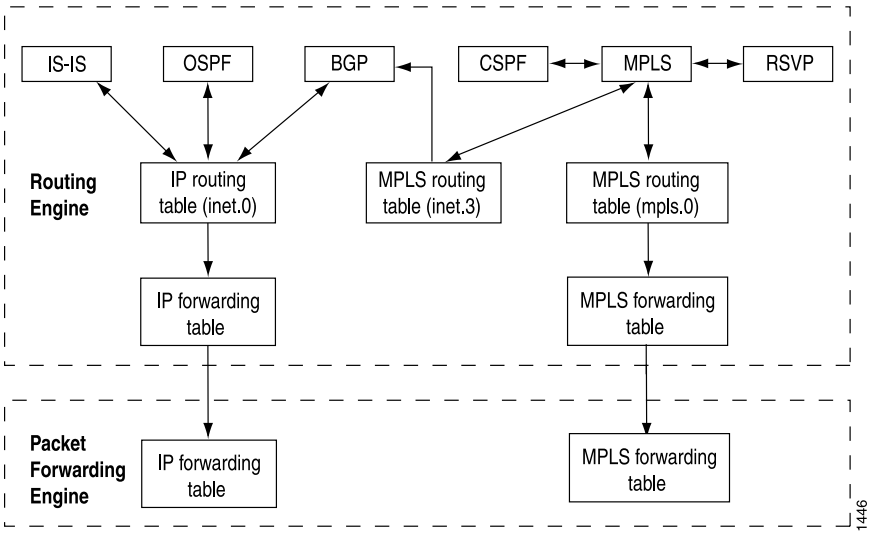
Selecting a Forwarding LSP Next Hop

If more than one LSP tunnel to a BGP next hop exists, the prefixes learned from the BGP next hop are randomly divided among the LSP tunnels. To control which LSP BGP uses to forward data for a given prefix, use the install-nexthop statement in the export policy applied to the forwarding table. For more information, see the *JUNOS Routing Protocols Configuration Guide*.

MPLS and Routing Tables

The IGPs and BGP store their routing information in the inet.0 routing table, the main IP routing table. If traffic-engineering bgp is configured, thereby allowing only BGP to use MPLS paths for forwarding traffic, MPLS path information is stored in a separate routing table, inet.3. Only BGP accesses the inet.3 routing table. BGP uses both inet.0 and inet.3 to resolve next-hop addresses. If traffic-engineering bgp-igp is configured, thereby allowing the IGPs to use MPLS paths for forwarding traffic, MPLS path information is stored in the inet.0 routing table. (Figure 13 on page 41 and Figure 14 on page 42 illustrate the routing tables in the two traffic engineering configurations.)

Figure 13: Routing and Forwarding Tables, traffic-engineering bgp



The inet.3 routing table contains the host address of each LSP's egress router. This routing table is used on ingress routers to route packets to the destination egress router. BGP uses the inet.3 routing table on the ingress router to help in resolving next-hop addresses.

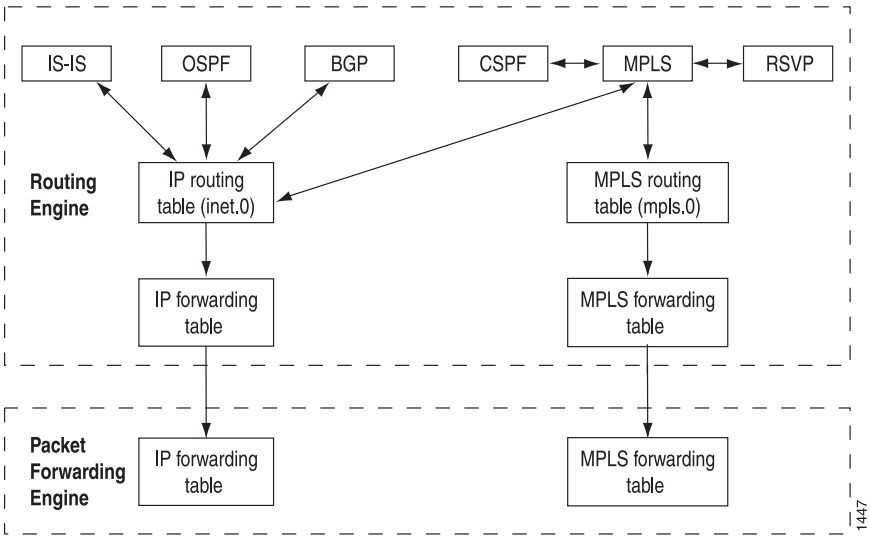
MPLS also maintains an MPLS path routing table (mpls.0), which contains a list of the next label-switched router in each LSP. This routing table is used on transit routers to route packets to the next router along an LSP.

Typically, the egress router in an LSP does not consult the mpls.0 routing table. (This router does not need to consult mpls.0 because the penultimate router in the LSP either changes the packet's label to a value of 0 or pops the label.) In either case, the egress router forwards it as an IPv4 packet, consulting the IP routing table, inet.0, to determine how to forward the packet.

When a transit or egress router receives an MPLS packet, information in the MPLS forwarding table is used to determine the next transit router in the LSP or to determine that this router is the egress router.

When BGP resolves a next-hop prefix, it examines both the inet.0 and inet.3 routing tables, seeking the next hop with the lowest preference. If it finds a next-hop entry with an equal preference in both routing tables, BGP prefers the entry in the inet.3 routing table.

Figure 14: Routing and Forwarding Tables, traffic-engineering bgp-igp



Generally, BGP selects next-hop entries in the inet.3 routing table because their preferences are always lower than OSPF and IS-IS next-hop preferences. When you configure LSPs, you can override the default preference for MPLS LSPs, which might alter the next-hop selection process.

When BGP selects a next-hop entry from the inet.3 routing table, it installs that LSP into the forwarding table in the Packet Forwarding Engine, which causes packets destined for that next hop to enter and travel along the LSP. If the LSP is removed or fails, the path is removed from the inet.3 routing table and from the forwarding table, and BGP reverts to using a next hop from the inet.0 routing table.

MPLS and Traffic Protection

Typically, when an LSP fails, the router immediately upstream from the failure signals the outage to the ingress router. The ingress router calculates a new path to the egress router, establishes the new LSP, and then directs the traffic from the failed path to the new path. This rerouting process can be time-consuming and prone to failure. For example, the outage signals to the ingress router might get lost, or the new path might take too long to come up, resulting in significant packet drops. The JUNOS software provides several complementary mechanisms for protecting against LSP failures:

- Standby secondary paths—You can configure primary and secondary paths. You configure secondary paths with the standby statement. To activate traffic protection, you need to configure these standby paths only on the ingress router. If the primary path fails, the ingress router immediately reroutes traffic from the failed path to the standby path, thereby eliminating the need to calculate a new route and signal a new path. For information about configuring standby LSPs, see “Configuring the Standby State” on page 99.
- Fast reroute—You configure fast reroute on an LSP to minimize the effect of a failure in the LSP. Fast reroute enables a router upstream from the failure to route around the failure quickly to the router downstream of the failure. The

upstream router then signals the outage to the ingress router, thereby maintaining connectivity before a new LSP is established. For a detailed overview of fast reroute, see “Fast Reroute” on page 43. For information about configuring fast reroute, see “Configuring Fast Reroute” on page 71.

- Link protection—You can configure link protection to help ensure that traffic traversing a specific interface from one router to another can continue to reach its destination in the event that this interface fails. When link protection is configured for an interface and configured for an LSP that traverses this interface, a bypass LSP is created that handles this traffic if the interface fails. The bypass LSP uses a different interface and path to reach the same destination. For information about configuring link protection, see “Configuring Node Protection or Link Protection” on page 278.

When standby secondary path, and fast reroute or link protection are configured on an LSP, full traffic protection is enabled. When a failure occurs in an LSP, the router upstream from the failure routes traffic around the failure and notifies the ingress router of the failure. This rerouting keeps the traffic flowing while waiting for the notification to be processed at the ingress router. After receiving the failure notification, the ingress router immediately reroutes the traffic from the patched primary path to the more optimal standby path.

Fast reroute and link protection provide a similar type of traffic protection. Both features provide a quick transfer service and employ a similar design. Fast reroute and link protection are both described in RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*. However, you need to configure only one or the other. Although you can configure both, there is little, if any, benefit in doing so.

Fast Reroute

The following sections provide an overview of how fast reroute works:

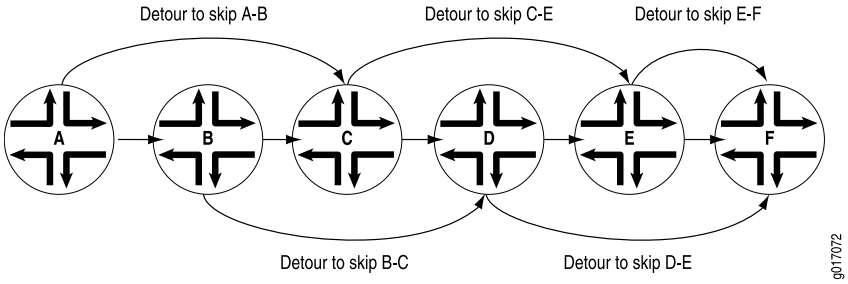
- Fast Reroute Overview on page 43
- Detour Merging Process on page 45
- Detour Computations on page 46
- Fast Reroute Path Optimization on page 46

Fast Reroute Overview

Fast rerouting is accomplished by precomputing and preestablishing a number of detours along the LSP. In case of a network failure on the current LSP path, the traffic is quickly routed to one of the detours. Figure 15 on page 44 illustrates an LSP from Router A to Router F, showing the established detours. Each detour is established by an upstream node to avoid the link toward the immediate downstream node and the immediate downstream node itself. Each detour might traverse through one or more label-switched routers that are not shown in the figure.

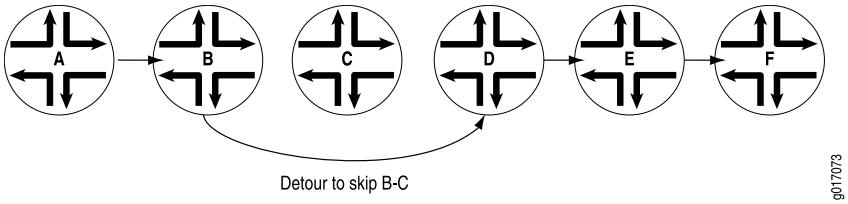
Fast reroute protects traffic against any single point of failure between the ingress and egress routers. If there are multiple failures along an LSP, fast reroute itself might fail. Also, fast reroute does not protect against failure of the ingress or egress routers.

Figure 15: Detours Established for an LSP Using Fast Reroute



If a node detects that a downstream link has failed (using a link-layer-specific liveness detection mechanism) or that a downstream node has failed (for example, using the RSVP neighbor hello protocol), the node quickly switches the traffic to the detour and, at the same time, signals the ingress router about the link or node failure. Figure 16 on page 44 illustrates the detour taken when the link between Router B and Router C fails.

Figure 16: Detour After the Link from Router B to Router C Fails



If the network topology is not rich enough (there are not enough routers with sufficient links to other routers), some of the detours might not succeed. For example, the detour from Router A to Router C in Figure 15 on page 44 cannot traverse link A-B and Router B. If such a path is not possible, the detour does not occur.

Note that after the node switches traffic to the detour, it might switch the traffic again to a newly calculated detour soon after. This is because the initial detour route might not be the best route. To make rerouting as fast as possible, the node switches traffic onto the initial detour without first verifying that the detour is valid. Once the switch is made, the node recomputes the detour. If the node determines that the initial detour is still valid, traffic continues to flow over this detour. If the node determines that the initial detour is no longer valid, it again switches the traffic to a newly computed detour.

NOTE: If you issue show commands after the node has switched traffic to the initial detour, the node might indicate that the traffic is still flowing over the original LSP. This situation is temporary and should correct itself quickly.

The time required for a fast-rerouting detour to take effect depends on two independent time intervals:

- Amount of time to detect that there is a link or node failure—This interval depends greatly on the link layer in use and the nature of the failure. For example, failure

detection on an SONET/SDH link typically is much faster than on a Gigabit Ethernet link, and both are much faster than detection of a router failure.

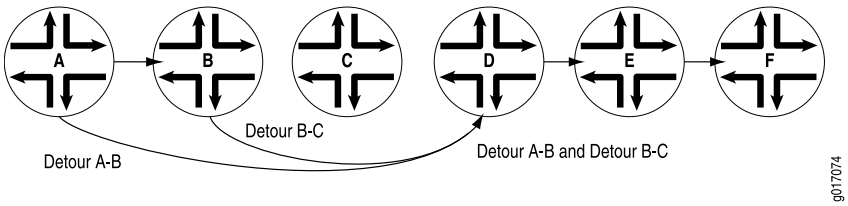
- Amount of time required to splice the traffic onto the detour—This operation is performed by the Packet Forwarding Engine, which requires little time to splice traffic onto the detour. The time needed can vary depending on the number of LSPs being switched to detours.

Fast reroute is a short-term patch to reduce packet loss. Because detour computation might not reserve adequate bandwidth, the detours might introduce congestion on the alternate links. The ingress router is the only router that is fully aware of LSP policy constraints and, therefore, is the only router able to come up with adequate long-term alternate paths.

Detours are created by use of RSVP and, like all RSVP sessions, they require extra state and overhead in the network. For this reason, each node establishes at most one detour for each LSP that has fast reroute enabled. Creating more than one detour for each LSP increases the overhead, but serves no practical purpose.

To reduce network overhead further, each detour attempts to merge back into the LSP as soon as possible after the failed node or link. If you can consider an LSP that travels through *n* router nodes, it is possible to create *n* – 1 detours. For instance, in Figure 17 on page 45, the detour tries to merge back into the LSP at Router D instead of at Router E or Router F. Merging back into the LSP makes the detour scalability problem more manageable. If topology limitations prevent the detour from quickly merging back into the LSP, detours merge with other detours automatically.

Figure 17: Detours Merging into Other Detours



Detour Merging Process

This section describes the process used by a router to determine which LSP to select when the router receives Path messages from different interfaces with identical Session and Sender Template objects. When this occurs, the router needs to merge the path states.

The router employs the following process to determine when and how to merge path states:

- When all the Path messages do not include a Fast Reroute or a Detour object, or when the router is the egress of the LSP, no merging is required. The messages are processed according to RSVP traffic engineering (TE).
- Otherwise, the router *must* record the path state in addition to the incoming interface. If the path messages do not share the same outgoing interface and

next-hop router, the router considers them to be independent LSPs and does not merge them.

- For all the Path messages that share the same outgoing interface and next-hop router, the router uses the following process to select the final LSP:
  - If only one LSP originates from this node, select it as the final LSP.
  - If only one LSP contains a Fast Reroute object, select it as the final LSP.
  - If there are several LSPs and some of them have a Detour object, eliminate those containing a Detour object from the final LSP selection process.
  - If several final LSP candidates remain (that is, there are still both Detour and protected LSPs), select the LSPs with Fast Reroute objects.
  - If none of the LSPs have Fast Reroute objects, select the ones without Detour objects. If all the LSPs have Detour objects, select them all.
  - Of the remaining LSP candidates, eliminate from consideration those that traverse nodes that other LSPs avoid.
  - If several candidate LSPs still remain, select the one with the shortest ERO path length. If more than one LSP has the same path length, select one randomly.
- Once the final LSP has been identified, the router must transmit only the Path messages that correspond to this LSP. All other LSPs are considered merged at this node.

Detour Computations

Computing and setting up detours is done independently at each node. On a node, if an LSP has fast reroute enabled and if a downstream link or node can be identified, the router performs a Constrained Shortest Path First (CSPF) computation using the information in the local TED. For this reason, detours rely on your IGP supporting traffic engineering extensions. Without the TED, detours cannot be established.

CSPF initially attempts to find a path that skips the next downstream node. Attempting to find this path provides protection against downstream failures in either nodes or links. If a node-skipping path is not available, CSPF attempts to find a path on an alternate link to the next downstream node. Attempting to find an alternate link provides protection against downstream failures in links only. Detour computations might not succeed the first time. If a computation fails, the router recomputes detours approximately once every refresh interval until the computation succeeds. The RSVP metric for each detour is set to a value in the range from 10,000 through 19,999.

Fast Reroute Path Optimization

A fast reroute protection path is nondeterministic. The actual protection path of a particular node depends on the history of the LSP and the network topology when the fast reroute path was computed. The lack of deterministic behavior can lead to operational difficulties and poorly optimized paths after multiple link flaps in a network. Even in a small network, after a few link flaps fast reroute paths can traverse

an arbitrarily large number of nodes and can remain in that state indefinitely. This is inefficient and makes the network less predictable.

Fast reroute optimization addresses this deficiency. It provides a global path optimization timer, allowing you to optimize all LSPs that have fast reroute enabled and a detour path up and running. The timer value can be varied depending on the expected RE processing load.

The fast reroute optimization algorithm is based on the IGP metric only. As long as the new path's IGP metric is lower than the old path's, the CSPF result is accepted, even if the new path might be more congested (higher bandwidth utilization) or traverses more hops.

In conformance with RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*, when a new path is computed and accepted for fast reroute optimization, the existing detour is destroyed first and then the new detour is established. To prevent traffic loss, detours actively protecting traffic are not optimized.

Automatic Bandwidth Allocation

Automatic bandwidth allocation allows an MPLS tunnel to automatically adjust its bandwidth allocation based on the volume of traffic flowing through the tunnel. You can configure an LSP with minimal bandwidth; this feature can dynamically adjust the LSP's bandwidth allocation based on current traffic patterns. The bandwidth adjustments do not interrupt traffic flow through the tunnel.

You set a sampling interval on an LSP configured with automatic bandwidth allocation. The average bandwidth is monitored during this interval. At the end of the interval, an attempt is made to signal a new path for the LSP with the bandwidth allocation set to the maximum average value for the preceding sampling interval. If the new path is successfully established and the original path is removed, the LSP is switched over to the new path. If a new path is not created, the LSP continues to use its current path until the end of the next sampling interval, when another attempt is made to establish a new path. Note that you can set minimum and maximum bandwidth values for the LSP.

During the automatic bandwidth allocation interval, the router might receive a steady increase in traffic (increasing bandwidth utilization) on an LSP, potentially causing congestion or packet loss. To prevent this, you can define a second trigger to prematurely expire the automatic bandwidth adjustment timer before the end of the current adjustment interval.

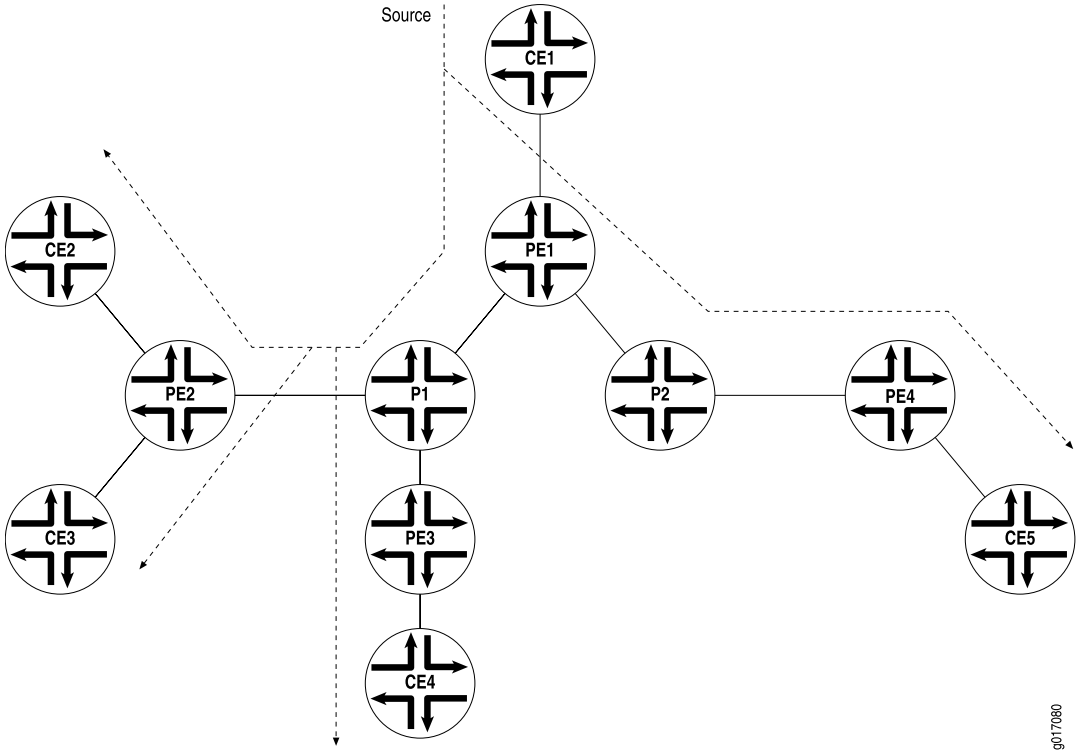
Point-to-Multipoint LSPs

A point-to-multipoint MPLS LSP is an RSVP-signaled LSP with a single source and multiple destinations. By taking advantage of the MPLS packet replication capability of the network, point-to-multipoint LSPs avoid unnecessary packet replication at the ingress router. Packet replication takes place only when packets are forwarded to two or more different destinations requiring different network paths.

This process is illustrated in Figure 18 on page 48. Router PE1 is configured with a point-to-multipoint LSP to Routers PE2, PE3, and PE4. When Router PE1 sends a

packet on the point-to-multipoint LSP to Routers P1 and P2, Router P1 replicates the packet and forwards it to Routers PE2 and PE3. Router P2 sends the packet to Router PE4.

Figure 18: Point-to-Multipoint LSPs



The following are some of the properties of point-to-multipoint LSPs:

- A point-to-multipoint LSP allows you to use MPLS for point-to-multipoint data distribution. This functionality is similar to that provided by IP multicast.
- You can add and remove branch LSPs from a main point-to-multipoint LSP without disrupting traffic. The unaffected parts of the point-to-multipoint LSP continue to function normally.
- You can configure a node to be both a transit and an egress router for different branch LSPs of the same point-to-multipoint LSP.
- You can enable link protection on a point-to-multipoint LSP. Link protection can provide a bypass LSP for each of the branch LSPs that make up the point-to-multipoint LSP. If any of the primary paths fail, traffic can be quickly switched to the bypass.
- You can configure branch LSPs either statically, dynamically, or as a combination of static and dynamic LSPs.
- You can enable graceful restart on point-to-multipoint LSPs.

For information on how to configure point-to-multipoint LSPs, see “Point-to-Multipoint LSP Configuration Guidelines” on page 143. This feature is described in detail in the

Internet drafts draft-raggarwa-mpls-p2mp-te-02.txt, *Establishing Point to Multipoint MPLS TE LSPs*, and draft-ietf-mpls-rsvp-te-p2mp-02.txt, *Extensions to RSVP-TE for Point to Multipoint TE LSPs*.

MPLS Load Balancing Based on the IP Header and MPLS Labels

Juniper Networks routing platforms can load-balance on a per-packet basis in MPLS. Load balancing can be performed on information in both the IP header and on up to three MPLS labels, providing a more uniform distribution of MPLS traffic to next hops. This feature is enabled on supported platforms by default and requires no configuration.

NOTE: This feature is only available on M320 and T-series routing platforms with enhanced FPCs.

The following information is extracted from the packet and used to load-balance the MPLS traffic:

- Interface index—24 bits
- MPLS label stack—bits 0 through 23 (the TTL bits are not examined)
- IPv4 header information:
  - Protocol—8 bits
  - Destination address—32 bits
  - Source address—32 bits
  - Source port—16 bits
  - Destination port—16 bits
- IPv6 header information:
  - Next header—8 bits
  - Least significant 4 bytes of destination address
  - Least significant 4 bytes of source address
  - Source port—16 bits
  - Destination port—16 bits

In summary, MPLS load balancing is performed using the following fields:

Interface index + MPLS label + IP header (IPv4 or IPv6)

Chapter 4

MPLS Configuration Statements

The following sections provide the complete hierarchy of MPLS statements and the minimum configuration necessary to enable MPLS:

- MPLS Configuration Statements on page 51
- Minimum MPLS Configuration on page 55

MPLS Configuration Statements

To configure Multiprotocol Label Switching (MPLS), you can include the following statements in the configuration:

```
disable;
admin-group [ group-names ];
admin-groups {
   group-name group-value;
}
advertisement-hold-time seconds;
auto-policing {
   class all (drop | loss-priority-high | loss-priority-low);
   class ctnumber (drop | loss-priority-high | loss-priority-low);
}
bandwidth bps {
   ct0 bps;
   ct1 bps;
   ct2 bps;
   ct3 bps;
}
class-of-service cos-value;
diffserv-te {
   bandwidth-model {
      extended-mam;
      mam;
      rdm;
   }
   te-class-matrix {
      tenumber {
         priority priority;
         traffic-class ctnumber priority priority;
      }
   }
}
explicit-null;
```

```
hop-limit number;
icmp-tunneling;
interface (interface-name | all) {
    disable;
    admin-group [ group-names ];
    label-map (in-label | default-route) {
        class-of-service cos-value;
        (next-hop (address | interface-name | address/interface-name) | (discard | reject));
        (pop | swap out-label);
        preference preference;
        swap-push swap-label push-label;
    }
}
ipv6-tunneling;
label-switched-path lsp-name {
    disable;
    adaptive;
    admin-down;
    admin-group {
        exclude [ group-names ];
        include-all [ group-names ];
        include-any [ group-names ];
    }
    auto-bandwidth {
        adjust-interval seconds;
        adjust-threshold percent;
        maximum-bandwidth bps;
        minimum-bandwidth bps;
        monitor-bandwidth;
    }
    bandwidth bps {
        ct0 bps;
        ct1 bps;
        ct2 bps;
        ct3 bps;
    }
    class-of-service cos-value;
    description text;
    fast-reroute {
        (bandwidth bps | bandwidth-percent percent);
        (exclude [ group-names ] | no-exclude);
        hop-limit number;
        (include-all [ group-names ] | no-include-all);
        (include-any [ group-names ] | no-include-any);
    }
    from address;
    hop-limit number;
    install {
        destination-prefix/prefix-length <active>;
    }
    ldp-tunneling;
    link-protection;
    lsp-attributes {
        encoding-type (ethernet | packet | pdh | sonet-sdh);
        gpid (ethernet | hdlc | ipv4 | ppp);
        signal-bandwidth type;
```

```
        switching-type (fiber | lambda | psc-1 | tdm);
    }
    metric metric;
    no-cspf;
    no-decrement-ttl;
    node-link-protection;
    optimize-timer seconds;
    p2mp path-name;
    policing {
        filter filter-name;
        no-automatic-policing;
    }
    preference preference;
    primary path-name {
        adaptive;
        admin-group {
            exclude [ group-names ];
            include-all [ group-names ];
            include-any [ group-names ];
        }
        bandwidth bps {
            ct0 bps;
            ct1 bps;
            ct2 bps;
            ct3 bps;
        }
        class-of-service cos-value;
        hop-limit number;
        no-cspf;
        no-decrement-ttl;
        optimize-timer seconds;
        preference preference;
        priority setup-priority reservation-priority;
        (record | no-record);
        select (manual | unconditional);
    }
    standby;
}
priority setup-priority reservation-priority;
(random | least-fill | most-fill);
(record | no-record);
retry-limit number;
retry-timer seconds;
revert-timer seconds;
secondary path-name {
    adaptive;
    admin-group {
        exclude [ group-names ];
        include-all [ group-names ];
        include-any [ group-names ];
    }
    bandwidth bps {
        ct0 bps;
        ct1 bps;
        ct2 bps;
        ct3 bps;
```

```
    }
    class-of-service cos-value;
    hop-limit number;
    no-cspf;
    no-decrement-ttl;
    optimize-timer seconds;
    preference preference;
    priority setup-priority reservation-priority;
    (record | no-record);
    select (manual | unconditional);
}
standby;
soft-preemption {
    cleanup-timer seconds;
}
standby;
to address;
traceoptions {
    file filename <replace> <size size> <files number> <no-stamp>
        <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
}
log-updown {
    no-trap {
        mpls-lsp-traps;
        rfc3812–traps;
    }
    (syslog | no-syslog);
    trap;
    trap-path-down;
    trap-path-up;
}
no-cspf;
no-decrement-ttl;
no-propagate-ttl;
optimize-aggressive;
optimize-timer seconds;
path path-name {
    (address | hostname) <strict | loose>;
}
path-mtu {
    allow-fragmentation;
    rsvp {
        mtu-signaling;
    }
}
preference preference;
priority setup-priority reservation-priority;
(record | no-record);
revert-timer seconds;
rsvp-error-hold-time seconds;
smart-optimize-timer seconds;
standby;
static-path inet {
    prefix {
        class-of-service value;
```

```
        next-hop (address | interface-name | address/interface-name);
        preference preference;
        push out-label;
    }
}
statistics {
    auto-bandwidth;
    file filename <size size> <files number> <no-stamp> <replace>
        <world-readable | no-world-readable>;
    interval seconds;
}
traceoptions {
    file filename <replace> <size size> <files number> <no-stamp>
        <world-readable | no-world-readable>;
    flag flag;
}
traffic-engineering (bgp | bgp-igp | bgp-igp-both-ribs | mpls-forwarding);
```

You can configure these statements at the following hierarchy levels:

- [edit logical-systems *logical-system-name* protocols mpls]
- [edit protocols mpls]

Minimum MPLS Configuration

To enable MPLS on the router, you must include at least the following statements. This minimum configuration enables MPLS on a logical interface. All other MPLS configuration statements are optional. Note that this configuration does nothing more than enable MPLS on the router and on the specified interface.

Include the **family mpls** statement:

```
family mpls;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

Include the interface in the MPLS and Resource Reservation Protocol (RSVP) protocol configuration:

```
mpls {
    interface (interface-name | all); # Required to enable MPLS on the interface
}
rsvp {# Required for RSVP-signaled MPLS only
interface interface-name;
```

You can configure these statements at the following hierarchy levels:

- [edit protocols]
- [edit logical-systems *logical-system-name* protocols]

For every interface you enable, two special routes are installed automatically in the MPLS forwarding table. One route has a label value of 0, and the second has a label value of 1. (For information about these labels, see “Special Labels” on page 25.)

Chapter 5

MPLS-Signaled LSPs Configuration Guidelines

To configure Multiprotocol Label Switching (MPLS)-signaled label-switched paths (LSPs), you create an LSP that runs from the ingress router to the egress router. (For information about Label Distribution Protocol [LDP]-signaled LSPs, see "LDP Configuration Guidelines" on page 337.) To create the LSP, you configure only the ingress router; you do not have to configure any other routers. You can configure the LSP so that the JUNOS software makes all forwarding decisions, or you can configure some or all routers in the path. The LSP is set up by the Resource Reservation Protocol (RSVP) through RSVP-signaling messages. The JUNOS software automatically negotiates, assigns, releases, and reuses labels.

To configure signaled LSPs, perform the following tasks:

- Configuring the Ingress Router for Signaled LSPs on page 57
- Configuring All Other MPLS Routers for Signaled LSPs on page 62
- Configuring an LSP on page 62
- Enabling RSVP on page 100
- Configuring MPLS Exception Monitoring on page 101
- Improving TED Accuracy with RSVP PathErr Messages on page 101
- Examples: Configuring Signaled LSPs on page 103
- Configuring MPLS over GRE Tunnels on page 106
- Configuring IPv6 Tunnels over MPLS on page 108
- Configuring ICMP Message Tunneling on page 112
- LSP Attributes for GMPLS on page 112

Configuring the Ingress Router for Signaled LSPs

To configure signaled LSPs, perform the following tasks on the ingress router:

- Creating a Named Path on page 58
- Configuring Alternate Backup Paths Using Fate Sharing on page 59

Creating a Named Path

To configure signaled LSPs, you must first create one or more named paths on the ingress router. For each path, you can specify some or all transit routers in the path, or you can leave it empty.

Each pathname can contain up to 32 characters and can include letters, digits, periods, and hyphens. The name must be unique within the ingress router. Once a named path is created, you can use the named path with the primary or secondary statement to configure LSPs at the [edit protocols mpls label-switched-path *label-path-name*] hierarchy level. You can specify the same named path on any number of LSPs.

To determine whether an LSP is associated with the primary or secondary path in an RSVP session, issue the show rsvp session detail command. For more information, see the *JUNOS Routing Protocols and Policies Command Reference*.

To create an empty path, create a named path by including the following form of the path statement. This form of the path statement is empty, which means that any path between the ingress and egress routers is accepted. In actuality, the path used tends to be the same path as is followed by destination-based, best-effort traffic.

```
path path-name;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

To create a path in which you specify some or all transit routers in the path, include the following form of the path statement, specifying one address for each transit router:

```
path path-name {
   address | hostname <strict | loose>;
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

In this form of the path statement, you specify one or more transit router addresses. Specifying the ingress and/or egress routers is optional. You can specify the address or hostname of each transit router, although you do not need to list each transit router if its type is loose. Specify the addresses in order, starting with the ingress router (optional) or the first transit router, and continuing sequentially along the path up to the egress router (optional) or the router immediately before the egress router. You need to specify only one address per router hop. If you specify more than one address for the same router, only the first address is used; the additional addresses are ignored and truncated.

For each router address, you specify the type, which can be one of the following:

- strict—(Default) The route taken from the previous router to this router is a direct path and cannot include any other routers. If *address* is an interface address, this router also ensures that the incoming interface is the one specified. Ensuring that the incoming interface is the one specified is important when there are parallel links between the previous router and this router. It also ensures that routing can be enforced on a per-link basis.

  For strict addresses, you must ensure that the router immediately preceding the router you are configuring has a direct connection to that router. The address can be a loopback interface address, in which case the incoming interface is not checked.

- loose—The route taken from the previous router to this router need not be a direct path, can include other routers, and can be received on any interface. The address can be any interface address or the address of the loopback interface.

Examples: Creating a Named Path

The following path, to-hastings, specifies the complete strict path from the ingress to the egress routers through 14.1.1.1, 13.1.1.1, 12.1.1.1, and 11.1.1.1, in that order. There cannot be any intermediate routers except the ones specified. However, there can be intermediate routers between 11.1.1.1 and the egress router because the egress router is not specifically listed in the path statement. To prevent intermediate routers before egress, configure the egress router as the last router, with a strict type.

```
[edit protocols mpls]
path to-hastings {
   14.1.1.1 strict;
   13.1.1.1 strict;
   12.1.1.1 strict;
   11.1.1.1 strict;
}
```

The following path, alt-hastings, allows any number of intermediate routers between routers 14.1.1.1 and 11.1.1.1. In addition, intermediate routers are permitted between 11.1.1.1 and the egress router.

```
[edit protocols mpls]
path alt-hastings {
   14.1.1.1 strict;
   11.1.1.1 loose;
}
```

Configuring Alternate Backup Paths Using Fate Sharing

You can create a database of information that CSPF uses to compute one or more backup paths in case the primary path becomes unstable. The database describes the relationships between elements of the network, such as routers and links. Because these network elements share the same fate, this relationship is called fate sharing.

You can configure backup paths that minimize the number of shared links and fiber paths with the primary paths as much as possible to ensure that, if a fiber is cut, the minimum amount of data is lost and a path still exists to the destination.

For a backup path to work optimally, it must not share links or physical fiber paths with the primary path. This ensures that a single point of failure will not affect the primary and backup paths at the same time.

The following sections describe how to configure fate sharing and how it affects CSPF, and provides a fate sharing configuration example:

- Configuring Fate Sharing on page 60
- Implications for CSPF on page 61
- Example: Configuring Fate Sharing on page 61

Configuring Fate Sharing

To configure fate sharing, include the fate-sharing statement:

```
fate-sharing {
    group group-name {
        cost value;
        from address <to address>;
    }
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Each fate-sharing group must have a name, which can be up to 32 characters long and can contain letters, digits, periods (.) and hyphens (-). You can define up to 512 groups.

Fate-sharing groups contain three types of objects:

- Point-to-point links—Identified by the IP addresses at each end of the link. Unnumbered point-to-point links are typically identified by borrowing IP addresses from other interfaces. Order is not important; from 1.2.3.4 to 1.2.3.5 and from 1.2.3.5 to 1.2.3.4 have the same meaning.
- Non-point-to-point links—Include links on a LAN interface (such as Gigabit Ethernet interfaces) or nonbroadcast multiaccess (NBMA) interfaces (such as Asynchronous Transfer Mode [ATM] or Frame Relay). You identify these links by their individual interface address. For example, if the LAN interface 192.168.200.0/24 has four routers attached to it, each router link is individually identified:

  from 192.168.200.1; # LAN interface of router 1

  from 192.168.200.2; # LAN interface of router 2

  from 192.168.200.3; # LAN interface of router 3

  from 192.168.200.4; # LAN interface of router 4

You can list the addresses in any order.

- A router node—Identified by its configured router ID.

All objects in a group share certain similarities. For example, you can define a group for all fibers that share the same fiber conduit, all optical channels that share the same fiber, all links that connect to the same LAN switch, all equipment that shares the same power source, and so on. All objects are treated as /32 host addresses.

For a group to be meaningful, it should contain at least two objects. You can configure groups with zero or one object; these groups are ignored during processing.

An object can be in any number of groups, and a group can contain any number of objects. Each group has a configurable cost attributed to it, which represents the level of impact this group has on CSPF computations. The higher the cost, the less likely a backup path will share with the primary path any objects in the group. The cost is directly comparable to traffic engineering metrics. By default, the cost is 1. Changing the fate-sharing database does not affect established LSPs until the next reoptimization of CSPF. The fate-sharing database does influence fast-reroute computations.

Implications for CSPF

When CSPF computes the primary paths of an LSP (or secondary paths when the primary path is not active), it ignores the fate-sharing information. You always want to find the best possible path (least IGP cost) for the primary path.

When CSPF computes a secondary path while the primary path (of the same LSP) is active, the following occurs:

1. CSPF identifies all fate-sharing groups that are associated with the primary path. CSPF does this by identifying all links and nodes that the primary path traverses and compiling group lists that contain at least one of the links or nodes. CSPF ignores the ingress and egress nodes in the search.
2. CSPF checks each link in the TED against the compiled group list. If the link is a member of a group, the cost of the link is increased by the cost of the group. If a link is a member of multiple groups, all group costs are added together.
3. CSPF performs the check for every node in the TED, except the ingress and egress node. Again, a node can belong to multiple groups, so costs are additive.
4. The router performs regular CSPF computation with the adjusted topology.

Example: Configuring Fate Sharing

Configure fate-sharing groups east and west. Because west has no objects, it is ignored during processing.

```
[edit routing-options]
fate-sharing {
   group east {
      cost 20; # Optional, default value is 1
      from 1.2.3.4 to 1.2.3.5; # A point-to-point link
```

```
        from 192.168.200.1; # LAN interface
        from 192.168.200.2; # LAN interface
        from 192.168.200.3; # LAN interface
        from 192.168.200.4; # LAN interface
        from 10.168.1.220; # Router ID of a router node
        from 10.168.1.221; # Router ID of a router node
    }
    group west {
        .....
    }
}
```

Configuring All Other MPLS Routers for Signaled LSPs

To configure signaled LSPs on all MPLS routers that should participate in MPLS, you need to enable MPLS and RSVP on these routers, as described in "Minimum MPLS Configuration" on page 55 and "Enabling RSVP" on page 100.

Configuring an LSP

The next step in configuring signaled LSPs is to create one or more LSPs and define the properties associated with the label-switched path on the ingress router. To configure an LSP, include the label-switched-path statement:

```
label-switched-path lsp-name {
    disable;
    adaptive;
    admin-down;
    admin-group {
        exclude [ group-names ];
        include-all [ group-names ];
        include-any [ group-names ];
    }
    auto-bandwidth {
        adjust-interval seconds;
        adjust-threshold percent;
        maximum-bandwidth bps;
        minimum-bandwidth bps;
        monitor-bandwidth;
    }
    bandwidth bps {
        ct0 bps;
        ct1 bps;
        ct2 bps;
        ct3 bps;
    }
    class-of-service cos-value;
    description text;
    fast-reroute {
        (bandwidth bps | bandwidth-percent percent);
        (exclude [ group-names ] | no-exclude);
        hop-limit number;
        (include-all [ group-names ] | no-include-all);
```

```
    (include-any [ group-names ] | no-include-any);
}
from address;
hop-limit number;
install {
    destination-prefix/prefix-length <active>;
}
ldp-tunneling;
link-protection;
lsp-attributes {
    encoding-type (ethernet | packet | pdh | sonet-sdh);
    gpid (ethernet | hdlc | ipv4 | ppp);
    signal-bandwidth type;
    switching-type (fiber | lambda | psc-1 | tdm);
}
metric number;
no-cspf;
no-decrement-ttl;
node-link-protection;
optimize-timer seconds;
p2mp path-name;
policing {
    filter filter-name;
    no-automatic-policing;
}
preference preference;
primary path-name {
    adaptive;
    admin-group {
        exclude [ group-names ];
        include-all [ group-names ];
        include-any [ group-names ];
    }
    bandwidth bps {
        ct0 bps;
        ct1 bps;
        ct2 bps;
        ct3 bps;
    }
    class-of-service cos-value;
    hop-limit number;
    no-cspf;
    no-decrement-ttl;
    optimize-timer seconds;
    preference preference;
    priority setup-priority reservation-priority;
    (record | no-record);
    select (manual | unconditional);
    standby;
}
priority setup-priority reservation-priority;
(random | least-fill | most-fill);
(record | no-record);
retry-limit number;
retry-timer seconds;
revert-timer seconds;
```

```
    secondary path-name {
        adaptive;
        admin-group {
            exclude [ group-names ];
            include-all [ group-names ];
            include-any [ group-names ];
        }
        bandwidth bps {
            ct0 bps;
            ct1 bps;
            ct2 bps;
            ct3 bps;
        }
        class-of-service cos-value;
        hop-limit number;
        no-cspf;
        no-decrement-ttl;
        optimize-timer seconds;
        preference preference;
        priority setup-priority reservation-priority;
        (record | no-record);
        select (manual | unconditional);
        standby;
    }
    soft-preemption {
        cleanup-timer seconds;
    }
    standby;
    to address;
    traceoptions {
        file filename <replace> <size size> <files number> <no-stamp>
            <world-readable | no-world-readable>;
        flag flag <flag-modifier> <disable>;
    }
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

Each LSP must have a name, *lsp-name*, which can be up to 32 characters long and can contain letters, digits, periods (.), and hyphens (-). The name must be unique within the ingress router. For ease of management and identification, configure unique names across the entire domain.

When you configure LSPs, you can specify the following statements either for each LSP or for each path. For statements that you configure on a per-LSP basis, the value applies to all paths in the LSP. For statements that you configure on a per-path basis, the path value overrides the per-LSP value.

- adaptive
- admin-group
- auto-bandwidth

- bandwidth
- class-of-service
- hop-limit
- no-cspf
- optimize-timer
- preference
- priority
- record or no-record
- standby

For maintenance purposes, you can also configure the following attributes across all LSPs and any paths within those LSPs:

- admin-group
- bandwidth
- class-of-service
- no-decrement-ttl
- no-record
- optimize-timer
- preference
- priority
- smart-optimize-timer
- standby

For each LSP, you can configure the following properties:

- Configuring the Address of the Egress and Ingress Routers on page 66
- Configuring the Primary and Secondary LSPs on page 68
- Configuring the Description on page 71
- Configuring Fast Reroute on page 71
- Configuring the Optimization Interval for Fast Reroute Paths on page 72
- Configuring Addresses to Associate with the LSP on page 73
- Configuring Path Connection Retry Information on page 74
- Configuring the LSP Metric on page 75
- Configuring CSPF Tie Breaking on page 76
- Configuring Load Balancing for MPLS LSPs on page 77
- Disabling Normal TTL Decrementing on page 79
- Configuring MPLS Soft Preemption on page 80

- Configuring Automatic Bandwidth Allocation on page 81
- Disabling Constrained-Path LSP Computation on page 88
- Configuring Administrative Groups on page 89
- Configuring the LSP Preference on page 91
- Configuring Path Route Recording on page 91
- Configuring Class of Service for MPLS on page 91
- Configuring Adaptive LSPs on page 94
- Configuring Priority and Preemption for LSPs on page 95
- Optimizing Signaled LSPs on page 96
- Configuring the Smart Optimize Timer on page 97
- Configuring the Maximum Path Length on page 98
- Configuring the Path Bandwidth on page 98
- Configuring the Standby State on page 99
- Configuring LSP Hold Time on page 100
- Configuring LDP Tunneling on page 100

Configuring the Address of the Egress and Ingress Routers

The following sections describe how to configure the address for the egress and ingress routers:

- Configuring the Address of the Egress Router on page 66
- Preventing the Addition of Egress Router Addresses to Routing Tables on page 67
- Configuring the Address of the Ingress Router on page 68

Configuring the Address of the Egress Router

When configuring an LSP, you must specify the address of the egress router by including the to statement:

```
to address;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name*]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]

When you are setting up an LSP, the to statement is the only required statement. All other statements are optional.

After the LSP is established, the address of the egress router is installed as a host route in the routing table. This route can then be used by Border Gateway Protocol (BGP) to forward traffic.

To have the software send BGP traffic over an LSP, the address of the egress router is the same as the address of the BGP next hop. You can specify the egress router's address as any one of the router's interface addresses or as the BGP router ID. If you specify a different address, even if the address is on the same router, BGP traffic is not sent over the LSP.

To determine the address of the BGP next hop, use the show route detail command. To determine the destination address of an LSP, use the show mpls lsp command. To determine whether a route has gone through an LSP, use the show route or show route forwarding-table command. In the output of these last two commands, the label-switched-path or push keyword included with the route indicates it has passed through an LSP. Also, use the traceroute command to trace the actual path to which the route leads. This is another indication as to whether a route has passed through an LSP.

You also can manipulate the address of the BGP next hop by defining a BGP import policy filter that sets the route's next-hop address.

Preventing the Addition of Egress Router Addresses to Routing Tables

You must configure an address using the to statement for all RSVP LSPs. This address is always installed as a /32 prefix in the inet.3 or inet.0 routing tables. You can prevent the egress router address configured using the to statement from being added to the inet.3 and inet.0 routing tables by including the no-install-to-address statement.

Some reasons not to install the to statement address in the inet.3 and inet.0 routing tables include the following:

- Allow CSPF RSVP LSPs to be mapped to traffic intended for secondary loopback addresses. If you configure an RSVP tunnel, including the no-install-to-address statement, and then configure an install pfx/ <active> policy later, you can do the following:
  - Verify that the LSP was set up correctly without impacting traffic.
  - Map traffic to the LSP in incremental steps.
  - Map traffic to the destination loopback address (the BGP next hop) by removing the no-install-to-address statement once troubleshooting is complete.
- Prevent CCC connections from losing IP traffic. When an LSP determines that it does not belong to a connection, it installs the address specified with the to statement in the inet.3 routing table. IP traffic is then forwarded to the CCC remote endpoint, which can cause some types of PICs to fail.

To prevent the egress router address configured using the to statement from being added to the inet.3 and inet.0 routing tables, include the no-install-to-address statement:

```
no-install-to-address;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name*]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]

Configuring the Address of the Ingress Router

The local router always is considered to be the ingress router, which is the beginning of the LSP. The software automatically determines the proper outgoing interface and IP address to use to reach the next router in an LSP.

By default, the router ID is chosen as the address of the ingress router. To override the automatic selection of the source address, specify a source address in the from statement:

```
from address;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name*]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]

The outgoing interface used by the LSP is not affected by the source address that you configure.

Configuring the Primary and Secondary LSPs

By default, an LSP routes itself hop-by-hop toward the egress router. The LSP tends to follow the shortest path as dictated by the local routing table, usually taking the same path as destination-based, best-effort traffic. These paths are "soft" in nature because they automatically reroute themselves whenever a change occurs in a routing table or in the status of a node or link.

To configure the path so that it follows a particular route, create a named path using the path statement, as described in "Creating a Named Path" on page 58. Then apply the named path by including the primary or secondary statement. A named path can be referenced by any number of LSPs.

To configure primary and secondary paths for an LSP, complete the steps in the following sections:

- Configuring Primary and Secondary Paths for an LSP on page 68
- Configuring the Revert Timer on page 69
- Specifying Path Selection on page 70

Configuring Primary and Secondary Paths for an LSP

The primary statement creates the primary path, which is the LSP's preferred path. The secondary statement creates an alternative path. If the primary path can no longer reach the egress router, the alternative path is used.

To configure primary and secondary paths, include the primary and secondary statements:

```
primary path-name {
    ...
}
```

```
secondary path-name {
   ...
}
```

You can include these statements at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name*]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]

When the software switches from the primary to a secondary path, it continuously attempts to revert to the primary path, switching back to it when it is again reachable, but no sooner than the retry time specified in the retry-timer statement. (For more information, see "Configuring Path Connection Retry Information" on page 74.)

You can configure zero or one primary path. If you do not configure a primary path, the first secondary path that is established is selected as the path.

You can configure zero or more secondary paths. All secondary paths are equal, and the software tries them in the order that they are listed in the configuration. The software does not attempt to switch among secondary paths. If the current secondary path is not available, the next one is tried. To create a set of equal paths, specify secondary paths without specifying a primary path.

If you do not specify any named paths, or if the path that you specify is empty, the software makes all routing decisions necessary to reach the egress router.

Configuring the Revert Timer

For LSPs configured with both primary and secondary paths, it is possible to configure the revert timer. If a primary path goes down and traffic is switched to the secondary path, the revert timer specifies the amount of time (in seconds) that the LSP must wait before it can revert traffic back to a primary path. If during this time, the primary path experiences any connectivity problems or stability problems, the timer is restarted.

The JUNOS software also makes a determination as to which path is the preferred path. The preferred path is the path which has not encountered any difficulty in the last revert timer period. If both the primary and secondary paths have encountered difficulty, neither path is considered preferred. However, if one of the paths is dynamic and the other static, the dynamic path is selected as the preferred path.

The range of values you can configure for the revert timer is 0 through 65,535 seconds. The default value is 60 seconds.

If you configure a value of 0 seconds, the traffic on the LSP, once switched from the primary path to the secondary path, remains on the secondary path permanently (until the network operator intervenes or until the secondary path goes down).

You can configure the revert timer for all LSPs on the router at the [edit protocols mpls] hierarchy level or for a specific LSP at the [edit protocols mpls label-switched-path *lsp-name*] hierarchy level.

To configure the revert timer, include the revert-timer statement:

revert-timer *seconds*;

For a list of hierarchy levels at which you can include this statement, see the summary section for this statement.

Specifying Path Selection

When you have configured both primary and secondary paths for an LSP, you may need to ensure that only a specific path is used.

The select statement is optional. If you do not configure this statement, an automatic path selection algorithm is used. If you include the select statement, you must specify either the manual option or the unconditional option. You cannot specify both.

The manual and unconditional options do the following:

- manual—The path is immediately selected for carrying traffic as long as it is up and stable. Traffic is sent to other working paths if the current path is down or degraded (receiving errors). This parameter overrides all other path attributes except the select unconditional statement.
- unconditional—The path is selected for carrying traffic unconditionally, regardless of whether the path is currently down or degraded (receiving errors). This parameter overrides all other path attributes.

  Because the unconditional option switches to a path without regard to its current status, be aware of the following potential consequences when using this parameter:

  - If a path is not currently up when you enable the unconditional option, it can cause traffic disruptions. Ensuring that a path is functional before specifying the unconditional option helps to avoid this issue.
  - Once a path is selected because it has the unconditional option enabled, all other paths for the LSP are gradually cleared, including the primary and standby paths. No path can act as a standby to an unconditional path, so signaling those paths serves no purpose.

You can configure only one path for an LSP with the select manual statement and one path for an LSP with the select statement with the unconditional option. These statements cannot be configured on two or more paths used by the same LSP.

You can enable and disable the manual and unconditional options for the select statement while LSPs and their paths are up and running without disrupting traffic.

To modify the behavior of the LSP such that a path is selected for carrying traffic if it is up and stable for at least the revert timer window, include the select statement with the manual option:

select manual;

For a list of hierarchy levels at which you can include this statement, see the summary section for this statement.

To modify the behavior of the LSP such that a path is selected for carrying traffic unconditionally, regardless of whether the path is currently down or degraded, include the select statement with the unconditional option:

```
select unconditional;
```

For a list of hierarchy levels at which you can include this statement, see the summary section for this statement.

Configuring the Description

You can provide a textual description for the LSP. Enclose any descriptive text that includes spaces in quotation marks (" "). Any descriptive text you include is displayed in the output of the show mpls lsp detail command and has no effect on the operation of the LSP.

To provide a textual description for the LSP, include the description statement:

```
description text;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name*]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]

The description text can be no more than 80 characters in length.

Configuring Fast Reroute

Fast reroute provides a mechanism for automatically rerouting traffic on an LSP if a node or link in an LSP fails, thus reducing the loss of packets traveling over the LSP.

To configure fast reroute on an LSP, include the fast-reroute statement on the ingress router:

```
fast-reroute {
    (bandwidth bps | bandwidth-percent percentage);
    (exclude group-names | no-exclude);
    hop-limit number;
    include-all [ group-names ];
    include-any [ group-names ];
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name*]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]

You do not need to configure fast reroute on the LSP's transit and egress routers. Once fast reroute is enabled, the ingress router signals all the downstream routers that fast reroute is enabled on the LSP, and each downstream router does its best to set up detours for the LSP. If a downstream router does not support fast reroute, it

ignores the request to set up detours and continues to support the LSP. A router that does not support fast reroute will cause some of the detours to fail, but otherwise has no impact on the LSP.

NOTE: To enable PFE fast reroute, configure a routing policy statement with the load-balance per-packet option at the [edit policy-options policy-statement *policy-name* then] hierarchy level on each of the routers where traffic might be rerouted. See also "Configuring RSVP LSP Load Balancing" on page 287.

By default, no bandwidth is reserved for the rerouted path. To allocate bandwidth for the rerouted path, include either the bandwidth statement or the bandwidth-percent statement. You can only include one of these statements at a time. If you do not include either the bandwidth statement or the bandwidth-percent statement, the default setting is to not reserve bandwidth for the detour path.

When you include the bandwidth statement, you can specify the specific amount of bandwidth (in bits per second [bps]) you want to reserve for the detour path. The bandwidth does not need to be identical to that allocated for the LSP.

When you specify a bandwidth percent using the bandwidth-percent statement, the detour path bandwidth is computed by multiplying the bandwidth percent by the bandwidth configured for the main traffic-engineered LSP. For information on how to configure the bandwidth for a traffic-engineered LSP, see "Configuring a Traffic Engineered LSP" on page 129.

Hop-limit constraints define how many more routers a detour is allowed to traverse compared with the LSP itself. By default, the hop limit is set to 6. For example, if an LSP traverses 4 routers, any detour for the LSP can be up to 10 (that is, 4 + 6) router hops, including the ingress and egress routers.

By default, a detour inherits the same administrative (coloring) group constraints as its parent LSP when CSPF is determining the alternate path. Administrative groups, also known as link coloring or resource class, are manually assigned attributes that describe the "color" of links, such that links with the same color conceptually belong to the same class. If you specify the include-any statement when configuring the parent LSP, all links traversed by the alternate session must have at least one color found in the list of groups. If you specify the include-all statement when configuring the parent LSP, all links traversed by the alternate session must have all of the colors found in the list of groups. If you specify the exclude statement when configuring the parent LSP, none of the links must have a color found in the list of groups. For more information about administrative group constraints, see "Configuring Administrative Groups" on page 89.

Configuring the Optimization Interval for Fast Reroute Paths

You can enable path optimization for fast reroute by configuring the fast reroute optimize timer. The optimize timer triggers a periodic optimization process that recomputes the fast reroute detour LSPs to use network resources more efficiently.

To enable fast reroute path optimization, specify the number of seconds including the fast-reroute optimize-timer statement:

```
fast-reroute optimize-timer seconds;
```

You can include this statement at the following hierarchy levels:

- [edit logical-systems *logical-system-name* protocols rsvp]
- [edit protocols rsvp]

Configuring Addresses to Associate with the LSP

By default, a host route toward the egress router is installed in the inet.3 routing table. (The host route address is the one you configure in the to statement.) Installing the host route allows BGP to perform next-hop resolution. It also prevents the host route from interfering with prefixes learned from dynamic routing protocols and stored in the inet.0 routing table.

Unlike the routes in the inet.0 table, routes in the inet.3 table are not copied to the Packet Forwarding Engine, and hence they cause no changes in the system forwarding table directly. You cannot use the ping or traceroute command through these routes. The only use for inet.3 is to permit BGP to perform next-hop resolution. To examine the inet.3 table, use the show route table inet.3 command.

To inject additional routes into the inet.3 routing table, include the install statement:

```
install {
   destination-prefix <active>;
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name*]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]

The specified routes are installed as aliases into the routing table when the LSP is established. Installing additional routes allows BGP to resolve next hops within the specified prefix and to direct additional traffic for these next hops to a particular LSP.

Including the active option with the install statement installs the specified prefix into the inet.0 routing table, which is the primary forwarding table. The result is a route that is installed in the forwarding table any time the LSP is established, which means you can ping or trace the route. Use this option with care, because this type of prefix is very similar to a static route.

You use alias routes for routers that have multiple addresses being used as BGP next hops, or for routers that are not MPLS capable. In either of these cases, the LSP can be configured to another MPLS capable system within the local domain, which then acts as a “border” router. The LSP then terminates on the border router and, from that router, Layer 3 forwarding takes the packet to the true next-hop router.

In the case of an interconnect, the domain’s border router can act as the proxy router and can advertise the prefix for the interconnect if the border router is not setting the BGP next hop to itself.

In the case of a point of presence (POP) that has routers that do not support MPLS, one router (for example, a core router) that supports MPLS can act as a proxy for the entire POP and can inject a set of prefixes that cover the POP. Thus, all routers within the POP can advertise themselves as interior BGP (IBGP) next hops, and traffic can follow the LSP to reach the core router. This means that normal IGP routing would prevail within the POP.

You cannot use the ping or traceroute commands on routes in the inet.3 routing table.

For BGP next-hop resolution, it makes no difference whether a route is in inet.0 or inet.3; the route with the best match (longest mask) is chosen. Among multiple best-match routes, the one with the highest preference value is chosen.

Configuring Path Connection Retry Information

The ingress router might make many attempts to connect and reconnect to the egress router using the primary path. You can control how often the ingress router tries to establish a connection using the primary path and how long it waits between retry attempts.

The retry timer configures how long the ingress router waits before trying to connect again to the egress router using the primary path. The default retry time is 30 seconds. The time can be from 1 through 600 seconds. To modify this value, include the retry-timer statement:

```
retry-timer seconds;
```

You can configure this statement at the following hierarchy levels:

- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]
- [edit protocols mpls label-switched-path *lsp-name*]

By default, no limit is set to the number of times an ingress router attempts to establish or reestablish a connection to the egress router using the primary path. To limit the number of attempts, include the retry-limit statement:

```
retry-limit number;
```

You can configure this statement at the following hierarchy levels:

- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]
- [edit protocols mpls label-switched-path *lsp-name*]

The limit can be a value up to 10,000. When the retry limit is exceeded, no more attempts are made to establish a path connection. At this point, intervention is required to restart the primary path.

If you set a retry limit, it is reset to 1 each time a successful primary path is created.

Configuring the LSP Metric

The LSP metric is used to indicate the ease or difficulty of sending traffic over a particular LSP. Lower LSP metric values (lower cost) increase the likelihood of an LSP being used. Conversely, high LSP metric values (higher cost) decrease the likelihood of an LSP being used.

The LSP metric can be specified dynamically by the router or explicitly by the user as described in the following sections:

- Configuring a Dynamic LSP Metric on page 75
- Configuring a Static LSP Metric on page 75

Configuring a Dynamic LSP Metric

If no specific metric is configured, an LSP attempts to track the IGP metric toward the same destination (the to address of the LSP). IGP includes Open Shortest Path First (OSPF), IS-IS, Routing Information Protocol (RIP), and static routes. BGP and other RSVP/LDP routes are excluded.

For example, if the OSPF metric toward a router is 20, all LSPs toward that router automatically inherit metric 20. If the OSPF toward a router later changes to a different value, all LSP metrics change accordingly. If there are no IGP routes toward the router, the LSP raises its metric to 65,535.

Note that in this case, the LSP metric is completely determined by IGP; it bears no relationship to the actual path the LSP is currently traversing. If LSP reroutes (such as through reoptimization), its metric does not change, and thus it remains transparent to users. Dynamic metric is the default behavior; no configuration is required.

Configuring a Static LSP Metric

You can manually assign a fixed metric value to an LSP. Once configured with the metric statement, the LSP metric is fixed and cannot change:

metric *number*;

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name*]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]

The LSP metric has several uses:

- When there are parallel LSPs with the same egress router, the metrics are compared to determine which LSP has the lowest metric value (the lowest cost) and therefore the preferred path to the destination. If the metrics are the same, the traffic is shared.

  Adjusting the metric values can force traffic to prefer some LSPs over others, regardless of the underlying IGP metric.

- When an IGP shortcut is enabled (see "IGP Shortcuts" on page 33), an IGP route might be installed in the routing table with an LSP as the next hop, if the LSP is on the shortest path to the destination. In this case, the LSP metric is added to the other IGP metrics to determine the total path metric. For example, if an LSP whose ingress router is X and egress router is Y is on the shortest path to destination Z, the LSP metric is added to the metric for the IGP route from Y to Z to determine the total cost of the path. If several LSPs are potential next hops, the total metrics of the paths are compared to determine which path is preferred (that is, has the lowest total metric). Or, IGP paths and LSPs leading to the same destination could be compared by means of the metric value to determine which path is preferred.

  By adjusting the LSP metric, you can force traffic to prefer LSPs, prefer the IGP path, or share the load among them.

- If router X and Y are BGP peers and if there is an LSP between them, the LSP metric represents the total cost to reach Y from X. If for any reason the LSP reroutes, the underlying path cost might change significantly, but X's cost to reach Y remains the same (the LSP metric), which allows X to report through a BGP multiple exit discriminator (MED) a stable metric to downstream neighbors. As long as Y remains reachable through the LSP, no changes are visible to downstream BGP neighbors.

It is possible to configure IS-IS to ignore the configured LSP metric by including the ignore-lsp-metrics statement at the [edit protocols isis traffic-engineering shortcuts] hierarchy level. This statement removes the mutual dependency between IS-IS and MPLS for path computation. For more information, see the *JUNOS Routing Protocols Configuration Guide*.

Configuring CSPF Tie Breaking

When selecting a path for an LSP, CSPF uses a tie-breaking process if there are several equal-cost paths. For information about how CSPF selects a path, see "How CSPF Selects a Path" on page 30.

You can configure one of the following statements (you can only configure one of these statements at a time) to alter the behavior of CSPF tie-breaking:

- To configure a random tie-breaking rule for CSPF to use to choose among equal-cost paths, include the random statement:

  ```
  random;
  ```

- To prefer the path with the least-utilized links, include the least-fill statement:

  ```
  least-fill;
  ```

- To prefer the path with the most-utilized links, include the most-fill statement:

  ```
  most-fill;
  ```

You can include each of these statements at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name*]

- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]

Configuring Load Balancing for MPLS LSPs

Load balancing is used to evenly distribute traffic when the following conditions apply:

- There are multiple equal-cost next hops over different interfaces to the same destination.
- There is a single next hop over an aggregated interface.

By default, when load balancing is used to help distribute traffic, the JUNOS software employs a hash algorithm to select a next-hop address to install into the forwarding table. Whenever the set of next hops for a destination changes in any way, the next-hop address is reselected by means of the hash algorithm.

You can configure how the hash algorithm is used to load-balance traffic across a set of equal-cost LSPs. The hash algorithm can be configured to use the first MPLS label, the first two MPLS labels, the IP payload, or the first and second MPLS labels and the IP payload.

For more information about statements configured under the [edit forwarding-options] hierarchy level, see the *JUNOS Policy Framework Configuration Guide*.

The following sections describe how to configure load balancing for MPLS LSPs:

- Using the First MPLS Label in the Hash Key on page 77
- Using the Second MPLS Label in the Hash Key on page 77
- Using the Third MPLS Label in the Hash Key on page 78
- Using the IP Payload in the Hash Key on page 78
- Using the First Two Labels and the IP Payload in the Hash Key on page 78
- Configuring Load Balancing for MPLS LSPs Without CSPF on page 79

Using the First MPLS Label in the Hash Key

To use the first MPLS label in the hash key, include the label-1 statement at the [edit forwarding-options hash-key family mpls] hierarchy level:

```
[edit forwarding-options hash-key family mpls]
label-1;
```

Using the Second MPLS Label in the Hash Key

To use the second MPLS label in the hash key, include both the label-1 statement and the label-2 statement at the [edit forwarding-options hash-key family mpls] hierarchy level:

```
[edit forwarding-options hash-key family mpls]
label-1;
label-2;
```

Using the Third MPLS Label in the Hash Key

To use the third MPLS label in the hash key, include the label-1, label-2, and label-3 statements at the [edit forwarding-options hash-key family mpls] hierarchy level:

```
[edit forwarding-options hash-key family mpls]
label-1;
label-2;
label-3;
```

Using the IP Payload in the Hash Key

To use the MPLS packet's IP payload (IP version 4 [IPv4] or IP version 6 [IPv6]) in the hash key, include the no-labels and payload statements at the [edit forwarding-options hash-key family mpls] hierarchy level. Specify the ip option to the payload statement at the [edit forwarding-options hash-key family mpls payload] hierarchy level:

```
[edit forwarding-options hash-key family mpls]
no-labels;
payload {
    ip;
}
```

NOTE: The router determines if the MPLS payload is an IP packet by checking the byte containing the IP version number. If the IP version number is 4 (IPv4) or 6 (IPv6), the packet is assumed to be an IP packet.

Using the First Two Labels and the IP Payload in the Hash Key

To use the first and second MPLS labels and the MPLS packet's IP payload in the hash key, include the label-1, label-2, and payload statements at the [edit forwarding-options hash-key family mpls] hierarchy level. Specify the ip option to the payload statement at the [edit forwarding-options hash-key family mpls payload] hierarchy level:

```
[edit forwarding-options hash-key family mpls]
label-1;
label-2;
payload {
    ip;
}
```

NOTE: This feature can be used on T-series and M320 routers only. If you configure this feature on an M-series router, only label-1 and the IP payload are used in the hash key.

Configuring Load Balancing for MPLS LSPs Without CSPF

An LSP tends to load-balance its placement by randomly selecting one of the equal-cost next hops and using it exclusively. The random selection is made independently at each transit router, which compares IGP metrics alone. No consideration is given to bandwidth or congestion levels.

Disabling Normal TTL Decrementing

By default, the time to live (TTL) field value in the packet header is decremented by 1 for every hop the packet traverses in the LSP, thereby preventing loops. If the TTL field value reaches 0, packets are dropped, and an Internet Control Message Protocol (ICMP) error packet can be sent to the originating router.

If normal TTL decrement is disabled, the TTL field of IP packets entering LSPs are decremented by only 1 on transiting the LSP, making the LSP appear as a one-hop router to diagnostic tools, such as traceroute. Decrementing the TTL field by 1 is done by the ingress router, which pushes a label on IP packets with the TTL field in the label initialized to 255. The label's TTL field value is decremented by 1 for every hop the MPLS packet traverses in the LSP. On the penultimate hop of the LSP, the router pops the label but does not write the label's TTL field value to the IP packet's TTL field. Instead, when the IP packet reaches the egress router, the IP packet's TTL field value is decremented by 1.

When you use traceroute to diagnose problems with an LSP from outside that LSP, traceroute sees the ingress router, although the egress router performs the TTL decrement. The behavior of traceroute is different if it is initiated from the ingress router of the LSP. In this case, the egress router would be the first router to respond to traceroute.

You can disable normal TTL decrementing in an LSP so that the TTL field value does not reach 0 before the packet reaches its destination, thus preventing the packet from being dropped. You can also disable normal TTL decrementing to make the MPLS cloud appear as a single hop, thereby hiding the network topology.

There are two ways to disable TTL decrementing:

- On the ingress of the LSP, if you include the no-decrement-ttl statement, the ingress router negotiates with all downstream routers using a proprietary RSVP object, to ensure all routers are in agreement. If negotiation succeeds, the whole LSP behaves as one hop to transit IP traffic.

  ```
  no-decrement-ttl;
  ```

  For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

  Note that the RSVP object is proprietary to the JUNOS software and might not work with other software. This potential incompatibility applies only to RSVP-signaled LSPs. When you include the no-decrement-ttl statement, TTL hiding can be enforced on a per-LSP basis.

- On the router, you can include the no-propagate-ttl statement. This statement applies to all LSPs, regardless of whether they are RSVP-signaled or LDP-signaled.

Once set, all future LSPs traversing through this router behave as a single hop to IP packets. LSPs established before you configure this statement are not affected.

```
no-propagate-ttl;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

If you include the no-propagate-ttl statement, make sure all routers are configured consistently within an MPLS domain; failing to do so might cause the IP packet TTL to increase while in transit within LSPs. This can happen, for example, when the ingress router has no-propagate-ttl configured but the penultimate router does not, so the penultimate router writes the MPLS TTL value (which starts from the ingress router as 255) into the IP packet.

The operation of the no-propagate-ttl statement is more interoperable with other vendors' equipment. However, you must ensure that all routers are configured identically.

Configuring MPLS Soft Preemption

Soft preemption attempts to establish a new path for a preempted LSP before tearing down the original LSP. The default behavior is to tear down a preempted LSP first, signal a new path, and then reestablish the LSP over the new path. In the interval between when the path is taken down and the new LSP is established, any traffic attempting to use the LSP is lost. Soft preemption prevents this type of traffic loss. The trade-off is that during the time when an LSP is being soft preempted, two LSPs with their corresponding bandwidth requirements are used until the original path is torn down.

MPLS soft preemption is useful for network maintenance. For example, you can move all LSPs away from a particular interface, then take the interface down for maintenance without interrupting traffic. MPLS soft preemption is described in detail in Internet draft draft-ietf-mpls-soft-preemption-02.txt, *MPLS Traffic Engineering Soft Preemption*.

Soft preemption is a property of the LSP and is disabled by default. You configure it at the ingress of an LSP by including the soft-preemption statement:

```
soft-preemption;
```

You can include this statement at the following hierarchy levels:

- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]
- [edit protocols mpls label-switched-path *lsp-name*]

You can also configure a timer for soft preemption. The timer designates the length of time the router should wait before initiating a hard preemption of the LSP. At the end of the time specified, the LSP is torn down and resignaled. The soft-preemption

cleanup timer has a default value of 30 seconds; the range of permissible values is 0 through 180 seconds. A value of 0 means that soft preemption is disabled. The soft-preemption cleanup timer is global for all LSPs.

Configure the timer by including the cleanup-timer statement:

```
cleanup-timer seconds;
```

You can include this statement at the following hierarchy levels:

- [edit logical-systems *logical-system-name* protocols rsvp preemption soft-preemption]
- [edit protocols rsvp preemption soft-preemption]

NOTE: Soft preemption cannot be configured on LSPs for which secondary paths or fast reroute has been configured. The configuration fails to commit.

Configuring Automatic Bandwidth Allocation

Automatic bandwidth allocation allows an MPLS tunnel to automatically adjust its bandwidth allocation based on the volume of traffic flowing through the tunnel. You can configure an LSP with minimal bandwidth, and this feature can dynamically adjust the LSP's bandwidth allocation based on current traffic patterns. The bandwidth adjustments do not interrupt traffic flow through the tunnel.

At the end of the automatic bandwidth allocation time interval, the current maximum average bandwidth usage is compared with the allocated bandwidth for the LSP. If the LSP needs more bandwidth, an attempt is made to set up a new path where bandwidth is equal to the current maximum average usage. If the attempt is successful, the LSP's traffic is routed through the new path and the old path is removed. If the attempt fails, the LSP continues to use its current path.

NOTE: You might not be able to use this feature to adjust the bandwidth of fast-reroute LSPs. Because the LSPs use a fixed filter (FF) reservation style, when a new path is signaled, the bandwidth might be double-counted. Double-counting can prevent a fast-reroute LSP from ever adjusting its bandwidth when automatic bandwidth allocation is enabled.

To configure automatic bandwidth allocation, complete the steps in the following sections:

- Configuring MPLS Statistics for Automatic Bandwidth Allocation on page 82
- Configuring Automatic Bandwidth Allocation on an LSP on page 82
- Requesting an Automatic Bandwidth Allocation Adjustment on page 87

Configuring MPLS Statistics for Automatic Bandwidth Allocation

To enable automatic bandwidth allocation, you first need to configure MPLS statistics. Include the auto-bandwidth option for the statistics statement. You can also use the interval option to specify the interval for calculating the average bandwidth usage.

These settings apply to all LSPs configured on the router on which you have also configured the auto-bandwidth statement at the [edit protocols mpls label-switched-path *label-switched-path-name*] hierarchy level. You can also set the adjustment interval on specific LSPs.

NOTE: To prevent unnecessary resignaling of LSPs, it is best to configure an MPLS automatic bandwidth statistics interval of no more than one third the corresponding LSP adjustment interval. For example, if you configure a value of 30 seconds for the interval statement at the [edit protocols mpls statistics] hierarchy level, you should configure a value of no more than 90 seconds for the adjust-interval statement at the [edit protocols mpls label-switched-path *label-switched-path-name* auto-bandwidth] hierarchy level. See also "Configuring the Automatic Bandwidth Allocation Interval" on page 83.

To configure the MPLS and automatic bandwidth allocation statistics, include the statistics statement:

```
statistics {
    auto-bandwidth;
    file filename <files number> <no-stamp> <replace> <size size> <world-readable |
        no-world-readable>;
    interval seconds;
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

Configuring Automatic Bandwidth Allocation on an LSP

To enable automatic bandwidth allocation on an LSP, include the auto-bandwidth statement:

```
auto-bandwidth {
    adjust-interval seconds;
    adjust-threshold percent;
    adjust-threshold-overflow-limit number;
    minimum-bandwidth bps;
    maximum-bandwidth bps;
    monitor-bandwidth;
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *label-switched-path-name*]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *label-switched-path-name*]

The statements configured at the [edit protocols mpls label-switched-path *label-switched-path-name* auto-bandwidth] hierarchy level are optional and explained in the following sections:

- Configuring the Automatic Bandwidth Allocation Interval on page 83
- Configuring the Maximum and Minimum Bounds of the LSP's Bandwidth on page 83
- Configuring Automatic Bandwidth Adjustment Threshold on page 84
- Configuring a Limit on Bandwidth Overflow Samples on page 85
- Configuring Passive Bandwidth Utilization Monitoring on page 86

Configuring the Automatic Bandwidth Allocation Interval

At the end of the automatic bandwidth allocation interval, the automatic bandwidth computation and new path setup process is triggered.

NOTE: To prevent unnecessary resignaling of LSPs, it is best to configure an LSP adjustment interval of no more than three times the corresponding MPLS automatic bandwidth statistics interval. For example, if you configure a value of 90 seconds for the adjust-interval statement at the [edit protocols mpls label-switched-path *label-switched-path-name* auto-bandwidth] hierarchy level, you should configure a value of no less than 30 seconds for the interval statement at the [edit protocols mpls statistics] hierarchy level. See also "Configuring MPLS Statistics for Automatic Bandwidth Allocation" on page 82.

To specify the bandwidth reallocation interval in seconds for a specific LSP, include the adjust-interval statement:

```
adjust-interval seconds;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *label-switched-path-name* auto-bandwidth]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *label-switched-path-name* auto-bandwidth]

Configuring the Maximum and Minimum Bounds of the LSP's Bandwidth

You can maintain the LSP's bandwidth between minimum and maximum bounds by specifying values for the minimum-bandwidth and maximum-bandwidth statements.

To specify the minimum amount of bandwidth allocated for a specific LSP, include the minimum-bandwidth statement:

minimum-bandwidth *bps*;

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *label-switched-path-name* auto-bandwidth]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *label-switched-path-name* auto-bandwidth]

To specify the maximum amount of bandwidth allocated for a specific LSP, include the maximum-bandwidth statement:

maximum-bandwidth *bps*;

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *label-switched-path-name* auto-bandwidth]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *label-switched-path-name* auto-bandwidth]

Configuring Automatic Bandwidth Adjustment Threshold

Use the adjust-threshold statement to specify the sensitivity of the automatic bandwidth adjustment of an LSP to changes in bandwidth utilization. You can set the threshold for when to trigger automatic bandwidth adjustments. When configured, bandwidth demand for the current interval is determined and compared to the LSP's current bandwidth allocation. If the percentage difference in bandwidth is greater than or equal to the specified adjust-threshold percentage, the LSP's bandwidth is adjusted to the current bandwidth demand.

For example, assume that the current bandwidth allocation is 100 megabits per second (Mbps) and that the percentage configured for the adjust-threshold statement is 15 percent. If the bandwidth demand increases to 110 Mbps, the bandwidth allocation is not adjusted. However, if the bandwidth demand increases to 120 Mbps (20 percent over the current allocation) or decreases to 80 Mbps (20 percent under the current allocation), the bandwidth allocation is increased to 120 Mbps or decreased to 80 Mbps, respectively.

To configure the threshold for automatic bandwidth adjustment, include the adjust-threshold statement:

adjust-threshold *percent*;

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name* auto-bandwidth]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* auto-bandwidth]

Configuring a Limit on Bandwidth Overflow Samples

The automatic bandwidth adjustment timer is a periodic timer which is triggered every adjust interval to determine whether any bandwidth adjustments are required on the LSP's active path. This interval is typically configured as a long period of time, usually hours. If, at the end of adjust interval, the change in bandwidth is above a certain adjust threshold, the LSP is resignaled with the new bandwidth.

During the automatic bandwidth adjustment interval, the router might receive a steady increase in traffic (increasing bandwidth utilization) on an LSP, potentially causing congestion or packet loss. To prevent this, you can define a second trigger to prematurely expire the automatic bandwidth adjustment timer before the end of the current adjustment interval.

Every statistics interval, the router samples the average bandwidth utilization of an LSP and if this has exceeded the current maximum average bandwidth utilization, the maximum average bandwidth utilization is updated.

During each sample period, the following conditions are also checked:

- Is the current average bandwidth utilization above the current maximum average bandwidth utilization.
- Has the change in maximum average bandwidth utilization exceeded the adjust threshold (bandwidth utilization has changed significantly).

If these conditions are true, it is considered to be one bandwidth overflow sample. Using the adjust-threshold-overflow-limit statement, you can define a limit on the number of bandwidth overflow samples such that when the limit is reached, the current automatic bandwidth adjustment timer is expired and a bandwidth adjustment is triggered. Once this adjustment is complete, the normal automatic bandwidth adjustment timer is reset to expire after the periodic adjustment interval.

To specify a limit on the number of bandwidth overflow samples before triggering an automatic bandwidth allocation adjustment, configure the adjust-threshold-overflow-limit statement:

```
adjust-threshold-overflow-limit number;
```

This statement can be configured at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name* auto-bandwidth]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* auto-bandwidth]

You must also configure the adjust-threshold and maximum-bandwidth statements whenever you configure the adjust-threshold-overflow-limit statement:

- You must configure a nonzero value for the adjust-threshold statement if you configure the adjust-threshold-overflow-limit statement. Any bandwidth increase below the value configured for the adjust-threshold statement does not constitute an overflow condition.

- To prevent unlimited increases in LSP bandwidth (to limit overflow beyond a certain bandwidth), you must also configure the maximum-bandwidth statement when you configure the adjust-threshold-overflow-limit statement.

Failure to configure either of these statements when you configure the adjust-threshold-overflow-limit statement results in a commit error.

The following describes the other aspects of the adjust-threshold-overflow-limit statement:

- It only applies to bandwidth overflows. If the bandwidth is decreasing, the normal automatic bandwidth adjustment interval is used.
- It does not affect manually triggered automatic bandwidth adjustment.
- It applies to single class DiffServ-TE LSPs.
- Because the adjust-threshold-overflow-limit statement can trigger a bandwidth adjustment, it cannot be enabled at the same time as the monitor-bandwidth statement (for information about that statement, see "Configuring Passive Bandwidth Utilization Monitoring" on page 86).
- You cannot configure automatic bandwidth adjustments to occur more often than every 300 seconds. The adjust-threshold-overflow-limit statement is subject to the same minimum value with regard to the minimum frequency of adjustment allowed. Overflow condition based adjustments can occur no sooner than 300 seconds from the start of the overflow condition. Therefore it is required that:

  sample interval x adjust-threshold-overflow-limit >= 300s

  These values are checked during the commit operation. An error is returned if the value is less than 300 seconds.
- If you change the value of the adjust-threshold-overflow-limit statement on a working router, you can expect the following behavior:
  - If you increase the current value of the adjust-threshold-overflow-limit statement, the old value is replaced with the new one.
  - If you decrease the current value of the adjust-threshold-overflow-limit statement and the current bandwidth overflow count is less than the new value, the old value is replaced with the new one.
  - If you decrease the current value of the adjust-threshold-overflow-limit statement and the current bandwidth overflow count is greater than the new value, the adjustment timer is immediately expired and a bandwidth adjustment is initiated.

Configuring Passive Bandwidth Utilization Monitoring

Use the monitor-bandwidth statement to switch to a passive bandwidth utilization monitoring mode. In this mode, no automatic bandwidth adjustments are made, but the maximum average bandwidth utilization is continuously monitored and recorded.

To configure passive bandwidth utilization monitoring, include the monitor-bandwidth statement:

```
monitor-bandwidth;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name* auto-bandwidth]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* auto-bandwidth]

If you have configured an LSP with primary and secondary paths, the automatic bandwidth allocation statistics are carried over to the secondary path if the primary path fails. For example, consider a primary path whose adjustment interval is half complete and whose maximum average bandwidth usage is currently calculated as 50 Mbps. If the primary path suddenly fails, the time remaining for the next adjustment and the maximum average bandwidth usage are carried over to the secondary path.

Requesting an Automatic Bandwidth Allocation Adjustment

For MPLS LSP automatic bandwidth allocation adjustment, the minimum value for the adjustment interval is 5 minutes (300s). You might find it necessary to trigger a bandwidth allocation adjustment manually. The following describe a couple of scenarios when you might want to do this:

- Testing automatic bandwidth allocation in a network lab.
- When you configure the LSP for automatic bandwidth allocation in monitor mode (you have configured the monitor-bandwidth statement), you might want to initiate a bandwidth adjustment at your own discretion.

To use the request mpls lsp adjust-autobandwidth command, the following must be true:

- Automatic bandwidth allocation must be enabled on the LSP.
- The criteria required to trigger a bandwidth adjustment have been met (the difference between the adjust bandwidth and the current LSP path bandwidth is greater than the threshold limit).

A manually triggered bandwidth adjustment operates only on the active LSP path. Also, if you have enabled periodic automatic bandwidth adjustment, the periodic automatic bandwidth adjustment parameters (the adjustment interval and the maximum average bandwidth) are not reset after a manual adjustment.

For example, suppose the periodic adjust interval is 10 hours and there are currently 5 hours remaining before an automatic bandwidth adjustment is triggered. If you initiate a manual adjustment with the request mpls lsp adjust-autobandwidth command, the adjust timer is not reset and still has 5 hours remaining.

To manually trigger a bandwidth allocation adjustment, you need to use the request mpls lsp adjust-autobandwidth command. You can trigger the command for all affected LSPs on the router, or you can specify a particular LSP:

```
user@host> request mpls lsp adjust-autobandwidth
```

Once you execute this command, the automatic bandwidth adjustment validation process is triggered. If all the criteria for adjustment are met, the LSP's active path bandwidth is adjusted to the adjusted bandwidth value determined during the validation process.

Disabling Constrained-Path LSP Computation

If the IGP is a link-state protocol (such as IS-IS or OSPF) and supports extensions that allow the current bandwidth reservation on each router's link to be reported, constrained-path LSPs are computed by default.

The JUNOS implementations of IS-IS and OSPF include the extensions that support constrained-path LSP computation.

- IS-IS—These extensions are enabled by default. To disable this support, include the disable statement at the [edit protocols isis traffic-engineering] hierarchy level, as discussed in the *JUNOS Routing Protocols Configuration Guide*.
- OSPF—These extensions are disabled by default. To enable this support, include the traffic-engineering statement in the configurations of all routers running OSPF, as described in the *JUNOS Routing Protocols Configuration Guide*.

If IS-IS is enabled on a router or you enable OSPF traffic engineering extensions, MPLS performs the constrained-path LSP computation by default. For information on how constrained-path LSP computation works, see "Constrained-Path LSP Computation" on page 29.

Constrained-path LSPs have a greater chance of being established quickly and successfully for the following reasons:

- The LSP computation takes into account the current bandwidth reservation.
- Constrained-path LSPs reroute themselves away from node failures and congestion.

When constrained-path LSP computation is enabled, you can configure the LSP so that it is periodically reoptimized, as described in "Optimizing Signaled LSPs" on page 96.

When an LSP is being established or when an existing LSP fails, the constrained-path LSP computation is repeated periodically at the interval specified by the retry timer until the LSP is set up successfully. Once the LSP is set up, no recomputation is done. For more information about the retry timer, see "Configuring Path Connection Retry Information" on page 74.

By default, constrained-path LSP computation is enabled. You might want to disable constrained-path LSP computation when all nodes do not support the necessary traffic engineering extensions. To disable constrained-path LSP computation, include the no-cspf statement:

```
no-cspf;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

If you disable constrained-path LSP computation on LSPs by configuring the no-cspf statement and then attempt to advertise other LSPs with lower metrics than the IGPs from this router in either IS-IS or OSPF, new LSPs cannot be established.

Configuring Administrative Groups

Administrative groups, also known as link coloring or resource class, are manually assigned attributes that describe the "color" of links, such that links with the same color conceptually belong to the same class. You can use administrative groups to implement a variety of policy-based LSP setups.

Administrative groups are meaningful only when constrained-path LSP computation is enabled.

You can assign up to 32 names and values (in the range 0 through 31), which define a series of names and their corresponding values. The administrative names and values must be identical across all routers within a single domain.

NOTE: The administrative value is distinct from the priority. You configure the priority for an LSP using the priority statement. See "Configuring Priority and Preemption for LSPs" on page 95.

To configure administrative groups, follow these steps:

1. Define multiple levels of service quality by including the admin-groups statement:

   ```
   admin-groups {
     group-name group-value;
   }
   ```

   You can include this statement at the following hierarchy levels:

   - [edit protocols mpls]
   - [edit logical-systems *logical-system-name* protocols mpls]

   The following configuration example illustrates how you might configure a set of administrative names and values for a domain:

   ```
   [edit protocols mpls]
   admin-groups {
     gold 1;
     silver 2;
     copper 3;
     best-effort 4;
   }
   ```

2. Define the administrative groups to which an interface belongs. You can assign multiple groups to an interface. Include the interface statement:

   ```
   interface interface-name {
     admin-group [ group-names ];
   }
   ```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

If you do not include the admin-group statement, an interface does not belong to any group.

IGPs use the group information to build link-state packets, which are then flooded throughout the network, providing information to all nodes in the network. At any router, the IGP topology, as well as administrative groups of all the links, is available.

Changing the interface's administrative group affects only new LSPs. Existing LSPs on the interface are not preempted or recomputed to keep the network stable. If LSPs need to be removed because of a group change, issue the clear rsvp session command.

3. Configure an administrative group constraint for each LSP or for each primary or secondary LSP path. Include the label-switched-path statement:

```
label-switched-path lsp-name {
    to address;
    ...
    admin-group {
        exclude [ group-names];
        include-all [ group-names];
        include-any [ group-names];
    }
    primary path-name {
        admin-group {
            exclude [ group-names];
            include-all [ group-names];
            include-any [ group-names];
        }
    }
    secondary path-name {
        admin-group {
            exclude [ group-names];
            include-all [ group-names];
            include-any [ group-names];
        }
    }
}
```

You can include the label-switched-path statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

If you omit the include-all, include-any, or exclude statements, the path computation proceeds unchanged. The path computation is based on the constrained-path

LSP computation. For information on how the constrained-path LSP computation is calculated, see “How CSPF Selects a Path” on page 30.

NOTE: Changing the LSP’s administrative group causes an immediate recomputation of the route; therefore, the LSP might be rerouted.

Configuring the LSP Preference

As an option, you can configure multiple LSPs between the same pair of ingress and egress routers. This is useful for balancing the load among the LSPs because all LSPs, by default, have the same preference level. To prefer one LSP over another, set different preference levels for individual LSPs. The LSP with the lowest preference value is used. The default preference for RSVP LSPs is 7 and for LDP LSPs is 9. These preference values are lower (more preferred) than all learned routes except direct interface routes.

To change the default preference value, include the preference statement:

```
preference preference;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Configuring Path Route Recording

The JUNOS implementation of RSVP supports the Record Route object, which allows an LSP to actively record the routers through which it transits. You can use this information for troubleshooting and to prevent routing loops. By default, path route information is recorded. To disable recording, include the no-record statement:

```
no-record;
```

For a list of hierarchy levels at which you can include the record (no-record) statement, see the statement summary section for the statement.

Configuring Class of Service for MPLS

The following sections provide an overview of MPLS class of service (CoS) and describe how to configure the MPLS CoS value:

- Class of Service for MPLS Overview on page 91
- Configuring the MPLS CoS Bits on page 92
- Rewriting IEEE 802.1p Packet Headers with the MPLS CoS Value on page 93

Class of Service for MPLS Overview

When IP traffic enters an LSP tunnel, the ingress router marks all packets with a CoS value, which is used to place the traffic into a transmission priority queue. On the router, for SDH/SONET and T3 interfaces, each interface has four transmit queues.

The CoS value is encoded as part of the MPLS header and remains in the packets until the MPLS header is removed when the packets exit from the egress router. The routers within the LSP utilize the CoS value set at the ingress router. The CoS value is encoded by means of the CoS bits (also known as the EXP or experimental bits). For more information, see "Label Allocation" on page 25.

MPLS class of service works in conjunction with the router's general CoS functionality. If you do not configure any CoS features, the default general CoS settings are used. For MPLS class of service, you might want to prioritize how the transmit queues are serviced by configuring weighted round-robin, and to configure congestion avoidance using random early detection (RED). The general CoS features are described in the *JUNOS Class of Service Configuration Guide*.

Configuring the MPLS CoS Bits

When traffic enters an LSP tunnel, the CoS bits in the MPLS header are set in one of two ways:

- The number of the output queue into which the packet was buffered and the packet loss priority (PLP) bit are written into the MPLS header and are used as the packet's CoS value. This behavior is the default, and no configuration is required. The *JUNOS Class of Service Configuration Guide* explains the IP CoS values, and summarizes how the CoS bits are treated.
- You set a fixed CoS value on all packets entering the LSP tunnel. A fixed CoS value means that all packets entering the LSP receive the same class of service.

To set a fixed CoS value on all packets entering the LSP, include the class-of-service statement:

```
class-of-service cos-value;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

The CoS value set using the class-of-service statement at the [edit protocols mpls] hierarchy level supersedes the CoS value set at the [edit class-of-service] hierarchy level for an interface. Effectively, the CoS value configured for an LSP overrides the CoS value set for an interface.

The CoS value can be a decimal number from 0 through 7. This number corresponds to a 3-bit binary number. The high-order 2 bits of the CoS value select which transmit queue to use on the outbound interface card.

The low-order bit of the CoS value is treated as the PLP bit and is used to select the RED drop profile to use on the output queue. If the low-order bit is 0, the non-PLP drop profile is used, and if the low-order bit is 1, the PLP drop profile is used. It is generally expected that RED will more aggressively drop packets that have the PLP bit set. For more information about RED and drop profiles, see the *JUNOS Class of Service Configuration Guide*.

NOTE: Configuring the PLP drop profile to drop packets more aggressively (for example, setting the CoS value from 6 to 7) decreases the likelihood of traffic getting through.

Table 7 on page 93 summarizes how MPLS CoS values correspond to the transmit queue and PLP bit. Note that in MPLS, the mapping between the CoS bit value and the output queue is hard-coded. You cannot configure the mapping for MPLS; you can configure it only for IPv4 traffic flows, as described in the *JUNOS Class of Service Configuration Guide*.

Table 7: MPLS CoS Values

MPLS CoS Value	Bits	Transmit Queue	PLP Bit
0	000	0	Not set
1	001	0	Set
2	010	1	Not set
3	011	1	Set
4	100	2	Not set
5	101	2	Set
6	110	3	Not set
7	111	3	Set

Because the CoS value is part of the MPLS header, the value is associated with the packets only as they travel through the LSP tunnel. The value is not copied back to the IP header when the packets exit from the LSP tunnel.

Rewriting IEEE 802.1p Packet Headers with the MPLS CoS Value

For Ethernet interfaces installed on a T-series platform or M320 router with a peer connection to an M-series router or a T-series platform, you can rewrite both MPLS CoS and IEEE 802.1p bits to a configured value (the MPLS CoS bits are also known as the EXP or experimental bits). Rewriting these bits allows you to pass the configured value to the Layer 2 VLAN path. To rewrite both the MPLS CoS and IEEE 802.1p bits, you must include the EXP and IEEE 802.1p rewrite rules in the class of service interface configuration. The EXP rewrite table is applied when you configure the IEEE 802.1p and EXP rewrite rules.

For information about how to configure the EXP and IEEE 802.1p rewrite rules, see the *JUNOS Class of Service Configuration Guide*.

For information on the CoS bits, see “Label Allocation” on page 25 and “Configuring Class of Service for MPLS” on page 91.

Configuring Adaptive LSPs

An LSP occasionally might need to reroute itself. Reasons include the following:

- Continuous reoptimization process is configured with the optimize-timer statement.
- The current path has connectivity problems.
- The LSP is preempted by another LSP configured with the priority statement and is forced to reroute.
- The explicit-path information for an active LSP is modified, or the LSP's bandwidth is increased.

You can configure an LSP to be *adaptive* when it is attempting to reroute itself. When it is adaptive, the LSP holds onto existing resources until the new path is successfully established and traffic has been cut over to the new LSP. To retain its resources, an adaptive LSP does the following:

- Maintains existing paths and allocated bandwidths—This ensures that the existing path is not torn down prematurely and allows the current traffic to continue flowing while the new path is being set up.
- Avoids double-counting for links that share the new and old paths—Double-counting occurs when an intermediate router does not recognize that the new and old paths belong to the same LSP and counts them as two separate LSPs, requiring separate bandwidth allocations. If some links are close to saturation, double-counting might cause the setup of the new path to fail.

By default, adaptive behavior is disabled. You can include the adaptive statement in two different hierarchy levels.

If you specify the adaptive statement at the LSP hierarchy levels, the adaptive behavior is enabled on all primary/secondary paths of the LSP. This means both the primary and secondary paths share the same bandwidth on common links.

To configure adaptive behavior for all LSP paths, include the adaptive statement in the LSP configuration:

```
adaptive;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name*]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]

If you specify the adaptive statement at the [edit protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*] hierarchy level, adaptive behavior is enabled only on the path on which it is specified. Bandwidth double-counting occurs between different paths. However, if you also have the adaptive statement configured at the [edit protocols mpls label-switched-path *lsp-name*] hierarchy level, it overrides the adaptive behavior of each individual path.

To configure adaptive behavior for either the primary or secondary level, include the adaptive statement:

adaptive;

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*]

Configuring Priority and Preemption for LSPs

When there is insufficient bandwidth to establish a more important LSP, you might want to tear down a less important existing LSP to free the bandwidth. You do this by preempting the existing LSP.

Whether an LSP can be preempted is determined by two properties associated with the LSP:

- Setup priority—Determines whether a new LSP that preempts an existing LSP can be established. For preemption to occur, the setup priority of the new LSP must be higher than that of the existing LSP. Also, the act of preempting the existing LSP must produce sufficient bandwidth to support the new LSP. That is, preemption occurs only if the new LSP can be set up successfully.
- Reservation priority—Determines the degree to which an LSP holds on to its session reservation after the LSP has been set up successfully. When the reservation priority is high, the existing LSP is less likely to give up its reservation and hence it is unlikely that the LSP can be preempted.

You cannot configure an LSP with a high setup priority and a low reservation priority, because permanent preemption loops might result if two LSPs are allowed to preempt each other. You must configure the reservation priority to be higher than or equal to the setup priority.

The setup priority also defines the relative importance of LSPs on the same ingress router. When the software starts, when a new LSP is established, or during fault recovery, the setup priority determines the order in which LSPs are serviced. Higher-priority LSPs tend to be established first and hence enjoy more optimal path selection.

To configure the LSP's preemption properties, include the priority statement:

priority *setup-priority reservation-priority*;

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Both *setup-priority* and *reservation-priority* can be a value from 0 through 7. The value 0 corresponds to the highest priority, and the value 7 to the lowest. By default, an LSP has a setup priority of 7 (that is, it cannot preempt any other LSPs) and a reservation priority of 0 (that is, other LSPs cannot preempt it). These defaults are such that preemption does not happen. When you are configuring these values, the setup priority should always be less than or equal to the hold priority.

Optimizing Signaled LSPs

Once an LSP has been established, topology or resources changes might, over time, make the path suboptimal. A new path might have become available that is less congested, has a lower metric, and traverses fewer hops. You can configure the router to recompute paths periodically to determine whether a more optimal path has become available.

If reoptimization is enabled, an LSP can be rerouted through different paths by constrained-path recomputations. However, if reoptimization is disabled, the LSP has a fixed path and cannot take advantage of newly available network resources. The LSP is fixed until the next topology change breaks the LSP and forces a recomputation.

Reoptimization is not related to failover. A new path is always computed when topology failures occur that disrupt an established path.

Because of the potential system overhead involved, you need to control carefully the frequency of reoptimization. Network stability might suffer when reoptimization is enabled. By default, the optimize-timer statement is set to 0 (that is, it is disabled).

Configuring LSP optimization is meaningful only when constrained-path LSP computation is enabled, which is the default behavior. For more information about constrained-path LSP computation, see “Disabling Constrained-Path LSP Computation” on page 88.

To enable path reoptimization, include the optimize-timer statement:

```
optimize-timer seconds;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Once you have configured the optimize-timer statement, the reoptimization timer continues its countdown to the configured value even if you delete the optimize-timer statement from the configuration. The next optimization uses the new value. You can force the JUNOS software to use a new value immediately by deleting the old value, committing the configuration, configuring the new value for the optimize-timer statement, and then committing the configuration again.

After reoptimization is run, the result is accepted only if it meets the following criteria:

1. The new path is not higher in IGP metric. (The metric for the old path is updated during computation, so if a recent link metric changed somewhere along the old path, it is accounted for.)
2. If the new path has the same IGP metric, it is not more hops away.
3. The new path does not cause preemption. (This is to reduce the ripple effect of preemption causing more preemption.)
4. The new path does not worsen congestion overall.

The relative congestion of the new path is determined as follows:

a. The percentage of available bandwidth on each link traversed by the new path is compared to that for the old path, starting from the most congested links.

b. For each current (old) path, the software stores the four smallest values for bandwidth availability for the links traversed in ascending order.

c. If one of those four values is smaller than any of the new bandwidth availability values, it indicates that the new path has at least one link that is more congested than the least congested link used by the old path. Traffic is not switched to this new path.

d. If none of those four values is smaller than any of the new bandwidth availability values, it indicates that the new path is less congested than the old path.

When all the above conditions are met, then:

5. If the new path has a lower IGP metric, it is accepted.
6. If the new path has an equal IGP metric and lower hop count, it is accepted.
7. If you choose least-fill as a load-balancing algorithm and if the new path reduces congestion by at least 10 percent aggregated over all links it traversed, it is accepted. For random or most-fill algorithms, this rule does not apply.
8. Otherwise, the new path is rejected.

You can disable the following reoptimization criteria (a subset of the criteria listed previously) by issuing the clear mpls optimize-aggressive command or including the optimize-aggressive statement at the [edit protocols mpls] hierarchy level:

- If the new path has the same IGP metric, it is not more hops away.
- The new path does not cause preemption. (This is to reduce the ripple effect of preemption causing more preemption.)
- The new path does not worsen congestion overall.
- If the new path has an equal IGP metric and lower hop count, it is accepted.

Including the optimize-aggressive statement in the configuration causes the reoptimization procedure to be triggered more often. Paths are rerouted more frequently. It also limits the reoptimization algorithm to the IGP metric only.

Configuring the Smart Optimize Timer

Due to network and router resource constraints, it is typically inadvisable to configure a short interval for the optimize timer. However, under certain circumstances, it might be desirable to reoptimize a path sooner than would normally be provided by the optimize timer.

For example, an LSP is traversing a preferred path which subsequently fails. The LSP is then switched to a less desirable path to reach the same destination. Even if the

original path is quickly restored, it could take an excessively long period of time for the LSP to use it again, because it has to wait for the optimize timer to reoptimize the network paths. For situations such as this, you might want to configure the smart optimize timer.

By enabling the smart optimize timer, an LSP is switched back to its original path so long as the original path has been restored within 3 minutes of going down. Also, if the original path goes down again within 60 minutes, the smart optimize timer is disabled and path optimization behaves as it normally does when the optimize timer alone is enabled. This prevents the router from using a flapping link.

To configure smart optimize timer, include the smart-optimize-timer statement:

```
smart-optimize-timer seconds;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

Configuring the Maximum Path Length

By default, each LSP can traverse a maximum of 255 hops, including the ingress and egress routers. To modify this value, include the hop-limit statement:

```
hop-limit number;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

The number of hops can be from 2 through 255. (A path with two hops consists of the ingress and egress routers only.)

Configuring the Path Bandwidth

Each LSP has a bandwidth value. This value is included in the sender's Tspec field in RSVP path setup messages. To specify a bandwidth value, include the bandwidth statement:

```
bandwidth bps;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

You specify the bandwidth value in bits per second, with a higher value implying a greater user traffic volume. The default bandwidth is 0 bits per second.

A nonzero bandwidth requires transit routers to reserve capacity along the outbound links for the path. RSVP's reservation scheme is used to reserve this capacity. Any failure in bandwidth reservation (such as failures at RSVP policy control or admission control) might cause the LSP setup to fail.

Configuring the Standby State

By default, secondary paths are set up only as needed. To have the system maintain a secondary path in a hot-standby state indefinitely, include the standby statement:

```
standby;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name* secondary]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* secondary]

The hot-standby state is meaningful only on secondary paths. Maintaining a path in a hot-standby state enables swift cutover to the secondary path when downstream routers on the current active path indicate connectivity problems. Although it is possible to configure the standby statement at the [edit protocols mpls label-switched-path *lsp-name* primary *path-name*] hierarchy level, it has no effect on router behavior.

If you configure the standby statement at the following hierarchy levels, the hot-standby state is activated on all secondary paths configured beneath that hierarchy level:

- [edit protocols mpls]
- [edit protocols mpls label-switched-path *lsp-name*]
- [edit logical-systems *logical-system-name* protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]

The hot-standby state has two advantages:

- It eliminates the call-setup delay during network topology changes. Call setup can suffer from significant delays when network failures trigger large numbers of LSP reroutes at the same time.
- A cutover to the secondary path can be made before RSVP learns that an LSP is down. There can be significant delays between the time the first failure is detected by protocol machinery (which can be an interface down, a neighbor becoming unreachable, a route becoming unreachable, or a transient routing loop being detected) and the time an LSP actually fails (which requires a timeout of soft state information between adjacent RSVP routers). When topology failures occur, hot-standby secondary paths can usually achieve the smallest cutover delays with minimal disruptions to user traffic.

When the primary path is considered to be stable again, traffic is automatically switched from the standby secondary path back to the primary path. The switch is performed no faster than twice the retry-timer interval and only if the primary path exhibits stability throughout the entire switch interval.

The drawback of the hot-standby state is that more state information must be maintained by all the routers along the path, which requires overhead from each of the routers.

Configuring LSP Hold Time

When an LSP changes from being up to being down, or from down to up, this transition takes effect immediately in the router software and hardware. However, when advertising LSPs into IS-IS and OSPF, you may want to damp LSP transitions, thereby not advertising the transition until a certain period of time has transpired (known as the hold time). In this case, if the LSP goes from up to down, the LSP is not advertised as being down until it has remained down for the hold-time period. Transitions from down to up are advertised into IS-IS and OSPF immediately. Note that LSP damping affects only the IS-IS and OSPF advertisements of the LSP; other routing software and hardware react immediately to LSP transitions.

To damp LSP transitions, include the advertisement-hold-time statement:

```
advertisement-hold-time seconds;
```

seconds can be a value from 0 through 65,535 seconds. The default is 5 seconds.

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

Configuring LDP Tunneling

To correctly identify an LDP session associated with an RSVP LSP, ensure that the RSVP LSP endpoint address is the same as the transport address of the LDP peer.

Enabling RSVP

For all routers that should participate in signaled LSPs, you must enable RSVP because it is used to set up LSPs. To enable RSVP, include the following statements in the configuration. In general, we recommend that you enable RSVP on all router interfaces, except those on the autonomous system (AS) border:

```
[edit]
interfaces {
    interface-name {
        unit logical-unit-number {
            family mpls;
        }
    }
}
protocols {
    mpls {
        interface all;
    }
    rsvp {
        interface all;
    }
}
```

For more information about RSVP, see “RSVP Configuration Guidelines” on page 269.

Configuring MPLS Exception Monitoring

You can process MPLS packets that have not been assigned label values and have no corresponding entry in the mpls.0 routing table. This allows you to assign a default route to unlabeled MPLS packets.

To configure a default label value for MPLS packets, include the default-route statement:

```
default-route {
    class-of-service cos-value;
    (next-hop (address | interface-name | address/interface-name) |
    (discard | reject);
    (pop | (swap out-label);
    preference preference;
    swap-push swap-label push-label;
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls interface *interface-name* label-map]
- [edit logical-systems *logical-system-name* protocols mpls interface *interface-name* label-map]

Improving TED Accuracy with RSVP PathErr Messages

An essential element of RSVP-based traffic engineering is the TED. The TED contains a complete list of all network nodes and links participating in traffic engineering, and a set of attributes each of those links can hold. (For more information about the TED, see “Constrained-Path LSP Computation” on page 29.) One of the most important link attributes is bandwidth.

Bandwidth availability on links changes quickly as RSVP LSPs are established and terminated. It is likely that the TED will develop inconsistencies relative to the real network. These inconsistencies cannot be fixed by increasing the rate of IGP updates.

Link availability can share the same inconsistency problem. A link that becomes unavailable can break all existing RSVP LSPs. However, its unavailability might not readily be known by the network.

When you configure the rsvp-error-hold-time statement, a source node (ingress of the RSVP LSPs) learns from the failures of its LSP by monitoring PathErr messages transmitted from downstream nodes. Information from the PathErr messages is incorporated into subsequent LSP computations, which can improve the accuracy and speed of LSP setup. Some PathErr messages are also used to update TED bandwidth information, reducing inconsistencies between the TED and the network.

You can control the frequency of IGP updates by using the update-threshold statement. See “Configuring the RSVP Update Threshold on an Interface” on page 277.

This section discusses the following topics:

- PathErr Messages on page 102
- Identifying the Problem Link on page 102
- Configuring the Router to Improve TED Accuracy on page 103

PathErr Messages

PathErr messages report a wide variety of problems by means of different code and subcode numbers. You can find a complete list of these PathErr messages in RFC 2205, *Resource Reservation Protocol (RSVP), Version 1, Functional Specification* and RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels*.

When you configure the rsvp-error-hold-time statement, two categories of PathErr messages, which specifically represent link failures, are examined:

- Link bandwidth is low for this LSP: Requested bandwidth unavailable—code 1, subcode 2

  This type of PathErr message represents a global problem that affects all LSPs transiting the link. They indicate that the actual link bandwidth is lower than that required by the LSP, and that it is likely that the bandwidth information in the TED is an overestimate.

  When this type of error is received, the available link bandwidth is reduced in the local TED, affecting all future LSP computations.

- Link unavailable for this LSP:
  - Admission Control failure—code 1, any subcode except 2
  - Policy Control failures—code 2
  - Service Preempted—code 12
  - Routing problem—no route available toward destination—code 24, subcode 5

  These types of PathErr messages are generally pertinent to the specified LSP. The failure of this LSP does not necessarily imply that other LSPs could also fail. These errors can indicate maximum transfer unit (MTU) problems, service preemption (either manually initiated by the operator or by another LSP with a higher priority), that a next-hop link is down, that a next-hop neighbor is down, or service rejection because of policy considerations. It is best to route this particular LSP away from the link.

Identifying the Problem Link

Each PathErr message includes the sender's IP address. This information is propagated unchanged toward the ingress router. A lookup in the TED can identify the node that originated the PathErr message.

Each PathErr message carries enough information to identify the RSVP session that triggered the message. If this is a transit router, it simply forwards the message. If this router is the ingress router (for this RSVP session), it has the complete list of all nodes and links the session should traverse. Coupled with the originating node information, the link can be uniquely identified.

Configuring the Router to Improve TED Accuracy

To improve the accuracy of the TED, configure the rsvp-error-hold-time statement. When this statement is configured, a source node (ingress of the RSVP LSPs) learns from the failures of its LSP by monitoring PathErr messages transmitted from downstream nodes. Information from the PathErr messages is incorporated into subsequent LSP computations, which can improve the accuracy and speed of LSP setup. Some PathErr messages also are used to update TED bandwidth information, reducing inconsistencies between the TED and the network.

To configure how long MPLS should remember RSVP PathErr messages and consider them in CSPF computation, include the rsvp-error-hold-time statement:

```
rsvp-error-hold-time seconds;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

The time can be a value from 1 to 240 seconds. The default is 25 seconds. Configuring a value of 0 disables the monitoring of PathErr messages.

Examples: Configuring Signaled LSPs

The following examples illustrate how to configure signaled LSPs:

- Example: Constrained-Path LSP, JUNOS Makes All Forwarding Decisions on page 103
- Example: Explicit-Path LSP on page 104
- Example: Constrained-Path LSP, JUNOS Makes Most Forwarding Decisions, Hop Constraints Accounted For on page 105
- Example: Constrained-Path LSP, JUNOS Makes Most Forwarding Decisions, Secondary Path Is Explicit on page 105

Example: Constrained-Path LSP, JUNOS Makes All Forwarding Decisions

On the ingress router, create a constrained-path LSP in which the JUNOS software makes all the forwarding decisions. When the LSP is successfully set up, a route toward 11.1.1.1/32 is installed in the inet.3 table so that all BGP routes with matching BGP next-hop addresses can be forwarded through the LSP.

```
[edit]
interfaces {
   so-0/0/0 {
```

```
        unit 0 {
            family mpls;
        }
    }
}
protocols {
    rsvp {
        interface so-0/0/0;
    }
    mpls {
        label-switched-path to-hastings {
            to 11.1.1.1;
        }
        interface so-0/0/0;
    }
}
```

Example: Explicit-Path LSP

On the ingress router, create an explicit-path LSP, and specify the transit routers between the ingress and egress routers. In this configuration, no constrained-path computation is performed. For the primary path, all intermediate hops are strictly specified so that its route cannot change. The secondary path must travel through router 14.1.1.1 first, then take whatever route is available to reach the destination. The remaining route taken by the secondary path is typically the shortest path computed by the IGP.

```
[edit]
interfaces {
    so-0/0/0 {
        unit 0 {
            family mpls;
        }
    }
}
protocols {
    rsvp {
        interface so-0/0/0;
    }
    mpls {
        path to-hastings {
            14.1.1.1 strict;
            13.1.1.1 strict;
            12.1.1.1 strict;
            11.1.1.1 strict;
        }
        path alt-hastings {
            14.1.1.1 strict;
            11.1.1.1 loose; # Any IGP route is acceptable
        }
        label-switched-path hastings {
            to 11.1.1.1;
            hop-limit 32;
            bandwidth 10m; # Reserve 10 Mbps
            no-cspf; # do not perform constrained-path computation
```

```
        primary to-hastings;
        secondary alt-hastings;
      }
      interface so-0/0/0;
    }
}
```

Example: Constrained-Path LSP, JUNOS Makes Most Forwarding Decisions, Hop Constraints Accounted For

On the ingress router, create a constrained-path LSP in which the JUNOS software makes most of the forwarding decisions, taking into account the hop constraints listed in the path statements. The LSP is adaptive so that no bandwidth double-counting occurs on links shared by primary and secondary paths. To acquire the necessary link bandwidth, this LSP is allowed to preempt lower priority sessions. Finally, this path always keeps the secondary path in hot-standby state for quick failover.

```
[edit protocols]
mpls {
   path to-hastings {
      14.1.1.1 loose;
   }
   path alt-hastings {
      12.1.1.1 loose;
      11.1.1.1 strict;
   }
   label-switched-path hastings {
      to 11.1.1.1;
      bandwidth 10m; # Reserve 10 Mbps
      priority 0 0; # Preemptive, but not preemptable
      adaptive; # Set adaptivity
      primary to-hastings;
      secondary alt-hastings {
         standby;
         bandwidth 1m; # Reserve only 1 Mbps for the secondary path
      }
   }
   interface all;
}
```

Example: Constrained-Path LSP, JUNOS Makes Most Forwarding Decisions, Secondary Path Is Explicit

On the ingress router, create a constrained-path LSP in which the JUNOS software makes most of the forwarding decisions for the primary path, subject to constraints of the path to-hastings, and in which the secondary path is an explicit path. The primary path must transit green or yellow links and must stay away from red links. The primary path is periodically recomputed and reoptimized. Finally, this path always keeps the secondary path in hot-standby state for quick failover.

When the LSP is up—either because the primary or secondary path is up, or because both paths are up—the prefix 16.0.0.0/8 is installed in the inet.3 table so that all

BGP routes whose BGP next hop falls within that range can use the LSP. Also, the prefix 17/8 is installed in the inet.0 table so that BGP can resolve only its next hop through that prefix. The route also can be reached with traceroute or ping. These two routes are in addition to the 11.1.1.1/32 route.

```
[edit protocols]
mpls {
   admin-groups {
      green 1;
      yellow 2;
      red 3;
   }
   path to-hastings {
      14.1.1.1 loose;
   }
   path alt-hastings {
      14.1.1.1 strict;
      13.1.1.1 strict;
      12.1.1.1 strict;
      11.1.1.1 strict;
   }
   label-switched-path hastings {
      to 11.1.1.1;
      bandwidth 100m;
      install 16.0.0.0/8; # in inet.3; cannot use to traceroute or ping
      install 17.0.0.0/8 active; # installed in inet.0; can use to traceroute or ping
      primary to-hastings {
         admin-group { # further constraints for path computation
         include-all [ green yellow ];
         exclude red;
      }
      optimize-timer 3600; # reoptimize every hour
   }
   secondary alt-hastings {
      standby;
      no-cspf; # do not perform constrained-path computation
   }
}
interface all;
```

Configuring MPLS over GRE Tunnels

MPLS LSPs can use generic routing encapsulation (GRE) tunnels to cross routing areas, autonomous systems, and ISPs. Bridging MPLS LSPs over an intervening IP domain is possible without disrupting the outlying MPLS domain.

LSPs can reach any destination that the GRE tunnels can reach. MPLS applications can be deployed without requiring all transit nodes to support MPLS, or requiring all transit nodes to support the same label distribution protocols (LDP or RSVP). If you use CSPF, you must configure OSPF or IS-IS through the GRE tunnel. Traffic engineering is not supported over GRE tunnels; for example, you cannot reserve bandwidth or set priority or preemption.

NOTE: Use the no-control word statement to disable the control word when the topology uses generic routing encapsulation (GRE) as the connection mechanism between PEs, and one of the PEs is an M-series router.

For more information about GRE tunnels, see the *JUNOS Services Interfaces Configuration Guide*.

Example: Configuring MPLS over GRE Tunnels

To configure MPLS over GRE tunnels:

1. Enable family mpls under the GRE interface configuration:

```
[edit interfaces]
interface gr-1/2/0 {
   unit 0 {
      tunnel {
         source 192.168.1.1;
         destination 192.168.1.2;
      }
      family inet {
         address 5.1.1.1/30;
      }
      family iso;
      family mpls;
   }
}
```

2. Enable RSVP and MPLS over the GRE tunnel:

```
[edit protocols]
rsvp {
   interface gr-1/2/0.0;
}
mpls {
   ...
   interface gr-1/2/0.0;
}
```

3. Configure LSPs to travel through the GRE tunnel endpoint address:

```
[edit protocols]
mpls {
   label-switched-path gre-tunnel {
      to 5.1.1.2;
      ...
   }
}
```

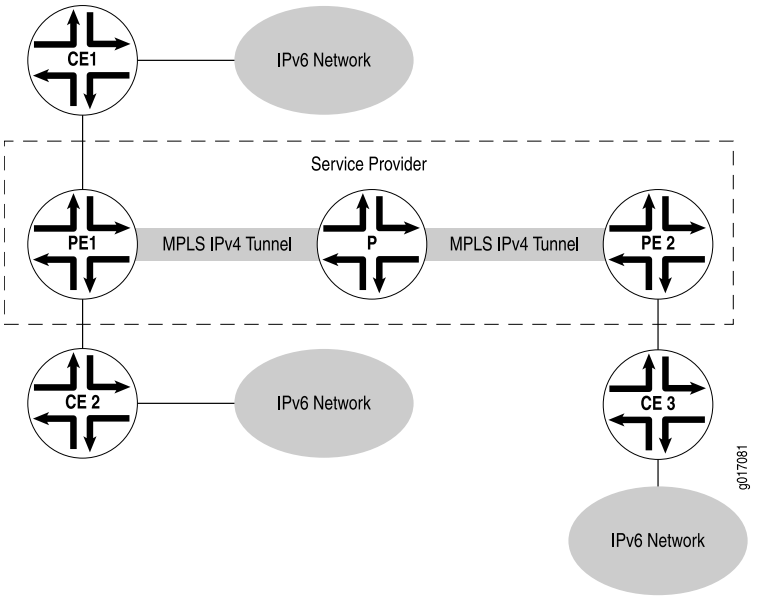
Standard LSP configuration options apply. If the routing table specifies that a particular route will traverse a GRE tunnel, the RSVP packets will traverse the tunnel as well.

Configuring IPv6 Tunnels over MPLS

You can configure the JUNOS software to tunnel IPv6 over an MPLS-based IPv4 network. This configuration allows you to interconnect a number of smaller IPv6 networks over an IPv4-based network core, giving you the ability to provide IPv6 service without having to upgrade the routers in your core network. Multiprotocol Border Gateway Protocol (MP-BGP) is configured to exchange routes between the IPv6 networks, and data is tunneled between these IPv6 networks by means of IPv4-based MPLS.

In Figure 19 on page 108, Routers PE1 and PE2 are dual-stack BGP routers, meaning they have both IPv4 and IPv6 stacks. The PE routers link the IPv6 networks through the customer edge (CE) routers to the IPv4 core network. The CE routers and the PE routers connect through a link layer that can carry IPv6 traffic. The PE routers use IPv6 on the CE router-facing interfaces and use IPv4 and MPLS on the core-facing interfaces. Note that one of the connected IPv6 networks could be the global IPv6 Internet.

Figure 19: IPv6 Networks Linked by MPLS IPv4 Tunnels



The two PE routers are linked through a MP-BGP session using IPv4 addresses. They use the session to exchange IPv6 routes with an IPv6 (value 2) address family indicator (AFI) and a Subsequent AFI (SAFI) (value 4). Each PE router sets the next hop for the IPv6 routes advertised on this session to its own IPv4 address. Because MP-BGP requires the BGP next hop to correspond to the same address family as the network layer reachability information (NLRI), this IPv4 address needs to be embedded within an IPv6 format.

The PE routers can learn the IPv6 routes from the CE routers connected to them by means of the routing protocols RIP next generation (RIPng) or MP-BGP, or through static configuration. Note that if BGP is used as the PE-router-to-CE-router protocol, the MP-BGP session between the PE router and CE router could occur over an IPv4

or IPv6 Transmission Control Protocol (TCP) session. Also, the BGP routes exchanged on that session would have SAFI unicast. You must configure an export policy to pass routes between IBGP and external BGP (EBGP), and between BGP and any other protocol.

The PE routers have MPLS LSPs routed to each others' IPv4 addresses. IPv4 provides signaling for the LSPs by means of either LDP or RSVP. These LSPs are used to resolve the next-hop addresses of the IPv6 routes learned from MP-BGP. The next hops use IPv4-mapped IPv6 addresses, while the LSPs use IPv4 addresses.

The PE routers always advertise IPv6 routes to each other using a label value of 2, the explicit null label for IPv6 as defined in RFC 3032, *MPLS Label Stack Encoding*. As a consequence, each of the forwarding next hops for the IPv6 routes learned from remote PE routers normally push two labels. The inner label is 2 (this label could be different if the advertising PE router is not a Juniper Networks routing platform), and the outer label is the LSP label. If the LSP is a single-hop LSP, then only label 2 is pushed.

It is also possible for the PE routers to exchange plain IPv6 routes using SAFI unicast. However, there is one major advantage in exchanging labeled IPv6 routes. The penultimate-hop router for an MPLS LSP can pop the outer label and then send the packet with the inner label as an MPLS packet. Without the inner label, the penultimate-hop router would need to discover whether the packet is an IPv4 or IPv6 packet to set the protocol field in the Layer 2 header correctly.

When the PE1 router in Figure 19 on page 108 receives an IPv6 packet from the CE1 router, it performs a lookup in the IPv6 forwarding table. If the destination matches a prefix learned from the CE2 router, then no labels need to be pushed and the packet is simply sent to the CE2 router. If the destination matches a prefix that was learned from the PE2 router, then the PE1 router pushes two labels onto the packet and sends it to the provider router. The inner label is 2 and the outer label is the LSP label for the PE2 router.

Each provider router in the service provider's network handles the packet as it would any MPLS packet, swapping labels as it passes from provider router to provider router. The penultimate-hop provider router for the LSP pops the outer label and sends the packet to the PE2 router. When the PE2 router receives the packet, it recognizes the IPv6 explicit null label on the packet (Label 2). It pops this label and treats it as an IPv6 packet, performing a lookup in the IPv6 forwarding table and forwarding the packet to the CE3 router.

This section discusses the following topics:

- IPv6 over MPLS Standards on page 109
- Configuring an IPv4 MPLS Tunnel to Carry IPv6 Traffic on page 110

IPv6 over MPLS Standards

Detailed information about the Juniper Networks implementation of IPv6 over MPLS is described in the following Internet drafts:

- Internet draft draft-ietf-l3vpn-bgp-ipv6-07.txt, *BGP-MPLS IP VPN extension for IPv6 VPN* (expires January 2006)

- Internet draft draft-ooms-v6ops-bgp-tunnel-06.txt, *Connecting IPv6 Islands over IPv4 MPLS using IPv6 Provider Edge Routers* (expires July 2006)

These Internet drafts are available on the IETF Web site at http://www.ietf.org/.

Configuring an IPv4 MPLS Tunnel to Carry IPv6 Traffic

You must perform the following tasks to allow IPv6 to be carried over an IPv4 MPLS tunnel:

- Configuring IPv6 on Both Core-Facing and CE Router–Facing Interfaces on page 110
- Configuring MPLS and RSVP Between PE Routers on page 110
- Enabling IPv6 Tunneling in MPLS on page 111
- Configuring Multiprotocol BGP to Carry IPv6 Traffic on page 111

Configuring IPv6 on Both Core-Facing and CE Router–Facing Interfaces

In addition to configuring the family inet6 statement on all the CE router–facing interfaces, you must also configure the statement on all the core-facing interfaces running MPLS. Both configurations are necessary because the router must be able to process any IPv6 packets it receives on these interfaces. You should not see any regular IPv6 traffic arrive on these interfaces, but you will receive MPLS packets tagged with label 2. Even though label 2 MPLS packets are sent in IPv4, these packets are treated as native IPv6 packets.

Include the family inet6 statement:

```
family inet6 {
    address inet6-address;
}
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* unit *logical-unit-number*]
- [edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

Configuring MPLS and RSVP Between PE Routers

For information about how to configure MPLS and RSVP, see the following sections:

- Configuring the Ingress Router for Signaled LSPs on page 57
- Configuring All Other MPLS Routers for Signaled LSPs on page 62
- Enabling RSVP on page 100

Enabling IPv6 Tunneling in MPLS

You enable IPv6 tunneling by including the ipv6-tunneling statement in the configuration for the PE routers. This statement allows IPv6 routes to be resolved over an MPLS network by converting all routes stored in the inet.3 routing table to IPv4-compatible IPv6 addresses and then copying them into the inet6.3 routing table. This routing table can be used to resolve next hops for both inet6 and inet6-vpn routes.

To configure IPv6 tunneling, include the ipv6-tunneling statement on the PE routers:

```
ipv6-tunneling;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

You also need to configure IPv6 tunneling when you configure IPv6 VPNs. For more information, see the *JUNOS VPNs Configuration Guide*.

Configuring Multiprotocol BGP to Carry IPv6 Traffic

At the [family inet6] hierarchy level in BGP, configure the labeled-unicast statement with the explicit-null option. As with regular BGP configuration, the family statement can be specified on a per-neighbor, per-group, or global basis, so it can be configured at the following hierarchy levels:

- [edit protocols bgp]
- [edit protocols bgp group *group-name*]
- [edit protocols bgp group *group-name* neighbor *neighbor-name*]
- [edit logical-systems *logical-system-name* protocols bgp]
- [edit logical-systems *logical-system-name* protocols bgp group *group-name*]
- [edit logical-systems *logical-system-name* protocols bgp group *group-name* neighbor *neighbor-name*]

Configuring these statements enables the IPv4 MPLS label to be removed at the destination PE router. The remaining IPv6 packet without a label can then be forwarded to the IPv6 network.

Include the labeled-unicast statement as follows:

```
family inet6 {
    labeled-unicast {
        explicit-null;
    }
}
```

Configuring ICMP Message Tunneling

When you configure MPLS to tunnel through a routing domain, it is difficult to route a fragmented packet to its source address; for example, when the IP addresses carried in a packet are private (not globally unique) and MPLS is used to tunnel the packets through a public backbone.

When you configure ICMP message tunneling, an Internet Control Message Protocol (ICMP) message is sent to the source of a packet. The label stack is copied from the original packet to the ICMP message. The ICMP message is then label switched across the network. This causes the message to go to the original packet destination, rather than its source. Unless the message is label switched all the way to the destination host, it ends up unlabeled in a router that does know the source of the original packet, at which point the message is sent in the proper direction.

ICMP message tunneling can be useful for debugging and tracing purposes if the message is an ICMP time exceeded message.

To configure ICMP message tunneling, include the icmp-tunneling statement:

```
icmp-tunneling;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

LSP Attributes for GMPLS

When configuring GMPLS, use the LSP attributes statements. For information, see “Configuring MPLS LSPs for GMPLS” on page 453.

Chapter 6

DiffServ-Aware Traffic Engineering Configuration Guidelines

Differentiated Services (DiffServ)-aware traffic engineering provides a way to guarantee a specified level of service over a Multiprotocol Label Switching (MPLS) network. The routers providing DiffServ-aware traffic engineering are part of a differentiated services network domain. All routers participating in a differentiated services domain must have DiffServ-aware traffic engineering enabled.

To help ensure that the specified service level is provided, it is necessary to ensure that no more than the amount of traffic specified is sent over the differentiated services domain. You can accomplish this goal by configuring a policer to police or rate limit the volume of traffic transiting the differentiated service domain. For more information about how to configure policers for label-switched paths (LSPs), see "Configuring Policers for LSPs" on page 162.

This feature can help to improve the quality of Internet services such as voice over IP (VoIP). It also makes it possible to better emulate an Asynchronous Transfer Mode (ATM) circuit over an MPLS network.

This chapter describes how to configure DiffServ-aware traffic engineering for LSPs and multiclass LSPs:

- DiffServ-Aware Traffic Engineering Standards on page 114
- DiffServ-Aware Traffic Engineering Terminology on page 114
- DiffServ-Aware Traffic Engineering Overview on page 115
- Configuring DiffServ-Aware Traffic Engineering on page 118
- Bandwidth Oversubscription Overview on page 122
- Configuring the Bandwidth Subscription Percentage for LSPs on page 126
- Configuring DiffServ-Aware Traffic Engineering for LSPs on page 128
- Configuring Multiclass LSPs on page 131

DiffServ-Aware Traffic Engineering Standards

The following RFCs and Internet drafts provide information on DiffServ-aware traffic engineering and multiclass LSPs:

- RFC 3270, *Multi-Protocol Label Switching (MPLS) Support of Differentiated Services*
- RFC 3564, *Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering*
- RFC 4124, *Protocol Extensions for Support of Differentiated-Service-Aware MPLS Traffic Engineering*
- RFC 4125, *Maximum Allocation Bandwidth Constraints Model for Diff-Serv-aware MPLS Traffic Engineering*
- RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diff-Serv-aware MPLS*

These RFCs and Internet drafts are available on the IETF Web site at http://www.ietf.org/.

DiffServ-Aware Traffic Engineering Terminology

The following terminology applies to DiffServ-aware traffic engineering:

- Bandwidth model—The bandwidth model determines the values of the available bandwidth advertised by the interior gateway protocols (IGPs).
- CAC—Call admission control (CAC) checks to ensure there is adequate bandwidth on the path before the LSP is established. If the bandwidth is insufficient, the LSP is not established and an error is reported.
- Class type—A collection of traffic flows that is treated equivalently in a differentiated services domain. A class type maps to a queue and is much like a class-of-service (CoS) forwarding class in concept. It is also known as a traffic class.
- Differentiated Services—Differentiated Services make it possible to give different treatment to traffic based on the experimental (EXP) bits in the MPLS header. Traffic must be marked appropriately and CoS must be configured.
- Differentiated Services domain—The routers in a network that have Differentiated Services enabled.
- DiffServ-aware traffic engineering—A type of constraint-based routing. It can enforce different bandwidth constraints for different classes of traffic. It can also do CAC on each traffic engineering class when an LSP is established.
- Multiclass LSP—A multiclass LSP functions like a standard LSP, but it also allows you to reserve bandwidth from multiple class types. The EXP bits of the MPLS header are used to distinguish between class types.
- MAM—The maximum allocation bandwidth constraint model divides the available bandwidth between the different classes. Sharing of bandwidth between the class types is not allowed.
- RDM—The Russian dolls bandwidth constraint model makes efficient use of bandwidth by allowing the class types to share bandwidth.

- Traffic engineering class—A paired class type and priority.
- Traffic engineering class map—A map between the class types, priorities, and traffic engineering classes. The traffic engineering class mapping must be consistent across the Differentiated Services domain.

DiffServ-Aware Traffic Engineering Overview

Differentiated Services give different treatment to traffic based on the EXP bits in the MPLS label header and allow you to provide multiple classes of service.

The following sections describe DiffServ-aware traffic engineering:

- DiffServ-Aware Traffic Engineering Features on page 115
- DiffServ-Aware Traffic Engineered LSPs on page 116
- Multiclass LSPs on page 117

DiffServ-Aware Traffic Engineering Features

DiffServ-aware traffic engineering provides the following features:

- Traffic engineering at a per-class level rather than at an aggregate level
- Different bandwidth constraints for different class types (traffic classes)
- Different queuing behaviors per class, allowing the router to forward traffic based on the class type

In comparison, standard traffic engineering does not consider CoS, and it completes its work on an aggregate basis across all Differentiated Service classes.

DiffServ-aware traffic engineering provides the following advantages:

- Traffic engineering can be performed on a specific class type instead of at the aggregate level.
- Bandwidth constraints can be enforced on each specific class type.
- It forwards traffic based on the EXP bits.

This makes it possible to guarantee service and bandwidth across an MPLS network. With DiffServ-aware traffic engineering, among other services, you can provide ATM circuit emulation, VoIP, and a guaranteed bandwidth service.

The following describes how the IGP, Constrained Shortest Path First (CSPF), and Resource Reservation Protocol (RSVP) participate in DiffServ-aware traffic engineering:

- The IGP can advertise the unreserved bandwidth for each traffic engineering class to the other members of the differentiated services domain. The traffic engineering database (TED) stores this information.
- A CSPF calculation is performed considering the bandwidth constraints for each class type. If all the constraints are met, the CSPF calculation is considered successful.

- When RSVP signals an LSP, it requests bandwidth for specified class types.

DiffServ-Aware Traffic Engineered LSPs

A DiffServ-aware traffic engineered LSP is an LSP configured to reserve bandwidth for one of the supported class types and to carry traffic for that class type. The following sections discuss this type of LSPs:

- DiffServ-Aware Traffic Engineered LSPs Overview on page 116
- DiffServ-Aware Traffic Engineered LSPs Operation on page 116

DiffServ-Aware Traffic Engineered LSPs Overview

A DiffServ-aware traffic engineered LSP is an LSP configured with a bandwidth reservation for a specific class type. This LSP can carry traffic for a single class type. On the packets, the class type is specified by the EXP bits (also known as the class-of-service bits) and the per-hop behavior (PHB) associated with the EXP bits. The mapping between the EXP bits and the PHB is static, rather than being signaled in RSVP.

The class type must be configured consistently across the Differentiated Services domain, meaning the class type configuration must be consistent from router to router in the network. You can unambiguously map a class type to a queue. On each node router, the class-of-service queue configuration for an interface translates to the available bandwidth for a particular class type on that link.

For more information about topics related to LSPs and DiffServ-aware traffic engineering, see the following:

- For forwarding classes and class of service, see the *JUNOS Class of Service Configuration Guide*.
- For EXP bits, see “Label Allocation” on page 25.
- For differentiated services, see RFC 3270, *Multi-Protocol Label Switching (MPLS) Support of Differentiated Services*.
- For information about how the IGPs and RSVP have been modified to support Differentiated Services-aware MPLS traffic engineering, see Internet draft draft-ietf-tewg-diff-te-proto-07.txt.

DiffServ-Aware Traffic Engineered LSPs Operation

When configuring a DiffServ-aware traffic engineered LSP, you specify the class type and the bandwidth associated with it. The following occurs when an LSP is established with bandwidth reservation from a specific class type:

1. The IGPs advertise how much unreserved bandwidth is available for the traffic engineering classes.
2. When calculating the path for an LSP, CSPF is used to ensure that the bandwidth constraints are met for the class type carried by the LSP at the specified priority level.

CSPF also checks to ensure that the bandwidth model is configured consistently on each router participating in the LSP. If the bandwidth model is inconsistent, CSPF does not compute the path (except for LSPs from class type ct0).

3. Once a path is found, RSVP signals the LSP using the Classtype object in the path message. At each node in the path, the available bandwidth for the class types is adjusted as the path is set up.

An LSP that requires bandwidth from a particular class (except class type ct0) cannot be established through routers that do not understand the Classtype object. Preventing the use of routers that do not understand the Classtype object helps to ensure consistency throughout the Differentiated Services domain by preventing the LSP from using a router that cannot support Differentiated Services.

By default, LSPs are signaled with setup priority 7 and holding priority 0. An LSP configured with these values cannot preempt another LSP at setup time and cannot be preempted.

It is possible to have both LSPs configured for DiffServ-aware traffic engineering and regular LSPs configured at the same time on the same physical interfaces. For this type of heterogeneous environment, regular LSPs carry best-effort traffic by default. Traffic carried in the regular LSPs must have the correct EXP settings (either by remarking the EXP settings or by assuming that the traffic arrived with the correct EXP settings from the upstream router).

Multiclass LSPs

Multiclass LSPs function like standard LSPs, but they also allow you to configure multiple class types with guaranteed bandwidth. The EXP bits of the MPLS header are used to distinguish between class types. Multiclass LSPs can be configured for a variety of purposes. For example, you can configure a multiclass LSP to emulate the behavior of an ATM circuit. An ATM circuit can provide service-level guarantees to a class type. A multiclass LSP can provide a similar guaranteed level of service.

The following sections discuss multiclass LSPs:

- Multiclass LSP Overview on page 117
- Establishing a Multiclass LSP on the Differentiated Services Domain on page 118

Multiclass LSP Overview

A multiclass LSP is an LSP that can carry several class types. One multiclass LSP can be used to support up to four class types. On the packets, the class type is specified by the EXP bits (also known as the class-of-service bits) and the per-hop behavior (PHB) associated with the EXP bits. The mapping between the EXP bits and the PHB is static, rather than being signaled in RSVP.

Once a multiclass LSP is configured, traffic from all of the class types can:

- Follow the same path
- Be rerouted along the same path
- Be taken down at the same time

Class types must be configured consistently across the Differentiated Services domain, meaning the class type configuration must be consistent from router to router in the network.

You can unambiguously map a class type to a queue. On each node router, the CoS queue configuration for an interface translates to the available bandwidth for a particular class type on that link.

The combination of a class type and a priority level forms a traffic engineering class. The IGPs can advertise up to eight traffic engineering classes for each link.

For more information about the EXP bits, see "Label Allocation" on page 25.

For more information about forwarding classes, see the *JUNOS Class of Service Configuration Guide*.

Establishing a Multiclass LSP on the Differentiated Services Domain

The following occurs when a multiclass LSP is established on the differentiated services domain:

1. The IGPs advertise how much unreserved bandwidth is available for the traffic engineering classes.
2. When calculating the path for a multiclass LSP, CSPF is used to ensure that the constraints are met for all the class types carried by the multiclass LSP (a set of constraints instead of a single constraint).
3. Once a path is found, RSVP signals the LSP using an RSVP object in the path message. At each node in the path, the available bandwidth for the class types is adjusted as the path is set up. The RSVP object is a hop-by-hop object. Multiclass LSPs cannot be established through routers that do not understand this object. Preventing routers that do not understand the RSVP object from carrying traffic helps to ensure consistency throughout the differentiated services domain by preventing the multiclass LSP from using a router that is incapable of supporting differentiated services.

By default, multiclass LSPs are signaled with setup priority 7 and holding priority 0. A multiclass LSP configured with these values cannot preempt another LSP at setup time and cannot be preempted.

It is possible to have both multiclass LSPs and regular LSPs configured at the same time on the same physical interfaces. For this type of heterogeneous environment, regular LSPs carry best-effort traffic by default. Traffic carried in the regular LSPs must have the correct EXP settings.

Configuring DiffServ-Aware Traffic Engineering

To configure DiffServ-aware traffic engineering, include the **diffserv-te** statement:

```
diffserv-te {
   bandwidth-model {
      extended-mam;
      mam;
```

```
        rdm;
    }
    te-class-matrix {
        traffic-class {
            te number {
                priority priority;
                traffic-class ct number priority priority;
            }
        }
    }
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

You must configure the diffserv-te statement on all routers participating in the Differentiated Services domain. However, you are not required to configure the traffic engineering class matrix (configured with the te-class-matrix statement).

To configure DiffServ-aware traffic engineering, complete the procedures in the following sections:

- Configuring the Bandwidth Model on page 119
- Configuring Traffic Engineering Classes on page 120
- Configuring Class of Service on page 121

Configuring the Bandwidth Model

You must configure a bandwidth model on all routers participating in the Differentiated Services domain. The bandwidth models available are MAM, extended MAM, and RDM:

- Maximum allocation bandwidth constraints model (MAM)—Defined in RFC 4125, *Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*.
- Extended MAM—A proprietary bandwidth model that behaves much like standard MAM. If you configure multiclass LSPs, you must configure the extended MAM bandwidth model.
- Russian-dolls bandwidth allocation model (RDM)—Makes efficient use of bandwidth by allowing the class types to share bandwidth. RDM is defined in RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*.

To configure a bandwidth model, include the bandwidth-model statement and specify one of the bandwidth model options:

```
bandwidth-model {
    extended-mam;
    mam;
    rdm;
```

}

You can include this statement at the following hierarchy levels:

- [edit protocols mpls diffserv-te]
- [edit logical-systems *logical-system-name* protocols mpls diffserv-te]

NOTE: If you change the bandwidth model on an ingress router, all the LSPs enabled on the router are taken down and resignaled.

Configuring Traffic Engineering Classes

You are not required to configure the traffic engineering classes. Table 8 on page 120 shows the default values for everything in the traffic engineering class matrix. The default mapping is expressed in terms of the default forwarding classes defined in the CoS configuration.

Table 8: Default Values for the Traffic Engineering Class Matrix

Traffic Engineering Class	Class Type	Queue	Priority
te0	ct0	0	7
te1	ct1	1	7
te2	ct2	2	7
te3	ct3	3	7
te4	ct0	0	0
te5	ct1	1	0
te6	ct2	2	0
te7	ct3	3	0

You can override the default mapping by configuring other values for the traffic engineering classes. You can configure traffic engineering classes 0 through 7. For each traffic engineering class, you configure a class type (or queue) from 0 through 3. For each class type, you configure a priority from 0 through 7.

To configure traffic engineering classes explicitly, include the te-class-matrix statement:

```
te-class-matrix {
    te number {
        priority priority;
        traffic-class {
            ct number priority priority;
        }
```

```
    }
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls diffserv-te]
- [edit logical-systems *logical-system-name* protocols mpls diffserv-te]

The following example shows how to configure traffic engineering class te0 with class type ct1 and a priority of 4:

```
[edit protocols mpls diffserv-te]
te-class-matrix {
   te0 traffic-class ct1 priority 4;
}
```

NOTE: If you explicitly configure a value for one of the traffic engineering classes, all the default values in the traffic engineering class matrix are dropped.

When you explicitly configure traffic engineering classes, you must also configure a bandwidth model; otherwise, the configuration commit operation fails. See "Configuring the Bandwidth Model" on page 119.

Requirements and Limitations for the Traffic Engineering Class Matrix

When you configure a traffic engineering class matrix, be aware of the following requirements and limitations:

- A mapping configuration is local and affects only the router on which it is configured. It does not affect other systems participating in the differentiated services domain. However, for a Differentiated Services domain to function properly, you need to configure the same traffic engineering class matrix on all the routers participating in the same domain.
- When explicitly configuring traffic engineering classes, you must configure the classes in sequence (te0, te1, te2, te3, and so on); otherwise, the configuration commit operation fails.

The first traffic engineering class you configure must be te0; otherwise, the configuration commit operation fails.

Configuring Class of Service

To configure Diffserv-aware traffic engineering, you must also configure class of service. The following example illustrates a class-of-service configuration that would allocate 25 percent of the link bandwidth to each class:

```
class-of-service {
   interfaces {
      all {
         scheduler-map simple-map;
```

```
        }
    }
    scheduler-maps {
        simple-map {
            forwarding-class assured-forwarding scheduler simple_sched;
                forwarding-class best-effort scheduler simple_sched;
                forwarding-class network-control scheduler simple_sched;
            forwarding-class expedited-forwarding scheduler simple_sched;
        }
    }
    schedulers {
        simple-sched {
            transmit-rate percent 25;
            buffer-size percent 25;
        }
    }
}
```

For more information on how to configure class of service, see the *JUNOS Class of Service Configuration Guide*.

Bandwidth Oversubscription Overview

LSPs are established with bandwidth reservations configured for the maximum amount of traffic you expect to traverse the LSP. Not all LSPs carry the maximum amount of traffic over their links at all times. For example, even if the bandwidth for link A has been completely reserved, actual bandwidth might still be available but not currently in use. This excess bandwidth can be used by allowing other LSPs to also use link A, oversubscribing the link. You can oversubscribe the bandwidth configured for individual class types or specify a single value for all of the class types using an interface.

You can use oversubscription to take advantage of the statistical nature of traffic patterns and to permit higher utilization of links.

The following examples describe how you might use bandwidth oversubscription and undersubscription:

- Use oversubscription on class types where peak periods of traffic do not coincide in time.
- Use oversubscription of class types carrying best-effort traffic. You take the risk of temporarily delaying or dropping traffic in exchange for making better utilization of network resources.
- Give different degrees of oversubscription or undersubscription of traffic for the different class types. For instance, you configure the subscription for classes of traffic as follows:
  - Best effort—ct0 1000
  - Voice—ct3 1

When you undersubscribe a class type for a multiclass LSP, the total demand of all RSVP sessions is always less than the actual capacity of the class type. You can use undersubscription to limit the utilization of a class type.

The bandwidth oversubscription calculation occurs on the local router only. Because no signaling or other interaction is required from other routers in the network, the feature can be enabled on individual routers without being enabled or available on other routers which might not support this feature. Neighboring routers do not need to know about the oversubscription calculation, they rely on the IGP.

The following sections describe the types of bandwidth oversubscription available in the JUNOS software:

- LSP Size Oversubscription on page 123
- Link Size Oversubscription on page 123
- Class Type Oversubscription and Local Oversubscription Multipliers on page 123

LSP Size Oversubscription

For LSP size oversubscription, you simply configure less bandwidth than the peak rate expected for the LSP. You also might need to adjust the configuration for automatic policers. Automatic policers manage the traffic assigned to an LSP, ensuring that it does not exceed the configured bandwidth values. LSP size oversubscription requires that the LSP can exceed its configured bandwidth allocation.

Policing is still possible. However, the policer must be manually configured to account for the maximum bandwidth planned for the LSP, rather than for the configured value.

Link Size Oversubscription

You can increase the maximum reservable bandwidth on the link and use the inflated values for bandwidth accounting. Use the subscription statement to oversubscribe the link. The configured value is applied to all class type bandwidth allocations on the link. For more information about link size oversubscription, see “Configuring the Bandwidth Subscription Percentage for LSPs” on page 126.

Class Type Oversubscription and Local Oversubscription Multipliers

Local oversubscription multipliers (LOMs) allow different oversubscription values for different class types. LOMs are useful for networks where the oversubscription ratio needs to be configured differently on different links and where oversubscription values are required for different classes. You might use this feature to oversubscribe class types handling best-effort traffic, but use no oversubscription for class types handling voice traffic. An LOM is calculated locally on the router. No information related to an LOM is signaled to other routers in the network.

An LOM is configurable on each link and for each class type. The per-class type LOM allows you to increase or decrease the oversubscription ratio. The per-class-type LOM is factored into all local bandwidth accounting for admission control and IGP advertisement of unreserved bandwidths.

The LOM calculation is tied to the bandwidth model (MAM, extended MAM, and Russian dolls) used, because the effect of oversubscription across class types must be accounted for accurately.

NOTE: All LOM calculations are performed by the JUNOS software and require no user intervention.

The formulas related to the oversubscription of class types are described in the following sections:

- Class Type Bandwidth and the LOM on page 124
- LOM Calculation for the MAM and Extended MAM Bandwidth Models on page 124
- LOM Calculation for the Russian Dolls Bandwidth Model on page 125
- Example: LOM Calculation on page 125

Class Type Bandwidth and the LOM

The following formula expresses the relationship between the bandwidth of the class type and the LOM. The normalized bandwidth of the class type (N_B) is equal to the reserved bandwidth of the class type (R_B) divided by the LOM of the class type (L_C):

$$N_B = R_B/L_C$$

When calculating available bandwidth, you need to subtract the normalized bandwidth from the relevant bandwidth constraint.

NOTE: When using an LOM, values advertised for the available bandwidth might be larger than the bandwidth constraint values. However, the values advertised in the maximum link bandwidth advertisement are not affected by local oversubscription.

LOM Calculation for the MAM and Extended MAM Bandwidth Models

The following formulas show how the LOM is calculated for the MAM and extended MAM bandwidth models.

Unreserved TE-Class(i) = LOM*c* x [BC*c* - SUM (Normalized (CT*c*, q))] for q <= *p*

Or

Unreserved TE-Class(i) = (LOM*c* x BC*c*) - SUM (Reserved (CT*c*, q)) for q <= *p*

where:

- LOM*c*—LOM for class type *c*.
- BC*c*—Bandwidth constraint for class type *c*.
- CT*c*—Class type *c*.
- TE-Class(i) <--> (CT*c* , preemption *p*) in the configured TE-Class mapping.

LOM Calculation for the Russian Dolls Bandwidth Model

The following formulas show how the LOM is calculated for the Russian dolls bandwidth model:

Unreserved TE-Class (i) = LOMc x MIN [

[BC*c* - SUM (Normalized (CT*b*, q))] for q <= *p* and *c* <= *b* <= 7,
. . .
[BC0 - SUM (Normalized (CT*b*, q))] for q <= *p* and 0 <= *b* <= 7,

]

where:

- LOM*c*—LOM for class type *c*.
- BC*c*—Bandwidth constraint for class type *c*.
- TE-Class(i) < – – > (CT*c* , preemption *p*) in the configured TE-Class mapping.

Note that the impact of an LSP on the unreserved bandwidth of a class type does not depend only on the LOM for that class type—it also depends on the LOM for the class type of the LSP.

Example: LOM Calculation

The following example illustrates how an LOM calculation is made for four classes of traffic: ct0, ct1, ct2, and ct3.

The class types have been assigned the following values:

ct0 = 40
ct1 = 30
ct2 = 20
ct3 = 10

These class type values yield the following bandwidth constraints:

BC0 = (ct3 + ct2 + ct1 + ct0) = 100
BC1 = (ct3 + ct2 + ct1) = 60
BC2 = (ct3 + ct2) = 30
BC3 = (ct3) = 10

LSPs from class type ct0 can take up to 100 percent of bandwidth on the link. LSPs from class type ct1 can take up to 60 percent of the bandwidth on the link, and so on.

If you assume for this example that the class types have the following LOM values:

LOM(ct0) = 8
LOM(ct1) = 4
LOM(ct2) = 2
LOM(ct3) = 1

In the absence of any other reservation, LSPs from class type ct0 can take up to 800 percent of the available bandwidth (8 x 100 = 800). In the absence of any other reservation, LSPs from class type ct1 can take up to 240 percent of the available bandwidth (4 x 60 = 240). and so on.

The maximum amount of bandwidth that can be reserved is:

ct0 = LOM(ct0) x BC0 = 800
ct1 = LOM(ct1) x BC1 = 240
ct2 = LOM(ct2) x BC2 = 60
ct3 = LOM(ct3) x BC3 = 10

For the undersubscribed class type ct3, the maximum reservable bandwidth is the same as the bandwidth constraint. For the overbooked class types, these values are not the values of the bandwidth constraint-taking into account the oversubscription for each class type separately. The oversubscription per class type in the sum is not taken into account because ultimately the entire bandwidth constraint can be filled with the bandwidth reservation of just one class type, so you have to account for that class type's bandwidth oversubscription only.

When calculating the available bandwidth for CTc, you need to express reservations from other classes as if they were from CTc. The reservation from class ctx is normalized with the LOM of ctx, but it is then multiplied by the LOM of CTc.

For the previous example, assume that LSP1 has class type ct3 configured with bandwidth of 10 and a priority of 0.

The values for the reservable bandwidth will be:

ct0 = 8 x (100 - 10) = 720
ct1 = 4 x min((100-10), (60-10)) = 200
ct2 = 2 x min((100-10), (60-10), (30-10)) = 40
ct3 = 1 x min((100-10), (60-10), (30-10), (10-10)) = 0

These numbers can be rationalized as follows: the normalized reservation is 10 percent. If this bandwidth came from class type ct0, it would be equivalent to an overbooked reservation of 80 percent. You can see that 720 percent (800 – 80 = 720) of the bandwidth remains available for other LSPs.

Configuring the Bandwidth Subscription Percentage for LSPs

By default, RSVP allows all of a class type's bandwidth (100 percent) to be used for RSVP reservations. When you oversubscribe a class type for a multiclass LSP, the aggregate demand of all RSVP sessions is allowed to exceed the actual capacity of the class type.

If you want to oversubscribe or undersubscribe all of the class types on an interface using the same percentage bandwidth, configure the percentage using the subscription statement:

subscription *percentage*;

For a list of hierarchy levels at which you can include this statement, see the statement summary section.

To undersubscribe or oversubscribe the bandwidth for each class type, configure a percentage for each class type (ct0, ct1, ct2, and ct3) option for the subscription statement. When you oversubscribe a class type, an LOM is applied to calculate the actual bandwidth reserved. See "Class Type Oversubscription and Local Oversubscription Multipliers" on page 123 for more information.

```
subscription {
   ct0 percentage;
   ct1 percentage;
   ct2 percentage;
   ct3 percentage;
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section.

percentage is the percentage of class type bandwidth that RSVP allows to be used for reservations. It can be a value from 0 through 65,000 percent. If you specify a value greater than 100, you are oversubscribing the interface or class type.

The value you configure when you oversubscribe a class type is a percentage of the class type bandwidth that can actually be used. The default subscription value is 100 percent.

You can use the subscription statement to disable new RSVP sessions for one or more class types. If you configure a percentage of 0, no new sessions (including those with zero bandwidth requirements) are permitted for the class type.

Existing RSVP sessions are not affected by changing the subscription factor. To clear an existing session, issue the clear rsvp session command. For more information on the clear rsvp session command, see the *JUNOS Routing Protocols and Policies Command Reference*.

Bandwidth Subscription Troubleshooting

Be aware of the following issues when configuring bandwidth subscription:

- If you configure the subscription statement at the [edit protocols rsvp interface all] hierarchy level, and then configure a different value at the [edit protocols rsvp interface *interface-name*] hierarchy level, the value configured at the [edit protocols rsvp interface *interface-name*] hierarchy level overrides the other value.
- Per-class-type subscription can only be configured if a bandwidth model is also configured. If no bandwidth model is configured, the configuration fails with the following error message:

```
user@host# commit check

[edit protocols rsvp interface all]
  'subscription'
RSVP: Must have a diffserv-te bandwidth model configured when configuring
```

```
 subscription per traffic class.
error: configuration check-out failed
```

- If you configure the subscription statement for a specific class type, you cannot configure the subscription statement for the whole interface. The configuration commit operation fails with the following error message:

```
user@host# commit check

[edit protocols rsvp interface all]
  'subscription'
    RSVP: Cannot configure both link subscription and per traffic class
subscription.
error: configuration check-out failed
```

Configuring DiffServ-Aware Traffic Engineering for LSPs

You must configure the Differentiated Services domain (see "Configuring DiffServ-Aware Traffic Engineering" on page 118) before you can enable DiffServ-aware traffic engineering for LSPs. The Differentiated Services domain provides the underlying class types and corresponding traffic engineering classes that you reference in the LSP configuration. The traffic engineering classes must be configured consistently on each router participating in the Differentiated Services domain for the LSP to function properly.

NOTE: You must configure either MAM or RDM as the bandwidth model when you configure DiffServ-aware traffic engineering for LSPs. See "Configuring the Bandwidth Model" on page 119.

The actual data transmitted over this Differentiated Services domain is carried by an LSP. Each LSP relies on the EXP bits of the MPLS packets to enable DiffServ-aware traffic engineering. Each LSP can carry traffic for a single class type.

All the routers participating in the LSP must be Juniper Networks routing platforms running JUNOS Release 6.3 or later. The network can include routers from other vendors and Juniper Networks routers running earlier versions of the JUNOS software. However, the DiffServ-aware traffic engineering LSP cannot traverse these routers.

NOTE: You cannot simultaneously configure multiclass LSPs and DiffServ-aware traffic engineering LSPs on the same router.

To enable DiffServ-aware traffic engineering for LSPs, you need to configure the following:

- Configuring Class of Service for the Interfaces on page 129
- Configuring IGP on page 129
- Configuring a Traffic Engineered LSP on page 129

- Configuring Policing for LSPs on page 130
- Configuring Fast Reroute for Traffic Engineered LSPs on page 130

Configuring Class of Service for the Interfaces

The existing class-of-service (CoS) infrastructure ensures that traffic that is consistently marked receives the scheduling guarantees for its class. The classification, marking, and scheduling necessary to accomplish this are configured using the existing JUNOS software CoS features.

NOTE: ATM interfaces are not supported.

For information on how to configure CoS, see the *JUNOS Class of Service Configuration Guide*.

Configuring IGP

You can configure either IS-IS or OSPF as the IGP. The IS-IS and OSPF configurations for routers supporting LSPs are standard. For information on how to configure these protocols, see the *JUNOS Routing Protocols Configuration Guide*.

Configuring a Traffic Engineered LSP

You configure an LSP by using the standard LSP configuration statements and procedures. To configure DiffServ-aware traffic engineering for the LSP, specify a class type bandwidth constraint by including the bandwidth statement:

```
label-switched-path lsp-name {
    bandwidth {
        ctnumber bps;
    }
}
```

For a list of hierarchy levels at which you can include the bandwidth statement, see the statement summary sections for this statement.

If you do not specify a bandwidth for a class type, ct0 is automatically specified as the queue for the LSP. You can configure only one class type for each LSP, unlike multiclass LSPs.

The class type statements specify bandwidth (in bits per second) for the following classes:

- ct0—Bandwidth reserved for class 0
- ct1—Bandwidth reserved for class 1
- ct2—Bandwidth reserved for class 2
- ct3—Bandwidth reserved for class 3

You can configure setup and holding priorities for an LSP, but the following restrictions apply:

- The combination of class and priority must be one of the configured traffic engineering classes. The default setup priority is 7 and the default holding priority is 0.
- Configuring an invalid combination of class type and priority causes the commit operation to fail.
- Automatic bandwidth allocation is not supported. If you configure automatic bandwidth allocation, the commit operation fails.
- LSPs configured with the bandwidth statement but without specifying a class type use the default class type ct0.
- For migration issues, see Internet draft draft-ietf-tewg-diff-te-proto-07.txt.

Configuring Policing for LSPs

Policing allows you to control the amount of traffic forwarded through a particular LSP. Policing helps to ensure that the amount of traffic forwarded through an LSP never exceeds the requested bandwidth allocation. You can configure multiple policers for each LSP.

For information on how to configure a policer for an LSP, see "Configuring Policers for LSPs" on page 162.

Configuring Fast Reroute for Traffic Engineered LSPs

You can configure fast reroute for traffic engineered LSPs (LSPs carrying a single class of traffic). It is also possible to reserve bandwidth on the detour path for the class of traffic when fast reroute is enabled. The same class type number is used for both the traffic engineered LSP and its detour.

If you configure the router to reserve bandwidth for the detour path, a check is made to ensure that the link is capable of handling DiffServ-aware traffic engineering and for CoS capability before accepting it as a potential detour path. Unsupported links are not used.

You can configure the amount of bandwidth to reserve for detours using either the bandwidth statement or the bandwidth-percent statement. You can only configure one these statements at a time. If you do not configure either the bandwidth statement or the bandwidth-percent statement, the default setting is to not reserve bandwidth for the detour path (the bandwidth guarantee will be lost if traffic is switched to the detour).

When you configure the bandwidth statement, you can specify the specific amount of bandwidth (in bits per second [bps]) you want to reserve for the detour path. For information, see "Configuring Fast Reroute" on page 71.

When you configure the bandwidth-percent statement, the detour path bandwidth is computed by multiplying it to the bandwidth configured for the main traffic

engineered LSP. For information on how to configure the bandwidth for a traffic engineered LSP, see “Configuring a Traffic Engineered LSP” on page 129.

To configure the percent of bandwidth used by the detour path based on the bandwidth of the protected path, include the bandwidth-percent statement:

```
bandwidth-percent percentage;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name* fast-reroute]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* fast-reroute]

Configuring Multiclass LSPs

A multiclass LSP is an LSP configured to reserve bandwidth for multiple class types and also carries the traffic for these class types. The differentiated service behavior is determined by the EXP bits.

You must configure the Differentiated Services domain (see “Configuring DiffServ-Aware Traffic Engineering” on page 118) before you can enable a multiclass LSP. The Differentiated Services domain provides the underlying class types and corresponding traffic engineering classes that you reference in a multiclass LSP configuration. The traffic engineering classes must be configured consistently on each router participating in the Differentiated Services domain for the multiclass LSP to function properly.

NOTE: You must configure extended MAM as the bandwidth model when you configure multiclass LSPs. See “Configuring the Bandwidth Model” on page 119.

All the routers participating in a multiclass LSP must be Juniper Networks routing platforms running JUNOS Release 6.2 or later. The network can include routers from other vendors and Juniper Networks routers running earlier versions of the JUNOS software. However, the multiclass LSP cannot traverse these routers.

To enable multiclass LSPs, you need to configure the following:

- Configuring Class of Service for the Interfaces on page 131
- Configuring the IGP on page 132
- Configuring a Multiclass LSP on page 132
- Configuring Policing for Multiclass LSPs on page 133
- Configuring Fast Reroute for Multiclass LSPs on page 133

Configuring Class of Service for the Interfaces

The existing class-of-service infrastructure ensures that traffic that is consistently marked receives the scheduling guarantees for its class. The classification, marking,

and scheduling necessary to consistently mark traffic are configured with the existing JUNOS software CoS features.

NOTE: ATM interfaces are not supported.

For information on how to configure CoS, see the *JUNOS Class of Service Configuration Guide*.

Configuring the IGP

You can configure either IS-IS or OSPF. The IS-IS and OSPF configurations for routers supporting multiclass LSPs are standard. For information about how to configure these protocols, see the *JUNOS Routing Protocols Configuration Guide*.

Configuring a Multiclass LSP

You configure a multiclass LSP by using the standard LSP configuration statements and procedures. To configure an LSP as a multiclass LSP, specify the class type bandwidth constraints by including the bandwidth statement:

```
bandwidth {
    ct0 bps;
    ct1 bps;
    ct2 bps;
    ct3 bps;
}
```

For a list of hierarchy levels at which you can include the bandwidth statement, see the statement summary sections for these statements.

The class type statements specify bandwidth (in bits per second) for the following classes:

- ct0—Bandwidth reserved for class 0
- ct1—Bandwidth reserved for class 1
- ct2—Bandwidth reserved for class 2
- ct3—Bandwidth reserved for class 3

For example, to configure 50 megabytes of bandwidth for class type 1 and 30 megabytes of bandwidth for class type 2, include the bandwidth statement as follows:

```
[edit protocols mpls]
label-switched-path traffic-class {
    bandwidth {
        ct1 50M;
        ct2 30M;
    }
}
```

You cannot configure a bandwidth for a class type and also configure a bandwidth at the [edit protocols mpls label-switched-path *lsp-name* bandwidth] hierarchy level. For example, the following configuration cannot be committed:

```
[edit protocols mpls]
label-switched-path traffic-class {
   bandwidth {
      20M;
      ct1 10M;
   }
}
```

You can configure setup and holding priorities for a multiclass LSP, but the following restrictions apply:

- The setup and holding priorities apply to all classes for which bandwidth is requested.
- The combination of class and priority must be one of the configured traffic engineering classes. The default traffic engineering class configuration results in multiclass LSPs that cannot preempt and cannot be preempted. The default setup priority is 7 and the default holding priority is 0.
- Configuring an invalid combination of class type and priority causes the commit operation to fail.
- Automatic bandwidth allocation is not supported for multiclass LSPs. If you configure automatic bandwidth allocation, the commit operation fails.
- LSPs configured with the bandwidth statement but without specifying a class type use the default class type ct0.

Configuring Policing for Multiclass LSPs

Policing allows you to control the amount of traffic forwarded through a particular multiclass LSP. Policing helps to ensure that the amount of traffic forwarded through an LSP never exceeds the requested bandwidth allocation. You can configure multiple policers for each multiclass LSP. You can also enable automatic policing for multiclass LSPs.

For information on how to configure a policer for a multiclass LSP, see “Configuring Policers for LSPs” on page 162 and “Configuring Automatic Policers” on page 164.

Configuring Fast Reroute for Multiclass LSPs

You can enable fast reroute for multiclass LSPs. The bandwidth guarantees for the class types can be carried over to the detour path in case the primary path of the multiclass LSP fails. The same traffic class types configured for the primary multiclass LSP are also signaled for the detour LSP.

The bandwidth guarantee for the detour path is a percentage of the bandwidth configured for the class types of the primary path. For example, you configure a value of 50 percent for the detour path and the protected LSP carries traffic for class types CT0 through CT3. The detour path is signaled with the same class types (CT0 through CT3) but with 50 percent of the bandwidth configured for the protected LSP.

If you configure the router to reserve bandwidth for the detour path, a check is made to ensure that the link is capable of handling DiffServ-aware traffic engineering, that all of the traffic class types needed are available, and for CoS capability before accepting it as a potential detour path. Unsupported links are not used.

The bandwidth percentage for fast reroute is signaled from the ingress router to the egress router. All of the intermediate devices must complete their own CSPF computations and signaling.

When you configure the bandwidth-percent statement, the detour path bandwidth is computed by multiplying it to the bandwidth configured for the primary multiclass LSP. For information on how to configure the bandwidth for the multiclass LSP, see "Configuring a Traffic Engineered LSP" on page 129.

To configure the percent of bandwidth used by the detour path based on the bandwidth of the protected path, include the bandwidth-percent statement:

```
bandwidth-percent percentage;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name* fast-reroute]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* fast-reroute]

Chapter 7

Static and Explicit-Path LSP Configuration Guidelines

The following sections describe how to configure static and explicit-path label-switched paths (LSPs):

- Configuring Static LSPs on page 135
- Configuring Explicit-Path LSPs on page 142

Configuring Static LSPs

To configure static LSPs, configure the ingress router and each router along the path up to and including the egress router.

For the ingress router, configure which packets to tag (based on the packet's IP destination address), the next router in the LSP, and the tag to apply to the packet. Manually assigned labels can have values from 1,000,000 through 1,048,575. Optionally, you can apply preference and class-of-service (CoS) values to the packets.

For the intermediate routers in the path, configure the next router in the path and the tag to apply to the packet. Again, you can optionally apply preference and CoS values to the packets.

For the egress router, you generally just remove the label and continue forwarding the packet to the next hop. However, if the previous router removed the label, the egress router examines the packet's IP header and forwards the packet toward its IP destination.

To configure static Multiprotocol Label Switching (MPLS), perform the following tasks:

- Configuring the Ingress Router for Static LSPs on page 135
- Configuring the Intermediate and Egress Routers for Static LSPs on page 138
- Configuring Static Unicast Routes for Point-to-Multipoint LSPs on page 140

Configuring the Ingress Router for Static LSPs

The ingress router checks the IP address in the incoming packet's destination address field and, if it finds a match in the routing table, applies the label associated with that address to the packets. The label has forwarding information associated with it, including the address of the next-hop router, and the route preference and CoS values.

To configure static LSPs on the ingress router, include the static-path statement:

```
static-path inet {
   prefix {
      class-of-service value;
      double-push bottom-label top-label;
      next-hop (address | interface-name | address/interface-name);
      preference preference;
      push out-label;
      triple-push bottom-label middle-label top-label;
   }
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

The next-hop and push statements are required; the other statements are optional.

Each static-path statement consists of the following parts:

- Criteria to use to analyze an incoming packet:
  - The inet option creates an LSP that handles IPv4 packets. All static MPLS routes created using the inet option are installed in the default IPv4 routing table (inet.0), and the creating protocol is identified as static. This process is no different from creating static IPv4 routes at the [edit routing-options static] hierarchy level.
  - In the *prefix* option, you configure the IP destination address to check when incoming packets are analyzed. If the address matches, the specified label, *out-label*, is assigned to the packet, and the packet enters an LSP. Each prefix that you specify is installed as a static route in the routing table. You can specify one or more *prefix* statements at the [edit protocols mpls static-path] hierarchy level.
- The next-hop statement, which supplies the IP address of the next hop to the destination. You can specify this as the IP address of the next hop, the interface name (for point-to-point interfaces only), or as *address/interface-name* to specify an IP address on an operational interface. When the next hop is on a directly attached interface, the route is installed in the routing table. You cannot configure a LAN or nonbroadcast multiaccess (NBMA) interface as a next-hop interface.
- Label properties applied to the packet in the LSP, which are defined by the following statements:
  - push *out-label*—Push one more label on top of the stack.
  - double-push *bottom-label top-label*—Push two more labels on top of the stack.
  - triple-push *bottom-label middle-label top-label*—Push three more labels on top of the stack.

    A label is a 20-bit integer, so it can be a number from 0 through 1,048,575 (220– 1). Labels 0 through 999,999 are for internal use. Labels 1,000,000

through 1,048,575 are unassigned by the JUNOS software and are available for static LSPs. When you configure static LSPs, you can use only this range of labels.

- Preference of this route (defined by the preference *preference* statement).
- CoS value to apply to the packet (defined by the class-of-service *cos-value* statement).

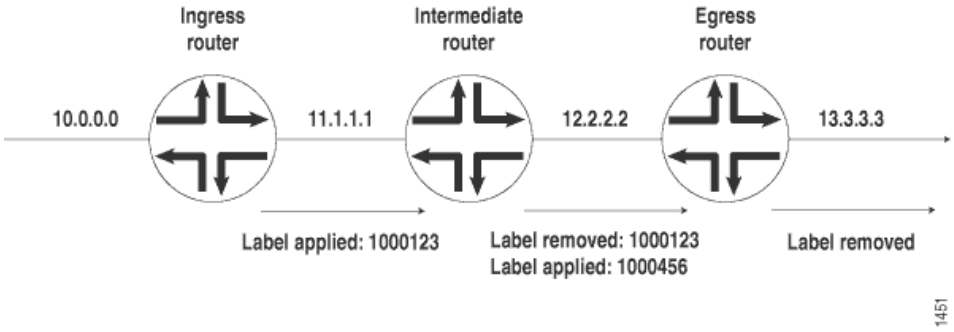
To determine whether a static ingress route is installed, use the command show route table inet.0 protocol static. The following is sample output. The push keyword identifies that a label is to be added in front of an IP packet.

```
10.0.0.0       *[Static/5] 00:01:48
> to 11.1.1.1 via so-0/0/0, push 1000123
```

Example: Configuring the Ingress Router

Configure the ingress router for a static LSP that consists of three routers (see Figure 20 on page 137).

Figure 20: Static MPLS Configuration



For packets addressed to 10.0.0.0, assign label 1000123 and transmit them to the next-hop router at 11.1.1.1:

```
[edit]
interfaces {
   so-0/0/0 {
      unit 0 {
         family mpls;
      }
   }
}
protocols {
   mpls {
      static-path inet {
         10.0.0.0 {
            next-hop 11.1.1.1;
            push 1000123;
         }
```

```
        }
        interface so-0/0/0;
    }
}
```

To determine whether the static ingress route is installed, use the following command:

```
user@host> show route table inet.0 protocol static
```

The following is a sample of the output. The push 1000123 keyword identifies the route.

```
10.0.0.0/8       *[Static/5] 00:01:48
> to 11.1.1.1 via so-0/0/0, push 1000123
```

Configuring the Intermediate and Egress Routers for Static LSPs

Intermediate and egress routers perform similar functions—they modify the label that has been applied to a packet. An intermediate router can change the label. An egress router removes the label (if the packet still contains a label) and continues forwarding the packet to its destination.

To configure static LSPs on intermediate and egress routers, include the interface statement:

```
interface (interface-name | all) {
    disable;
    admin-group [ group-names ];
    label-map in-label {
        class-of-service cos-value;
        next-hop (address | interface-name | address/interface-name) | (discard | reject);
        (pop | swap <out-label>);
        preference preference;
        swap-push swap-label push-label;
    }
}
```

You can include these statements at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

For the label-map statement configuration, the next-hop | (reject | discard) and pop | swap statements are required. The remaining statements are optional.

Each statement within the interface statement consists of the following parts:

- Criteria to use to analyze the labeled packet. Two criteria are used: the interface on which the packet was received (specified in the opening interface statement itself) and the packet's label (specified in the label-map statement).
- The next-hop statement, which supplies the IP address of the next hop to the destination. The address is specified as the IP address of the next hop, or the interface name (for point-to-point interfaces only), or *address* and *interface-name*

to specify an IP address on an operational interface. When the specified next hop is on a directly attached interface, this route is installed in the routing table. You cannot configure a LAN or NBMA interface as a next-hop interface.

- Operation to perform on the labeled packet:
  - For egress routers, remove the packet's label altogether (pop).
  - For intermediate routers only, exchange the label for another label (swap *out-label*).
  - Discard the packet, sending an ICMP unreachable message to the packet's originator (reject).
  - Discard the packet without sending an ICMP unreachable message to the packet's originator (discard).
- Label properties to apply to the packet (all are optional):
  - Preference value for this route (preference *preference*).
  - For intermediate routers only, the CoS value to apply to the packet (class-of-service *cos-value*).

You can specify any number of label-map statements at the [edit protocols mpls interface *interface-name*] hierarchy level.

The static routes are installed in the default MPLS routing table, mpls.0, and the creating protocol is identified as static. To verify that a static route is properly installed, use the command show route table mpls.0 protocol static. The following is an example of the output:

```
1000123       *[Static/5] 00:00:38
> to 12.2.2.2 via so-5/0/0.0, swap 1000456
```

Example: Configuring an Intermediate Router

For packets labeled 1000123 arriving on interface so-0/0/0, assign the label 1000456, and transmit them to the next-hop router at 12.2.2.2:

```
[edit]
interfaces {
   so-0/0/0 {
      unit 0 {
         family mpls;
      }
   }
}
protocols {
   mpls {
      interface so-0/0/0 {
         label-map 1000123 {
            next-hop 12.2.2.2;
            swap 1000456;
         }
      }
```

```
    }
  }
```

To determine whether the static intermediate route is installed, use the following command:

```
user@host> show route table mpls.0 protocol static
```

The following is a sample of the output. The swap 1000456 keyword identifies the route.

```
1000123       *[Static/5] 00:01:48
> to 12.2.2.2 via so-0/0/0, swap 1000456
```

Example: Configuring an Egress Router

For packets labeled 1000456 arriving on interface so-0/0/0, remove the label and transmit the packets to the next-hop router at 13.3.3.3:

```
[edit]
interfaces {
   so-0/0/0 {
      unit 0 {
         family mpls;
      }
   }
}
protocols {
   mpls {
      interface so-0/0/0 {
         label-map 1000456 {
            next-hop 13.3.3.3;
            pop;
         }
      }
   }
}
```

To determine whether the static egress route is installed, use the following command:

```
user@host> show route table mpls.0 protocol static
```

The following is a sample of the output. The pop keyword identifies the egress route.

```
1000456        *[Static/5] 00:01:48
> to 13.3.3.3 via so-0/0/0, pop
```

Configuring Static Unicast Routes for Point-to-Multipoint LSPs

You can configure a static unicast IP route with a point-to-multipoint LSP as the next hop. For more information on point-to-multipoint LSPs, see “Point-to-Multipoint LSPs” on page 47, “Point-to-Multipoint LSP Configuration Guidelines” on page 143, and “Configuring CCC Switching for Point-to-Multipoint LSPs” on page 417.

To configure a static unicast route for a point-to-multipoint LSP, complete the following steps:

1. On the ingress PE router, configure a static IP unicast route with the point-to-multipoint LSP name as the next hop by including the p2mp-lsp-next-hop statement:

   p2mp-lsp-next-hop *point-to-multipoint-lsp-next-hop*;

   You can include this statement at the following hierarchy levels:

   - [edit routing-options static route *route-name*]
   - [edit logical-systems *logical-system-name* routing-options static route *route-name*]

2. On the egress PE router, configure a static IP unicast route with the same destination address configured in Step 1 (the address configured at the [edit routing-options static route] hierarchy level) by including the next-hop statement:

   next-hop *address*;

   You can include this statement at the following hierarchy levels:

   - [edit logical-systems *logical-system-name* routing-options static route *route-name*]
   - [edit routing-options static route *route-name*]

NOTE: CCC and static routes cannot use the same point-to-multipoint LSP.

For more information on static routes, see the *JUNOS Routing Protocols Configuration Guide*.

The following show route command output displays a unicast static route pointing to a point-to-multipoint LSP on the ingress PE router where the LSP has two branch next hops:

```
user@host> show route 5.5.5.5 detail
inet.0: 29 destinations, 30 routes (28 active, 0 holddown, 1 hidden)
5.5.5.5/32 (1 entry, 1 announced)
        *Static Preference: 5
                Next hop type: Flood
                Next hop: via so-0/3/2.0 weight 1
                Label operation: Push 100000
                Next hop: via t1-0/1/1.0 weight 1
                Label operation: Push 100064
                State: <Active Int Ext>
                Local AS: 10458
                Age: 2:41:15
                Task: RT
                Announcement bits (2): 0-KRT 3-BGP.0.0.0.0+179
                AS path: I
```

Configuring Explicit-Path LSPs

If you disable constrained-path label-switched path (LSP) computation, as described in "Disabling Constrained-Path LSP Computation" on page 88, you can configure LSPs manually or allow the LSPs to follow the IGP path.

When explicit-path LSPs are configured, the LSP is established along the path you specified. If the path is topologically not feasible, either because the network is partitioned or insufficient resources are available along some parts of the path, the LSP will fail. No alternative paths can be used. If the setup succeeds, the LSP stays on the defined path indefinitely.

To configure an explicit-path LSP, follow these steps:

1. Configure the path information in a named path, as described in "Creating a Named Path" on page 58. To configure complete path information, specify every router hop between the ingress and egress routers, preferably using the strict attribute. To configure incomplete path information, specify only a subset of router hops, using the loose attribute in places where the path is incomplete.

   For incomplete paths, the MPLS routers complete the path by querying the local routing table. This query is done on a hop-by-hop basis, and each router can figure out only enough information to reach the next explicit hop. It might be necessary to traverse a number of routers to reach the next (loose) explicit hop.

   Configuring incomplete path information creates portions of the path that depend on the current routing table, and this portion of the path can reroute itself as the topology changes. Therefore, an explicit-path LSP that contains incomplete path information is not completely fixed. These types of LSPs have only a limited ability to repair themselves, and they tend to create loops or flaps depending on the contents of the local routing table.
2. To configure the LSP and point it to the named path, use either the primary or secondary statement, as described in "Configuring the Primary and Secondary LSPs" on page 68.
3. Disable constrained-path LSP computation by including the no-cspf statement either as part of the LSP or as part of a primary or secondary statement. For more information, see "Disabling Constrained-Path LSP Computation" on page 88.
4. Configure any other LSP properties.

Using explicit-path LSPs has the following drawbacks:

- More configuration effort is required.
- Configured path information cannot take into account dynamic network bandwidth reservation, so the LSPs tend to fail when resources become depleted.
- When an explicit-path LSP fails, you might need to manually repair it.

Because of these limitations, we recommend that you use explicit-path LSPs only in controlled situations, such as to enforce an optimized LSP placement strategy resulting from computations with an offline simulation software package.

Chapter 8

Point-to-Multipoint LSP Configuration Guidelines

A point-to-multipoint MPLS LSP is an RSVP LSP with multiple destinations. By taking advantage of the MPLS packet replication capability of the network, point-to-multipoint LSPs avoid unnecessary packet replication at the ingress router.

This chapter discusses the following topics:

- Configuring Primary and Branch LSPs on page 143
- Example: Configuring Point-to-Multipoint LSPs on page 145
- Configuring Link Protection for Point-to-Multipoint LSPs on page 146
- Configuring Graceful Restart for Point-to-Multipoint LSPs on page 146
- Configuring a Multicast RPF Check Policy for Point-to-Multipoint LSPs on page 147
- Configuring Ingress PE Router Redundancy for Point-to-Multipoint LSPs on page 148
- Binding Point-to-Point LSPs to PE Routers and Backup PE Router Groups on page 149
- Ensuring Compatibility with JUNOS 9.1 and Earlier Releases for P2MP LSPs on page 149

Configuring Primary and Branch LSPs

For more information about point-to-multipoint LSPs, see “Point-to-Multipoint LSPs” on page 47.

To configure a point-to-multipoint LSP, you need to configure the primary LSP from the ingress router and the branch LSPs that carry traffic to the egress routers:

- Configuring the Primary Point-to-Multipoint LSP on page 143
- Configuring a Branch LSP for the Point-to-Multipoint LSP on page 144

Configuring the Primary Point-to-Multipoint LSP

To configure point-to-multipoint LSPs, you begin by configuring the primary point-to-multipoint LSP, which carries traffic from the ingress router. The configuration of the primary point-to-multipoint LSP is similar to a signaled LSP. See “Configuring the Ingress Router for Signaled LSPs” on page 57 for more information. In addition

to the conventional LSP configuration, you need to specify a path name for the primary point-to-multipoint LSP by including the p2mp statement:

```
p2mp p2mp-lsp-name;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name*]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]

You can enable the optimization timer for point-to-multipoint LSPs. See "Optimizing Signaled LSPs" on page 96 for more information.

Configuring a Branch LSP for the Point-to-Multipoint LSP

The primary point-to-multipoint LSP sends traffic to two or more branch LSPs carrying traffic to each of the egress provider edge (PE) routers. In the configuration for each of these branch LSPs, the point-to-multipoint LSP path name you specify must be identical to the path name configured for the primary point-to-multipoint LSP. See "Configuring the Primary Point-to-Multipoint LSP" on page 143 for more information.

To associate a branch LSP with the primary point-to-multipoint LSP, specify the point-to-multipoint LSP name by including the p2mp statement:

```
p2mp p2mp-lsp-name;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name*]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]

NOTE: Any change in any of the branch LSPs of a point-to-multipoint LSP, either due to a user action or an automatic adjustment made by the router, causes the primary and branch LSPs to be resignaled. The new point-to-multipoint LSP is signaled first before the old path is taken down.

The following sections describe how you can configure the branch LSP to be dynamically signaled using CSPF, as a static path, or as a combination of dynamic and static paths:

- Configuring the Branch LSP as a Dynamic Path on page 144
- Configuring the Branch LSP as a Static Path on page 145

Configuring the Branch LSP as a Dynamic Path

By default, the branch LSP for a point-to-multipoint LSP is signaled dynamically using CSPF and requires no configuration.

When a point-to-multipoint LSP is changed, either by the addition or deletion of new destinations or by the recalculation of the path to existing destinations, certain nodes in the tree might receive data from more than one incoming interface. This can happen under the following conditions:

- Some of the branch LSPs to destinations are statically configured and might intersect with statically or dynamically calculated paths to other destinations.
- When a dynamically calculated path for a branch LSP results in a change of incoming interface for one of the nodes in the network, the older path is not immediately torn down after the new one has been signaled. This ensures that any data in transit relying on the older path can reach its destination. However, network traffic can potentially use either path to reach the destination.
- A faulty router at the ingress calculates the paths to two different branch destinations such that a different incoming interface is chosen for these branch LSPs on a router node common to these branch LSPs.

Configuring the Branch LSP as a Static Path

You can configure the branch LSP for a point-to-multipoint LSP as a static path. See "Configuring Static LSPs" on page 135 for more information.

Example: Configuring Point-to-Multipoint LSPs

The following example shows a configuration based on the topology shown in Figure 18 on page 48. There are four branch LSPs, each belonging to a single point-to-multipoint LSP called p2mp-lsp-sample.

```
[edit protocols mpls]
label-switched-path branch-LSP-to-PE2 {
    to 10.255.235.25;
    p2mp p2mp-lsp-sample;
    primary path1;
}
label-switched-path branch-LSP-to-PE2 {
    to 10.255.235.25;
    p2mp p2mp-lsp-sample;
    primary path2;
}
label-switched-path branch-LSP-to-PE3 {
    to 10.255.241.34;
    p2mp p2mp-lsp-sample;
    primary path3;
}
label-switched-path branch-LSP-to-CE4 {
    to 10.255.244.125;
    p2mp p2mp-lsp-sample;
    primary path4;
}
```

Configuring Link Protection for Point-to-Multipoint LSPs

Link protection helps to ensure that traffic going over a specific interface to a neighboring router can continue to reach this router if that interface fails. When link protection is configured for an interface and a point-to-multipoint LSP that traverses this interface, a bypass LSP is created that handles this traffic if the interface fails. The bypass LSP uses a different interface and path to reach the same destination.

To extend link protection to all of the paths used by a point-to-multipoint LSP, link protection must be configured on each router that each branch LSP traverses. If you enable link protection on a point-to-multipoint LSP, you must enable link protection on all of the branch LSPs.

The Internet draft draft-ietf-mpls-rsvp-te-p2mp-01.txt, *Extensions to RSVP-TE for Point to Multipoint TE LSPs*, describes link protection for point-to-multipoint LSPs.

To enable link protection on point-to-multipoint LSPs, complete the following steps:

1. Configure link protection on each branch LSP. To configure link protection, include the link-protection statement:

   ```
   link-protection;
   ```

   You can include this statement at the following hierarchy levels:

   - [edit protocols mpls label-switched-path *branch-lsp-name*]
   - [edit logical-systems *logical-system-name* protocols mpls label-switched-path *branch-lsp-name*]

2. Configure link protection for each RSVP interface on each router that the branch LSP traverses. For information on how to configure link protection on the RSVP interfaces, see "Configuring Link Protection on the Interfaces Used by the LSPs" on page 279.

For more information on how to configure link protection, see "Configuring Node Protection or Link Protection" on page 278.

Configuring Graceful Restart for Point-to-Multipoint LSPs

You can configure graceful restart on point-to-multipoint LSPs. Graceful restart allows a router undergoing a restart to inform its adjacent neighbors of its condition. The restarting router requests a grace period from the neighbor or peer, which can then cooperate with the restarting router. The restarting router can still forward MPLS traffic during the restart period; convergence in the network is not disrupted. The restart is not apparent to the rest of the network, and the restarting router is not removed from the network topology. RSVP graceful restart can be enabled on both transit routers and ingress routers.

To enable graceful restart on a router handling point-to-multipoint LSP traffic, include the graceful-restart statement:

```
graceful-restart;
```

You can include this statement at the following hierarchy levels:

- [edit routing-options]
- [edit logical-systems *logical-system-name* routing-options]

The graceful restart configuration for point-to-multipoint LSPs is identical to that of point-to-point LSPs. For more information on how to configure graceful restart, see "Configuring RSVP Graceful Restart" on page 286.

Configuring a Multicast RPF Check Policy for Point-to-Multipoint LSPs

You can control whether a reverse path forwarding (RPF) check is performed for a source and group entry before installing a route in the multicast forwarding cache. This makes it possible to use point-to-multipoint LSPs to distribute multicast traffic to PIM islands situated downstream from the egress routers of the point-to-multipoint LSPs.

By configuring the rpf-check-policy statement, you can disable RPF checks for a source and group pair. You would typically configure this statement on the egress routers of a point-to-multipoint LSP, because the interface receiving the multicast traffic on a point-to-multipoint LSP egress router might not always be the RPF interface.

You can also configure a routing policy to act upon a source and group pair. This policy behaves like an import policy, so if no policy term matches the input data, the default policy action is "acceptance." An accept policy action enables RPF checks. A reject policy action (applied to all source and group pairs that are not accepted) disables RPF checks for the pair.

To configure a multicast RPF check policy for a point-to-multipoint LSP, specify the RPF check policy using the rpf-check-policy statement:

```
rpf-check-policy policy;
```

You can include this statement at the following hierarchy levels:

- [edit routing-options multicast]
- [edit logical-systems *logical-system-name* routing-options multicast]

You also must configure a policy for the multicast RPF check. You configure policies at the [edit policy-options] hierarchy level. For more information, see the *JUNOS Policy Framework Configuration Guide*.

NOTE: When you configure the rpf-check-policy statement, the JUNOS software cannot perform RPF checks on incoming traffic and therefore cannot detect traffic arriving on the wrong interface. This might cause routing loops to form.

Example: Multicast RPF Check Policy for Point-to-Multipoint LSPs

The following example shows a policy configuration that ensures that an RPF check is not performed for sources with prefix 128.83/16 or longer that belong to groups having a prefix of 228/8 or longer:

```
[edit]
policy-options {
   policy-statement rpf-sg-policy {
      from {
         route-filter 228.0.0.0/8 orlonger;
         source-address-filter 128.83.0.0/16 orlonger;
      }
      then {
         reject;
      }
   }
}
```

Configuring Ingress PE Router Redundancy for Point-to-Multipoint LSPs

You can configure one or more PE routers as part of a backup PE router group to enable ingress PE router redundancy. You accomplish this by configuring the IP addresses of the backup PE routers (at least one backup PE router is required) and the local IP address used by the local PE router.

You must also configure a full mesh of point-to-point LSPs between the primary and backup PE routers. You also need to configure BFD on these LSPs. See “Configuring BFD for RSVP LSPs” on page 169 and “Configuring BFD for LDP LSPs” on page 350 for more information.

To configure ingress PE router redundancy for point-to-multipoint LSPs, include the backup-pe-group statement:

```
backup-pe-group pe-group-name {
   backups [addresses];
   local-address address;
}
```

For a list of hierarchy levels at which you can include these statements, see the statement summary sections for these statements.

After you configure the ingress PE router redundancy backup group, you must also apply the group to a static route on the PE router. This ensures that the static route is active (installed in the forwarding table) when the local PE router is the designated forwarder for the backup PE group. You can only associate a backup PE router group with a static route that also has the p2mp-lsp-next-hop statement configured. For more information, see “Configuring Static Unicast Routes for Point-to-Multipoint LSPs” on page 140.

Binding Point-to-Point LSPs to PE Routers and Backup PE Router Groups

Configuring an LSP with the associate-backup-pe-groups statement enables it to monitor the status of the PE router to which it is configured. You can configure multiple backup PE router groups using the same router's address. A failure of this LSP indicates to all of the backup PE router groups that the destination PE router is down. The associate-backup-pe-groups statement is not tied to a specific backup PE router group. It applies to all groups that are interested in the status of the LSP to that address.

To allow an LSP to monitor the status of the egress PE router, include the associate-backup-pe-groups statement:

```
associate-backup-pe-groups;
```

This statement can be configured at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name*]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]

If you configure the associate-backup-pe-groups statement, you must configure BFD for the point-to-point LSP. For information on how to configure BFD for an LSP, see "Configuring BFD for MPLS LSPs" on page 169 and "Configuring BFD for LDP LSPs" on page 350.

You also must configure a full mesh of point-to-point LSPs between the PE routers in the backup PE router group. A full mesh is required so that each PE router within the group can independently determine the status of the other PE routers, allowing each router to independently determine which PE router is currently the designated forwarder for the backup PE router group.

If you configure multiple LSPs with the associate-backup-pe-groups statement to the same destination PE router, the first LSP configured is used to monitor the forwarding state to that PE router. If you configure multiple LSPs to the same destination, make sure to configure similar parameters for the LSPs. With this configuration scenario, a failure notification might be triggered even though the remote PE router is still up.

Ensuring Compatibility with JUNOS 9.1 and Earlier Releases for P2MP LSPs

By default, Resv messages which include the S2L_SUB_LSP object are accepted. However, in a network which includes Juniper Networks devices running both JUNOS 9.2 and later releases and JUNOS 9.1 and earlier releases, it is necessary to configure the no-p2mp-sublsp statement on the JUNOS 9.2 and later devices to ensure that P2MP LSPs function properly. In JUNOS 9.1 and earlier releases, Resv messages which included the S2L_SUB_LSP object were rejected by default.

To ensure compatibility with JUNOS 9.1 and earlier releases, include the no-p2mp-sublsp statement:

```
no-p2mp-sublsp;
```

You can include this statement at the following hierarchy levels:

- [edit protocols rsvp]
- [edit logical-systems *logical-system-name* protocols rsvp]

Chapter 9

Miscellaneous MPLS Properties Configuration Guidelines

This chapter discusses the following topics:

- Configuring MPLS to Pop the Label on the Ultimate-Hop Router on page 151
- Configuring Traffic Engineering for LSPs on page 152
- Enabling Interarea Traffic Engineering on page 154
- Enabling Inter-AS Traffic Engineering for LSPs on page 155
- Configuring MPLS to Gather Statistics on page 158
- Controlling MPLS System Log Messages and SNMP Traps on page 159
- Configuring MPLS Firewall Filters and Policers on page 160
- Configuring MPLS Rewrite Rules on page 167
- Configuring BFD for MPLS LSPs on page 169
- Pinging LSPs on page 170
- Tracing MPLS and LSP Packets and Operations on page 172

Configuring MPLS to Pop the Label on the Ultimate-Hop Router

You can control the label value advertised on the egress router of a label-switched path (LSP). The default advertised label is label 3 (Implicit Null Label). If label 3 is advertised, the penultimate-hop router removes the label and sends the packet to the egress router. By enabling ultimate-hop popping, label 0 (IPv4 Explicit Null Label) is advertised. Ultimate-hop popping ensures that any packets traversing an MPLS network include a label.

To configure MPLS to pop the label on the ultimate-hop router, include the explicit-null statement:

```
explicit-null;
```

You can configure this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

NOTE: Juniper Networks routers queue packets based on the incoming label. Routers from other vendors might queue packets differently. Keep this in mind when working with networks containing routers from multiple vendors.

For more information about labels, see "Label Description" on page 25 and "Label Allocation" on page 25.

Configuring Traffic Engineering for LSPs

When you configure an LSP, a host route (a 32-bit mask) is installed in the ingress router toward the egress router; the address of the host route is the destination address of the LSP. Typically, you configure the BGP option (traffic-engineering bgp), allowing only BGP to use LSPs in its route calculations . The other traffic-engineering statement options, allow you to alter this behavior in the master instance. This functionality is not available for specific routing instances. Also, you can enable only one of the traffic-engineering statement options (bgp, bgp-igp, bgp-igp-both-ribs, or mpls-forwarding) at a time.

NOTE: Enabling or disabling any of the traffic-engineering statement options causes all the MPLS routes to be removed and then reinserted into the routing tables.

You can configure Open Shortest Path First (OSPF) and traffic engineering to advertise the LSP metric in summary link-state advertisements (LSAs) as described in the section "Advertising the LSP Metric in Summary LSAs" on page 154.

The following sections describe how to configure traffic engineering for LSPs:

- Using RSVP and LDP Routes for Traffic Forwarding on page 152
- Using RSVP and LDP Routes for Forwarding in VPNs on page 153
- Using RSVP and LDP Routes for Forwarding But Not Route Selection on page 153
- Advertising the LSP Metric in Summary LSAs on page 154

Using RSVP and LDP Routes for Traffic Forwarding

Configure the bgp-igp option of the traffic-engineering statement to cause BGP and the interior gateway protocols (IGPs) to use LSPs for forwarding traffic destined for egress routers. The bgp-igp option causes all inet.3 routes to be moved to the inet.0 routing table.

On the ingress router, include the traffic-engineering bgp-igp statement:

```
traffic-engineering bgp-igp;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]

- [edit logical-systems *logical-system-name* protocols mpls]

NOTE: The bgp-igp option of the traffic-engineering statement cannot be configured for VPNs. VPN routing instances require that routes be in the inet.3 routing table.

Using RSVP and LDP Routes for Forwarding in VPNs

VPNs rely on the routes in the inet.3 routing table to function properly. For VPNs, configure the bgp-igp-both-ribs option of the traffic-engineering statement to cause BGP and the IGPs to use LSPs for forwarding traffic destined for egress routers. The bgp-igp-both-ribs option installs the ingress routes in both the inet.0 routing table (for IPv4 unicast routes) and the inet.3 routing table (for MPLS path information).

On the ingress router, include the traffic-engineering bgp-igp-both-ribs statement:

```
traffic-engineering bgp-igp-both-ribs;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

Using RSVP and LDP Routes for Forwarding But Not Route Selection

If you configure the traffic-engineering bgp-igp statement or the traffic-engineering bgp-igp-both-ribs statement, high-priority RSVP and LDP routes can supersede IGP routes in the inet.0 routing table. IGP routes might no longer be redistributed since they are no longer the active routes.

When you configure the mpls-forwarding option at either the [edit logical-systems *logical-system-name* protocols mpls traffic-engineering] hierarchy level or the [edit protocols mpls traffic-engineering] hierarchy level, RSVP and LDP routes are used for forwarding but are excluded from route selection. These routes are added to both the inet.0 and inet.3 routing tables. The RSVP and LDP routes in the inet.0 routing table are given a low preference when the active route is selected. However, the RSVP and LDP routes in the inet.3 routing table are given a normal preference and are therefore used for selecting forwarding next hops.

When you activate the mpls-forwarding option, routes whose state is ForwardingOnly are preferred for forwarding even if their preference is lower than that of the currently active route. To examine the state of a route, execute a show route detail command.

To configure, include the traffic-engineering mpls-forwarding statement:

```
traffic-engineering mpls-forwarding;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]

- [edit logical-systems *logical-system-name* protocols mpls]

When you configure the mpls-forwarding option, IGP shortcut routes are copied to the inet.0 routing table only.

Advertising the LSP Metric in Summary LSAs

You can configure MPLS and OSPF to treat an LSP as a link. This configuration allows other routers in the network to use this LSP. To accomplish this goal, you need to configure MPLS and OSPF traffic engineering to advertise the LSP metric in summary LSAs.

For MPLS, include the traffic-engineering bgp-igp and label-switched-path statements:

```
traffic-engineering bgp-igp;
label-switched-path lsp-name {
    to address;
}
```

You can include these statements at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

For OSPF, include the lsp-metric-into-summary statement:

```
lsp-metric-into-summary;
```

You can include this statement at the following hierarchy levels:

- [edit protocols ospf traffic-engineering shortcuts]
- [edit logical-systems *logical-system-name* protocols ospf traffic-engineering shortcuts]

For more information about MPLS traffic engineering, see “Configuring Traffic Engineering for LSPs” on page 152. For more information about OSPF traffic engineering, see the *JUNOS Routing Protocols Configuration Guide*.

Enabling Interarea Traffic Engineering

The JUNOS software can signal a contiguous traffic-engineered LSP across multiple OSPF areas. The LSP signaling must be done using either nesting or contiguous signaling, as described in RFC 4206, *Label-Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)*. However, contiguous signaling support is limited to just basic signaling. Reoptimization is not supported with contiguous signaling.

The following describes some of the interarea traffic engineering features:

- Interarea traffic engineering can be enabled when the loose-hop area border routers (ABRs) are configured on the ingress router using CSPF for the Explicit

Route Object (ERO) calculation within an OSPF area. ERO expansion is completed on the ABRs.

- Interarea traffic engineering can be enabled when CSPF is enabled, but without ABRs specified in the LSP configuration on the ingress router (ABRs can be automatically designated).
- Differentiated Services (DiffServ) traffic engineering is supported as long as the class type mappings are uniform across multiple areas.

To enable interarea traffic engineering, include the **expand-loose-hop** statement in the configuration for each LSP transit router:

```
expand-loose-hop;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

Enabling Inter-AS Traffic Engineering for LSPs

Generally, traffic engineering is possible for LSPs that meet the following conditions:

- Both ends of the LSP are in the same OSPF area or at the same IS-IS level.
- The two ends of the LSP are in different OSPF areas within the same autonomous system (AS). LSPs that end in different IS-IS levels are not supported.
- The two ends of an explicit-path LSP are in different OSPF ASs and the autonomous system border routers (ASBRs) are configured statically as the loose hops supported on the explicit-path LSP. For more information about explicit-path LSPs, see “Static and Explicit-Path LSP Configuration Guidelines” on page 135.

Without statically defined ASBRs on LSPs, traffic engineering is not possible between one routing domain, or AS, and another. However, when the ASs are under the control of single service provider, it is possible in some cases to have traffic engineered LSPs span the ASs and dynamically discover the OSPF ASBRs linking them (IS-IS is not supported with this feature).

Inter-AS traffic engineered LSPs are possible as long as certain network requirements are met, none of the limiting conditions apply, and OSPF passive mode is configured with EBGP. Details are provided in the following sections:

- Inter-AS Traffic Engineering Requirements on page 155
- Inter-AS Traffic Engineering Limitations on page 156
- Configuring OSPF Passive TE Mode on page 157

Inter-AS Traffic Engineering Requirements

The proper establishment and functioning of inter-AS traffic engineered LSPs depend on the following network requirements, all of which must be met:

- All ASs are under control of a single service provider.
- OSPF is used as the routing protocol within each AS, and EBGP is used as the routing protocol between the ASs.
- ASBR information is available inside each AS.
- EBGP routing information is distributed by OSPF, and an IBGP full mesh is in place within each AS.
- Transit LSPs are *not* configured on the inter-AS links, but *are* configured between entry and exit point ASBRs on each AS.
- The EBGP link between ASBRs in different ASs is a direct link and must be configured as a passive traffic engineering link under OSPF. The remote link address itself, not the loopback or any other link address, is used as the remote node identifier for this passive link. For more information about OSPF passive traffic engineering mode configuration, see "Configuring OSPF Passive TE Mode" on page 157.

In addition, the address used for the remote node of the OSPF passive traffic engineering link must be the same as the address used for the EBGP link. For more information about OSPF and BGP in general, see the *JUNOS Routing Protocols Configuration Guide*.

Inter-AS Traffic Engineering Limitations

Only LSP hierarchical, or nested, signaling is supported for inter-AS traffic engineered LSPs. Only point-to-point LSPs are supported (there is no point-to-multipoint support).

In addition, the following limitations apply. Any one of these conditions is sufficient to render inter-AS traffic engineered LSPs impossible, even if the above requirements are met.

- The use of multihop BGP is not supported.
- The use of policers or topologies that prevent BGP routes from being known inside the AS is not supported.
- Multiple ASBRs on a LAN between EBGP peers are not supported. Only one ASBR on a LAN between EBGP peers is supported (others ASBRs can exist on the LAN, but cannot be advertised).
- Route reflectors or policies that hide ASBR information or prevent ASBR information from being distributed inside the ASs are not supported.
- Bidirectional LSPs are not supported (LSPs are unidirectional from the traffic engineering perspective).
- Topologies with both inter-AS and intra-AS paths to the same destination are not supported.

In addition, several features that are routine with all LSPs are not supported with inter-AS traffic engineering:

- Admin group link colors are not supported.
- Secondary standby is not supported.

- Reoptimization is not supported.
- Crankback on transit routers is not supported.
- Diverse path calculation is not supported.
- Graceful restart is not supported.

These lists of limitations or unsupported features with inter-AS traffic engineered LSPs are not exhaustive.

Configuring OSPF Passive TE Mode

Ordinarily, interior routing protocols such as OSPF are not run on links between ASs. However, for inter-AS traffic engineering to function properly, information about the inter-AS link, in particular, the address on the remote interface, must be made available inside the AS. This information is not normally included either in EBGP reachability messages or in OSPF routing advertisements.

To flood this link address information within the AS and make it available for traffic engineering calculations, you must configure OSPF passive mode for traffic engineering on each inter-AS interface. You must also supply the remote address for OSPF to distribute and include in the traffic engineering database (TED).

To configure OSPF passive mode for traffic engineering on an inter-AS interface, include the passive statement for the link at the [edit protocols ospf area *area-id* interface *interface-name*] hierarchy level:

```
passive {
    traffic-engineering {
        remote-node-id ip-address; /* IP address at far end of inter-AS link */
    }
}
```

OSPF must be properly configured on the router. The following example configures the inter-AS link so-1/1/0 to distribute traffic engineering information with OSPF within the AS. The local IP address on the link is 192.168.207.1 and the remote address is 192.168.207.2.

```
[edit protocols ospf area 0.0.0.0]
interface so-1/1/0 {
    unit 0 {
        passive {
            traffic-engineering {
                remote-node-id 192.168.207.2;
            }
        }
        family inet {
            address 192.168.207.1;
        }
    }
}
```

Configuring MPLS to Gather Statistics

You can configure MPLS so that it periodically gathers traffic statistics about all MPLS sessions, including transit sessions, by configuring the **statistics** statement. You must configure the **statistics** statement if you want to collect MPLS traffic statistics using Simple Network Management Protocol (SNMP) polling of MPLS Management Information Bases (MIBs).

To enable MPLS statistics collection, include the **statistics** statement:

```
statistics {
    auto-bandwidth;
    file filename <size size> <files number> <no-stamp> <replace>
    (world-readable | <no-world-readable>);
    interval seconds;
}
```

You can configure these statements at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

The default interval is 300 seconds.

The statistics are placed in a file, with one entry per LSP. During the specified interval, the following information is recorded in this file:

- The number of packets, number of bytes, packets per second, and bytes per second transmitted by each LSP.
- The percent of bandwidth transmitted over a given LSP in relation to the bandwidth percentage configured for that LSP. If no bandwidth is configured for an LSP, 0 percent is recorded in the percentage column.

NOTE: If you configure the **replace** option, an existing trace file is replaced if there is one. However, the change does not take effect after you commit the configuration. The change takes effect only after the routing protocol process restarts.

At the end of each periodic report, a summary shows the current time, total number of sessions, number of sessions read, number of sessions ignored, and read errors, if any. Ignored sessions are typically those not in the up state or those with a reserved (0 through 15) incoming label (typically the egress point of an LSP). The reason for a read error appears on the same line as the entry for the LSP on which the error occurred. Gathering statistics is an unreliable process; occasional read errors might affect their accuracy. The following is a sample of the information included in the output file:

```
lsp6                    0 pkt              0 Byte      0 pps        0 Bps    0
lsp5                    0 pkt              0 Byte      0 pps        0 Bps    0
lsp6.1              34845 pkt        2926980 Byte   1049 pps    88179 Bps  132
lsp5.1                  0 pkt              0 Byte      0 pps        0 Bps    0
```

```
lsp4                    0 pkt             0 Byte      0 pps        0 Bps    0
Dec  7 17:28:38 Total 6 sessions: 5 success, 0 fail, 1 ignored
```

Controlling MPLS System Log Messages and SNMP Traps

Whenever an LSP makes a transition from up to down, or down to up, and whenever an LSP switches from one active path to another, the ingress router generates a system log message and sends an SNMP trap. The following shows a sample system log message:

```
MPLS lsp sheep1 up on primary(any) Route  192.168.1.1 192.168.1.2 192.168.1.3
MPLS lsp sheep1 change on primary(any) Route  192.168.1.1 192.168.1.2 192.168.1.3
MPLS lsp sheep1 down on primary(any)
MPLS lsp sheep1 up on secondary(any) Route  192.168.1.1 192.168.1.2 192.168.1.3
MPLS lsp sheep1 change on secondary(any) to primary(any), Route  192.168.1.1
192.168.1.2 192.168.1.3
```

For information about the MPLS SNMP traps and the proprietary MPLS MIBs, see the *JUNOS Network Management Configuration Guide*.

To generate system log messages for LSPs, include the **syslog** option to the **log-updown** statement:

```
log-updown {
   syslog;
}
```

To generate SNMP traps for LSPs, include the **trap** option to the **log-updown** statement:

```
log-updown {
   trap;
}
```

To generate SNMP traps whenever an LSP path goes down, include the **trap-path-down** option to the **log-updown** statement:

```
log-updown {
   trap-path-down;
}
```

To generate SNMP traps whenever an LSP path comes up, include the **trap-path-up** option to the **log-updown** statement:

```
log-updown {
   trap-path-up;
}
```

To disable the generation of system log messages, include the **no-syslog** option to the **log-updown** statement:

```
log-updown {
   no-syslog;
}
```

To disable the generation of SNMP traps, include the no-trap statement:

```
no-trap {
   mpls-lsp-traps;
   rfc3812–traps;
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls log-updown]
- [edit logical-systems *logical-system-name* protocols mpls log-updown]

For scalability reasons, only the ingress router generates SNMP traps. By default, MPLS issues traps for all configured LSPs. If you have many LSPs, the number of traps can become quite large. To disable the generation of SNMP traps, configure the no-trap statement.

The no-trap statement also includes the following options which allow you to block certain categories of MPLS SNMP traps:

- mpls-lsp-traps—Blocks the MPLS LSP traps defined in the jnx-mpls.mib, but allows the rfc3812.mib traps.
- rfc-3812-traps—Blocks the traps defined in the rfc3812.mib, but allows the MPLS LSP traps defined in the jnx-mpls.mib.

Configuring MPLS Firewall Filters and Policers

You can configure an MPLS firewall filter to count packets based on the EXP bits for the top-level MPLS label in a packet. You can also configure policers for MPLS LSPs.

The following sections discuss MPLS firewall filters and policers:

- Configuring MPLS Firewall Filters on page 160
- Examples: Configuring MPLS Firewall Filters on page 161
- Configuring Policers for LSPs on page 162
- Example: Configuring an LSP Policer on page 163
- Configuring Automatic Policers on page 164
- Writing Different DSCP and EXP Values in MPLS-Tagged IP Packets on page 167

Configuring MPLS Firewall Filters

You can configure an MPLS firewall filter to count packets based on the experimental (EXP) bits for the top-level MPLS label in a packet. You can then apply this filter to a specific interface. You can also configure a policer for the MPLS filter to police (that is, rate-limit) the traffic on the interface to which the filter is attached. You cannot apply MPLS firewall filters to Ethernet (fxp0) or loopback (lo0) interfaces.

You can configure an MPLS firewall filter on the M-series and the T-series platforms.

You can configure the following match criteria attributes for MPLS filters at the [edit firewall family mpls filter *filter-name* term *term-name* from] hierarchy level:

- exp
- exp-except

These attributes can accept EXP bits in the range 0 through 7. You can configure the following choices:

- A single EXP bit—for example, exp 3;
- Several EXP bits—for example, exp 0, 4;
- A range of EXP bits—for example, exp [0-5];

If you do not specify a match criterion (that is, you do not configure the from statement and use only the then statement with the count action keyword), all the MPLS packets passing through the interface on which the filter is applied will be counted.

You also can configure any of the following action keywords at the [edit firewall family mpls filter *filter-name* term *term-name* then] hierarchy level:

- count
- accept
- discard
- next
- policer

For more information about how to configure firewall filters, see the *JUNOS Policy Framework Configuration Guide*. For more information about how to configure interfaces, see the *JUNOS Network Interfaces Configuration Guide* and the *JUNOS Services Interfaces Configuration Guide*.

Examples: Configuring MPLS Firewall Filters

The following examples illustrate how you might configure an MPLS firewall filter and then apply the filter to an interface. This filter is configured to count MPLS packets with EXP bits set to either 0 or 4.

The following shows a configuration for an MPLS firewall filter:

```
[edit firewall]
family mpls {
   filter expf {
      term expt0 {
         from {
            exp 0,4;
         }
         then {
            count counter0;
            accept;
```

```
        }
      }
    }
  }
```

The following shows how to apply the MPLS firewall filter to an interface:

```
[edit interfaces]
so-0/0/0 {
    mtu 4474;
    encapsulation ppp;
    sonet-options {
        fcs 32;
    }
    unit 0 {
        point-to-point;
        family mpls {
            filter {
                input expf;
                output expf;
            }
        }
    }
}
```

The MPLS firewall filter is applied to the input and output of an interface (see the input and output statements in the preceding example).

Configuring Policers for LSPs

MPLS LSP policing allows you to control the amount of traffic forwarded through a particular LSP. Policing helps to ensure that the amount of traffic forwarded through an LSP never exceeds the requested bandwidth allocation. LSP policing is supported on regular LSPs, LSPs configured with DiffServ-aware traffic engineering, and multiclass LSPs. You can configure multiple policers for each multiclass LSP. For regular LSPs, each LSP policer is applied to all of the traffic traversing the LSP. The policer's bandwidth limitations become effective as soon as the total sum of traffic traversing the LSP exceeds the configured limit.

You configure the multiclass LSP and DiffServ-aware traffic engineering LSP policers in a filter. The filter can be configured to distinguish between the different class types and apply the relevant policer to each class type. The policers distinguish between class types based on the EXP bits.

You configure LSP policers under the family any filter. The family any filter is used because the policer is applied to traffic entering the LSP. This traffic might be from different families: IPv6, MPLS, and so on. You do not need to know what sort of traffic is entering the LSP, as long as the match conditions apply to all types of traffic.

You can configure only those match conditions that apply across all types of traffic. The following are the supported match conditions for LSP policers:

- forwarding-class
- packet-length

- interface
- interface-set

To enable a policer on an LSP, first you need to configure a policing filter and then include it in the LSP configuration. For information on how to configure policers, see the *JUNOS Policy Framework Configuration Guide*.

To configure a policer for an LSP, specify a filter by including the filter option to the policing statement:

```
policing {
   filter filter-name;
}
```

You can include the policing statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name*]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]

LSP Policer Limitations

When configuring MPLS LSP policers, be aware of the following limitations:

- LSP policers are supported for packet LSPs only.
- LSP policers are supported for unicast next hops only. Multicast next hops are not supported.
- LSP policers are not supported on aggregated interfaces.
- The LSP policer runs before any output filters.
- Traffic sourced from the Routing Engine (for example, ping traffic) does not take the same forwarding path as transit traffic. This type of traffic cannot be policed.
- LSP policers work on all T-series routing platforms and on M-series routers that have the Internet Processor II application-specific integrated circuit (ASIC).

Example: Configuring an LSP Policer

The following example shows how you can configure a policing filter for an LSP:

```
[edit firewall]
policer police-ct1 {
   if-exceeding {
      bandwidth-limit 50m;
      burst-size-limit 1500;
   }
   then {
      discard;
   }
}
policer police-ct0 {
   if-exceeding {
```

```
        bandwidth-limit 200m;
        burst-size-limit 1500;
    }
    then {
        discard;
    }
}
family any {
    filter bar {
        term discard-ct0 {
            then {
                policer police-ct0;
                accept;
            }
        }
    }
    term discard-ct1 {
        then {
            policer police-ct1;
            accept;
        }
    }
}
```

Configuring Automatic Policers

Automatic policing of LSPs allows you to provide strict service guarantees for network traffic. Such guarantees are especially useful in the context of Differentiated Services for traffic engineered LSPs, providing better emulation for ATM wires over an MPLS network. For more information about Differentiated Services for LSPs, see "DiffServ-Aware Traffic Engineering Configuration Guidelines" on page 113.

Differentiated Services for traffic engineered LSPs allow you to provide differential treatment to MPLS traffic based on the EXP bits. To ensure these traffic guarantees, it is insufficient to simply mark the traffic appropriately. If traffic follows a congested path, the requirements might not be met.

LSPs are guaranteed to be established along paths where enough resources are available to meet the requirements. However, even if the LSPs are established along such paths and are marked properly, these requirements cannot be guaranteed unless you ensure that no more traffic is sent to an LSP than there is bandwidth available.

It is possible to police LSP traffic by manually configuring an appropriate filter and applying it to the LSP in the configuration. However, for large deployments it is cumbersome to configure thousands of different filters. Configuration groups cannot solve this problem either, since different LSPs might have different bandwidth requirements, requiring different filters. To police traffic for numerous LSPs, it is best to configure automatic policers.

When you configure automatic policers for LSPs, a policer is applied to all of the LSPs configured on the router. However, you can disable automatic policing on specific LSPs.

NOTE: You cannot configure automatic policing for LSPs carrying CCC traffic.

The following sections describe how to configure automatic policers for LSPs:

- Configuring Automatic Policers for LSPs on page 165
- Configuring Automatic Policers for DiffServ-Traffic Engineering LSPs on page 165
- Disabling Automatic Policing on an LSP on page 166
- Example: Configuring Automatic Policers for LSPs on page 166

Configuring Automatic Policers for LSPs

To configure automatic policers for standard LSPs (neither DiffServ-aware traffic engineered LSPs nor multiclass LSPs), include the auto-policing statement with either the class all *policer-action* option or the class ct0 *policer-action* option:

```
auto-policing {
   class all policer-action;
   class ct0 policer-action;
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

You can configure the following policer actions for automatic policers:

- drop—Drop all packets.
- loss-priority-high—Set the packet loss priority (PLP) to high.
- loss-priority-low—Set the PLP to low.

These policer actions are applicable to all types of LSPs. The default policer action is to do nothing.

NOTE: You cannot configure automatic policers for LSPs that traverse aggregated interfaces or Multilink Point-to-Point Protocol (MLPPP) interfaces.

Configuring Automatic Policers for DiffServ-Traffic Engineering LSPs

To configure automatic policers for DiffServ-traffic engineering LSPs and for multiclass LSPs, include the auto-policing statement with either the class all *policer-action* option or the class ct*number policer-action* option. You can configure a different policer action for each class type.

To configure automatic policers for DiffServ-aware LSPs, include the auto-policing statement:

```
auto-policing {
   class all policer-action;
   class ctnumber policer-action;
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

For a list of the actions available for automatic policers, see "Configuring Automatic Policers for LSPs" on page 165. The default policer action is to do nothing.

NOTE: You cannot configure automatic policers for LSPs that traverse aggregated interfaces or MLPPP interfaces.

Disabling Automatic Policing on an LSP

When you enable automatic policing, all of the LSPs on the router or logical system are affected. To disable automatic policing on a specific LSP on a router where you have enabled automatic policing, include the policing statement with the no-automatic-policing option:

```
policing no-automatic-policing;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name*]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]

Example: Configuring Automatic Policers for LSPs

This example shows how you could configure automatic policing for LSPs. It shows automatic policing configured for a multiclass LSP with class types ct0, ct1, ct2, and ct3 configured.

```
[edit protocols mpls]
diffserv-te {
   bandwidth-model extended-mam;
}
auto-policing {
   class ct1 loss-priority-low;
   class ct0 loss-priority-high;
   class ct2 drop;
   class ct3 loss-priority-low;
}
traffic-engineering bgp-igp;
label-switched-path sample-lsp {
   to 3.3.3.3;
   bandwidth {
```

```
        ct0 11;
        ct1 1;
        ct2 1;
        ct3 1;
    }
}
interface fxp0.0 {
    disable;
}
interface t1-0/5/3.0;
interface t1-0/5/4.0;
```

Writing Different DSCP and EXP Values in MPLS-Tagged IP Packets

You can selectively set the DiffServ code point (DSCP) field of MPLS-tagged IPv4 and IPv6 packets to 0 without affecting output queue assignment, and continue to set the MPLS EXP field according to the configured rewrite table, which is based on forwarding classes. You can accomplish this by configuring a firewall filter for the MPLS-tagged packets.

For instructions on how to write different DSCP and EXP values in MPLS-tagged IP packets, see the *JUNOS Class of Service Configuration Guide*. For instructions on how to configure firewall filters, see the *JUNOS Policy Framework Configuration Guide*.

Configuring MPLS Rewrite Rules

You can apply a number of different rewrite rules to MPLS packets.

For more information about how to configure statements at the [edit class-of-service] hierarchy level, see the *JUNOS Class of Service Configuration Guide*.

The following sections describe how you can apply rewrite rules to MPLS packets:

- Rewriting the EXP Bits of All Three Labels of an Outgoing Packet on page 167
- Rewriting MPLS and IPv4 Packet Headers on page 168

Rewriting the EXP Bits of All Three Labels of an Outgoing Packet

In interprovider, carrier-of-carrier, and complex traffic engineering scenarios, it is sometimes necessary to push three labels on the next hop, using a swap-push-push or triple-push operation.

By default, on M-series routing platforms except the M320, the top MPLS EXP label of an outgoing packet is not rewritten when you configure swap-push-push and triple-push operations. You can rewrite the EXP bits of all three labels of an outgoing packet, thereby maintaining the class of service (CoS) of an incoming MPLS or non-MPLS packet.

To push three labels on incoming MPLS packets, include the exp-swap-push-push default statement at the [edit class-of-service interfaces *interface-name* unit *logical-unit-number* rewrite-rules] hierarchy level:

```
[edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules]
exp-swap-push-push default;
```

To push three labels on incoming non-MPLS packets, include the **exp-push-push-push default** statement at the **[edit class-of-service interfaces *interface-name* unit *logical-unit-number* rewrite-rules]** hierarchy level:

```
[edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules]
exp-push-push-push default;
```

For more information about how to configure statements at the **[edit class-of-service]** hierarchy level, see the *JUNOS Class of Service Configuration Guide*.

Rewriting MPLS and IPv4 Packet Headers

You can apply a rewrite rule to MPLS and IPv4 packet headers simultaneously. This allows you to initialize MPLS EXP and IP precedence bits at LSP ingress. You can configure different rewrite rules depending on whether the traffic is VPN or non-VPN.

To rewrite MPLS and IPv4 packet headers, include the **protocol** statement at the **[edit class-of-service interfaces *interface-name* unit *logical-unit-number* rewrite-rules exp *rewrite-rule-name*]** hierarchy level:

```
[edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules
    exp rewrite-rule-name]
protocol types;
```

Use the **protocol** statement to specify the types of MPLS packets and packet headers to which to apply the rewrite rule. The MPLS packet can be a standard MPLS packet or an MPLS packet with an IPv4 payload. Specify the type of MPLS packet by using the following options:

- **mpls-any**—Applies the rewrite rule to MPLS packets and writes the code point value to MPLS headers.
- **mpls-inet-both**—Applies the rewrite rule to VPN MPLS packets with IPv4 payloads. Writes the code point value to the MPLS and IPv4 headers in T-series and M320 routers. On M-series routing platforms, except the M320, the **mpls-inet-both** option causes all ingress MPLS LSP packets with IPv4 payloads to be initialized with 000 code points for IP precedence and MPLS EXP values.
- **mpls-inet-both-non-vpn**—Applies the rewrite rule to any non-VPN MPLS packets with IPv4 payloads. Writes the code point value to the MPLS and IPv4 headers in T-series and M320 routers. On M-series routing platforms, except the M320, the **mpls-inet-both-non-vpn** option causes all ingress MPLS LSP packets with IPv4 payloads to be initialized with 000 code points for IP precedence and MPLS EXP values.

For a detailed example on how to configure rewrite rules for MPLS and IPv4 packets and for more information about how to configure class of service, see the *JUNOS Class of Service Configuration Guide*.

Configuring BFD for MPLS LSPs

You can configure Bidirectional Forwarding Detection (BFD) on MPLS IPv4 LSPs as outlined in the Internet draft draft-ietf-bfd-mpls-02.txt, *BFD for MPLS LSPs*. You can configure BFD for LSPs using either LDP or RSVP as the signaling protocol. BFD is used as a periodic Operation, Administration, and Maintenance (OAM) feature for LSPs to detect LSP data plane faults.

NOTE: You cannot enable BFD on multiple MPLS LSP paths. For example, if an LSP has a primary path and a secondary path, you can only enable OAM on the primary path.

You can also use the LSP ping commands to detect LSP data plane faults. However, there are a couple of benefits to using BFD. It requires less computer processing than LSP ping. It can also quickly detect faults in large numbers of LSPs (LSP ping commands must be issued manually for each LSP).

Although you can use BFD to detect LSP data plane faults, it does not have the equivalent functionality of LSP ping. Specifically, you cannot use it to check the control plane against the data plane. An LSP ping echo request can be associated with a forwarding equivalence class (FEC).

An LSP ping echo request can be associated with an FEC. This makes it possible to verify the control plane against the data plane at the egress LSR.

To configure BFD for MPLS LSPs, complete the procedures in the following section:

- Configuring BFD for RSVP LSPs on page 169

Configuring BFD for RSVP LSPs

BFD for RSVP supports unicast IPv4 LSPs. When BFD is configured for an RSVP LSP on the ingress router, it is enabled on the primary path and on all standby secondary paths for that LSP. You can enable BFD for all LSPs on a router or for specific LSPs. If you configure BFD for a specific LSP, whatever values configured globally for BFD are overridden. The BFD sessions originate only at the ingress router and terminate at the egress router.

An error is logged whenever a BFD session for a path fails. The following shows how BFD for RSVP LSP log messages might appear:

```
RPD_MPLS_PATH_BFD_UP: MPLS BFD session for path path1 up on LSP R0_to_R3
RPD_MPLS_PATH_BFD_DOWN: MPLS BFD session for path path1 down on LSP R0_to_R3
```

You can configure BFD for all of the RSVP LSPs on the router, a specific LSP, or the primary path of a specific LSP. To configure BFD for RSVP LSPs, include the oam and bfd-liveness-detection statements.

```
oam {
   bfd-liveness-detection {
      failure-action teardown;
```

```
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        minimum-transmit-interval milliseconds;
        multiplier detection-time-multiplier;
    }
}
```

You can configure this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit protocols mpls label-switched-path *lsp-name*]
- [edit protocols mpls label-switched-path *lsp-name* primary *path-name*]

The bfd-liveness-detection statement includes the following options:

- failure-action teardown—When the BFD session for an RSVP LSP goes down, the LSP is torn down and resignaled. Traffic can be switched to a standby LSP if one is configured and available. Any actions performed are logged.
- minimum-interval—Specifies the minimum transmit and receive interval.
- minimum-receive-interval—Specifies the minimum receive interval. The range is from 1 through 255,000 milliseconds.
- minimum-transmit-interval—Specifies the minimum transmit interval. The range is from 1 through 255,000 milliseconds.
- multiplier—Specifies the detection time multiplier. The range is from 1 through 255.

NOTE: To avoid triggering false negatives, configure a BFD fault detection time that is longer than the fast reroute time.

Pinging LSPs

The following sections describe the various functions of the ping mpls command:

- Pinging an MPLS LSP on page 171
- Pinging a P2MP LSP on page 171
- Pinging an MPLS LSP Endpoint on page 171
- Pinging a CCC LSP on page 171
- Pinging a Layer 3 VPN on page 172
- LSP Ping and Traceroute Based on RFC 4379 on page 172

NOTE: The ping mpls command is not supported within routing instances.

Pinging an MPLS LSP

You can ping a specific LSP. Echo requests are sent over the LSP as MPLS packets. The payload is a User Datagram Protocol (UDP) packet forwarded to an address in the 127/8 range (127.0.0.1 by default, this address is configurable) and port 3503. The label and interface information for building and sending this information as an MPLS packet is the same as for standard LSP traffic.

When the echo request arrives at the egress node, the receiver checks the contents of the packet and sends a reply containing the correct return value, by using UDP. The router sending the echo request waits to receive an echo reply after a timeout of 2 seconds (you cannot configure this value).

You must configure MPLS at the [edit protocols mpls] hierarchy level on the remote router to be able to ping an LSP terminating there. You must configure MPLS even if you intend to ping only LDP forwarding equivalence classes (FECs).

To ping an MPLS LSP use the ping mpls <count *count*> <ldp <fec>> <rsvp <exp *forwarding-class*> <*lsp-name*>> command. To ping a secondary MPLS LSP, use the ping mpls <count *count*> <rsvp <*lsp-name*>> standby *path-name* command. For a detailed description of this command, see the *JUNOS Routing Protocols and Policies Command Reference*.

Pinging a P2MP LSP

To ping a point-to-multipoint LSP, use the ping mpls rsvp *lsp-name* multipoint or ping mpls rsvp egress *address* commands. The ping mpls rsvp *lsp-name* multipoint command returns a list of all of the egress router identifiers and the current status of the point-to-multipoint LSP egress routers. The ping mpls rsvp *lsp-name* multipoint egress *address* command returns the current status of the specified egress router.

Pinging an MPLS LSP Endpoint

To determine whether an LSP between two provider edge (PE) routers is up and running, you can ping the endpoint address of the LSP. To ping an MPLS LSP endpoint, use the ping mpls lsp-end-point *address* command. This command tells you what type of LSP (RSVP or LDP) terminates at the address specified and whether that LSP is up or down.

For a detailed description of this command, see the *JUNOS Routing Protocols and Policies Command Reference*.

Pinging a CCC LSP

You can ping a specific CCC LSP. The CCC LSP ping command is identical to the one used for MPLS LSPs. The command you use is ping mpls <count *count*> <rsvp <*lsp-name*>>. You can also ping a secondary standby CCC LSP by using the ping mpls <count *count*> <rsvp <*lsp-name*>> standby *path-name* command.

For a detailed description of this command, see the *JUNOS Routing Protocols and Policies Command Reference*.

Pinging a Layer 3 VPN

You can use a similar command, ping mpls l3vpn *vpn-name* prefix *prefix* <count *count*>, to ping a Layer 3 VPN. For more information about this command, see the *JUNOS VPNs Configuration Guide* and the *JUNOS Routing Protocols and Policies Command Reference*.

LSP Ping and Traceroute Based on RFC 4379

The JUNOS software now partially supports LSP ping and traceroute commands based on RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*. However, the JUNOS software only supports this functionality on LSP transit routers. If a ping or traceroute command is issued from a router that fully supports RFC 4379, it can propagate correctly on routing platforms running the JUNOS software.

LSP ping and traceroute commands based on RFC 4379 attempt to trace the path taken by an LSP by relying on MPLS TTL expiration. An LSP can take multiple paths from ingress to egress. This occurs in particular with Equal Cost Multipath (ECMP). The LSP traceroute command can trace all possible paths to an LSP egress node.

Tracing MPLS and LSP Packets and Operations

To trace MPLS and LSP packets and operations, include the traceoptions statement:

```
traceoptions {
    file filename <replace> <size size> <files number> <no-stamp> <world-readable |
        no-world-readable>;
    flag flag;
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

You can specify the following MPLS-specific flags in the MPLS traceoptions statement:

- all—Trace all operations.
- connection—Trace all circuit cross-connect (CCC) activity.
- connection-detail—Trace detailed CCC activity.
- cspf—Trace CSPF computations.
- cspf-link—Trace links visited during CSPF computations.
- cspf-node—Trace nodes visited during CSPF computations.
- error—Trace MPLS error conditions.
- graceful-restart—Trace MPLS graceful restart events.
- lsping—Trace LSP ping packets and return codes.
- state—Trace all LSP state transitions.

When you configure trace options to track an MPLS LSP using the cspf option, the CSPF log displays information about the MPLS LSP using the term “generalized MPLS” (GMPLS). For example, a message in the CSPF log might state that the “link passes GMPLS constraints”. Generalized MPLS (GMPLS) is a superset of MPLS, so this message is normal and does not affect proper MPLS LSP operation.

For general information about tracing and global tracing options, see the *JUNOS Routing Protocols Configuration Guide*.

Chapter 10

Summary of MPLS Configuration Statements

This chapter shows the complete Multiprotocol Label Switching (MPLS) configuration statements. The statements are organized alphabetically.

adaptive

Syntax adaptive;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*],
[edit protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description During reroute, do not double-count bandwidth on links shared by the old and new paths. Including this statement causes the Resource Reservation Protocol (RSVP) to use shared explicit (SE) reservation styles and assists in smooth transition during rerouting.

Default The configured object is disabled.

Usage Guidelines See "Configuring Adaptive LSPs" on page 94.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

adjust-interval

Syntax adjust-interval *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* auto-bandwidth],
[edit protocols mpls label-switched-path *lsp-name* auto-bandwidth]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the bandwidth reallocation interval.

Options *seconds*—Bandwidth reallocation interval, in seconds.
Range: 300 through 4,294,967,295 seconds
Default: 86,400 seconds

Usage Guidelines See "Configuring the Automatic Bandwidth Allocation Interval" on page 83.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

adjust-threshold

Syntax adjust-threshold *percent*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* auto-bandwidth],
[edit protocols mpls label-switched-path *lsp-name* auto-bandwidth]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify how sensitive the automatic bandwidth adjustment for a label-switched path (LSP) is to changes in bandwidth utilization.

Options *percent*—Bandwidth demand for the current bandwidth adjustment interval is determined and compared to the LSP's current bandwidth allocation. If the percentage difference in bandwidth is greater than or equal to the specified adjust-threshold percentage, the LSP's bandwidth is adjusted to the current bandwidth demand.

Usage Guidelines See "Configuring Automatic Bandwidth Adjustment Threshold" on page 84.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

adjust-threshold-overflow-limit

Syntax adjust-threshold-overflow-limit *number*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* auto-bandwidth],
[edit protocols mpls label-switched-path *lsp-name* auto-bandwidth]

Release Information Statement introduced in JUNOS Release 7.5.

Description Specify the number of consecutive bandwidth overflow samples before triggering a bandwidth adjustment.

Options *number*—Number of consecutive bandwidth overflow samples.
Range: 1 through 65,535
Default: This feature is disabled by default.

Usage Guidelines See "Configuring a Limit on Bandwidth Overflow Samples" on page 85.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

admin-down

Syntax admin-down;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced in JUNOS Release 8.2.

Description Set the A-bit in the Admin Status object. When set, this bit indicates the administrative down status for an LSP. This feature is used specifically by non-packet GMPLS LSPs. It does not affect control path setup or data forwarding for packet LSPs.

Usage Guidelines See "Allowing Non-Packet GMPLS LSPs to Establish Paths Through a JUNOS-based Router" on page 455.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

admin-group

See the following sections:

- admin-group (for Interfaces) on page 178
- admin-group (for LSPs) on page 179

admin-group (for Interfaces)

Syntax admin-group [*group-names*];

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls interface *interface-name*], [edit protocols mpls interface *interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Define administrative groups for an interface.

Options *group-names*—One or more names of groups defined with the admin-groups statement at the [edit protocols mpls] hierarchy level.

Usage Guidelines See "Configuring Administrative Groups" on page 89.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics admin-groups

admin-group (for LSPs)

Syntax

```
admin-group {
    exclude [ group-names ];
    include-all [ group-names ];
    include-any [ group-names ];
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols mpls],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*],
[edit protocols mpls],
[edit protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Define the administrative groups to include or exclude for an LSP and for a path's primary and secondary paths.

Options The statements are explained separately.

Usage Guidelines See "Configuring Administrative Groups" on page 89.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

admin-groups

Syntax
```
admin-groups {
   group-name group-value;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced before JUNOS Release 7.4.

Description Configure administrative groups to implement link coloring of resource classes.

Options *group-name*—Name of the group. You can assign up to 32 names. The names and their corresponding values must be identical across all routers within a single domain.

group-value—Value assigned to the group. The names and their corresponding values must be identical across all routers within a single domain.
Range: 0 through 31

Usage Guidelines See "Configuring Administrative Groups" on page 89.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics admin-group

advertisement-hold-time

Syntax advertisement-hold-time *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced before JUNOS Release 7.4.

Description Do not advertise when the LSP goes from up to down, for a certain period of time known as hold time.

Options *seconds*—Hold time, in seconds.
Range: 0 through 65,535 seconds
Default: 5 seconds

Usage Guidelines See "Configuring LSP Hold Time" on page 100.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

allow-fragmentation

Syntax allow-fragmentation;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls path-mtu],
[edit protocols mpls path-mtu]

Release Information Statement introduced before JUNOS Release 7.4.

Description Allow IP packets to be fragmented before they are encapsulated in MPLS.

Usage Guidelines See "Enabling Packet Fragmentation" on page 291.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

associate-backup-pe-groups

Syntax associate-backup-pe-groups;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced in JUNOS Release 9.0.

Description Enable an LSP to monitor the status of its destination PE router. You can configure multiple backup PE router groups using the same router's address. Backup PE router groups provide ingress PE router redundancy when point-to-multipoint (P2MP) LSPs are configured for multicast distribution. A failure of this LSP indicates to all of the backup PE router groups that the destination PE router is down. This statement is not tied to a specific backup PE router group. It applies to all groups that are interested in the status of the LSP to the destination address.

Usage Guidelines See "Binding Point-to-Point LSPs to PE Routers and Backup PE Router Groups" on page 149.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

auto-bandwidth

Syntax

```
auto-bandwidth {
   adjust-interval seconds;
   adjust-threshold percent;
   adjust-threshold-overflow-limit number;
   maximum-bandwidth bps;
   minimum-bandwidth bps;
   monitor-bandwidth;
}
```

Hierarchy Level [edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Allow an MPLS tunnel to automatically adjust its bandwidth allocation based on the volume of traffic flowing through the tunnel.

Options The statements are explained separately.

Usage Guidelines See “Configuring Automatic Bandwidth Allocation” on page 81 and “Configuring Automatic Bandwidth Allocation on an LSP” on page 82.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

auto-policing

Syntax

```
auto-policing {
    class all (drop | loss-priority-high | loss-priority-low);
    class ctnumber (drop | loss-priority-high | loss-priority-low);
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable the automatic policing of all the MPLS LSPs on the router or logical system.

Options class all—Apply the same policer action to all the class types (ct0, ct1, ct2, and ct3).

class ct*number*—Specific class type (ct0, ct1, ct2, or ct3) to which to apply a policer action.

Policer actions—You can specify the following policer actions:
Default: no action

- drop—Drop all packets.
- loss-priority-high—Set the packet loss priority (PLP) to high.
- loss-priority-low—Set the PLP to low.

Usage Guidelines See "Configuring Automatic Policers" on page 164.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics policing

backup-pe-group

Syntax

```
backup-pe-group pe-group-name {
    backups [ addresses ];
    local-address address;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* routing-options multicast],
[edit logical-systems *logical-system-name* routing-options multicast],
[edit routing-instances *routing-instance-name* routing-options multicast],
[edit routing-options multicast]

Release Information

Statement introduced in JUNOS Release 9.0.

Description

Configure a backup provider edge (PE) group for ingress PE router redundancy when point-to-multipoint (P2MP) label-switched paths (LSPs) are used for multicast distribution.

Options

backups *addresses*—Specify the address of backup PE routers for ingress PE redundancy when point-to-multipoint LSPs are used for multicast distribution.

local-address—Specify the address of the local PE router for ingress PE redundancy when point-to-multipoint LSPs are used for multicast distribution.

pe-group-name—Specify the name for the group of PE routers that provide ingress PE router redundancy for P2MP LSPs.

Usage Guidelines

See "Configuring Ingress PE Router Redundancy for Point-to-Multipoint LSPs" on page 148.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

bandwidth

Syntax

```
bandwidth bps {
    ct0 bps;
    ct1 bps;
    ct2 bps;
    ct3 bps;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols mpls],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* fast-reroute],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*],
[edit protocols mpls],
[edit protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls label-switched-path *lsp-name* fast-reroute],
[edit protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*]

Release Information

Statement introduced before JUNOS Release 7.4.

Description

When configuring an LSP, specify the traffic rate associated with the LSP.

When configuring fast reroute, allocate bandwidth for the reroute path. By default, no bandwidth is reserved for the rerouted path. The fast reroute bandwidth does not need to be identical to that allocated for the LSP itself.

When configuring a multiclass LSP, use the ct*number bandwidth* statements to specify the bandwidth to be allocated for each class type.

Options

bps—Bandwidth, in bits per second. You can specify this as an integer value. You can also use the abbreviations k (for a thousand), m (for a million), or g (for a billion).
Range: Any positive integer
Default: 0 (no bandwidth is reserved)

ct*number bps*—Bandwidth for the specified class type, in bits per second. You can specify this as an integer value. If you do so, count your zeros carefully, or you can use the abbreviations k (for a thousand), m (for a million), or g (for a billion [also called a thousand million]).
Range: Any positive integer
Default: 0 (no bandwidth is reserved)

Usage Guidelines

See "Configuring Fast Reroute" on page 71, "Configuring the Path Bandwidth" on page 98, "Configuring a Traffic Engineered LSP" on page 129, and "Configuring a Multiclass LSP" on page 132.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

bandwidth-model

Syntax

```
bandwidth-model {
    extended-mam;
    mam;
    rdm;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls diffserv-te],
[edit protocols mpls diffserv-te]

Release Information Statement introduced before JUNOS Release 7.4.

Description Configure the bandwidth model for differentiated services. Note that you cannot configure both bandwidth models at the same time.

Options

extended-mam—The extended maximum allocation model (MAM) is a bandwidth model based on MAM.

mam—The MAM is defined in RFC 4125, *Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*.

rdm—The Russian dolls bandwidth allocation model (RDM) is defined in RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*. RDM makes efficient use of bandwidth by allowing the class types to share bandwidth.

Usage Guidelines See “Configuring the Bandwidth Model” on page 119.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

bandwidth-percent

Syntax bandwidth-percent *percentage*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* fast-reroute],
[edit protocols mpls label-switched-path *lsp-name* fast-reroute]

Release Information Statement introduced before JUNOS Release 7.4.

Description Configure the percentage of bandwidth to reserve for the detour path in case the primary path for a traffic engineered LSP or a multiclass LSP fails. The percentage configured indicates the percentage of the protected path's bandwidth that is reserved for the detour path.

Options *percent*—The percentage of the protected path's bandwidth that is reserved for the detour path.

Usage Guidelines See "Configuring Fast Reroute" on page 71, "Configuring Fast Reroute for Traffic Engineered LSPs" on page 130 and "Configuring Fast Reroute for Multiclass LSPs" on page 133.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

bfd-liveness-detection

Syntax

```
bfd-liveness-detection {
    failure-action teardown;
    minimum-interval milliseconds;
    minimum-receive-interval milliseconds;
    minimum-transmit-interval milliseconds;
    multiplier detection-time-multiplier;
}
```

Hierarchy Level [edit protocols mpls label-switched-path *lsp-name* oam],
[edit protocols mpls oam]

Release Information Statement introduced in JUNOS Release 7.6. The failure-action statement option was added in JUNOS Release 8.5.

Description Enable Bidirectional Forwarding Detection (BFD) for all of the MPLS LSPs or for just a specific LSP.

Options

failure-action teardown—When the BFD session for an RSVP LSP goes down, the LSP is torn down and resignaled. Traffic can be switched to a standby LSP if one is configured and available. Any actions performed are logged.

minimum-interval—Minimum transmit and receive interval.
Range: 50 through 255,000 milliseconds
Default: 50

minimum-receive-interval—Minimum receive interval.
Range: 50 through 255,000 milliseconds
Default: 50

minimum-transmit-interval—Minimum transmit interval.
Range: 50 through 255,000 milliseconds
Default: 50

multiplier—Detection time multiplier.
Range: 1 through 255
Default: 3

Usage Guidelines See “Configuring BFD for MPLS LSPs” on page 169.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

class-of-service

Syntax class-of-service *cos-value*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols mpls],
[edit logical-systems *logical-system-name* protocols mpls interface *interface-name* label-map label-map (default-route | *in-label*)],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*],
[edit logical-systems *logical-system-name* protocols mpls static-path inet *address*],
[edit protocols mpls],
[edit protocols mpls interface *interface-name* label-map (default-route | *in-label*)],
[edit protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*],
[edit protocols mpls static-path inet *prefix*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Class-of-service (CoS) value given to all packets in the LSP.

The CoS value might affect the scheduling or queuing algorithm of traffic traveling along an LSP.

Options *cos-value*—CoS value. A higher value typically corresponds to a higher level of service.
Range: 0 through 7
Default: If you do not specify a CoS value, the IP precedence bits from the packet's IP header are used as the packet's CoS value.

Usage Guidelines See "Configuring Class of Service for MPLS" on page 91, "Configuring the Ingress Router for Static LSPs" on page 135, and "Configuring the Intermediate and Egress Routers for Static LSPs" on page 138.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

default-route

Syntax

```
default-route {
    class-of-service cos-value;
    (next-hop (address | interface-name | address/interface-name) | (reject | discard);
    (pop | (swap <out-label>);
    preference preference;
    swap-push swap-label push-label;
}
```

Hierarchy Level

```
[edit logical-systems logical-system-name protocols mpls interface (interface-name | all)
    label-map],
[edit protocols mpls interface (interface-name | all) label-map]
```

Release Information Statement introduced before JUNOS Release 7.4.

Description Process MPLS packets that have not been assigned label values and have no corresponding entry in the mpls.0 table.

The remaining statements are explained separately.

Usage Guidelines See "Configuring MPLS Exception Monitoring" on page 101.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

description

Syntax

```
description text;
```

Hierarchy Level

```
[edit logical-systems logical-system-name protocols mpls label-switched-path lsp-name],
[edit protocols mpls label-switched-path lsp-name]
```

Release Information Statement introduced before JUNOS Release 7.4.

Description Provides a textual description of the LSP. Enclose any descriptive text that includes spaces in quotation marks (" "). Any descriptive text you include is displayed in the output of the show mpls lsp detail command and has no effect on the operation of the LSP.

Options *text*—Provide a textual description of the LSP.

Usage Guidelines See "Configuring the Description" on page 71.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

diffserv-te

Syntax

```
diffserv-te {
    bandwidth-model {
        extended-mam;
        mam;
        rdm;
    }
    te-class-matrix {
        te number {
            priority priority;
            traffic-class {
                ct number priority priority;
            }
        }
    }
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify properties for differentiated services in traffic engineering.

Options The statements are explained separately.

Usage Guidelines See “Configuring DiffServ-Aware Traffic Engineering” on page 118.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

disable

Syntax disable;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit logical-systems *logical-system-name* protocols mpls interface *interface-name*],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* auto-bandwidth],
[edit protocols mpls],
[edit protocols mpls interface *interface-name*],
[edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Disable the functionality of the configured object.

Default The configured object is enabled (operational) unless explicitly disabled.

Usage Guidelines See "Configuring an LSP" on page 62.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

discard

Syntax discard;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls interface *interface-name* label-map (default-route | *in-label*)],
[edit protocols mpls interface *interface-name* label-map (default-route | *in-label*)],

Release Information Statement introduced before JUNOS Release 7.4.

Description Do not forward packets that match the incoming label. Instead, drop the packets and do not send an ICMP unreachable message.

Usage Guidelines See "Configuring the Intermediate and Egress Routers for Static LSPs" on page 138.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

double-push

Syntax double-push *bottom-label top-label*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced before JUNOS Release 7.4.

Description Push two more labels on top of the stack.

Options *bottom-label*—(Optional) Label value.

top-label—(Optional) Label value.
Range: Labels 0 through 999,999 are for internal use. Labels 1,000,000 through 1,048,575 are unassigned by the JUNOS software and are available for static LSPs. When you configure static LSPs, you can use only this range of labels.

Usage Guidelines See "Configuring the Ingress Router for Static LSPs" on page 135.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

encoding-type

Syntax encoding-type (ethernet | packet | pdh | sonet-sdh);

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* lsp-attributes],
[edit protocols mpls label-switched-path *lsp-name* lsp-attributes]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the encoding type of payload carried by the LSP. It can be any of the following:

- ethernet—Ethernet
- packet—Packet
- pdh—Plesiochronous digital hierarchy (PDH)
- sonet-sdh—SONET/SDH

Default packet

Usage Guidelines See "Configuring the Encoding Type" on page 454.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

exclude

See the following sections:

- exclude (for Administrative Groups) on page 194
- exclude (for Fast Reroute) on page 195

exclude (for Administrative Groups)

Syntax exclude [*group-names*];

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* admin-group],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name* admin-group],
[edit protocols mpls label-switched-path *lsp-name* admin-group],
[edit protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name* admin-group]

Release Information Statement introduced before JUNOS Release 7.4.

Description Define the administrative groups to exclude for an LSP or for a path's primary and secondary paths.

Options *group-names*—Names of one or more groups defined with the admin-groups statement.

Usage Guidelines See "Configuring Administrative Groups" on page 89.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

exclude (for Fast Reroute)

Syntax (exclude [*group-names*] | no-exclude);

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* fast-reroute],
[edit protocols mpls label-switched-path *lsp-name* fast-reroute]

Release Information Statement introduced before JUNOS Release 7.4.

Description Control exclusion of administrative groups:

- exclude—Define the administrative groups to exclude for fast reroute.
- no-exclude—Disable administrative group exclusion.

Options *group-names*—Names of one or more groups defined with the admin-groups statement.

Usage Guidelines See "Configuring Fast Reroute" on page 71.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics admin-groups

expand-loose-hop

Syntax expand-loose-hop;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced in JUNOS Release 7.6.

Description Allow an LSP to traverse multiple OSPF areas within a service provider's network.

Usage Guidelines See "Enabling Interarea Traffic Engineering" on page 154.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

explicit-null

Syntax explicit-null;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced before JUNOS Release 7.4.

Description Advertise label 0 to the egress router of an LSP.

Default If you do not include the explicit-null statement in the MPLS configuration, label 3 (implicit null) is advertised.

Usage Guidelines See "Configuring RSVP to Pop the Label on the Ultimate-Hop Router" on page 291.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

fast-reroute

Syntax
```
fast-reroute {
   (bandwidth bps | bandwidth-percent percent);
   (exclude [ group-names ] | no-exclude);
   hop-limit number;
   (include-all [ group-names ] | no-include-all);
   (include-any [ group-names ] | no-include-any);
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Establish detours for the LSP so that if a node or link in the LSP fails, the traffic on the LSP can be rerouted with minimal packet loss.

Options The statements are explained separately.

Usage Guidelines See "Configuring Fast Reroute" on page 71.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

fate-sharing

Syntax

```
fate-sharing {
    group group-name {
        cost value;
        from address <to address>;
    }
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-options],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* routing-options],
[edit routing-options],
[edit routing-instances *routing-instance-name* routing-options]

Release Information

Statement introduced before JUNOS Release 7.4.

Description

Specify groups of objects that share characteristics resulting in backup paths to be used if primary paths fail. All objects are treated as /32 host addresses. You specify one or more objects within a group. The objects can be LAN interfaces, router IDs, or point-to-point links. The sequence is insignificant.

Options

cost *value*—Cost assigned to the group.
Range: 1 through 65,535
Default: 1

from *address*—Address of the router or address of the LAN/NBMA interface. For example, an Ethernet network with four hosts in the same fate-sharing group would require you to list all four of the separate from addresses in the group.

group *group-name*—Each fate-sharing group must have a name, which can have a maximum of 32 characters, including letters, numbers, periods (.), and hyphens (-). You can define up to 512 groups.

to *address*—(Optional) Address of egress router. For point-to-point link objects, you must specify both a from and a to address.

Usage Guidelines

See "Configuring Alternate Backup Paths Using Fate Sharing" on page 59.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

from

Syntax from *address*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*], [edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the source address to use for the LSP.

The address you specify does not affect the outgoing interface used by the LSP.

Default If you do not include this statement, the software automatically selects the loopback interface as the address.

Options *address*—IP address.

Usage Guidelines See "Configuring the Address of the Ingress Router" on page 68.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

gpid

Syntax gpid (ethernet | hdlc | ipv4 | pos-scrambling-crc-16 | pos-no-scrambling-crc-16 | pos-scrambling-crc-32 | pos-no-scrambling-crc-32 | ppp);

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* lsp-attributes],
[edit protocols mpls label-switched-path *lsp-name* lsp-attributes]

Release Information Statement introduced before JUNOS Release 7.4.
pos-scrambling-crc-16, pos-no-scrambling-crc-16, pos-scrambling-crc-32, and pos-no-scrambling-crc-32 options added in JUNOS Release 8.0.

Description Specify the type of payload carried by the LSP. It can be any of the following:

- ethernet—Ethernet (GPID value: 33)
- hdlc—High-level Data Link Control (HDLC) (GPID value: 44)
- ipv4—IP version 4 (GPID value: 0x0800)
- pos-no-scrambling-crc-16—for interoperability with other vendors' equipment (GPID value: 29)
- pos-no-scrambling-crc-32—for interoperability with other vendors' equipment (GPID value: 30)
- pos-scrambling-crc-16—for interoperability with other vendors' equipment (GPID value: 31)
- pos-scrambling-crc-32—for interoperability with other vendors' equipment (GPID value: 32)
- ppp—Point-to-Point Protocol (PPP) (GPID value: 50)

Default ipv4

Usage Guidelines See "Configuring the GPID" on page 454.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

hop-limit

Syntax hop-limit *number*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* fast-reroute],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*],
[edit protocols mpls],
[edit protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls label-switched-path *lsp-name* fast-reroute],
[edit protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description For an LSP, specify the maximum number of routers that the LSP can traverse, including the ingress and egress routers.

For fast reroute, how many more routers a detour is allowed to traverse compared with the LSP itself. For example, if an LSP traverses 4 routers, any detour for the LSP can be no more than 10 router hops, including the ingress and egress routers.

Options *number*—Maximum number of hops.
Range: 2 through 255 (for an LSP); 0 through 255 (for fast reroute)
Default: 255 (for an LSP); 6 (for fast reroute)

Usage Guidelines See "Configuring Fast Reroute" on page 71 and "Configuring the Maximum Path Length" on page 98.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

icmp-tunneling

Syntax icmp-tunneling;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable ICMP tunneling, which can be used for debugging and tracing purposes.

Usage Guidelines See "Configuring ICMP Message Tunneling" on page 112.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

include-all

See the following sections:

- include-all (for Administrative Groups) on page 201
- include-all (for Fast Reroute) on page 202

include-all (for Administrative Groups)

Syntax include-all [*group-names*];

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* admin-group],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name* admin-group],
[edit protocols mpls label-switched-path *lsp-name* admin-group],
[edit protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name* admin-group]

Release Information Statement introduced before JUNOS Release 7.4.

Description Require the LSP to traverse links that include all of the defined administrative groups.

Options *group-names*—One or more names of groups defined with the admin-groups statement.

Usage Guidelines See "Configuring Administrative Groups" on page 89.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics admin-groups

include-all (for Fast Reroute)

Syntax (include-all [*group-names*] | no-include-all);

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* fast-reroute],
[edit protocols mpls label-switched-path *lsp-name* fast-reroute]

Release Information Statement introduced before JUNOS Release 7.4.

Description Control inclusion of administrative groups:

- include-all—Define the administrative groups that must all be included for fast reroute.
- no-include-all—Disable administrative group inclusion.

Options *group-names*—One or more names of groups defined with the admin-groups statement.

Usage Guidelines See “Configuring Fast Reroute” on page 71.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

include-any

See the following sections:

- include-any (for Administrative Groups) on page 203
- include-any (for Fast Reroute) on page 204

include-any (for Administrative Groups)

Syntax include-any [*group-names*];

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* admin-group],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name* admin-group],
[edit protocols mpls label-switched-path *lsp-name* admin-group],
[edit protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name* admin-group]

Release Information Statement introduced before JUNOS Release 7.4.

Description Define the administrative groups to include for an LSP or for a path's primary and secondary paths.

Options *group-names*—One or more names of groups defined with the admin-groups statement.

Usage Guidelines See "Configuring Administrative Groups" on page 89.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

include-any (for Fast Reroute)

Syntax (include-any [*group-names*] | no-include-any);

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* fast-reroute],
[edit protocols mpls label-switched-path *lsp-name* fast-reroute]

Release Information Statement introduced before JUNOS Release 7.4.

Description Control inclusion of administrative groups:

- include-any—Define the administrative groups to include for fast reroute.
- no-include-any—Disable administrative group inclusion.

Options *group-names*—One or more names of groups defined with the admin-groups statement.

Usage Guidelines See "Configuring Fast Reroute" on page 71.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

install

Syntax
```
install {
  destination-prefix <active>;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Associate one or more prefixes with an LSP. When the LSP is up, all the prefixes are installed as entries into the inet.3 routing table.

Options active—(Optional) Install the route into the inet.0 routing table. This allows you to issue a ping or traceroute command on this address.

destination-prefix—Address to associate with the LSP.

Usage Guidelines See "Configuring Addresses to Associate with the LSP" on page 73.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

interface

Syntax

```
interface (interface-name | all) {
    disable;
    admin-group [ group-names ];
}
label-map (in-label | default-route) {
    class-of-service cos-value;
    next-hop (address | interface-name | address/interface-name) | (reject | discard);
    pop | (swap out-label);
    preference preference;
    swap-pushswap-label push-label;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable MPLS on one or more interfaces.

Options *interface-name*—Name of the interface on which to configure MPLS. To configure all interfaces, specify **all**. For details about specifying interfaces, see the *JUNOS Network Interfaces Configuration Guide*.

The remaining options are explained separately.

Usage Guidelines See "Minimum MPLS Configuration" on page 55 and "Configuring the Intermediate and Egress Routers for Static LSPs" on page 138.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

ipv6-tunneling

Syntax ipv6-tunneling;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced before JUNOS Release 7.4.

Description Allow IPv6 routes to be resolved over an MPLS network by converting all routes stored in the inet.3 routing table to IPv4-compatible IPv6 addresses and then copying them into the inet6.3 routing table. This routing table can be used to resolve next hops for both inet6 and inet6-vpn routes.

Usage Guidelines See "Enabling IPv6 Tunneling in MPLS" on page 111.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

label-map

Syntax
```
label-map (in-label | default-route) {
   class-of-service cos-value;
   next-hop (address | interface-name | address/interface-name) | (reject | discard);
   pop | (swap out-label);
   preference preference;
   swap-push swap-labelpush-label;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls interface *interface-name*],
[edit protocols mpls interface *interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description For static MPLS only, specify the label to match.

Options *in-label*—Incoming label value.

Range: 0 through 1,048,575. Labels 0 through 999,999 are for internal use. Labels 1,000,000 through 1,048,575 are unassigned by the JUNOS software and are available for static LSPs. When you configure static LSPs, you can use only this range of labels.

The remaining statements are explained separately.

Usage Guidelines See "Configuring the Intermediate and Egress Routers for Static LSPs" on page 138.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

label-switched-path

Syntax

```
label-switched-path lsp-name {
    disable;
    adaptive;
    admin-down;
    admin-group {
        exclude [ group-names ];
        include-all [ group-names ];
        include-any [ group-names ];
    }
    auto-bandwidth {
        adjust-interval seconds;
        adjust-threshold percentage;
        maximum-bandwidth bps;
        minimum-bandwidth bps;
        monitor-bandwidth;
    }
    bandwidth bps {
        ct0 bps;
        ct1 bps;
        ct2 bps;
        ct3 bps;
    }
    class-of-service cos-value;
    description text;
    fast-reroute {
        (bandwidth bps | bandwidth-percent percentage);
        (exclude [ group-names ] | no-exclude);
        hop-limit number;
        (include-all [ group-names ] | no-include-all);
        (include-any [ group-names ] | no-include-any);
    }
    from address;
    hop-limit number;
    install {
        destination-prefix/prefix-length <active>;
    }
    ldp-tunneling;
    link-protection;
    lsp-attributes {
        encoding-type (ethernet | packet | pdh | sonet-sdh);
        gpid (ethernet | hdlc | ipv4 | ppp);
        signal-bandwidth type;
        switching-type type;
    }
    metric metric;
    no-cspf;
    no-decrement-ttl;
    node-link-protection;
    optimize-timer seconds;
    p2mp path-name;
    policing {
```

```
    filter filter-name;
    no-automatic-policing;
}
preference preference;
primary path-name {
    adaptive;
    admin-group {
        exclude [ group-names ];
        include-all [ group-names ];
        include-any [ group-names ];
    }
    bandwidth bps {
        ct0 bps;
        ct1 bps;
        ct2 bps;
        ct3 bps;
    }
    class-of-service cos-value;
    hop-limit number;
    no-cspf;
    no-decrement-ttl;
    optimize-timer seconds;
    preference preference;
    priority setup-priority reservation-priority;
    (record | no-record);
    select (manual | unconditional);
    standby;
}
priority setup-priority reservation-priority;
(random | least-fill | most-fill);
(record | no-record);
retry-limit number;
retry-timer seconds;
revert-timer seconds;
secondary path-name {
    adaptive;
    admin-group {
        exclude [ group-names ];
        include-all [ group-names ];
        include-any [ group-names ];
    }
    bandwidth bps{
        ct0 bps;
        ct1 bps;
        ct2 bps;
        ct3 bps;
    }
    class-of-service cos-value;
    hop-limit number;
    no-cspf;
    no-decrement-ttl;
    optimize-timer seconds;
    preference preference;
    priority setup-priority reservation-priority;
    (record | no-record);
    select (manual | unconditional);
```

```
    standby;
  }
  soft-preemption {
    cleanup-timer seconds;
  }
  standby;
  to address;
  traceoptions {
    file filename <replace> <size size> <files number> <no-stamp> <world-readable |
      no-world-readable>;
    flag flag <flag-modifier> <disable>;
  }
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced before JUNOS Release 7.4.

Description Configure an LSP to use in dynamic MPLS. When configuring an LSP, you must specify the address of the egress router in the to statement. All remaining statements are optional.

Options *lsp-name*—Name that identifies the LSP. The name can be up to 32 characters and can contain letters, digits, periods, and hyphens. To include other characters, enclose the name in quotation marks. The name must be unique within the ingress router.

The remaining statements are explained separately.

Usage Guidelines See "Configuring an LSP" on page 62.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

ldp-tunneling

Syntax ldp-tunneling;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable the LSP to be used for Label Distribution Protocol (LDP) tunneling.

Usage Guidelines See "Enabling LDP over RSVP-Established LSPs" on page 360.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

least-fill

See random

link-protection

Syntax link-protection;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*], [edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Extend link protection to all of the paths used by a point-to-multipoint LSP. Link protection helps to ensure that traffic going over a specific interface to a neighboring router can continue to reach this router if that interface fails.

Usage Guidelines See “Configuring Link Protection for Point-to-Multipoint LSPs” on page 146.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

log-updown

Syntax

```
log-updown {
    no-trap {
        mpls-lsp-traps;
        rfc3812–traps;
    }
    (syslog | no-syslog);
    trap;
    trap-path-down;
    trap-path-up;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced before JUNOS Release 7.4.
The mpls-lsp-traps and rfc-3812-traps options added in JUNOS Release 9.0.

Description Log a message or send a Simple Network Management Protocol (SNMP) trap whenever an LSP makes a transition from up to down, or vice versa, and whenever an LSP switches from one active path to another. Only the ingress router performs these operations.

Default There is no default behavior for this statement. If you do not specify the options, the configuration cannot be committed.

Options no-syslog—Do not log a message to the system log file.

no-trap—Do not send an SNMP trap.

syslog—Log a message to the system log file.

trap—Send an SNMP trap.

trap-path-down—Send an SNMP trap when an LSP path goes down.

trap-path-up—Send an SNMP trap when an LSP path comes up.

The no-trap statement is explained separately.

Usage Guidelines See "Controlling MPLS System Log Messages and SNMP Traps" on page 159 and the *JUNOS Network Management Configuration Guide*.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics no-trap, traceoptions

lsp-attributes

Syntax
```
lsp-attributes {
    encoding-type (ethernet | packet | pdh | sonet-sdh);
    gpid (ethernet | hdlc | ipv4 | pos-scrambling-crc-16 | pos-no-scrambling-crc-16 |
        pos-scrambling-crc-32 | pos-no-scrambling-crc-32 | ppp);
    signal-bandwidth type;
    switching-type (fiber | lambda | psc-1 | tdm);
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*], [edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced before JUNOS Release 7.4.
pos-scrambling-crc-16, pos-no-scrambling-crc-16, pos-scrambling-crc-32, and pos-no-scrambling-crc-32 options added in JUNOS Release 8.0.

Description Define the parameters signaled during LSP setup. These usually determine the nature of the resource (label) allocated for the LSP.

The options are explained separately.

Usage Guidelines See "Configuring MPLS LSPs for GMPLS" on page 453.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

maximum-bandwidth

Syntax maximum-bandwidth *bps*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* auto-bandwidth],
[edit protocols mpls label-switched-path *lsp-name* auto-bandwidth]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the maximum amount of bandwidth.

Options *bps*—Bits per second.

Usage Guidelines See "Configuring the Maximum and Minimum Bounds of the LSP's Bandwidth" on page 83.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

metric

Syntax metric *metric*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*], [edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Compare against another LSP or against an IGP route. To disable dynamic metric tracking, assign a fixed metric value to an LSP. If no metric is assigned, the LSP metric is dynamic and automatically tracks underlying IGP metrics.

Options *metric*—LSP metric value.
Default: No metric assigned (dynamic)
Range: 1 through 16,777,215

Usage Guidelines See "Configuring a Static LSP Metric" on page 75.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

minimum-bandwidth

Syntax minimum-bandwidth *bps*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* auto-bandwidth],
[edit protocols mpls label-switched-path *lsp-name* auto-bandwidth]

Release Information Statement introduced before JUNOS Release 7.4.

Description Set the minimum bandwidth for an LSP with automatic bandwidth allocation enabled.

Options *bps*—Bits per second.

Usage Guidelines See "Configuring the Maximum and Minimum Bounds of the LSP's Bandwidth" on page 83.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

monitor-bandwidth

Syntax monitor-bandwidth;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* auto-bandwidth],
[edit protocols mpls label-switched-path *lsp-name* auto-bandwidth]

Release Information Statement introduced before JUNOS Release 7.4.

Description Do not automatically adjust bandwidth allocation. However, the maximum average bandwidth utilization is monitored on the LSP, and the information is recorded in the MPLS statistics file.

Usage Guidelines See "Configuring Passive Bandwidth Utilization Monitoring" on page 86.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

most-fill

See random

mpls

Syntax mpls { ... }

Hierarchy Level [edit logical-systems *logical-system-name* protocols],
[edit protocols]

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable MPLS on the router.

Usage Guidelines See "Minimum MPLS Configuration" on page 55.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

mtu-signaling

Syntax mtu-signaling;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls path-mtu rsvp],
[edit protocols mpls path-mtu rsvp]

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable MTU signaling in RSVP.

Usage Guidelines See "Enabling MTU Signaling in RSVP" on page 291.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

next-hop

Syntax next-hop (*address* | *interface-name* | *address/interface-name*);

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls interface *interface-name* label-map *in-label*],
[edit logical-systems *logical-system-name* protocols mpls interface *interface-name* label-map *in-label* default-route],
[edit logical-systems *logical-system-name* protocols mpls static-path inet *address*],
[edit protocols mpls interface *interface-name* label-map *in-label*],
[edit protocols mpls interface *interface-name* label-map *in-label* default-route],
[edit protocols mpls static-path inet *prefix*]

Release Information Statement introduced before JUNOS Release 7.4.

Description IP address of the next hop to the destination, specified as the IP address of the next hop, the interface name (for point-to-point interfaces only), or the *address/interface-name* to specify an IP address on an operational interface.

Options *address*—IP address of the next-hop router.

interface-name—IP address of the outgoing interface. It must be a point-to-point interface. The name can be a simple or fully qualified domain name.

Usage Guidelines See "Configuring the Ingress Router for Static LSPs" on page 135 and "Configuring the Intermediate and Egress Routers for Static LSPs" on page 138.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

no-cspf

Syntax no-cspf;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*],
[edit protocols mpls],
[edit protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Disable constrained-path LSP computation.

An explicit-path LSP is completely configured through operator action. Once configured, it is initiated only along the explicitly specified path.

A constrained-path LSP relies on an ingress router to compute the complete path. The ingress router takes into account the following information during the computation:

- Interior gateway protocol (IGP) topology database
- Link utilization information from extensions in the IGP link-state database
- Administrative group information from extensions in the IGP link-state database
- LSP requirements, including bandwidth, hop count, and administrative group

Constrained-path LSPs can generally avoid link failures and congested links. They also permit recomputation (therefore, a new path) during topology changes or unsuccessful setup.

Default Constrained-path LSP computation enabled.

Usage Guidelines See “Disabling Constrained-Path LSP Computation” on page 88 and “Configuring Explicit-Path LSPs” on page 142.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

no-decrement-ttl

Syntax no-decrement-ttl;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*],
[edit protocols mpls],
[edit protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Disable normal TTL decrementing, which decrements the TTL field in the IP header by 1. This statement decrements the IP TTL by 1 before encapsulating the IP packet within an MPLS packet. When the penultimate router pops off the top label, it does not use the standard write-back procedure of writing the MPLS TTL into the IP TTL field. Therefore, the IP packet is decremented by 1. The ultimate router then decrements the packet by one more for a total cloud appearance of 2, thus hiding the network topology.

Default Normal TTL decrementing enabled; the TTL field value is decremented by 1 as the packet passes through each label-switched router in the LSP.

Usage Guidelines See "Disabling Normal TTL Decrementing" on page 79.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics no-propagate-ttl

no-exclude

See exclude

no-include-all

See include-all

no-include-any

See include-any

no-install-to-address

Syntax no-install-to-address;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*], [edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced in JUNOS Release 7.4.

Description Prevent the egress router address configured using the to statement from being installed into the inet.3 and inet.0 routing tables.

Default The egress router address for an LSP is installed into the inet.3 and inet.0 routing tables.

Usage Guidelines See "Preventing the Addition of Egress Router Addresses to Routing Tables" on page 67.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics to

no-propagate-ttl

Syntax no-propagate-ttl;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls], [edit protocols mpls]

Release Information Statement introduced before JUNOS Release 7.4.

Description Disable normal TTL decrementing. You configure this statement once per router, and it affects all RSVP-signaled or LDP-signaled LSPs. When this router acts as an ingress router for an LSP, it pushes an MPLS header with a TTL value of 255, regardless of the IP packet TTL. When the router acts as the penultimate router, it pops the MPLS header without writing the MPLS TTL into the IP packet.

Default Normal TTL decrementing enabled; the TTL field value is decremented by 1 as the packet passes through each label-switched router in the LSP.

Usage Guidelines See "Disabling Normal TTL Decrementing" on page 79.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics no-decrement-ttl

no-record

See record

no-trap

Syntax
```
no-trap {
    mpls-lsp-traps;
    rfc-3812-traps;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls log-updown], [edit protocols mpls log-updown]

Release Information Statement introduced before JUNOS Release 7.4.
The mpls-lsp-traps and rfc-3812-traps options added in JUNOS Release 9.0.

Description Prevents the transmission of SNMP traps.

Options mpls-lsp-traps—Blocks the MPLS LSP traps defined in the jnx-mpls.mib, but allows the rfc3812.mib traps.

rfc-3812-traps—Blocks the traps defined in the rfc3812.mib, but allows the MPLS LSP traps defined in the jnx-mpls.mib.

Usage Guidelines See "Controlling MPLS System Log Messages and SNMP Traps" on page 159 and the *JUNOS Network Management Configuration Guide*.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics traceoptions

oam

Syntax

```
oam {
   bfd-liveness-detection{
      failure-action teardown;
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      minimum-transmit-interval milliseconds;
      multiplier detection-time-multiplier;
   }
}
```

Hierarchy Level [edit protocols mpls],
[edit protocols mpls label-switched-path *lsp-name*]
[edit protocols mpls label-switched-path *lsp-name* primary *path-name*]

Release Information Statement introduced in JUNOS Release 7.6.

Description Enable operation, administration, and maintenance (OAM) for all MPLS LSPs or for just a specific LSP.

The remaining statements are explained separately.

Usage Guidelines See "Configuring BFD for MPLS LSPs" on page 169.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

optimize-aggressive

Syntax optimize-aggressive;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced before JUNOS Release 7.4.

Description If enabled, the LSP reoptimization is based solely on the IGP metric. The reoptimization process ignores the available bandwidth ratio calculations, the least-fill 10 percent congestion improvement rule, and the hop-counts rule. This statement makes reoptimization more aggressive than the default.

Default Aggressive optimization is disabled.

Usage Guidelines See "Optimizing Signaled LSPs" on page 96.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

optimize-timer

Syntax optimize-timer *seconds*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols mpls],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* (primary | secondary)],
[edit protocols mpls],
[edit protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable periodic reoptimization of an LSP that is already set up. If topology changes occur, an existing path might become suboptimal, and a subsequent recomputation might be able to determine a better path. This option is useful only on LSPs for which constrained-path computation is enabled; that is, for which the no-cspf statement is not configured.

To avoid extensive resource consumption that might result because of frequent path recomputations, or to avoid destabilizing the network as a result of constantly changing LSPs, we recommend that you either leave the timer value sufficiently large or disable the timer value.

Default The optimize timer is disabled.

Options *seconds*—Length of the optimize timer, in seconds.
Range: 0 through 65,535 seconds
Default: 0 seconds (the optimize timer is disabled)

Usage Guidelines See "Optimizing Signaled LSPs" on page 96.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

p2mp

Syntax p2mp *p2mp-lsp-name*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*], [edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify an LSP as either a point-to-multipoint LSP or as a branch LSP of a point-to-multipoint LSP by specifying the point-to-multipoint LSP path name.

Options *p2mp-lsp-name*—Name of the point-to-multipoint LSP path that identifies the sequence of nodes that form the point-to-multipoint LSP. The name can contain up to 32 characters and can include letters, digits, periods, and hyphens. To include other characters or use a longer name, enclose the name in quotation marks. The name must be unique within the ingress router.

Usage Guidelines See "Configuring the Primary Point-to-Multipoint LSP" on page 143.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

p2mp-lsp-next-hop

Syntax p2mp-lsp-next-hop *lsp-name*;

Hierarchy Level [edit logical-systems *logical-system-name* routing-options static route *route-name*], [edit routing-options static route *route-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the name of the point-to-multipoint LSP to be used as a next hop for the static route.

Options *point-to-multipoint-lsp-next-hop*—Name of the point-to-multipoint LSP.

Usage Guidelines See "Configuring Static Unicast Routes for Point-to-Multipoint LSPs" on page 140.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

path

Syntax

```
path path-name {
   <address | hostname> <strict | loose>
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced before JUNOS Release 7.4.

Description Create a named path and optionally specify the sequence of explicit routers that form the path.

You must include this statement when configuring explicit LSPs.

Options

address—(Optional) IP address of each transit router in the LSP. You must specify the address or hostname of each transit router, although you do not need to list each transit router if its type is loose. As an option, you can include the ingress and egress routers in the path. Specify the addresses in order, starting with the ingress router (optional) or the first transit router, and continuing sequentially along the path until reaching the egress router (optional) or the router immediately before the egress router.
Default: If you do not specify any routers explicitly, no routing limitations are imposed on the LSP.

hostname—(Optional) See *address*.
Default: If you do not specify any routers explicitly, no routing limitations are imposed on the LSP.

loose—(Optional) Indicate that the next address in the path statement is a loose link. This means that the LSP can traverse through other routers before reaching this router.
Default: strict

path-name—Name that identifies the sequence of nodes that form an LSP. The name can contain up to 32 characters and can include letters, digits, periods, and hyphens. To include other characters or use a longer name, enclose the name in quotation marks. The name must be unique within the ingress router.

strict—(Optional) Indicate that the LSP must go to the next address specified in the path statement without traversing other nodes. This is the default.

Usage Guidelines See "Creating a Named Path" on page 58.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics static-path

path-mtu

Syntax

```
path-mtu {
    allow-fragmentation;
    rsvp {
        mtu-signaling;
    }
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced before JUNOS Release 7.4.

Description Configure MTU options for MPLS paths, including packet fragmentation and MTU signaling.

The remaining statements are explained separately.

Usage Guidelines See "Configuring MTU Signaling in RSVP" on page 290.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

policing

Syntax

```
policing {
    filter filter-name;
    no-automatic-policing;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the policing filter for the LSP.

Options filter—Specify the name of the policing filter.

no-automatic-policing—Disable automatic policing on this LSP.

Usage Guidelines See "Configuring Policers for LSPs" on page 162.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics auto-policing

pop

Syntax pop;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls interface *interface-name* label-map default-route],
[edit logical-systems *logical-system-name* protocols mpls interface *interface-name* label-map *in-label*],
[edit protocols mpls interface *interface-name* label-map default-route],
[edit protocols mpls interface *interface-name* label-map *in-label*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Remove the label from the top of the label stack. If there is another label in the stack, that label becomes the label at the top of the label stack. Otherwise, the packet is forwarded as a native protocol packet (typically, as an IP packet).

Usage Guidelines See "Configuring the Intermediate and Egress Routers for Static LSPs" on page 138.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics swap

preference

Syntax preference *preference*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols mpls],
[edit logical-systems *logical-system-name* protocols mpls interface *interface-name* label-map (default-route | *in-label*)],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*],
[edit logical-systems *logical-system-name* protocols mpls static-path inet *address*],
[edit protocols mpls],
[edit protocols mpls interface *interface-name* label-map (default-route | *in-label*)],
[edit protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*],
[edit protocols mpls static-path inet *prefix*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Preference for the route.

You can optionally configure multiple LSPs between the same pair of ingress and egress routers. This is useful for balancing the load among the LSPs because all LSPs, by default, have the same preference level. To prefer one LSP over another, set different preference levels for individual LSPs. The LSP with the lowest preference value is used. The default preference for LSPs is lower (more preferred) than all learned routes except direct interface routes.

Options *preference*—Preference to assign to the route. A route with a lower preference value is preferred.
Range: 1 through 255
Default: 5 for static MPLS LSPs, 7 for RSVP MPLS LSPs, 9 for LDP MPLS LSPs

Usage Guidelines See "Configuring the LSP Preference" on page 91, "Configuring the Ingress Router for Static LSPs" on page 135, and "Configuring the Intermediate and Egress Routers for Static LSPs" on page 138.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

primary

Syntax

```
primary path-name {
    adaptive;
    admin-group {
        exclude [ group-names ];
        include-all [ group-names ];
        include-any [ group-names ];
    }
    bandwidth bps;
    class-of-service cos-value;
    hop-limit number;
    no-cspf;
    no-decrement-ttl;
    optimize-timer seconds;
    preference preference;
    priority setup-priority reservation-priority;
    (record | no-record);
    select (manual | unconditional);
    standby;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*], [edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the primary path to use for an LSP. You can configure only one primary path.

You can optionally specify preference, CoS, and bandwidth values for the primary path, which override any equivalent values that you configure for the LSP (at the [edit mpls label-switched-path *lsp-name*] hierarchy level).

Options *path-name*—Name of a path that you created with the path statement.

The remaining statements are explained separately.

Usage Guidelines See “Configuring the Primary and Secondary LSPs” on page 68.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

priority

Syntax priority *setup-priority reservation-priority*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols mpls],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*],
[edit protocols mpls],
[edit protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Configure the setup priority and reservation priority for an LSP. If insufficient link bandwidth is available during session establishment, the setup priority is compared with other setup priorities for established sessions on the link to determine whether some of them should be preempted to accommodate the new session. Sessions with lower hold priorities are preempted.

Options
reservation-priority—Reservation priority, used to keep a reservation after it has been set up. A smaller number has a higher priority. The priority must be greater than or equal to the setup priority to prevent preemption loops.
Range: 0 through 7, where 0 is the highest and 7 is the lowest priority.
Default: 0 (Once the session is set up, no other session can preempt it.)

setup-priority—Setup priority.
Range: 0 through 7, where 0 is the highest and 7 is the lowest priority.
Default: 7 (The session cannot preempt any existing sessions.)

Usage Guidelines See “Configuring Priority and Preemption for LSPs” on page 95.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

push

Syntax push *out-label*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls static-path inet *address*], [edit protocols mpls static-path inet *address*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Add a new label to the top of the label stack.

Options *out-label*—Label value.

Range: 0 through 1,048,575. Labels 0 through 999,999 are for internal use. Labels 1,000,000 through 1,048,575 are unassigned by the JUNOS software and are available for static LSPs. When you configure static LSPs, you can use only this range of labels.

Usage Guidelines See "Configuring the Ingress Router for Static LSPs" on page 135.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

random

Syntax (random | least-fill | most-fill);

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*], [edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Configure the preferred path when several equal-cost candidate paths to a destination exist, and prefer the path with the highest available bandwidth (with the largest minimum available bandwidth ratio). The available bandwidth ratio of a link is the available bandwidth on a link divided by the maximum reservable bandwidth on the link.

- least-fill—Prefer the path with the most available bandwidth (with the largest minimum available bandwidth ratio).
- most-fill—Prefer the path with the least available bandwidth (with the minimum available bandwidth ratio). The minimum available bandwidth ratio of a path is the smallest available bandwidth ratio belonging to any of the links in the path.
- random—Choose the path at random.

Default random

Usage Guidelines See “Configuring CSPF Tie Breaking” on page 76.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

record

Syntax (record | no-record);

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*],
[edit protocols mpls],
[edit protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify whether an LSP should actively record the routes in the path. Recording routes requires that all transit routers support the RSVP Record Route object. Recording routes can be useful for diagnostics and loop detection.

Default Record routes.

Usage Guidelines See "Configuring Path Route Recording" on page 91.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

reject

Syntax reject;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls interface *interface-name* label-map *in-label*],
[edit logical-systems *logical-system-name* protocols mpls interface *interface-name* label-map *in-label* default-route],
[edit protocols mpls interface *interface-name* label-map *in-label*],
[edit protocols mpls interface *interface-name* label-map *in-label* default-route]

Release Information Statement introduced before JUNOS Release 7.4.

Description Do not forward a packet with the matching incoming label. Instead, drop the packet and, for IP packets, send an ICMP unreachable message to the packet's originator.

Usage Guidelines See "Configuring the Intermediate and Egress Routers for Static LSPs" on page 138.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

retry-limit

Syntax retry-limit *number*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*], [edit protocols mpls label-switched-path *lsp-name*],

Release Information Statement introduced before JUNOS Release 7.4.

Description Maximum number of times the ingress router tries to establish the primary path. This counter is reset each time a primary path is created successfully. When the limit is exceeded, no more connection attempts are made. Intervention is then required to restart the connection.

Options *number*—Maximum number of tries to establish the primary path.
Range: 0 through 10,000
Default: 0 (The ingress node never stops trying to establish the primary path.)

Usage Guidelines See "Configuring Path Connection Retry Information" on page 74.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

retry-timer

Syntax retry-timer *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*], [edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Amount of time the ingress router waits between attempts to establish the primary path.

Options *seconds*—Amount of time between attempts to connect to the primary path.
Range: 1 through 600 seconds
Default: 30 seconds

Usage Guidelines See "Configuring Path Connection Retry Information" on page 74.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

revert-timer

Syntax revert-timer *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls],
[edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced before JUNOS Release 7.4.
BFD behavior modified in JUNOS Release 9.0.

Description Specify the amount of time (in seconds) that an LSP must wait before traffic reverts to a primary path. If during this time the primary path experiences any connectivity problem or stability problem, the timer is restarted.

If you have configured BFD on the LSP, the JUNOS software waits until the BFD session is restored before starting the revert timer counter.

If you have configured a value of 0 seconds for the revert-timer statement and traffic is switched to the secondary path, the traffic remains on that path indefinitely. It is never switched back to the primary path unless you intervene.

Options *seconds*—Time in seconds.
Range: 0 through 65,535 seconds
Default: 60 seconds

Usage Guidelines See "Configuring the Revert Timer" on page 69.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

rpf-check-policy

Syntax rpf-check-policy *policy*;

Hierarchy Level [edit logical-systems *logical-system-name* routing-options multicast],
[edit routing-options multicast]

Release Information Statement introduced in JUNOS Release 8.0.

Description Allows you to control whether an reverse path forwarding (RPF) check is performed for a source and group entry before installing a route in the multicast forwarding cache. This makes it possible to use point-to-multipoint LSPs to distribute multicast traffic to PIM islands situated downstream from the egress routers of the point-to-multipoint LSPs.

Options *policy*—Name of the RPF check routing policy.

Usage Guidelines See "Configuring a Multicast RPF Check Policy for Point-to-Multipoint LSPs" on page 147.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

rsvp-error-hold-time

Syntax rsvp-error-hold-time *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced before JUNOS Release 7.4.

Description Amount of time MPLS retains RSVP PathErr messages and considers them for CSPF computations. The more time you configure, the more time a source node (ingress of the RSVP LSPs) can have to learn about the failures of its LSP by monitoring PathErr messages transmitted from downstream nodes.

Information from the PathErr messages is incorporated into subsequent LSP computations, which can improve the accuracy and speed of LSP setup. Some PathErr messages are also used to update traffic engineering database (TED) bandwidth information, reducing inconsistencies between the database and the network.

Options *seconds*—Amount of time MPLS retains RSVP PathErr messages and considers them for CSPF computations.
Range: 0 through 240 seconds
Default: 25 seconds

Usage Guidelines See "Improving TED Accuracy with RSVP PathErr Messages" on page 101.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

secondary

Syntax

```
secondary path-name {
   adaptive;
   admin-group {
      exclude [ group-names ];
      include-all [ group-names ];
      include-any [ group-names ];
   }
   bandwidth bps;
   class-of-service cos-value;
   hop-limit number;
   no-cspf;
   no-decrement-ttl;
   optimize-timer seconds;
   preference preference;
   priority setup-priority reservation-priority;
   (record | no-record);
   retry-limit number;
   retry-timer seconds;
   select {
      manual;
      unconditional;
   }
   standby;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*], [edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify one or more secondary paths to use for the LSP. You can configure more than one secondary path. All secondary paths are equal, and the first one that is available is chosen.

You can specify secondary paths even if you have not specified any primary paths.

Optionally, you can specify preference, CoS, and bandwidth values for the secondary path, which override any equivalent values that you configure for the LSP (at the [edit mpls label-switched-path] hierarchy level).

Options *path-name*—Name of a path that you created with the path statement.

The remaining statements are explained separately.

Usage Guidelines See “Configuring the Primary and Secondary LSPs” on page 68.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

select

Syntax select (manual | unconditional);

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*],
[edit protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description You must specify either the manual option or the unconditional option. You cannot specify both.

Options manual—The path is selected for carrying traffic if it is up and stable for at least the revert timer window (potentially before the revert timer has elapsed). Traffic is sent to other working paths if the current path is down or degraded (receiving errors).

unconditional—The path is selected for carrying traffic unconditionally, regardless of whether the path is currently down or degraded (receiving errors).

Usage Guidelines See "Specifying Path Selection" on page 70.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

signal-bandwidth

Syntax signal-bandwidth *type*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* lsp-attributes],
[edit protocols mpls label-switched-path *lsp-name* lsp-attributes]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the bandwidth encoding of the signal used for path computation and admission control.

Options *type*—Configure the type of bandwidth encoding used on the LSP. It can be any of the following values: 10gigether, ds1, ds3, e1, e3, ethernet, fastether, gigether, stm-1, stm-4, stm-16, stm-64, stm-256, sts-1, vt1-5, or vt2.

Usage Guidelines See "Configuring the Signal Bandwidth Type" on page 455.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

smart-optimize-timer

Syntax smart-optimize-timer *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced before JUNOS Release 7.4.

Description When a link fails and traffic is moved to an alternate path, the smart optimize timer waits for the specified period of time and then switches the traffic back to the original path (if that path is back up). If the original path fails again, the traffic is shifted to an alternate path and the smart optimization timer is disabled for one hour. This statement is disabled by default.

Options *seconds*—Specify the number of seconds for the smart optimize timer.
Range: 0 through 65,535 seconds
Default: 180 seconds

Usage Guidelines See "Configuring the Smart Optimize Timer" on page 97.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

soft-preemption

Syntax
```
soft-preemption {
   cleanup-timer seconds;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Soft preemption attempts to establish a new path for a preempted LSP before tearing it down.

Options cleanup-timer—Configure the length of time, in seconds, that the router should wait before initiating a hard preemption of the LSP.

Usage Guidelines See "Configuring MPLS Soft Preemption" on page 80.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

standby

Syntax standby;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*],
[edit protocols mpls],
[edit protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls label-switched-path *lsp-name* (primary | secondary) *path-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Have the path remain up at all times to provide instant switchover if connectivity problems occur.

Usage Guidelines See "Configuring the Standby State" on page 99.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

static-path

Syntax

```
static-path inet {
    prefix {
        class-of-service cos-value;
        double-push bottom-label top-label;
        next-hop (address | interface-name | address/interface-name);
        preference preference;
        push out-label;
        triple-push bottom-label middle-label top-label;
    }
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced before JUNOS Release 7.4.

Description Statically configure an LSP. You configure the LSP on the ingress router only.

You can specify one or more static-path statements.

Options *prefix*—IP address that matches the packet's destination field. You can specify one or more addresses. You can specify the prefix in one of the following ways:

- IP address; for example, 10.0.0.2
- Range of IP addresses; for example, 10.0.0.0/8

inet—Configure the path for packets with IPv4 destinations.

The remaining statements are explained separately.

Usage Guidelines See "Configuring the Ingress Router for Static LSPs" on page 135.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

statistics

Syntax

```
statistics {
    auto-bandwidth;
    file filename <size size> <files number> <no-stamp> <replace> <world-readable |
        no-world-readable>;
    interval seconds;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable MPLS statistics collection and reporting.

Options auto-bandwidth—Collect statistics related to automatic bandwidth.

file *filename*—Name of the file to receive the output. We recommend that you place MPLS tracing output in the file mpls-stat in the /var/log directory.

files *number*—Maximum number of trace files. When a trace file named *file* reaches its maximum size, it is renamed *file*.0, then *file*.1, and so on, until the maximum number of files is reached. Then, the oldest file is overwritten.
Range: 2 or more
Default: 2 files

If you specify a maximum number of files, you also must specify a maximum file size with the size option.

interval *seconds*—Interval at which to periodically collect statistics.
Range: 1 through 65,535
Default: 300 seconds

no-world-readable—(Optional) Prevents users from reading the log file.

replace—(Optional) Replace an existing trace file if there is one. However, the change does not take effect after you commit the configuration. The change takes effect only after the routing protocol process restarts.
Default: If you do not include this option, tracing output is appended to an existing trace file.

size *size*—(Optional) Maximum size of each file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a file named *file* reaches this size, it is renamed *file*.0. When the *file* again reaches its maximum size, *file*.0 is renamed *file*.1 and *file* is renamed *file*.0. This renaming scheme continues until the maximum number of files is reached. Then the oldest trace file is overwritten.
Syntax: Syntax: *x*k to specify KB, *x*m to specify MB, or *x*g to specify GB
Range: 10 KB through the maximum file size supported on your system
Default: 1 MB

If you specify a maximum file size, you also must specify a maximum number of files with the files option.

world-readable—(Optional) Enables users to read the log file.

Usage Guidelines See "Configuring MPLS to Gather Statistics" on page 158, and "Configuring MPLS Statistics for Automatic Bandwidth Allocation" on page 82.

Required Privilege Level routing and trace—To view this statement in the configuration.
routing-control and trace-control—To add this statement to the configuration.

swap

Syntax swap *out-label*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls interface *interface-name* label-map *in-label*],
[edit logical-systems *logical-system-name* protocols mpls interface *interface-name* label-map *in-label* default-route],
[edit protocols mpls interface *interface-name* label-map *in-label*],
[edit protocols mpls interface *interface-name* label-map *in-label* default-route]

Release Information Statement introduced before JUNOS Release 7.4.

Description Remove the label at the top of the label stack and replace it with the specified label.

Options *out-label*—Label value.

Range: 0 through 1,048,575. Labels 0 through 999,999 are for internal use. Labels 1,000,000 through 1,048,575 are unassigned by the JUNOS software and are available for static LSPs. When you configure static LSPs, you can use only this range of labels.

Default: If you do not define the *out-label* option, the original label value remains unchanged.

Usage Guidelines See "Configuring the Intermediate and Egress Routers for Static LSPs" on page 138.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics pop

swap-push

Syntax swap-push *swap-label push-label*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls interface *interface-name* label-map *in-label*],
[edit logical-systems *logical-system-name* protocols mpls interface *interface-name* label-map *in-label* default-route],
[edit protocols mpls interface *interface-name* label-map *in-label*],
[edit protocols mpls interface *interface-name* label-map *in-label* default-route]

Release Information Statement introduced before JUNOS Release 7.4.

Description Replace the stack's top label and then push one more label on top of the stack.

Options *push-label*—Label value.

swap-label—Label value.

The following range and default values apply to both *push-label* and *swap-label*:

Range: 0 through 1,048,575. Labels 0 through 999,999 are for internal use. Labels 1,000,000 through 1,048,575 are unassigned by the JUNOS software and are available for static LSPs. When you configure static LSPs, you can use only this range of labels.

Default: If you do not define the *swap-label* option, the original label value remains unchanged.

Usage Guidelines See "Configuring the Intermediate and Egress Routers for Static LSPs" on page 138.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics pop and swap

switching-type

Syntax switching-type (fiber | lambda | psc-1 | tdm);

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name* lsp-attributes],
[edit protocols mpls label-switched-path *lsp-name* lsp-attributes]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the switching method for the LSP. The switching method can be one of the following values:

- fiber—Fiber switching
- lambda—Lambda switching
- psc-1—Packet switching
- tdm—Time-division multiplexing (TDM) switching

Default psc-1

Usage Guidelines See “Configuring MPLS LSPs for GMPLS” on page 453.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

te-class-matrix

Syntax

```
te-class-matrix {
   tenumber {
      priority priority;
      traffic-class {
         ctnumber priority priority;
      }
   }
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls diffserv-te], [edit protocols mpls diffserv-te]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the traffic engineering class matrix for a multiclass LSP or a DiffServ-aware traffic engineering LSP.

Default The default traffic engineering class matrix is:

```
te-class-matrix {
   te0 traffic-class ct0 priority 7;
   te1 traffic-class ct1 priority 7;
   te2 traffic-class ct2 priority 7;
   te3 traffic-class ct3 priority 7;
   te4 traffic-class ct0 priority 0;
   te5 traffic-class ct1 priority 0;
   te6 traffic-class ct2 priority 0;
   te7 traffic-class ct3 priority 0;
}
```

If you define any of the traffic engineering classes, all the default values are dropped.

Options

ct*number*—Specify the number of the class type. It can be one of four values: ct0, ct1, ct2, or ct3.

priority—Specify the priority of the class type. It can be one of eight values from 0 through 7.

te*number*—Specify the number of the traffic engineering class. It can be one of eight values: te0, te1, te2, te3, te4, te5, te6, or te7. You must configure the traffic engineering classes in order, starting with te0.

traffic-class—Specify the traffic class for the traffic engineering class.

Usage Guidelines See "Configuring Traffic Engineering Classes" on page 120.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

to

Syntax to *address*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*], [edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the egress router of a dynamic LSP.

Options *address*—Address of the egress router.

Usage Guidelines See "Configuring the Address of the Egress Router" on page 66.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

traceoptions

Syntax

```
traceoptions {
   file filename <replace> <size size> <files number> <no-stamp>
      <world-readable | no-world-readable>;
   flag flag;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols mpls],
[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls],
[edit protocols mpls label-switched-path *lsp-name*]

Release Information

Statement introduced before JUNOS Release 7.4.

Description

Configure MPLS tracing options at the protocol level or for a label-switched path.

To specify more than one tracing operation, include multiple flag statements.

Default

The default MPLS protocol-level tracing options are inherited from the routing protocols traceoptions statement included at the [edit routing-options] hierarchy level.

Options

filename—Name of the file to receive the output of the tracing operation. All files are placed in the directory /var/log. We recommend that you place MPLS tracing output in the file mpls-log.

files *number*—(Optional) Maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed *trace-file*.0, then *trace-file*.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.
Range: 2 through 1000
Default: 2 files

If you specify a maximum number of files, you must also include the size statement to specify the maximum file size.

flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.

MPLS Tracing Flags

- all—Trace all operations
- connection—All circuit cross-connect (CCC) activity
- connection-detail—Detailed CCC activity
- cspf—CSPF computations
- cspf-link—Links visited during CSPF computations
- cspf-node—Nodes visited during CSPF computations
- error—MPLS error packets

- graceful-restart—Trace MPLS graceful restart events
- lsping—Trace lsping packets and return codes
- state—All LSP state transitions
- timer—Timer usage

no-stamp—(Optional) Do not place timestamp information at the beginning of each line in the trace file.
Default: If you omit this option, timestamp information is placed at the beginning of each line of the tracing output.

no-world-readable—(Optional) Allow only certain users to read the log file.

replace—(Optional) Replace an existing trace file if there is one.
Default: If you do not include this option, tracing output is appended to an existing trace file.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file*.0. When the *trace-file* again reaches this size, *trace-file*.0 is renamed *trace-file*.1 and *trace-file* is renamed *trace-file*.0. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.
Syntax: *x*k to specify KB, *x*m to specify MB, or *x*g to specify GB
Range: 10 KB through the maximum file size supported on your system
Default: 1 MB

If you specify a maximum file size, you must also include the files statement to specify the maximum number of files.

world-readable—(Optional) Allow any user to read the log file.

Usage Guidelines See "Tracing MPLS and LSP Packets and Operations" on page 172.

Required Privilege Level routing and trace—To view this statement in the configuration.
routing-control and trace-control—To add this statement to the configuration.

traffic-engineering

Syntax traffic-engineering (bgp | bgp-igp | bgp-igp-both-ribs | mpls-forwarding);

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced before JUNOS Release 7.4.

Description Select whether MPLS performs traffic engineering on BGP destinations only or on both BGP and IGP destinations. Affects only LSPs originating from this router, not transit or egress LSPs.

Default bgp

Options bgp—On BGP destinations only. Ingress routes are installed in the inet.3 routing table.

bgp-igp—On both BGP and IGP destinations. Ingress routes are installed in the inet.0 routing table. If IGP shortcuts are enabled, the shortcut routes are automatically installed in the inet.0 routing table.

bgp-igp-both-ribs—On both BGP and IGP destinations. Ingress routes are installed in the inet.0 and inet.3 routing tables. This option is used to support VPNs.

mpls-forwarding—On both BGP and IGP destinations. Use ingress routes for forwarding only, not for routing.

Usage Guidelines See "Configuring Traffic Engineering for LSPs" on page 152.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

triple-push

Syntax triple-push <*bottom-label*> <*middle-label*> <*top-label*>;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls static-path inet *prefix*], [edit protocols mpls static-path inet *prefix*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Push three more labels on top of the stack.

Options *bottom-label*—(Optional) Label value.

middle-label—(Optional) Label value.

top-label—(Optional) Label value.

The labels all have the same range and default actions:

Range: 0 through 1,048,575. Labels 0 through 999,999 are for internal use. Labels 1,000,000 through 1,048,575 are unassigned by the JUNOS software and are available for static LSPs. When you configure static LSPs, you can use only this range of labels.

Default: If you do not define the *push-label* option, the original label value remains unchanged.

Usage Guidelines See "Configuring the Ingress Router for Static LSPs" on page 135.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Part 3
RSVP

- RSVP Overview on page 253
- RSVP Configuration Guidelines on page 269
- Summary of RSVP Configuration Statements on page 297

Chapter 11

RSVP Overview

The Resource Reservation Protocol (RSVP) is a resource reservation setup protocol that is used by both network hosts and routers. Hosts use RSVP to request a specific class of service (CoS) from the network for particular application flows. Routers use RSVP to deliver CoS requests to all routers along the data path. RSVP also can maintain and refresh states for a requested CoS application flow.

RSVP treats an application flow as a simplex connection. That is, the CoS request travels only in one direction—from the sender to the receiver. RSVP is a transport layer protocol that uses IP as its network layer. However, RSVP does not transport application flows. Rather, it is more of an Internet control protocol, similar to the Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP). RSVP runs as a separate software process in the JUNOS software and is not in the packet forwarding path.

RSVP is not a routing protocol, but rather is designed to operate with current and future unicast and multicast routing protocols. The routing protocols are responsible for choosing the routes to use to forward packets, and RSVP consults local routing tables to obtain routes. RSVP only ensures the CoS of packets traveling along a data path.

The receiver in an application flow requests the preferred CoS from the sender. To do this, the receiver issues an RSVP CoS request on behalf of the local application. The request propagates to all routers in reverse direction of the data paths toward the sender. In this process, RSVP requests might be merged, resulting in a protocol that scales well when there are a large number of receivers.

Because the number of receivers in an application flow is likely to change and the flow of delivery paths might change during the life of an application flow, RSVP takes a soft-state approach in its design, creating and removing the protocol states in routers and hosts incrementally over time. RSVP sends periodic refresh messages to maintain its state and to recover from occasional lost messages. In the absence of refresh messages, the RSVP states automatically time out and are deleted.

This chapter discusses the following topics:

- RSVP Standards on page 254
- JUNOS Software RSVP Protocol Implementation on page 255
- RSVP Operation on page 255
- RSVP Message Types on page 257
- RSVP Reservation Styles on page 259

- RSVP Refresh Reduction on page 259
- MTU Signaling in RSVP on page 260
- Link Protection on page 263
- Node Protection on page 265
- RSVP Graceful Restart on page 266

RSVP Standards

RSVP is described in several RFCs and drafts.

The following RFCs provide an overview of RSVP and RSVP features:

- RFC 2205, *Resource Reservation Protocol (RSVP), Version 1, Functional Specification*
- RFC 2209, *Resource Reservation Protocol (RSVP), Version 1, Message Processing Rules*
- RFC 2210, *The Use of RSVP with IETF Integrated Services*
- RFC 2211, *Specification of the Controlled-Load Network Element Service*
- RFC 2212, *Specification of Guaranteed Quality of Service*
- RFC 2215, *General Characterization Parameters for Integrated Service Network Elements*
- RFC 2216, *Network Element Service Specification Template*
- RFC 2745, *RSVP Diagnostic Messages*
- RFC 2747, *RSVP Cryptographic Authentication* (see also RFC 3097)
- RFC 2961, *RSVP Refresh Overhead Reduction Extensions*
- RFC 3097, *RSVP Cryptographic Authentication -- Updated Message Type Value* (see also RFC 2747)
- RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels* (the JUNOS software does not support the Null Service Object for maximum transmission unit [MTU] signaling in RSVP)
- RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions* (only Section 9, *Fault Handling*)
- RFC 3477, *Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)*
- RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels* (except node protection in facility backup)
- RFC 4125, *Maximum Allocation Bandwidth Constraints Model for Diff-Serv-aware MPLS Traffic Engineering*
- RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diff-Serv-aware MPLS Traffic Engineering*

- RFC 4203, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)* (OSPF extensions can carry traffic engineering information over unnumbered links)
- RFC 4205, *Intermediate System to Intermediate System (IS-IS) Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)* (IS-IS extensions can carry traffic engineering information over unnumbered links)

The following Internet draft also provides information about RSVP:

- Internet draft draft-ietf-mpls-rsvp-te-p2mp-01.txt, *Extensions to RSVP-TE for Point to Multipoint TE LSPs* (expires June 2005)

To access RFCs and drafts, go to the IETF Web site at http://www.ietf.org.

JUNOS Software RSVP Protocol Implementation

The JUNOS implementation of RSVP supports RSVP version 1. The software includes support for all mandatory objects and RSVP message types, and supports message integrity and node authentications through the Integrity object.

The primary purpose of the JUNOS RSVP software is to support dynamic signaling within Multiprotocol Label Switching (MPLS) label-switched paths (LSPs). Supporting resource reservations over the Internet is only a secondary purpose of the JUNOS software implementation. Since supporting resource reservations is secondary, the RSVP software does not support the following features:

- IP multicasting sessions.
- Traffic control—The software cannot make resource reservations for real-time video or audio sessions.

With regard to the protocol mechanism, packet processing, and RSVP objects supported, the JUNOS software implementation of the software is interoperable with other RSVP implementations.

RSVP Operation

The following sections describe RSVP operation:

- RSVP Operation Overview on page 255
- RSVP Authentication on page 256
- RSVP and IGP Hello Packets and Timers on page 256

RSVP Operation Overview

RSVP creates independent sessions to handle each data flow. A session is identified by a combination of the destination address, an optional destination port, and a protocol. Within a session, there can be one or more senders. Each sender is identified by a combination of its source address and source port. An out-of-band mechanism,

such as a session announcement protocol or human communication, is used to communicate the session identifier to all senders and receivers.

A typical RSVP session involves the following sequence of events:

1. A potential sender starts sending RSVP path messages to the session address.
2. A receiver, wanting to join the session, registers itself if necessary. For example, a receiver in a multicast application would register itself with IGMP.
3. The receiver receives the path messages.
4. The receiver sends appropriate Resv messages toward the sender. These messages carry a flow descriptor, which is used by routers along the path to make reservations in their link-layer media.
5. The sender receives the Resv message and then starts sending application data.

This sequence of events is not necessarily strictly synchronized. For example, receivers can register themselves before receiving path messages from the sender, and application data can flow before the sender receives Resv messages. Application data that is delivered before the actual reservation contained in the Resv message typically is treated as best-effort, non-real-time traffic with no CoS guarantee.

RSVP Authentication

JUNOS software supports both the RSVP authentication style described in RFC 2747 (allowing for multivendor compatibility) and the RSVP authentication style described in Internet draft draft-ietf-rsvp-md5-03.txt. The JUNOS software uses the authentication style described in Internet draft draft-ietf-rsvp-md5-08.txt by default. If the router receives an RFC 2747-style RSVP authentication from a neighbor, it switches to this style of authentication for that neighbor. The RSVP authentication style for each neighboring router is determined separately.

RSVP and IGP Hello Packets and Timers

RSVP monitors the status of the interior gateway protocol (IGP) (IS-IS or OSPF) neighbors and relies on the IGP protocols to detect when a node fails. If an IGP protocol declares a neighbor down (because hello packets are no longer being received), RSVP also brings down that neighbor. However, the IGP protocols and RSVP still act independently when bringing a neighbor up.

In JUNOS software, RSVP typically relies on IGP hello packet detection to check for node failures. RSVP sessions are kept up even if RSVP hello packets are no longer being received, so long as the router continues to receive IGP hello packets. RSVP sessions are maintained until either the router stops receiving IGP hello packets or the RSVP Path and Resv messages time out. Configuring a short time for the IS-IS or OSPF hello timers allows these protocols to detect node failures quickly.

RSVP hellos can be relied on when the IGP does not recognize a particular neighbor (for example, if IGP is not enabled on the interface) or if the IGP is RIP (not IS-IS or OSPF). Also, the equipment of other vendors might be configured to monitor RSVP sessions based on RSVP hello packets. This equipment might also take an RSVP session down due to a loss of RSVP hello packets.

Juniper Networks does not recommend configuring a short RSVP hello timer. If quick discovery of a failed neighbor is needed, configure short IGP (OSPF or IS-IS) hello timers.

OSPF and IS-IS have infrastructure to manage rapid hello message sending and receiving reliably, even if the routing protocols or some other process are straining the processing capability of the router. Under the same circumstances, RSVP hellos might timeout prematurely even though the neighbor is functioning normally.

RSVP Message Types

RSVP uses the following types of messages to establish and remove paths for data flows, establish and remove reservation information, confirm the establishment of reservations, and report errors:

- Path Messages on page 257
- Resv Messages on page 257
- PathTear Messages on page 258
- ResvTear Messages on page 258
- PathErr Messages on page 258
- ResvErr Messages on page 258
- ResvConfirm Messages on page 258

Path Messages

Each sender host transmits path messages downstream along the routes provided by the unicast and multicast routing protocols. Path messages follow the exact paths of application data, creating path states in the routers along the way, thus enabling routers to learn the previous-hop and next-hop node for the session. Path messages are sent periodically to refresh path states.

The refresh interval is controlled by a variable called the *refresh-time*, which is the periodical refresh timer expressed in seconds. A path state times out if a router does not receive a specified number of consecutive path messages. This number is specified by a variable called *keep-multiplier*. Path states are kept for ((*keep-multiplier* + 0.5) x 1.5 x *refresh-time*) seconds.

Resv Messages

Each receiver host sends reservation request (Resv) messages upstream toward senders and sender applications. Resv messages must follow exactly the reverse path of path messages. Resv messages create and maintain a reservation state in each router along the way.

Resv messages are sent periodically to refresh reservation states. The refresh interval is controlled by the same refresh time variable, and reservation states are kept for ((*keep-multiplier* + 0.5) x 1.5 x *refresh-time*) seconds.

PathTear Messages

PathTear messages remove (tear down) path states as well as dependent reservation states in any routers along a path. PathTear messages follow the same path as path messages. A PathTear typically is initiated by a sender application or by a router when its path state times out.

PathTear messages are not required, but they enhance network performance because they release network resources quickly. If PathTear messages are lost or not generated, path states eventually time out when they are not refreshed, and the resources associated with the path are released.

ResvTear Messages

ResvTear messages remove reservation states along a path. These messages travel upstream toward senders of the session. In a sense, ResvTear messages are the reverse of Resv messages. ResvTear messages typically are initiated by a receiver application or by a router when its reservation state times out.

ResvTear messages are not required, but they enhance network performance because they release network resources quickly. If ResvTear messages are lost or not generated, reservation states eventually time out when they are not refreshed, and the resources associated with the reservation are released.

PathErr Messages

When path errors occur (usually because of parameter problems in a path message), the router sends a unicast PathErr message to the sender that issued the path message. PathErr messages are advisory; these messages do not alter any path state along the way.

ResvErr Messages

When a reservation request fails, a ResvErr error message is delivered to all the receivers involved. ResvErr messages are advisory; these messages do not alter any reservation state along the way.

ResvConfirm Messages

Receivers can request confirmation of a reservation request, and this confirmation is sent with a ResvConfirm message. Because of the complex RSVP flow-merging rules, a confirmation message does not necessarily provide end-to-end confirmation of the entire path. Therefore, ResvConfirm messages are an indication, not a guarantee, of potential success.

Juniper Networks routers never request confirmation using the ResvConfirm message; however, a Juniper Networks router can send a ResvConfirm message if it receives a request from another vendor's equipment.

RSVP Reservation Styles

A reservation request includes options for specifying the reservation style. The reservation styles define how reservations for different senders within the same session are treated and how senders are selected.

Two options specify how reservations for different senders within the same session are treated:

- Distinct reservation—Each receiver establishes its own reservation with each upstream sender.
- Shared reservation—All receivers make a single reservation that is shared among many senders.

Two options specify how senders are selected:

- Explicit sender—List all selected senders.
- Wildcard sender—Select all senders, which then participate in the session.

The following reservation styles, formed by a combination of these four options, currently are defined:

- Fixed filter (FF)—This reservation style consists of distinct reservations among explicit senders. Examples of applications that use fixed-filter-style reservations are video applications and unicast applications, which both require flows that have a separate reservation for each sender. The fixed filter reservation style is enabled on RSVP LSPs by default.
- Wildcard filter (WF)—This reservation style consists of shared reservations among wildcard senders. This type of reservation reserves bandwidth for any and all senders, and propagates upstream toward all senders, automatically extending to new senders as they appear. A sample application for wildcard filter reservations is an audio application in which each sender transmits a distinct data stream. Typically, only a few senders are transmitting at any one time. Such a flow does not require a separate reservation for each sender; a single reservation is sufficient.
- Shared explicit (SE)—This reservation style consists of shared reservations among explicit senders. This type of reservation reserves bandwidth for a limited group of senders. A sample application is an audio application similar to that described for wildcard filter reservations.

RSVP Refresh Reduction

RSVP relies on soft-state to maintain the path and reservation states on each router. If the corresponding refresh messages are not sent periodically, the states eventually time out and reservations are deleted. RSVP also sends its control messages as IP datagrams with no reliability guarantee. It relies on periodic refresh messages to handle the occasional loss of Path or Resv messages.

The RSVP refresh reduction extensions, based on RFC 2961, addresses the following problems that result from relying on periodic refresh messages to handle message loss:

- Scalability—The scaling problem arises from the periodic transmission and processing overhead of refresh messages, which increases as the number of RSVP sessions increases.
- Reliability and latency—The reliability and latency problem stems from the loss of nonrefresh RSVP messages or one-time RSVP messages such as PathTear or PathErr. The time to recover from such a loss is usually tied to refresh interval and the keepalive timer.

The RSVP refresh reduction capability is advertised by enabling the refresh reduction (RR) capable bit in the RSVP common header. This bit is only significant between RSVP neighbors.

RSVP refresh reduction includes the following features:

- RSVP message bundling using the bundle message
- RSVP Message ID to reduce message processing overhead
- Reliable delivery of RSVP messages using Message ID, Message Ack, and Message Nack
- Summary refresh to reduce the amount of information transmitted every refresh interval

The RSVP refresh reduction specification (RFC 2961) allows you to enable some or all of the above capabilities on a router. It also describes various procedures that a router can use to detect the refresh reduction capabilities of its neighbor.

The JUNOS software supports all of the refresh reduction extensions, some of which can be selectively enabled or disabled. The JUNOS software supports Message ID and therefore can perform reliable message delivery only for Path and Resv messages.

For information on how to configure RSVP refresh reduction, see “Configuring RSVP Refresh Reduction” on page 273.

MTU Signaling in RSVP

The maximum transmission unit (MTU) is the largest size packet or frame, in bytes, that can be sent in a network. An MTU that is too large might cause retransmissions. Too small an MTU might cause the router to send and handle relatively more header overhead and acknowledgments. There are default values for MTUs associated with various protocols. You can also explicitly configure an MTU on an interface.

When an LSP is created across a set of links with different MTU sizes, the ingress router does not know what the smallest MTU is on the LSP path. By default, the maximum packet size for the LSP is based on the MTU for the outgoing interface for the LSP on the ingress router.

If this MTU is larger than the MTU of one of the intermediate links, traffic might be dropped, because MPLS packets cannot be fragmented. Also, the ingress router is

not aware of this type of traffic loss, because the control plane for the LSP would still function normally.

To prevent this type of packet loss in MPLS LSPs, you can configure MTU signaling in RSVP. This feature is described in RFC 3209. Juniper Networks supports the Integrated Services object for MTU signaling in RSVP. The Integrated Services object is described in RFCs 2210 and 2215. MTU signaling in RSVP is disabled by default.

To avoid packet loss due to MTU mismatches, the ingress router needs to do the following:

- Signal the MTU on the RSVP LSP—To prevent packet loss from an MTU mismatch, the ingress router needs to know what the smallest MTU value is along the path taken by the LSP. Once this MTU value is obtained, the ingress router can assign it to the LSP.
- Fragment packets—Using the assigned MTU value, packets that exceed the size of the MTU can be fragmented into smaller packets on the ingress router before they are sent over the RSVP LSP.

Once both MTU signaling and packet fragmentation have been enabled on an ingress router, any route resolving to an RSVP LSP on this router uses the signaled MTU value. For information on how to configure this feature, see "Configuring MTU Signaling in RSVP" on page 290.

The following sections describe how MTU signaling in RSVP works:

- How the Correct MTU Is Signaled in RSVP on page 261
- Determining an Outgoing MTU Value on page 262
- MTU Signaling in RSVP Limitations on page 262

How the Correct MTU Is Signaled in RSVP

How the correct MTU is signaled in RSVP varies depending on whether the network devices (for example, routers) explicitly support MTU signaling in RSVP or not.

If the network devices support MTU signaling in RSVP, the following occur when you enable MTU signaling:

- The MTU is signaled from the ingress router to the egress router by means of the Adspec object. Before forwarding this object, the ingress router enters the MTU value associated with the interface over which the path message is sent. At each hop in the path, the MTU value in the Adspec object is updated to the minimum of the received value and the value of the outgoing interface.
- The ingress router uses the traffic specification (Tspec) object to specify the parameters for the traffic it is going to send. The MTU value signaled for the Tspec object at the ingress router is the maximum MTU value (9192 bytes). This value does not change en route to the egress router.
- When the Adspec object arrives at the egress router, the MTU value is correct for the path (meaning it is the smallest MTU value discovered). The egress router

compares the MTU value in the Adspec object to the MTU value in the Tspec object. It signals the smaller MTU using the Flowspec object in the Resv message.

- When the Resv object arrives at the ingress router, the MTU value in this object is used as the MTU for the next hops that use the LSP.

In a network where there are devices that do not support MTU signaling in RSVP, you might have the following behaviors:

- If the egress router does not support MTU signaling in RSVP, the MTU is set to the value of the outgoing interface on the ingress router. Setting the MTU to the value of the outgoing interface is the same as the default behavior when MTU signaling is not configured.
- A Juniper Networks transit router that does not support MTU signaling in RSVP always propagates an MTU value of 1500 in the Adspec object.

Determining an Outgoing MTU Value

The outgoing MTU value is the smaller of the values received in the Adspec object compared to the MTU value of the outgoing interface. The MTU value of the outgoing interface is determined as follows:

- If you configure an MTU value under the [family mpls] hierarchy level, this value is signaled.
- If you do not configure an MTU, the inet MTU is signaled.

MTU Signaling in RSVP Limitations

The following are limitations to the MTU signaling in RSVP feature:

- Changes in the MTU value might cause a temporary loss of traffic in the following situations:
  - For link protection and node protection, the MTU of the bypass is only signaled at the time the bypass becomes active. During the time it takes for the new path MTU to be propagated, packet loss might occur because of an MTU mismatch.
  - For fast reroute, the MTU of the path is updated only after the detour becomes active, causing a delay in an update to the MTU at the ingress router. Until the MTU is updated, packet loss might occur if there is an MTU mismatch.

    In both cases, only packets that are larger than the detour or bypass MTU are lost.
- When an MTU is updated, it triggers a change in the next hop. Any change in the next hop causes the route statistics to be lost.
- The minimum MTU supported for MTU signaling in RSVP is 1488 bytes. This value prevents a false or incorrectly configured value from being used.
- For single-hop LSPs, the MTU value displayed by the show commands is the RSVP-signaled value. However, this MPLS value is ignored and the correct IP value is used.

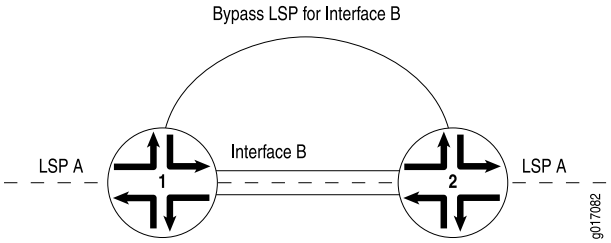
Link Protection

Link protection helps to ensure that traffic going over a specific interface to a neighboring router can continue to reach this router if that interface fails. When link protection is configured for an interface and an LSP that traverses this interface, a bypass LSP is created that will handle this traffic if the interface fails. The bypass LSP uses a different interface and path to reach the same destination. The path used can be configured explicitly, or you can rely on CSPF. The RSVP metric for the bypass LSP is set in the range of 20,000 through 29,999 (this value is not user configurable).

If a link-protected interface fails, traffic is quickly switched to the bypass LSP. Note that a bypass LSP cannot share the same egress interface with the LSPs it monitors.

In Figure 21 on page 263, link protection is enabled on Interface B between Router 1 and Router 2. It is also enabled on LSP A, an LSP that traverses the link between Router 1 and Router 2. If the link between Router 1 and Router 2 fails, traffic from LSP A is quickly switched to the bypass LSP generated by link protection.

Figure 21: Link Protection Creating a Bypass LSP for the Protected Interface



Although LSPs traversing an interface can be configured to take advantage of link protection, it is important to note that it is specifically the interface that benefits from link protection. If link protection is enabled on an interface but not on a particular LSP traversing that interface, then if the interface fails, that LSP will also fail.

NOTE: Link protection does not work on unnumbered interfaces.

To protect traffic over the entire route taken by an LSP, you should configure fast reroute. For more information, see "Configuring Fast Reroute" on page 71.

The following sections provide more information on link protection:

- Fast Reroute, Node Protection, and Link Protection on page 263
- Multiple Bypass LSPs on page 264

Fast Reroute, Node Protection, and Link Protection

RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*, describes two different types of traffic protection for RSVP-signaled LSPs:

- One-to-one backup—In the JUNOS software this type of traffic protection is provided by fast reroute. Each LSP requires a protecting LSP to be signaled at each hop except the egress router. This protecting LSP cannot be shared.
- Facility backup—This is sometimes called many-to-one backup. In the JUNOS software this type of traffic protection is provided by node and link protection. Each LSP requires a protecting LSP to be signaled at each hop except the egress router. Unlike fast reroute, this protecting LSP can be shared by other LSPs.

The information above is summarized in Table 9 on page 264.

Table 9: One-to-One Backup Compared with Facility Backup

	One-to-One Backup	Facility Backup
Name of the protecting LSP	Detour LSP	Bypass LSP
Sharing of the protecting LSP	Cannot be shared	Can be shared by multiple LSPs
JUNOS configuration statements	fast-reroute	node-link-protection and link-protection

Multiple Bypass LSPs

By default, link protection relies on a single bypass LSP to provide path protection for an interface. However, you can also specify multiple bypass LSPs to provide link protection for an interface. You can individually configure each of these bypass LSPs or create a single configuration for all of the bypass LSPs. If you do not configure the bypass LSPs individually, they all share the same path and bandwidth constraints.

The following algorithm describes how and when an additional bypass LSP is activated for an LSP:

1. If any currently active bypass can satisfy the requirements of the LSP (bandwidth, link protection, or node-link protection), the traffic is directed to that bypass.
2. If no active bypass LSP is available, scan through the manual bypass LSPs in first-in, first-out (FIFO) order, skipping those that are already active (each manual bypass can only be activated once). The first inactive manual bypass that can satisfy the requirements is activated and traffic is directed to that bypass.
3. If no manual bypass LSPs are available and if the max-bypasses statement activates multiple bypass LSPs for link protection, determine whether an automatically configured bypass LSP can satisfy the requirements. If an automatically configured bypass LSP is available and if the total number of active automatically configured bypass LSPs does not exceed the maximum bypass LSP limit (configured with the max-bypasses statement), activate another bypass LSP.

For information on how to configure multiple bypass LSPs for link protection, see "Configuring Bypass LSPs" on page 280.

Node Protection

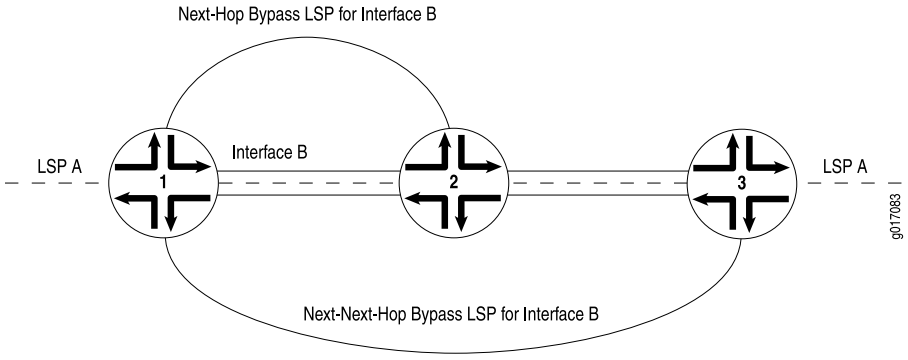
Node protection extends the capabilities of link protection. Link protection helps to ensure that traffic going over a specific interface to a neighboring router can continue to reach this router if that interface fails. Node protection ensures that traffic from an LSP traversing a neighboring router can continue to reach its destination even if the neighboring router fails.

When you enable node protection for an LSP, you must also enable link protection. Once enabled, node protection and link protection establish the following types of bypass LSPs:

- Next-hop bypass LSP—Provides an alternate route for an LSP to reach a neighboring router. This type of bypass LSP is established when you enable either node protection or link protection.
- Next-next-hop bypass LSP—Provides an alternate route for an LSP to get around a neighboring router en route to the destination router. This type of bypass LSP is established exclusively when node protection is configured.

In Figure 22 on page 265, both node protection and link protection are enabled on Interface B on Router 1. Both node protection and link protection are also enabled on LSP A, an LSP that traverses the link transiting Router 1, Router 2, and Router 3. If the link between Router 1 and Router 2 fails, traffic from LSP A is quickly switched to the next-hop bypass LSP generated by link protection. If Router 2 suffers a hardware or software failure, traffic from LSP A is switched to the next-next-hop bypass LSP generated by node protection.

Figure 22: Node Protection Creating a Next-Next-Hop Bypass LSP



The time needed by node protection to switch traffic to a next-next-hop bypass LSP can be significantly longer than the time needed by link protection to switch traffic to a next-hop bypass LSP. Link protection relies on a hardware mechanism to detect a link failure, allowing it to quickly switch traffic to a next-hop bypass LSP.

Node failures are often due to software problems on the node router. Node protection relies on the receipt of hello messages from a neighboring router to determine whether it is still functioning. The time it takes node protection to divert traffic partly depends on how often the node router sends hello messages and how long it takes the node-protected router to react to having not received a hello message. However,

once the failure is detected, traffic can be quickly diverted to the next-next-hop bypass LSP.

RSVP Graceful Restart

RSVP graceful restart allows a router undergoing a restart to inform its adjacent neighbors of its condition. The restarting router requests a grace period from the neighbor or peer, which can then cooperate with the restarting router. The restarting router can still forward MPLS traffic during the restart period; convergence in the network is not disrupted. The restart is not visible to the rest of the network, and the restarting router is not removed from the network topology. RSVP graceful restart can be enabled on both transit routers and ingress routers. It is available for both point-to-point LSPs and point-to-multipoint LSPs.

RSVP graceful restart is described in the following sections:

- RSVP Graceful Restart Standard on page 266
- RSVP Graceful Restart Terminology on page 266
- RSVP Graceful Restart Operation on page 267
- Processing the Restart Cap Object on page 268

RSVP Graceful Restart Standard

RSVP graceful restart is described in RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions* (only Section 9, *Fault Handling*).

RSVP Graceful Restart Terminology

The following terminology is specific to RSVP graceful restart:

- Restart time (in milliseconds)—The default value is 60,000 milliseconds (1 minute). The restart time is advertised in the hello message. The time indicates how long a neighbor should wait to receive a hello message from a restarting router before declaring that router dead and purging states.

  The JUNOS software can override a neighbor's advertised restart time if the time is greater than one-third the local restart time. For example, given the default restart time of 60 seconds, a router would wait 20 seconds or less to receive a hello message from a restarting neighbor. If the restart time is zero, the restarting neighbor can immediately be declared dead.

- Recovery time (in milliseconds)—Applies only when the control channel is up (the hello exchange is complete) before the restart time. Applies only to nodal faults.

  When a graceful restart is in progress, the time left to complete a recovery is advertised. At other times, this value is zero. The maximum advertised recovery time is 2 minutes (120,000 milliseconds).

  During the recovery time, a restarting node attempts to recover its lost states with assistance from its neighbors. The neighbor of the restarting node must

send the path messages with the recovery labels to the restarting node within a period of one-half the recovery time. The restarting node considers its graceful restart complete after its advertised recovery time.

RSVP Graceful Restart Operation

For RSVP graceful restart to function, the feature must be enabled on the global routing instance. RSVP graceful restart can be disabled at the protocol level (for RSVP alone) or at the global level for all protocols.

RSVP graceful restart requires the following of a restarting router and the router's neighbors:

- For the restarting router, RSVP graceful restart attempts to maintain the routes installed by RSVP and the allocated labels, so that traffic continues to be forwarded without disruption. RSVP graceful restart is done quickly enough to reduce or eliminate the impact on neighboring nodes.
- The neighboring routers must have RSVP graceful restart helper mode enabled, thus allowing them to assist a router attempting to restart RSVP.

An object called Restart Cap that is sent in RSVP hello messages advertises a node's restart capability. The neighboring node sends a Recover Label object to the restarting node to recover its forwarding state. This object is essentially the old label that the restarting node advertised before the node went down.

The following lists the RSVP graceful restart behaviors, which vary depending on the configuration and on which features are enabled:

- If you disable helper mode, the JUNOS software does not attempt to help a neighbor restart RSVP. Any information that arrives with a Restart Cap object from a neighbor is ignored.
- When you enable graceful restart under the routing instance configuration, the router can restart gracefully with the help of its neighbors. RSVP advertises a Restart Cap object (RSVP RESTART) in hello messages in which restart and recovery times are specified (neither value is 0).
- If you explicitly disable RSVP graceful restart under the [protocols rsvp] hierarchy level, the Restart Cap object is advertised with restart and recovery times specified as 0. The restart of neighboring routers is supported (unless helper mode is disabled), but the router itself does not preserve the RSVP forwarding state and cannot recover its control state.
- If after a restart RSVP realizes that no forwarding state has been preserved, the Restart Cap object is advertised with restart and recovery times specified as 0.
- If graceful restart and helper mode are disabled, RSVP graceful restart is completely disabled. The router neither recognizes nor advertises the RSVP graceful restart objects.

You cannot explicitly configure values for the restart and recovery times.

Unlike other protocols, there is no way for RSVP to determine that it has completed a restart procedure, other than a fixed timeout. All RSVP graceful restart procedures

are timer-based. A show rsvp version command might indicate that the restart is still in progress even if all RSVP sessions are back up and the routes are restored.

Processing the Restart Cap Object

The following assumptions are made about a neighbor based on the Restart Cap object (assuming that a control channel failure can be distinguished unambiguously from a node restart):

- A neighbor that does not advertise the Restart Cap object in its hello messages cannot assist a router with state or label recovery, nor can it perform an RSVP graceful restart.
- After a restart, a neighbor advertising a Restart Cap object with a restart time equal to any value and a recovery time equal to 0 has not preserved its forwarding state. When a recovery time equals 0, the neighbor is considered dead and any states related to this neighbor are purged, regardless of the value of the restart time.
- After a restart, a neighbor advertising recovery-time with a value other than 0 can keep or has kept the forwarding state. If the local router is helping its neighbor with restart or recovery procedures, it sends a Recover Label object to this neighbor.

Chapter 12

RSVP Configuration Guidelines

To configure the Resource Reservation Protocol (RSVP), you include the rsvp statement:

```
protocols {
    rsvp {
        disable;
        fast-reroute optimize-timer seconds;
    graceful-deletion-timeout seconds;
        graceful-restart {
            disable;
            helper-disable;
            maximum-helper-recovery-time seconds;
            maximum-helper-restart-time seconds;
        }
        interface interface-name {
            disable;
            (aggregate | no-aggregate);
            authentication-key key;
            bandwidth bps;
            hello-interval seconds;
            link-protection {
                disable;
                admin-group {
                    exclude group-names;
                    include-all group-names;
                    include-any group-names;
                }
                bandwidth bps;
                bypass bypass-name {
                    bandwidth bps;
                    hop-limit number;
                    no-cspf;
                    path address <strict | loose>;
                    priority setup-priority reservation-priority;
                    to address;
                }
                class-of-service cos-value;
                hop-limit number;
                max-bypasses number;
                no-cspf;
                no-node-protection;
                optimize-timer seconds;
                path address <strict | loose>;
```

```
            priority setup-priority reservation-priority;
            subscription percent;
        }
        (reliable | no-reliable);
        subscription percentage {
            ct0 percentage;
            ct1 percentage;
            ct2 percentage;
            ct3 percentage;
        }
        update-threshold percentage;
    }
    keep-multiplier number;
    load-balance {
        bandwidth;
    }
    peer-interface peer-interface-name {
        (aggregate | no-aggregate);
        authentication-key key;
        disable;
        hello-interval seconds;
        (reliable | no-reliable);
    }
    preemption {
        (aggressive | disabled | normal);
        soft-preemption {
            cleanup-timer seconds;
        }
    }
    refresh-time seconds;
    traceoptions {
        file filename <replace> <size size> <files number> <no-stamp>
            <world-readable | no-world-readable>;
        flag flag <flag-modifier> <disable>;
    }
    tunnel-services {
        devices device-name;
    }
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols]
- [edit logical-systems *logical-system-name* protocols]

By default, RSVP is disabled.

This chapter describes the minimum required RSVP configuration and discusses the following configuration tasks:

- Minimum RSVP Configuration on page 271
- Configuring RSVP and MPLS on page 271
- Configuring RSVP Interface Properties on page 273
- Configuring Node Protection or Link Protection on page 278

- Configuring RSVP Graceful Restart on page 286
- Configuring RSVP LSP Load Balancing on page 287
- Configuring RSVP Timers on page 289
- Preempting RSVP Sessions on page 290
- Configuring MTU Signaling in RSVP on page 290
- Configuring RSVP to Pop the Label on the Ultimate-Hop Router on page 291
- Disabling Adjacency Down and Neighbor Down Notification in IS-IS and OSPF on page 292
- Enabling Ultimate-Hop Popping on Point-to-Multipoint LSPs on page 293
- Tracing RSVP Protocol Traffic on page 294

Minimum RSVP Configuration

To enable RSVP on a single interface, include the **rsvp** statement and specify the interface using the **interface** statement. This is the minimum RSVP configuration. All other RSVP configuration statements are optional.

```
rsvp {
    interface interface-name;
}
```

You can include these statements at the following hierarchy levels:

- [edit protocols]
- [edit logical-systems *logical-system-name* protocols]

To enable RSVP on all interfaces, specify **all** for *interface-name*.

If you have configured interface properties on a group of interfaces and want to disable RSVP on one of the interfaces, include the **disable** statement:

```
protocols {
    rsvp {
        interface interface-name {
            disable;
        }
    }
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name*]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*]

Configuring RSVP and MPLS

The primary purpose of the JUNOS RSVP software is to support dynamic signaling within label-switched paths (LSPs). When you enable both MPLS and RSVP on a

router, MPLS becomes a client of RSVP. No additional configuration is required to bind MPLS and RSVP.

You can configure MPLS to set up signaled paths by using the label-switched-path statement at the [edit protocols mpls] hierarchy level. Each LSP translates into a request for RSVP to initiate an RSVP session. This request is passed through the internal interface between label switching and RSVP. After examining the request information, checking RSVP states, and checking the local routing tables, RSVP initiates one session for each LSP. The session is sourced from the local router and is destined for the target of the LSP.

When an RSVP session is successfully created, the LSP is set up along the paths created by the RSVP session. If the RSVP session is unsuccessful, RSVP notifies MPLS of its status. It is up to MPLS to initiate backup paths or continue retrying the initial path.

To pass label-switching signaling information, RSVP supports four additional objects: Label Request object, Label object, Explicit Route object, and Record Route object. For an LSP to be set up successfully, all routers along the path must support MPLS, RSVP, and the four objects. Of the four objects, the Record Route object is not mandatory.

To configure MPLS and make it a client of RSVP, do the following:

- Enable MPLS on all routers that will participate in the label switching (this is, on all routers that might be part of a label-switching path).
- Enable RSVP on all routers and on all router interfaces that form the LSP.
- Configure the routers at the beginning of the LSP.

Example: Configuring RSVP and MPLS

The following shows a sample configuration for a router at the beginning of an LSP:

```
[edit]
protocols {
    mpls {
        label-switched-path sf-to-london {
            to 192.168.1.4;
        }
    }
    rsvp {
        interface so-0/0/0;
    }
}
```

The following shows a sample configuration for all the other routers that form the LSP:

```
[edit]
protocols {
    mpls {
        interface so-0/0/0;
    }
```

```
    rsvp {
        interface so-0/0/0;
    }
}
```

Configuring RSVP Interface Properties

The following sections describe how to configure the interface properties for RSVP:

- Configuring RSVP Refresh Reduction on page 273
- Configuring the RSVP Hello Interval on page 276
- Configuring RSVP Authentication on page 276
- Configuring the Bandwidth Subscription for Class Types on page 277
- Configuring the RSVP Update Threshold on an Interface on page 277
- Configuring RSVP for Unnumbered Interfaces on page 278

Configuring RSVP Refresh Reduction

You can configure RSVP refresh reduction on each interface. The following statements allow you to configure the RSVP refresh reduction features:

- aggregate—Enable all RSVP refresh reduction features: RSVP message bundling, RSVP message ID, reliable message delivery, and summary refresh.
- no-aggregate—Disable RSVP message bundling and summary refresh.
- reliable—Enable RSVP message ID and reliable message delivery.
- no-reliable—Disable RSVP message ID, reliable message delivery, and summary refresh.

For more information on RSVP refresh reduction, see “RSVP Refresh Reduction” on page 259.

Table 10 on page 273 lists various combinations of the RSVP refresh reduction configuration statements and how they alter the behavior of the JUNOS software. The table describes only the expected behavior based on the configuration on the router. The actual behavior is dictated not only by the local configuration on this router, but also on the refresh reduction capabilities of its RSVP neighbors. Note that by configuring the aggregate statement, you enable all RSVP refresh reduction features, including reliable message delivery.

Table 10: RSVP Refresh Reduction Behavior

Configuration Statement	Send Capability	Receive Capability
aggregate or aggregate and reliable	RR bit = 1BundleMessage ID (Path/Resv messages)Ack/Nack (all messages)Summary Refresh	BundleAck/Nack (all messages)Summary Refresh
aggregate and no-reliable	RR bit = 1BundleAck/Nack (all messages)	BundleMessage ID (all messages)

Table 10: RSVP Refresh Reduction Behavior *(continued)*

Configuration Statement	Send Capability	Receive Capability
reliable or reliable and no-aggregate	RR bit = 0Message ID (Path/Resv messages)Ack/Nack (all messages)	BundleMessage ID (all messages)Ack/Nack

The send capability shown in Table 10 on page 273 lists the RSVP messages and objects related to RSVP refresh reduction that the router is capable of sending. This does not mean that all these messages are exchanged between this router and a neighbor. For example, if the router is configured with the aggregate statement, but RSVP refresh reduction is not enabled on its neighbor, then no Summary Refresh message is sent to this neighbor even though the router is capable of sending it.

The receive capability shown in Table 10 on page 273 lists the messages and objects related to RSVP refresh reduction that the router is capable of receiving and processing without generating any errors or resulting in error conditions.

If the no-reliable statement is configured on the router (reliable message delivery is disabled), the router accepts RSVP messages that include the Message ID object but ignore the Message ID object and continue performing standard message processing. No error is generated in this case, and RSVP operates normally.

However, not all combinations between two neighbors with different refresh reduction capabilities function correctly. For example, a router is configured with either the aggregate statement and no-reliable statement or with the reliable and no-aggregate statements. If an RSVP neighbor sends a Summary Refresh object to this router, no error is generated, but the Summary Refresh object cannot be processed. Consequently, RSVP states can time out on this router if the neighbor is relying only on Summary Refresh to refresh those RSVP states.

We recommend, unless there are specific requirements, that you configure RSVP refresh reduction in a similar manner on each RSVP neighbor.

To enable all RSVP refresh reduction features on an interface, include the aggregate statement:

```
aggregate;
```

You can include this statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name*]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*]

To disable RSVP message bundling and summary refresh, include the no-aggregate statement:

```
no-aggregate;
```

You can include this statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name*]

- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*]

To enable RSVP message ID and reliable message delivery on an interface, include the reliable statement:

```
reliable;
```

You can include this statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name*]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*]

To disable RSVP message ID, reliable message delivery, and summary refresh, include the no-reliable statement:

```
no-reliable;
```

You can include this statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name*]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*]

Determining the Refresh Reduction Capability of RSVP Neighbors

To determine the RSVP refresh reduction capability of an RSVP neighbor, you need the following information:

- The RR bit advertised by the neighbor
- The local configuration of RSVP refresh reduction
- The actual RSVP messages received from the neighbor

To obtain this information, you can issue a show rsvp neighbor detail command. The following is a sample of output from this command:

```
user@host> show rsvp neighbor detail
RSVP neighbor: 6 learned
    Address: 192.168.224.178 via: fxp1.0 status: Up
      Last changed time: 10:06, Idle: 5 sec, Up cnt: 1, Down cnt: 0
      Message received: 36
      Hello: sent 69, received: 69, interval: 9 sec
      Remote instance: 0x60b8feba, Local instance: 0x74bc7a8d
      Refresh reduction:  not operational

    Address: 192.168.224.186 via: fxp2.0 status: Down
      Last changed time: 10:17, Idle: 40 sec, Up cnt: 0, Down cnt: 0
      Message received: 6
      Hello: sent 20, received: 0, interval: 9 sec
      Remote instance: 0x0, Local instance: 0x2ae1b339
      Refresh reduction:  incomplete
        Remote end: disabled, Ack-extension: enabled

    Address: 192.168.224.188 via: fxp2.0 status: Up
      Last changed time: 4:15, Idle: 0 sec, Up cnt: 1, Down cnt: 0
```

```
Message received: 55
Hello: sent 47, received: 31, interval: 9 sec
Remote instance: 0x6436a35b, Local instance: 0x663849f0
Refresh reduction:  operational
  Remote end: enabled, Ack-extension: enabled
```

For more information on the show rsvp neighbor detail command, see the *JUNOS Routing Protocols and Policies Command Reference*.

Configuring the RSVP Hello Interval

RSVP monitors the status of the interior gateway protocol (IGP) (IS-IS or OSPF) neighbors and relies on the IGP protocols to detect when a node fails. If an IGP protocol declares a neighbor down (because hello packets are no longer being received), RSVP also brings down that neighbor. However, the IGP protocols and RSVP still act independently when bringing a neighbor up.

For Juniper Networks routers, configuring a shorter or longer RSVP hello interval has no impact on whether or not an RSVP session is brought down. RSVP sessions are kept up even if RSVP hello packets are no longer being received. RSVP sessions are maintained until either the router stops receiving IGP hello packets or the RSVP Path and Resv messages time out.

However, the RSVP hello interval might impact when another vendor's equipment brings down an RSVP session. For example, a neighboring non-Juniper Networks router might be configured to monitor RSVP hello packets.

To modify how often RSVP sends hello packets, include the hello-interval statement:

hello-interval *seconds*;

For a list of hierarchy levels at which you can include this statement, see the statement summary section.

Configuring RSVP Authentication

All RSVP protocol exchanges can be authenticated to guarantee that only trusted neighbors participate in setting up reservations. By default, RSVP authentication is disabled.

RSVP authentication uses an HMAC-MD5 message-based digest. This scheme produces a message digest based on a secret authentication key and the message contents. (The message contents also include a sequence number.) The computed digest is transmitted with RSVP messages. Once you have configured authentication, all received and transmitted RSVP messages with all neighbors are authenticated on this interface.

MD5 authentication provides protection against forgery and message modification. It also can prevent replay attacks. However, it does not provide confidentiality, because all messages are sent in clear text.

By default, authentication is disabled. To enable authentication, configure a key on each interface by including the authentication-key statement:

authentication-key *key*;

You can include this statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name*]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*]

Configuring the Bandwidth Subscription for Class Types

By default, RSVP allows all of a class type's bandwidth (100 percent) to be used for RSVP reservations. When you oversubscribe a class type for a multiclass LSP, the aggregate demand of all RSVP sessions is allowed to exceed the actual capacity of the class type.

For detailed instructions on how to configure the bandwidth subscription for class types, see "Configuring the Bandwidth Subscription Percentage for LSPs" on page 126.

Configuring the RSVP Update Threshold on an Interface

The interior gateway protocols (IGPs) maintain the traffic engineering database, but the current available bandwidth on the traffic engineering database links originates from RSVP. When a link's bandwidth changes, RSVP informs the IGPs, which can then update the TED and forward the new bandwidth information to all network nodes. The network nodes then know how much bandwidth is available on the traffic engineering database link (local or remote), and CSPF can correctly compute the paths.

However, IGP updates can consume excessive system resources. Depending on the number of nodes in a network, it might not be desirable to perform an IGP update for small changes in bandwidth. By configuring the update-threshold statement at the [edit protocols rsvp] hierarchy level, you can adjust the threshold at which a change in the reserved bandwidth triggers an IGP update.

You can configure a value of from 1 percent through 20 percent (the default is 10 percent) for when to trigger an IGP update. If the change in the reserved bandwidth is greater than or equal to the configured threshold percentage of the static bandwidth on that interface, then an IGP update occurs. For example, if you have configured the update-threshold statement to be 15 percent and the router discovers that the reserved bandwidth on a link has changed by 10 percent of the link bandwidth, RSVP does not trigger an IGP update. However, if the reserved bandwidth on a link changes by 20 percent of the link bandwidth, RSVP triggers an IGP update.

To adjust the threshold at which a change in the reserved bandwidth triggers an IGP update, include the update-threshold statement:

update-threshold *percentage*;

You can include this statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name*]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*]

Because of the update threshold, it is possible for Constrained Shortest Path First (CSPF) to compute a path using outdated traffic engineering database bandwidth information on a link. If RSVP attempts to establish an LSP over that path, it might find that there is insufficient bandwidth on that link. When this happens, RSVP triggers an IGP traffic engineering database update, flooding the updated bandwidth information on the network. CSPF can then recompute the path by using the updated bandwidth information, and attempt to find a different path, avoiding the congested link. Note that this functionality is the default and does not need any additional configuration.

You can configure the rsvp-error-hold-time statement at the [edit protocols mpls] hierarchy level or the [edit logical-systems *logical-system-name* protocols mpls] hierarchy level to improve the accuracy of the traffic engineering database (including the accuracy of bandwidth estimates for LSPs) using information provided by PathErr messages. See "Improving TED Accuracy with RSVP PathErr Messages" on page 101.

Configuring RSVP for Unnumbered Interfaces

The JUNOS software supports RSVP traffic engineering over unnumbered interfaces. Traffic engineering information about unnumbered links is carried in the IGP traffic engineering extensions for OSPF and IS-IS as described in RFC 4203, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*, and RFC 4205, *Intermediate System to Intermediate System (IS-IS) Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*. Unnumbered links can also be specified in the MPLS traffic engineering signaling as described in RFC 3477, *Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)*. This feature allows you avoid having to configure IP addresses for each interface participating in the RSVP-signalled network.

To configure RSVP for unnumbered interfaces, you must configure the router with a router ID using the router-id statement specified at the [edit routing-options] hierarchy level. The router ID must be available for routing (you can typically use the loopback address). The RSVP control messages for the unnumbered links are sent using the router ID address (rather than a randomly selected address).

To configure link protection and fast reroute on a router with unnumbered interfaces enabled, you must configure at least two addresses. We recommend that you configure a secondary interface on the loopback in addition to configuring the router ID.

Configuring Node Protection or Link Protection

When enabled, node protection or link protection provides bypass LSPs to the next-hop or next-next-hop routers for the LSPs traversing the configured router. To extend node protection or link protection along the entire path used by an LSP, node protection or link protection must be configured on each router that the LSP traverses.

To enable node protection or link protection, see the following sections:

- Configuring Node Protection or Link Protection on an LSP on page 279
- Configuring Link Protection on the Interfaces Used by the LSPs on page 279

Configuring Node Protection or Link Protection on an LSP

To enable node protection or link protection, configure the node-link-protection statement or the link-protection statement for each LSP that you want protected. You must also configure the link-protection statement on all unidirectional RSVP interfaces that the LSPs traverse.

To configure node protection for the LSP, include the node-link-protection statement:

```
node-link-protection;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name*]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]

To configure link protection for the LSP, include the link-protection statement:

```
link-protection;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name*]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]

Configuring Link Protection on the Interfaces Used by the LSPs

Whether you are configuring node protection or link protection, configure the link-protection statement on the RSVP interfaces used by the LSPs you configured in "Configuring Node Protection or Link Protection on an LSP" on page 279.

To configure link protection on the interfaces used by the LSPs, include the link-protection statement:

```
link-protection {
    disable;
    admin-group
        exclude group-names;
        include-all group-names;
        include-any group-names;
    }
    bandwidth bps;
    bypass bypass-name {
        bandwidth bps;
        hop-limit number;
        no-cspf;
        path address <strict | loose>;
        priority setup-priority reservation-priority;
        to address;
    }
    class-of-service cos-value;
    hop-limit number;
    max-bypasses number;
```

```
    no-cspf;
    no-node-protection;
    optimize-timer seconds;
    path address <strict | loose>;
    priority setup-priority reservation-priority;
    subscription percent {
      ct0 percent;
      ct1 percent;
      ct2 percent;
      ct3 percent;
    }
  }
```

You can include this statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name*]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*]

All the statements under link-protection are optional.

The following sections describe how to configure link protection:

- Configuring Bypass LSPs on page 280
- Configuring Administrative Groups for Bypass LSPs on page 281
- Configuring the Bandwidth for Bypass LSPs on page 282
- Configuring the Class of Service for Bypass LSPs on page 282
- Configuring the Hop Limit for Bypass LSPs on page 283
- Configuring the Maximum Number of Bypass LSPs on page 283
- Disabling CSPF for Bypass LSPs on page 284
- Disabling Node Protection for Bypass LSPs on page 284
- Configuring the Optimization Interval for Bypass LSPs on page 284
- Configuring an Explicit Path for Bypass LSPs on page 285
- Configuring the Amount of Bandwidth Subscribed for Bypass LSPs on page 285
- Configuring Priority and Preemption for Bypass LSPs on page 286

Configuring Bypass LSPs

You can configure specific bandwidth and path constraints for a bypass LSP. You can also individually configure each bypass LSP generated when you enable multiple bypass LSPs. If you do not configure the bypass LSPs individually, they all share the same path and bandwidth constraints (if any).

If you specify the bandwidth, hop-limit, and path statements for the bypass LSP, these values take precedence over the values configured at the [edit protocols rsvp interface *interface-name* link-protection] hierarchy level. The other attributes (subscription, no-node-protection, and optimize-timer) are inherited from the general constraints.

To configure a bypass LSP, include the bypass statement:

```
bypass bypass-name {
    bandwidth bps;
    class-of-service cos-value;
    hop-limit number;
    no-cspf;
    path address <strict | loose>;
    priority setup-priority reservation-priority;
    to address;
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name* link-protection]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection]

Configuring the Next-Hop or Next-Next-Hop Node Address for Bypass LSPs

If you configure a bypass LSP, you must also configure the to statement. The to statement specifies the address for the interface of the immediate next-hop node (for link protection) or the next-next-hop node (for node-link protection). The address specified determines whether this is a link protection bypass or a node-link protection bypass. On multiaccess networks (for example, a LAN), this address is also used to specify which next-hop node is being protected.

Configuring Administrative Groups for Bypass LSPs

Administrative groups, also known as link coloring or resource class, are manually assigned attributes that describe the "color" of links, such that links with the same color conceptually belong to the same class. You can use administrative groups to implement a variety of policy-based LSP setups. You can configure administrative groups for bypass LSPs. For more information about configuring administrative groups, see "Configuring Administrative Groups" on page 89.

To configure administrative groups for bypass LSPs, include the admin-group statement:

```
admin-group {
    exclude group-names;
    include-all group-names;
    include-any group-names;
}
```

To configure an administrative group for all of the bypass LSPs, include the admin-group statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name* link-protection]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection]

To configure an administrative groups for a specific bypass LSP, include the admin-group statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]

- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]

Configuring the Bandwidth for Bypass LSPs

You can specify the amount of bandwidth allocated for automatically generated bypass LSPs or you can individually specify the amount of bandwidth allocated for each LSP.

To specify the bandwidth allocation, include the bandwidth statement:

```
bandwidth bps;
```

For automatically generated bypass LSPs, include the bandwidth statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name* link-protection]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection]

For individually configured bypass LSPs, include the bandwidth statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]

If you have enabled multiple bypass LSPs, this statement is required. See also "Configuring the Maximum Number of Bypass LSPs" on page 283.

Configuring the Class of Service for Bypass LSPs

You can specify the class-of-service value for bypass LSPs by including the class-of-service statement:

```
class-of-service cos-value;
```

To apply a class-of-service value to all the automatically generated bypass LSPs, include the class-of-service statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name* link-protection]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection]

To configure a class-of-service value for a specific bypass LSPs, include the class-of-service statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]

Configuring the Hop Limit for Bypass LSPs

You can specify the maximum number of hops a bypass can traverse. By default, each bypass can traverse a maximum of 255 hops (the ingress and egress routers count as one hop each, so the minimum hop limit is two).

To configure the hop limit for bypass LSPs, include the hop-limit statement:

```
hop-limit number;
```

For automatically generated bypass LSPs, include the hop-limit statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name* link-protection]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection]

For individually configured bypass LSPs, include the hop-limit statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]

Configuring the Maximum Number of Bypass LSPs

You can specify the maximum number of dynamic bypass LSPs permitted for protecting an interface using the max-bypasses statement at the [edit protocols rsvp interface *interface-name* link-protection] hierarchy level. When this statement is configured, multiple bypasses for link protection are enabled. Call admission control (CAC) is also enabled.

By default, this option is disabled and only one bypass is enabled for each interface. You can configure a value of between 0 through 99 for the max-bypasses statement. Configuring a value of 0 prevents the creation of any dynamic bypass LSPs for the interface. If you configure a value of 0 for the max-bypasses statement, you need to configure one or more static bypass LSPs to enable link protection on the interface.

If you configure the max-bypasses statement, you must also configure the bandwidth statement (discussed in “Configuring the Bandwidth for Bypass LSPs” on page 282).

To configure the maximum number of bypass LSPs for a protected interface, include the max-bypasses statement:

```
max-bypasses number;
```

You can include this statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name* link-protection]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection]

Disabling CSPF for Bypass LSPs

Under certain circumstances, you might need to disable CSPF computation for bypass LSPs and use the configured Explicit route object (ERO) if available. For example, a bypass LSP might need to traverse multiple OSPF areas or IS-IS levels, preventing the CSPF computation from working. To ensure that link and node protection function properly in this case, you have to disable CSPF computation for the bypass LSP.

You can disable CSPF computation for all bypass LSPs or for specific bypass LSPs.

To disable CSPF computation for bypass LSPs, include the no-cspf statement:

```
no-cspf;
```

For a list of hierarchy levels where you can include this statement, see the statement summary for this statement.

Disabling Node Protection for Bypass LSPs

You can disable node protection on the RSVP interface. Link protection remains active. When this option is configured, the router can only initiate a next-hop bypass, not a next-next-hop bypass.

To disable node protection for bypass LSPs, include the no-node-protection statement:

```
no-node-protection;
```

You can include this statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name* link-protection]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection]

Configuring the Optimization Interval for Bypass LSPs

You can configure an optimization interval for bypass LSPs. At the end of this interval, an optimization process is initiated that attempts to either minimize the number of bypasses currently in use, minimize the total amount of bandwidth reserved for all of the bypasses, or both. You can configure an optimization interval from 1 through 65,535 seconds. A default value of 0 disables bypass LSP optimization.

To configure the optimization interval for bypass LSPs, include the optimize-timer statement:

```
optimize-timer seconds;
```

You can include this statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name* link-protection]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection]

Configuring an Explicit Path for Bypass LSPs

By default, when you establish a bypass LSP to an adjacent neighbor, CSPF is used to discover the least-cost path. The path statement allows you to configure an explicit path (a sequence of strict or loose routes), giving you control over where and how the bypass LSP is established. To configure an explicit path, include the path statement:

```
path address <strict | loose>;
```

For automatically generated bypass LSPs, include the path statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name* link-protection]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection]

For individually configured bypass LSPs, include the path statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]

Configuring the Amount of Bandwidth Subscribed for Bypass LSPs

You can configure the amount of bandwidth subscribed to bypass LSPs. You can configure the bandwidth subscription for the whole bypass LSP or for each class type that might traverse the bypass LSP. You can configure any value between 1 percent and 65,535 percent. By configuring a value less than 100 percent, you are undersubscribing the bypass LSPs. By configuring a value greater than 100 percent, you are oversubscribing the bypass LSPs.

The ability to oversubscribe the bandwidth for the bypass LSPs makes it possible to more efficiently use network resources. You can configure the bandwidth for the bypass LSPs based on the average network load as opposed to the peak load.

To configure the amount of bandwidth subscribed for bypass LSPs, include the subscription statement:

```
subscription percentage {
    ct0 percentage;
    ct1 percentage;
    ct2 percentage;
    ct3 percentage;
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols rsvp interface *interface-name* link-protection]
- [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection]

Configuring Priority and Preemption for Bypass LSPs

When there is insufficient bandwidth to establish a more important LSP, you might want to tear down a less important existing LSP to release the bandwidth. You do this by preempting the existing LSP.

For more detailed information on configuring setup priority and reservation priority for LSPs, see "Configuring Priority and Preemption for LSPs" on page 95.

To configure the bypass LSP's priority and preemption properties, include the priority statement:

priority *setup-priority reservation-priority*;

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Configuring RSVP Graceful Restart

The following RSVP graceful restart configurations are possible:

- Graceful restart and helper mode are both enabled (the default).
- Graceful restart is enabled but helper mode is disabled. A router configured in this way can restart gracefully, but cannot help a neighbor with its restart and recovery procedures.
- Graceful restart is disabled but helper mode is enabled. A router configured in this way cannot restart gracefully, but can help a restarting neighbor.
- Graceful restart and helper mode both are disabled. This configuration completely disables RSVP graceful restart (including restart and recovery procedures and helper mode). The router behaves like a router that does not support RSVP graceful restart.

The following sections describe how to configure RSVP graceful restart:

- Enabling Graceful Restart on the Router on page 286
- Disabling Graceful Restart for RSVP on page 287
- Disabling RSVP Helper Mode on page 287
- Configuring the Maximum Helper Recovery Time on page 287
- Configuring the Maximum Helper Restart Time on page 287

Enabling Graceful Restart on the Router

To enable graceful restart for RSVP, you need to enable graceful restart for all the protocols that support graceful restart on the router. For more information about graceful restart, see the *JUNOS Routing Protocols Configuration Guide*.

To enable graceful restart on the router, include the graceful-restart statement:

graceful-restart;

You can include this statement at the following hierarchy levels:

- [edit routing-options]
- [edit logical-systems *logical-system-name* routing-options]

Disabling Graceful Restart for RSVP

By default, RSVP graceful restart and RSVP helper mode are enabled when you enable graceful restart. However, you can disable one or both of these capabilities.

To disable RSVP graceful restart and recovery, include the disable statement at the [edit protocols rsvp graceful-restart] hierarchy level:

```
disable;
```

Disabling RSVP Helper Mode

To disable RSVP helper mode, include the helper-disable statement at the [edit protocols rsvp graceful-restart] hierarchy level:

```
helper-disable;
```

Configuring the Maximum Helper Recovery Time

To configure the amount of time the router retains the state of its RSVP neighbors while they undergo a graceful restart, include the maximum-helper-recovery-time statement at the [edit protocols rsvp graceful-restart] hierarchy level. This value is applied to all neighboring routers, so it should be based on the time required by the slowest RSVP neighbor to recover.

```
maximum-helper-recovery-time seconds;
```

Configuring the Maximum Helper Restart Time

To configure the delay between when the router discovers that a neighboring router has gone down and when it declares the neighbor down, include the maximum-helper-restart-time statement at the [edit protocols rsvp graceful-restart] hierarchy level. This value is applied to all neighboring routers, so it should be based on the time required by the slowest RSVP neighbor to restart.

```
maximum-helper-restart-time seconds;
```

Configuring RSVP LSP Load Balancing

By default, when you have configured several RSVP LSPs to the same egress router, the LSP with the lowest metric is selected and carries all traffic. If all of the LSPs have the same metric, one of the LSPs is selected at random and all traffic is forwarded over it.

Alternatively, you can load balance traffic across all of the LSPs by enabling per-packet load balancing.

To enable per-packet load balancing on an ingress LSP, configure the policy-statement statement as follows:

```
[edit policy-options]
policy-statement policy-name {
    then {
        load-balance per-packet;
    }
    accept;
}
```

You then need to apply this statement as an export policy to the forwarding table. For more information on how to configure the policy-statement statement, see the *JUNOS Policy Framework Configuration Guide*.

Once per-packet load balancing is applied, traffic is distributed equally between the LSPs (by default).

You need to configure per-packet load balancing if you want to enable PFE fast reroute. To enable PFE fast reroute, include the policy statement for per-packet load balancing shown in this section in the configuration of each of the routers where a reroute might take place. See also "Configuring Fast Reroute" on page 71.

You can also load-balance the traffic between the LSPs in proportion to the amount of bandwidth configured for each LSP. This capability can better distribute traffic in networks with asymmetric bandwidth capabilities across external links, since the configured bandwidth of an LSP typically reflects the traffic capacity of that LSP.

To configure RSVP LSP load balancing, include the load-balance statement with the bandwidth option:

```
load-balance {
    bandwidth;
}
```

You can configure this statement at the following hierarchy levels:

- [edit logical-systems *logical-system-name* protocols rsvp]
- [edit protocols rsvp]

Keep the following information in mind when you use the load-balance statement:

- If you configure the load-balance statement, the behavior of currently running LSPs is not altered. To force currently running LSPs to use the new behavior, you can issue a clear mpls lsp command.
- The load-balance statement only applies to ingress LSPs that have per-packet load balancing enabled.
- For differentiated services aware traffic engineered LSPs, the bandwidth of an LSP is calculated by summing the bandwidth of all of the class types.

Configuring RSVP Timers

RSVP uses two related timing parameters:

- refresh-time—The refresh time controls the interval between the generation of successive refresh messages. The default value for the refresh time is 45 seconds. This number is derived from the refresh-time statement's default value of 30, multiplied by a fixed value of 1.5. This computation differs from RFC 2205, which states that the refresh time should be multiplied by a random value in the range from 0.5 through 1.5.

  Refresh messages include path and Resv messages. Refresh messages are sent periodically so that reservation states in neighboring nodes do not time out. Each path and Resv message carries the refresh timer value, and the receiving node extracts this value from the messages.

- keep-multiplier—The keep multiplier is a small, locally configured integer from 1 through 255. The default value is 3. It indicates the number of messages that can be lost before a particular state is declared stale and must be deleted. The keep multiplier directly affects the lifetime of an RSVP state.

To determine the lifetime of a reservation state, use the following formula:

lifetime = (*keep-multiplier* + 0.5) x (1.5 x *refresh-time*)

In the worst case, (*keep-multiplier* – 1) successive refresh messages must be lost before a reservation state is deleted.

Juniper Networks does not recommend configuring a short RSVP hello timer. If quick discovery of a failed neighbor is needed, configure short IGP (OSPF or IS-IS) hello timers.

By default, the refresh timer value is 30 seconds. To modify this value, include the refresh-time statement:

refresh-time *seconds*;

You can include this statement at the following hierarchy levels:

- [edit protocols rsvp]
- [edit logical-systems *logical-system-name* protocols rsvp]

The default value of the keep multiplier is 3. To modify this value, include the keep-multiplier statement:

keep-multiplier *number*;

You can include this statement at the following hierarchy levels:

- [edit protocols rsvp]
- [edit logical-systems *logical-system-name* protocols rsvp]

Preempting RSVP Sessions

Whenever bandwidth is insufficient to handle all RSVP sessions, you can control the preemption of RSVP sessions. By default, an RSVP session is preempted only by a new higher-priority session.

To always preempt a session when the bandwidth is insufficient, include the preemption statement with the aggressive option:

```
preemption aggressive;
```

You can include this statement at the following hierarchy levels:

- [edit protocols rsvp]
- [edit logical-systems *logical-system-name* protocols rsvp]

To disable RSVP session preemption, include the preemption statement with the disabled option:

```
preemption disabled;
```

To return to the default (that is, preempt a session only for a new higher-priority session), include the preemption statement with the normal option:

```
preemption normal;
```

You can include this statement at the following hierarchy levels:

- [edit protocols rsvp]
- [edit logical-systems *logical-system-name* protocols rsvp]

Configuring MTU Signaling in RSVP

To configure maximum transmission unit (MTU) signaling in RSVP, you need to configure MPLS to allow IP packets to be fragmented before they are encapsulated in MPLS. You also need to configure MTU signaling in RSVP. For troubleshooting purposes, you can configure MTU signaling alone without enabling packet fragmentation.

To configure MTU signaling in RSVP, include the path-mtu statement:

```
path-mtu {
    allow-fragmentation;
    rsvp {
        mtu-signaling;
    }
}
```

You can include this statement at the following hierarchy levels:

- [edit logical-systems *logical-system-name* protocols mpls]
- [edit protocols mpls]

The following sections describe how to enable packet fragmentation and MTU signaling in RSVP:

- Enabling MTU Signaling in RSVP on page 291
- Enabling Packet Fragmentation on page 291

Enabling MTU Signaling in RSVP

To enable MTU signaling in RSVP, include the rsvp mtu-signaling statement:

```
rsvp mtu-signaling;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls path-mtu]
- [edit logical-systems *logical-system-name* protocols mpls path-mtu]

Once you have committed the configuration, changes in the MTU signaling behavior for RSVP take effect the next time the path is refreshed.

You can configure the mtu-signaling statement by itself at the [edit protocols mpls path-mtu rsvp] hierarchy level. This can be useful for troubleshooting. If you configure just the mtu-signaling statement, you can use the show rsvp session detail command to determine what the smallest MTU is on an LSP. The show rsvp session detail command displays the MTU value received and sent in the Adspec object.

Enabling Packet Fragmentation

To allow IP packets to be fragmented before they are encapsulated in MPLS, include the allow-fragmentation statement:

```
allow-fragmentation;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls path-mtu]
- [edit logical-systems *logical-system-name* protocols mpls path-mtu]

NOTE: Do not configure the allow-fragmentation statement alone. Always configure it in conjunction with the mtu-signaling statement.

Configuring RSVP to Pop the Label on the Ultimate-Hop Router

You can control the label value advertised on the egress router of an LSP. The default advertised label is label 3 (Implicit Null label). If label 3 is advertised, the penultimate-hop router removes the label and sends the packet to the egress router. When ultimate-hop popping is enabled, label 0 (IP version 4 [IPv4] Explicit Null label)

is advertised. Ultimate-hop popping ensures that any packets traversing an MPLS network include a label.

To configure ultimate-hop popping for RSVP, include the explicit-null statement:

```
explicit-null;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

NOTE: Juniper Networks routers queue packets based on the incoming label. Routers from other vendors might queue packets differently. Keep this in mind when working with networks containing routers from multiple vendors.

For more information about labels, see "Label Description" on page 25 and "Label Allocation" on page 25.

Disabling Adjacency Down and Neighbor Down Notification in IS-IS and OSPF

Whenever IS-IS is deactivated, the IS-IS adjacencies are brought down. IS-IS signals to RSVP to bring down any RSVP neighbors associated with the IS-IS adjacencies, and this further causes the associated LSPs signaled by RSVP to go down as well.

A similar process occurs whenever OSPF is deactivated. The OSPF neighbors are brought down. OSPF signals to RSVP to bring down any of the RSVP neighbors associated with the OSPF neighbors, and this further causes the associated LSPs signaled by RSVP to go down as well.

If you need to migrate from IS-IS to OSPF or from OSPF to IS-IS, the IGP notification to RSVP for an adjacency or neighbor down event needs to be ignored. Using the no-adjacency-down-notification or no-neighbor-down-notification statements, you can disable IS-IS adjacency down notification or OSPF neighbor down notification, respectively, until the migration is complete. The network administrator is responsible for configuring the statements before the migration, and then removing them from the configuration afterward, so that IGP notification can function normally.

To disable adjacency down notification in IS-IS, include the no-adjacency-down-notification statement:

```
no-adjacency-down-notification;
```

You can include this statement at the following hierarchy levels:

- [edit protocols isis interface *interface-name*]
- [edit logical-systems *logical-system-name* protocols isis interface *interface-name*]

To disable neighbor down notification in OSPF, include the no-neighbor-down-notification statement:

```
no-neighbor-down-notification;
```

You can include this statement at the following hierarchy levels:

- [edit protocols ospf area *area-id* interface *interface-name*]
- [edit logical-systems *logical-system-name* protocols ospf area *area-id* interface *interface-name*]

Enabling Ultimate-Hop Popping on Point-to-Multipoint LSPs

By default, for both point-to-point and point-to-multipoint LSPs, penultimate-hop popping is used for MPLS traffic. MPLS labels are removed from packets on the router just before the egress router of the LSP. The plain IP packets are then forwarded to the egress router. For ultimate-hop popping, the egress router is responsible for both removing the MPLS label and processing the plain IP packet.

It can be beneficial to enable ultimate-hop popping on point-to-multipoint LSPs, particularly when transit traffic is traversing the same egress device. If you enable ultimate-hop popping, a single copy of traffic can be sent over the incoming link, saving significant bandwidth. By default, ultimate-hop popping is disabled. Ultimate-hop popping is not available for point-to-point LSPs.

You enable ultimate-hop popping for point-to-multipoint LSPs by configuring the tunnel-services statement. When you enable ultimate-hop popping, the JUNOS software selects one of the available virtual loopback tunnel (VT) interfaces to loop back the packets to the PFE for IP forwarding. By default, the VT interface selection process is performed automatically. Bandwidth admission control is used to limit the number of LSPs that can be used on one VT interface. Once all the bandwidth is consumed on one interface, the JUNOS software selects another VT interface with sufficient bandwidth for admission control.

If an LSP requires more bandwidth than is available from any of the VT interfaces, ultimate-hop popping cannot be enabled and penultimate-hop popping is enabled instead.

You can explicitly configure which VT interfaces handle the RSVP traffic by including the devices option for the tunnel-services statement. The devices option allows you to specify which VT interfaces are to be used by RSVP. If you do not configure this option, all of the VT interfaces available to the router can be used.

For ultimate-hop popping on point-to-multipoint LSPs to function properly, the egress router must have a PIC that provides tunnel services, such as the tunnel services PIC or the adaptive services PIC. Tunnel services are needed for popping the final MPLS label and for returning packets for IP address lookups.

If you configure the tunnel-services statement on an operating router, only the behavior of newly signaled LSPs changes. Existing LSPs are not affected. To force all existing LSPs to use ultimate-hop popping, issue a clear mpls lsp command. Note that this causes all of the MPLS LSPs on the router to be signaled again.

To enable ultimate-hop popping for the egress point-to-multipoint LSPs on a router, configure the tunnel-services statement:

```
tunnel-services {
    devices device-names;
}
```

You can configure this statement at the [edit protocols rsvp] hierarchy level.

To enable ultimate-hop popping for egress point-to-multipoint LSPs, you must also configure the interface statement with the all option:

```
interface all;
```

You must configure this statement at the [edit protocols rsvp] hierarchy level.

Tracing RSVP Protocol Traffic

To trace RSVP protocol traffic, include the traceoptions statement:

```
traceoptions {
    file filename <replace> <size size> <files number> <no-stamp> <world-readable |
        no-world-readable>;
    flag flag <flag-modifier> <disable>;
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols rsvp]
- [edit logical-systems *logical-system-name* protocols rsvp]

Use the file statement to specify the name of the file that receives the output of the tracing operation. All files are placed in the directory /var/log. We recommend that you place RSVP tracing output in the file rsvp-log.

You can specify the following RSVP-specific flags in the RSVP traceoptions statement:

- all—All tracing operations.
- error—All detected error conditions
- event—RSVP-related events (helps to trace events related to RSVP graceful restart)
- lmp—RSVP-Link Management Protocol (LMP) interactions
- packets—All RSVP packets
- path—All path messages
- pathtear—PathTear messages
- resv—Resv messages
- resvtear—ResvTear messages
- route—Routing information
- state—Session state transitions

For general information about tracing and global tracing options, see the *JUNOS Routing Protocols Configuration Guide*.

Examples: Tracing RSVP Protocol Traffic

Trace RSVP path messages in detail:

```
[edit]
protocols {
   rsvp {
      traceoptions {
         file rsvp size 10m files 5;
         flag path;
      }
   }
}
```

Trace all RSVP messages:

```
[edit]
protocols {
   rsvp {
      traceoptions {
         file rsvp size 10m files 5;
         flag packets;
      }
   }
}
```

Trace all RSVP error conditions:

```
[edit]
protocols {
   rsvp {
      traceoptions {
         file rsvp size 10m files 5;
         flag error;
      }
   }
}
```

Chapter 13

Summary of RSVP Configuration Statements

This chapter provides a reference for each of the RSVP configuration statements. The statements are organized alphabetically.

admin-group

Syntax

```
admin-group {
    exclude group-names;
    include-all group-names;
    include-any group-names;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection bypass *bypass-name*],
[edit protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]

Release Information

Statement introduced in JUNOS Release 9.2.

Description

Allows you to configure administrative groups for bypass label-switched paths (LSPs). You can configure administrative groups either globally for all bypass LSPs traversing an interface or for just a specific bypass LSP.

Options

exclude—Specifies the administrative groups to exclude for a bypass LSP.

include-all—Specifies the administrative groups whose links the bypass LSP must traverse.

include-any—Specifies the administrative groups whose links the bypass LSP can traverse.

Usage Guidelines

See "Configuring Administrative Groups for Bypass LSPs" on page 281.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

aggregate

Syntax (aggregate | no-aggregate);

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*],
[edit logical-systems *logical-system-name* protocols rsvp peer-interface *peer-interface-name*],
[edit protocols rsvp interface *interface-name*],
[edit protocols rsvp peer-interface *peer-interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Control the use of RSVP aggregate messages on an interface or peer interface:

- aggregate—Use RSVP aggregate messages.
- no-aggregate—Do not use RSVP aggregate messages.

  Aggregate messages can pack multiple RSVP messages into a single transmission, thereby reducing network overhead and enhancing efficiency. The number of supportable sessions and processing overhead are significantly improved when aggregation is enabled.

  Not all routers connected to a subnet need to support aggregation simultaneously. Each RSVP router negotiates its intention to use aggregate messages on a per-neighbor basis. Only when both routers agree are aggregate messages sent.

Default Aggregation is disabled.

Usage Guidelines See “Configuring RSVP Refresh Reduction” on page 273.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

authentication-key

Syntax authentication-key *key*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*],
[edit logical-systems *logical-system-name* protocols rsvp peer-interface *peer-interface-name*],
[edit protocols rsvp interface *interface-name*],
[edit protocols rsvp peer-interface *peer-interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Authentication key (password). Neighboring routers use the password to verify the authenticity of packets sent from this interface or peer interface.

RSVP uses HMAC-MD5 authentication, which is defined in RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*.

All routers that are connected to the same IP subnet must use the same authentication scheme and password.

Options *key*—Authentication password. It can be 1 through 16 contiguous digits or letters. Separate decimal digits with periods. Separate hexadecimal digits with periods and precede the string with 0x. If you include spaces in the password, enclose the entire password in quotation marks (" ").

Usage Guidelines See "Configuring RSVP Authentication" on page 276.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

bandwidth

Syntax bandwidth *bps*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection bypass *bypass-name*],
[edit protocols rsvp interface *interface-name*],
[edit protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description For certain logical interfaces (such as Asynchronous Transfer Mode [ATM], Permanent Virtual Circuit [PVC], or Frame Relay), you cannot determine the correct bandwidth from the hardware. This statement allows you to specify the actual available bandwidth.

This statement also allows you to specify the bandwidth for a bypass label switched path (LSP). If you have configured multiple bypasses, this statement is mandatory and is applied to all of the bypass LSPs.

Default The hardware raw bandwidth is used.

Options *bps*—Bandwidth in bits per second. You can specify this as an integer value. If you do so, count your zeros carefully, or you can use the abbreviations k (for a thousand), m (for a million), or g (for a billion [also called a thousand million]).
Range: Any positive integer
Default: 0 (no bandwidth is reserved)

Usage Guidelines See "Configuring the Bandwidth for Bypass LSPs" on page 282, "Configuring Node Protection or Link Protection" on page 278, and "Configuring Bypass LSPs" on page 280.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

bypass

Syntax

```
bypass bypass-name {
    bandwidth bps;
    hop-limit number;
    no-cspf;
    path address <strict | loose>;
    priority setup-priority reservation-priority;
    to address;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp interface *interface-name* link-protection]

Release Information

Statement introduced before JUNOS Release 7.4.

Description

Allows you to configure specific bandwidth and path constraints for a bypass LSP. It is possible to individually configure multiple bypass LSPs. If you do not configure the bypass LSPs individually, they all share the same path and bandwidth constraints.

If you specify the bandwidth, hop-limit, and path statements for the bypass LSP, these values take precedence over the values configured at the [edit protocols rsvp interface *interface-name* link-protection] hierarchy level. The other attributes (subscription, no-node-protection, and optimize-timer) are inherited from the general constraints.

Options

to—(Required) Specify the address for the interface of the immediate next-hop node (for link protection) or the next-next-hop node (for node-link protection). The address specified determines whether this is a link protection bypass or a node-link protection bypass. On multiaccess networks (for example, a LAN), this address is also used to specify which next-hop node is being protected.

The remaining statements are explained separately.

Usage Guidelines

See "Configuring Bypass LSPs" on page 280.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

class-of-service

Syntax class-of-service *cos-value*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection bypass *bypass-name*],
[edit protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Class-of-service (CoS) value given to all packets in the bypass LSP. You can specify a single CoS value for all the bypass LSPs traversing an interface. You can also configure CoS values for specific bypass LSPs traversing an interface.

The CoS value might affect the scheduling or queuing algorithm of traffic traveling along an LSP.

Options *cos-value*—CoS value. A higher value typically corresponds to a higher level of service.
Range: 0 through 7
Default: If you do not specify a CoS value, the IP precedence bits from the packet's IP header are used as the packet's CoS value.

Usage Guidelines See "Configuring the Class of Service for Bypass LSPs" on page 282.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

disable

Syntax disable;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit logical-systems *logical-system-name* protocols rsvp graceful-restart],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit logical-systems *logical-system-name* protocols rsvp peer-interface *peer-interface-name*],
[edit protocols rsvp],
[edit protocols rsvp graceful-restart],
[edit protocols rsvp interface *interface-name*],
[edit protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp peer-interface *peer-interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Explicitly disable RSVP or RSVP graceful restart. Explicitly disable link protection on the specified interface.

Default RSVP is enabled on interfaces and peer interfaces configured with the RSVP interface statement. RSVP graceful restart is enabled on the router. Link protection is disabled.

Usage Guidelines See "Minimum RSVP Configuration" on page 271, "Configuring RSVP Graceful Restart" on page 286, and "Configuring Node Protection or Link Protection" on page 278.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

fast-reroute optimize-timer

Syntax fast-reroute optimize-timer *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement added in JUNOS Release 7.5.

Description Configure the optimize timer for fast reroute. The optimize timer triggers a periodic optimization process that recomputes the fast reroute detour LSPs to use network resources more efficiently.

Options *seconds*—Specify the number of seconds between fast reroute detour LSP optimizations.
Range: 0 through 65,535 seconds
Default: 0 (disabled)

Usage Guidelines See "Configuring the Optimization Interval for Fast Reroute Paths" on page 72.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

graceful-deletion-timeout

Syntax graceful-deletion-timeout *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the time, in seconds, before completing graceful deletion of signaling.

Options *seconds*—Time before completing graceful deletion of signaling.
Range: 1 through 300 seconds
Default: 30 seconds

Usage Guidelines See "Configuring the Graceful Deletion Timeout Interval" on page 457.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

graceful-restart

Syntax

```
graceful-restart {
    disable;
    helper-disable;
    maximum-helper-recovery-time seconds;
    maximum-helper-restart-time seconds;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* routing-options],
[edit protocols rsvp],
[edit routing-options]

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable graceful restart on the router. You must configure the graceful-restart statement at the [edit routing-options] hierarchy level to enable graceful restart on the router.

Options

disable—Disable graceful restart on the router or for RSVP.

helper-disable—Disable RSVP graceful restart helper mode (this option is only available at the [edit protocols rsvp] hierarchy level).
Default: Helper mode is enabled by default.

maximum-helper-recovery-time—The maximum length of time the router stores the state of neighboring routers when they undergo a graceful restart. The value applies to all neighboring routers, so it should be based on the time that the slowest RSVP neighbor requires for restart.
Default: 180 seconds
Range: 1 through 3600 seconds

maximum-helper-restart-time—The maximum length of time the router waits between when it discovers that a neighboring router has gone down and when it declares the neighbor down. This value is applied to all neighboring routers, so it should be based on the time that the slowest RSVP neighbor requires for restart.
Default: 20 seconds
Range: 1 through 1800 seconds

Usage Guidelines See "Configuring RSVP Graceful Restart" on page 286.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

hello-interval

Syntax hello-interval *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*],
[edit logical-systems *logical-system-name* protocols rsvp peer-interface *peer-interface-name*],
[edit protocols rsvp interface *interface-name*],
[edit protocols rsvp peer-interface *peer-interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable the sending of hello packets on the interface.

Options *seconds*—Length of time between hello packets. A value of 0 disables the sending of hello packets on the interface.
Range: 1 through 60 seconds
Default: 9 seconds

Usage Guidelines See "Configuring the RSVP Hello Interval" on page 276.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

hop-limit

Syntax hop-limit *number*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection bypass *bypass-name*],
[edit protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the maximum number of hops a bypass can traverse. By default, each bypass can traverse a maximum of 255 hops, including the ingress and egress routers.

Options *number*—Maximum number of hops a bypass can traverse.
Range: 2 through 255 hops
Default: 255 hops

Usage Guidelines See "Configuring the Hop Limit for Bypass LSPs" on page 283.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

interface

Syntax

```
interface interface-name {
    disable;
    (aggregate | no-aggregate);
    authentication-key key;
    bandwidth bps;
    hello-interval seconds;
    link-protection {
        admin-group {
            exclude group-names;
            include-all group-names;
            include-any group-names;
        }
        disable;
        bandwidth bps;
        bypass bypass-name {
            bandwidth bps {
                ct0 bps;
                ct1 bps;
                ct2 bps;
                ct3 bps;
            }
            hop-limit number;
            path address <strict | loose>;
            to address;
        }
        class-of-service cos-value;
        hop-limit number;
        max-bypasses number;
        no-node-protection;
        optimize-timer number;
        path address <strict | loose>;
        subscription percentage;
    }
    (reliable | no-reliable);
    subscription percentage {
        ct0 percentage;
        ct1 percentage;
        ct2 percentage;
        ct3 percentage;
    }
    update-threshold threshold;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp], [edit protocols rsvp]

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable RSVP on one or more router interfaces.

Default RSVP is disabled on all interfaces.

Options *interface-name*—Name of an interface. To configure all interfaces, specify **all**. For details about specifying interfaces, see the *JUNOS Network Interfaces Configuration Guide*.

The remaining statements are explained separately.

Usage Guidelines See "Minimum RSVP Configuration" on page 271.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

keep-multiplier

Syntax keep-multiplier *number*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement introduced before JUNOS Release 7.4.

Description Set the keep multiplier value.

Options *number*—Multiplier value.
Range: 1 through 255
Default: 3

Usage Guidelines See "Configuring RSVP Timers" on page 289.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

link-protection

See the following sections:

- link-protection (MPLS) on page 309
- link-protection (RSVP) on page 310

link-protection (MPLS)

Syntax link-protection;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*], [edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable link protection on the specified LSP. To fully enable link protection, you also need to configure the link-protection statement at the [edit protocols rsvp interface *interface-name*] hierarchy level.

Default Link protection is disabled.

Usage Guidelines See "Configuring Node Protection or Link Protection" on page 278.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

link-protection (RSVP)

Syntax

```
link-protection {
    disable;
    admin-group {
        exclude group-names;
        include-all group-names;
        include-any group-names;
    }
    bandwidth bps;
    bypass bypass-name {
        bandwidth bps {
            ct0 bps;
            ct1 bps;
            ct2 bps;
            ct3 bps;
        }
        hop-limit number;
        no-cspf;
        path address <strict | loose>;
        priority setup-priority reservation-priority;
        to address;
    }
    class-of-service cos-value;
    hop-limit number;
    max-bypasses number;
    no-cspf;
    no-node-protection;
    optimize-timer seconds;
    path address <strict | loose>;
    priority setup-priority reservation-priority;
    subscription percentage {
        ct0 percentage;
        ct1 percentage;
        ct2 percentage;
        ct3 percentage;
    }
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*], [edit protocols rsvp interface *interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable link protection on the specified interface. Using link protection, you can configure a network to reroute traffic quickly around broken links. To fully enable link protection, you also need to configure the link-protection statement at the [edit protocols mpls label-switched-path *lsp-name*] hierarchy level. You can configure single or multiple bypasses for protected interface.

Default Link protection is disabled.

Options no-node-protection—Disables node-link protection on the RSVP interface. Link protection remains active. When this option is configured, the router can only initiate a next-hop bypass, not a next-next-hop bypass.

The remaining statements are explained separately.

Usage Guidelines See "Configuring Node Protection or Link Protection" on page 278.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

load-balance

Syntax

```
load-balance {
   bandwidth;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement introduced before JUNOS Release 7.4.

Description Load-balance traffic between RSVP LSPs.

Options bandwidth—Load-balance traffic between RSVP LSPs based on the bandwidth configured for each LSP.

Usage Guidelines See "Configuring RSVP LSP Load Balancing" on page 287.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

max-bypasses

Syntax max-bypasses *number*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*], [edit protocols rsvp interface *interface-name*]

Release Information Statement introduced before JUNOS Release 7.4. Range modified in JUNOS Release 9.3.

Description Specify the maximum number of dynamic bypass LSPs permitted for protecting this interface. When this option is configured, multiple bypasses for link protection are enabled. Call admission control (CAC) is also enabled. The limit on bypasses configured applies only to dynamically generated bypass LSPs. By default, this option is disabled and only one dynamic bypass LSP is enabled for each interface. If you configure max-bypasses, you must also configure the bandwidth statement.

Options *number*—Configure the maximum number of bypass LSPs. If you configure a value of 0, no dynamic bypass LSPs are allowed to be established for the interface. Only static bypass LSPs can be configured.
Default: 1
Range: 0 through 99

Usage Guidelines See "Configuring the Maximum Number of Bypass LSPs" on page 283.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

no-adjacency-down-notification

Syntax no-adjacency-down-notification;

Hierarchy Level [edit logical-systems *logical-system-name* protocols isis interface *interface-name*], [edit protocols isis interface *interface-name*]

Release Information Statement introduced in JUNOS Release 8.0.

Description Disables adjacency down notification for IS-IS to allow for migration from IS-IS to Open Shortest Path First (OSPF) without disruption of the RSVP neighbors and associated RSVP-signaled LSPs.

Usage Guidelines See "Disabling Adjacency Down and Neighbor Down Notification in IS-IS and OSPF" on page 292.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

no-aggregate

See aggregate.

no-cspf

Syntax no-cspf;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection bypass *bypass-name*],
[edit protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]

Release Information Statement introduced in JUNOS Release 7.5.

Description Disable CSPF computation on all bypass LSPs or on a specific bypass LSP. You need to disable CSPF for link protection to function properly on interarea paths.

Default CSPF is enabled.

Usage Guidelines See "Disabling CSPF for Bypass LSPs" on page 284.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

no-neighbor-down-notification

Syntax no-neighbor-down-notification;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-id* interface *interface-name*],
[edit protocols ospf area *area-id* interface *interface-name*]

Release Information Statement introduced in JUNOS Release 8.0.

Description Disables neighbor down notification for OSPF to allow for migration from OSPF to IS-IS without disruption of the RSVP neighbors and associated RSVP-signaled LSPs.

Usage Guidelines See "Disabling Adjacency Down and Neighbor Down Notification in IS-IS and OSPF" on page 292.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

no-p2mp-sublsp

Syntax no-p2mp-sublsp;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement introduced in JUNOS Release 9.2.

Description Rejects Resv messages which include the S2L_SUB_LSP object. By default, Resv messages which include the S2L_SUB_LSP object are accepted. However, in a network which includes Juniper Networks devices running both JUNOS 9.2 and later releases and JUNOS 9.1 and earlier releases, it is necessary to configure the no-p2mp-sublsp statement on the JUNOS 9.2 and later devices to ensure that P2MP LSPs function properly.

Default Resv messages which include the S2L_SUB_LSP object are accepted.

Usage Guidelines See "Ensuring Compatibility with JUNOS 9.1 and Earlier Releases for P2MP LSPs" on page 149.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

no-reliable

See reliable.

node-link-protection

Syntax node-link-protection;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*],
[edit protocols mpls label-switched-path *lsp-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable node and link protection on the specified LSP. To fully enable node and link protection, you also need to include the link-protection statement at the [edit protocols rsvp interface *interface-name*] hierarchy level.

Default Node and link protection is disabled.

Usage Guidelines See "Configuring Node Protection or Link Protection" on page 278.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

optimize-timer

Syntax optimize-timer *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp interface *interface-name* link-protection]

Release Information Statement introduced before JUNOS Release 7.4.

Description Configure an optimize timer for a bypass LSP. The optimize timer initiates a periodic optimization process that reshuffles data LSPs among bypass LSPs to achieve the most efficient use of network resources. The optimization process attempts to either minimize the number of bypasses currently in use, minimize the total amount of bandwidth reserved for all bypasses, or both.

Options *seconds*—Specify the number of seconds between optimizations.
Range: 0 through 65,535 seconds
Default: 0 (disabled)

Usage Guidelines See "Configuring the Optimization Interval for Bypass LSPs" on page 284.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

path

Syntax path *address* <strict | loose>;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection bypass *bypass-name*],
[edit protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Configure an explicit path (a sequence of strict or loose routes) to control where and how a bypass LSP is established. If multiple bypasses are configured, they all will use the same explicit path.

Default No path is configured. CSPF automatically calculates the path the bypass LSP takes.

Options *address*—IP address of each transit router in the LSP. You must specify the address or hostname of each transit router, although you do not need to list each transit router if its type is loose. As an option, you can include the ingress and egress routers in the path. Specify the addresses in order, starting with the ingress router (optional) or the first transit router, and continuing sequentially along the path until reaching the egress router (optional) or the router immediately before the egress router.
Default: If you do not specify any routers explicitly, no routing limitations are imposed on the bypass LSP.

loose—The next address in the path statement is loose. The LSP can traverse other routers before reaching this router.
Default: strict

strict—The LSP must go to the next address specified in the path statement without traversing other nodes. This is the default.

Usage Guidelines See “Configuring an Explicit Path for Bypass LSPs” on page 285.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

peer-interface

Syntax

```
peer-interface peer-interface-name {
    disable;
    (aggregate | no-aggregate);
    authentication-key key;
    hello-interval seconds;
    (reliable | no-reliable);
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement introduced before JUNOS Release 7.4.

Description Configure the name of the LMP peer device.

The remaining statements are explained separately.

Usage Guidelines See "Configuring Peer Interfaces in RSVP and OSPF" on page 451.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

preemption

Syntax

```
preemption {
   (aggressive | disabled | normal);
   soft-preemption {
      cleanup-timer seconds;
   }
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement introduced before JUNOS Release 7.4.

Description Control RSVP session preemption.

Default normal

Options aggressive—Preempt RSVP sessions whenever bandwidth is insufficient to handle all sessions. A session is preempted whenever bandwidth is lowered or a new higher-priority session is established.

disabled—Do not preempt RSVP sessions.

normal—Preempt RSVP sessions to accommodate new higher-priority sessions when bandwidth is insufficient to handle all sessions.

The remaining statements are explained separately.

Usage Guidelines See “Preempting RSVP Sessions” on page 290.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

priority

Syntax priority *setup-priority reservation-priority*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection bypass *bypass-name*],
[edit protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*],

Release Information Statement introduced before JUNOS Release 7.4.

Description Configure the setup priority and reservation priority for a bypass LSP. If insufficient link bandwidth is available during session establishment, the setup priority is compared with other setup priorities for established sessions on the link to determine whether some of them should be preempted to accommodate the new session. The session with the lower-hold priority is preempted.

Options *reservation-priority*—Reservation priority, used to keep a reservation after it has been set up. A smaller number has a higher priority. The priority must be greater than or equal to the setup priority to prevent preemption loops.
Range: 0 through 7, where 0 is the highest and 7 is the lowest priority.
Default: 0 (Once the session is set up, no other session can preempt it.)

setup-priority—Setup priority.
Range: 0 through 7, where 0 is the highest and 7 is the lowest priority.
Default: 7 (The session cannot preempt any existing sessions.)

Usage Guidelines See "Configuring Priority and Preemption for Bypass LSPs" on page 286 and "Configuring Priority and Preemption for LSPs" on page 95.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

refresh-time

Syntax refresh-time *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement introduced before JUNOS Release 7.4.

Description Set the refresh time.

Options *seconds*—Refresh time.
Range: 1 through 65,535
Default: 30 seconds

Usage Guidelines See "Configuring RSVP Timers" on page 289.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

reliable

Syntax (reliable | no-reliable);

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*],
[edit logical-systems *logical-system-name* protocols rsvp peer-interface *peer-interface-name*],
[edit protocols rsvp interface *interface-name*],
[edit protocols rsvp peer-interface *peer-interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable reliable message delivery on the interface.

Usage Guidelines See "Configuring RSVP Refresh Reduction" on page 273.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

rsvp

Syntax rsvp { ... }

Hierarchy Level [edit logical-systems *logical-system-name* protocols],
[edit protocols]

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable RSVP routing on the router.

You must include the rsvp statement in the configuration to enable RSVP on the router.

Default RSVP is disabled on the router.

Usage Guidelines See "Minimum RSVP Configuration" on page 271.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

soft-preemption

Syntax
```
soft-preemption {
   cleanup-timer seconds;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp preemption],
[edit protocols rsvp preemption]

Release Information Statement introduced before JUNOS Release 7.4.

Description Soft preemption attempts to establish a new path for a preempted LSP before tearing it down.

Options cleanup-timer—A value of 0 disables soft preemption.
Range: 0 through 180 seconds
Default: 30 seconds

Usage Guidelines See "Configuring MPLS Soft Preemption" on page 80.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

subscription

Syntax

```
subscription percentage {
    ct0 percentage;
    ct1 percentage;
    ct2 percentage;
    ct3 percentage;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp interface *interface-name*],
[edit protocols rsvp interface *interface-name* link-protection]

Release Information

Statement introduced before JUNOS Release 7.4.

Description

Configures the amount of bandwidth subscribed to a class type (when you have enabled Differentiated Services), or bypass LSP (when you have enabled link protection). The subscription is the percentage of the link bandwidth that can be used for the RSVP reservation process.

Options

ct*number percentage*—Percent of the class-type bandwidth that RSVP allows to be used for reservations. If you specify a value greater than 100, you are oversubscribing the class type. You can specify bandwidth subscriptions for class types 0 through 3. This option is not available for bypass LSPs.
Range: 0 through 65,000
Default: 100 percent

percentage—Percent of the class-type or bypass LSP bandwidth that RSVP allows to be used for reservations. If you specify a value greater than 100, you are oversubscribing the class type or bypass LSP.
Range: 0 through 65,000
Default: 100 percent

Usage Guidelines

See "Configuring the Bandwidth Subscription Percentage for LSPs" on page 126 and "Configuring the Amount of Bandwidth Subscribed for Bypass LSPs" on page 285.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

traceoptions

Syntax

```
traceoptions {
   file filename <replace> <size size> <files number> <no-stamp> <world-readable |
      no-world-readable>;
   flag flag <flag-modifier> <disable>;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement introduced before JUNOS Release 7.4.

Description RSVP protocol–level trace options.

Default The default RSVP protocol–level trace options are those inherited from the routing protocols traceoptions statement included at the [edit routing-options] hierarchy level.

Options disable—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as all.

filename—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log. We recommend that you place RSVP tracing output in the file rsvp-log.

files *number*—(Optional) Maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed *trace-file*.0, then *trace-file*.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.
Range: 2 through 1000
Default: 2 files

If you specify a maximum number of files, you must also include the size statement to specify the maximum file size.

flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.

- all—All tracing operations
- error—All detected error conditions
- event—RSVP-related events
- lmp—RSVP-LMP interactions
- packets—All RSVP packets
- path—All path messages
- pathtear—PathTear messages
- resv—Resv messages

- resvtear—ResvTear messages
- route—Routing information
- state—Session state transitions

flag-modifier—(Optional) Modifier for the tracing flag. You can specify one or more of these modifiers:

- detail—Provide detailed trace information
- receive—Packets being received
- send—Packets being transmitted

no-stamp—(Optional) Do not place timestamp information at the beginning of each line in the trace file.
Default: If you omit this option, timestamp information is placed at the beginning of each line of the tracing output.

no-world-readable—(Optional) Enable only certain users to read the log file.

replace—(Optional) Replace an existing trace file if there is one.
Default: If you do not include this option, tracing output is appended to an existing trace file.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file*.0. When the *trace-file* again reaches this size, *trace-file*.0 is renamed *trace-file*.1 and *trace-file* is renamed *trace-file*.0. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.
Syntax: *x*k to specify KB, *x*m to specify MB, or *x*g to specify GB
Range: 10 KB through the maximum file size supported on your system
Default: 1 MB

If you specify a maximum file size, you must also include the files statement to specify the maximum number of files.

world-readable—(Optional) Enable any user to read the log file.

Usage Guidelines See "Tracing RSVP Protocol Traffic" on page 294.

Required Privilege Level routing and trace—To view this statement in the configuration.
routing-control and trace-control—To add this statement to the configuration.

tunnel-services

Syntax
```
tunnel-services {
    devices device-names;
}
```

Hierarchy Level [edit protocols rsvp]

Release Information Statement introduced in JUNOS Release 8.1.

Description Enables ultimate-hop popping on point-to-multipoint LSPs. The JUNOS software selects one of the available virtual tunnel (VT) interfaces to de-encapsulate the egress traffic. By default, the selection process is performed automatically.

Default Ultimate-hop popping is disabled.

Options devices *device-names*—Specifies which VT interfaces are used to handle the RSVP traffic.
Range: 0 to 8 devices

Usage Guidelines See "Enabling Ultimate-Hop Popping on Point-to-Multipoint LSPs" on page 293.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

update-threshold

Syntax update-threshold *threshold*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*], [edit protocols rsvp interface *interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Adjust the threshold at which a change in bandwidth triggers an interior gateway protocol (IGP) update.

Options *threshold*—Specifies the percentage change in bandwidth to trigger an IGP update.
Range: 1 through 20 percent
Default: 10 percent

Usage Guidelines See "Configuring the RSVP Update Threshold on an Interface" on page 277.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Part 4
LDP

- LDP Overview on page 329
- LDP Configuration Guidelines on page 337
- Summary of LDP Configuration Statements on page 365

Chapter 14

LDP Overview

The Label Distribution Protocol (LDP) is a protocol for distributing labels in non-traffic-engineered applications. LDP allows routers to establish label-switched paths (LSPs) through a network by mapping network-layer routing information directly to data link layer-switched paths.

These LSPs might have an endpoint at a directly attached neighbor (comparable to IP hop-by-hop forwarding), or at a network egress node, enabling switching through all intermediary nodes. LSPs established by LDP can also traverse traffic-engineered LSPs created by RSVP.

LDP associates a forwarding equivalence class (FEC) with each LSP it creates. The FEC associated with an LSP specifies which packets are mapped to that LSP. LSPs are extended through a network as each router chooses the label advertised by the next hop for the FEC and splices it to the label it advertises to all other routers. This process forms a tree of LSPs that converge on the egress router.

This chapter discusses the following topics:

- LDP Standards on page 329
- JUNOS Software LDP Protocol Implementation on page 330
- LDP Operation on page 330
- LDP Label Filtering on page 331
- Tunneling LDP LSPs in RSVP LSPs on page 331
- LDP Message Types on page 333
- LDP Graceful Restart on page 334

LDP Standards

LDP is described in the following RFC and Internet draft:

- RFC 3036, *LDP Specification*

The JUNOS software supports the required elements of RFC 3036, except the following:

- loop detection
- CR-LDP

The RFC establishes three modes that the JUNOS software only partially supports:

- Label distribution control mode
- Label retention mode
- Label advertisement mode

The following values for these modes are supported:

- Label distribution control mode: ordered
- Label retention mode: liberal
- Label advertisement mode: downstream unsolicited

The following values for these modes are not supported:

- Label distribution control mode: independent
- Label retention mode: conservative
- Label advertisement mode: downstream on demand
- RFC 3212, *Constraint-Based LSP Setup using LDP*
- RFC 3215, *LDP State Machine*
- RFC 3478, *Graceful Restart Mechanism for Label Distribution Protocol*

To access Internet RFCs and drafts, go to the IETF Web site at http://www.ietf.org/.

JUNOS Software LDP Protocol Implementation

The JUNOS software implementation of LDP supports LDP version 1. The JUNOS software supports a simple mechanism for tunneling between routers in an interior gateway protocol (IGP), to eliminate the required distribution of external routes within the core. The JUNOS software allows a Multiprotocol Label Switching (MPLS) tunnel next hop to all egress routers in the network, with only an IGP running in the core to distribute routes to egress routers. Edge routers run BGP but do not distribute external routes to the core. Instead, the recursive route lookup at the edge resolves to an LSP switched to the egress router. No external routes are necessary on the transit LDP routers.

LDP Operation

You must configure LDP for each interface on which you want LDP to run. LDP creates LSP trees rooted at each egress router for the router ID address that is the subsequent Border Gateway Protocol (BGP) next hop. The ingress point is at every router running LDP. This process provides an inet.3 route to every egress router. If BGP is running, it will attempt to resolve next hops by using the inet.3 table first, which binds most, if not all, of the BGP routes to MPLS tunnel next hops.

Two adjacent routers running LDP become neighbors. If the two routers are connected by more than one interface, they become neighbors on each interface. When LDP routers become neighbors, they establish an LDP session to exchange label

information. If per-router labels are in use on both routers, only one LDP session is established between them, even if they are neighbors on multiple interfaces. For this reason, an LDP session is not related to a particular interface.

LDP operates in conjunction with a unicast routing protocol. LDP installs LSPs only when both LDP and the routing protocol are enabled. For this reason, you must enable both LDP and the routing protocol on the same set of interfaces. If this is not done, LSPs might not be established between each egress router and all ingress routers, which might result in loss of BGP-routed traffic.

For LDP to run on an interface, MPLS must be enabled on a logical interface on that interface. For more information, see the *JUNOS Network Interfaces Configuration Guide*.

LDP Label Filtering

You can apply policy filters to labels received from and distributed to other routers through LDP. Policy filters provide you with a mechanism to control the establishment of LSPs.

Tunneling LDP LSPs in RSVP LSPs

You can tunnel LDP LSPs over RSVP LSPs. The following sections describe how tunneling LDP LSPs in RSVP LSPs works:

- Tunneling LDP LSPs in RSVP LSPs Overview on page 331
- Label Operations on page 331

Tunneling LDP LSPs in RSVP LSPs Overview

If you are using RSVP for traffic engineering, you can run LDP simultaneously to eliminate the distribution of external routes in the core. The LSPs established by LDP are tunneled through the LSPs established by RSVP. LDP effectively treats the traffic-engineered LSPs as single hops.

When you configure the router to run LDP across RSVP-established LSPs, LDP automatically establishes sessions with the router at the other end of the LSP. LDP control packets are routed hop-by-hop, rather than carried through the LSP. This routing allows you to use simplex (one-way) traffic-engineered LSPs. Traffic in the opposite direction flows through LDP-established LSPs that follow unicast routing rather than through traffic-engineered tunnels.

If you configure LDP over RSVP LSPs, you can still configure multiple Open Shortest Path First (OSPF) areas and IS-IS levels in the traffic engineered core and in the surrounding LDP cloud.

Label Operations

Figure 23 on page 332 depicts an LDP LSP being tunneled through an RSVP LSP. (For definitions of label operations, see “Label Description” on page 25.) The shaded inner oval represents the RSVP domain, whereas the outer oval depicts the LDP

domain. RSVP establishes an LSP through routers B, C, D, and E, with the sequence of labels L3, L4. LDP establishes an LSP through Routers A, B, E, F, and G, with the sequence of labels L1, L2, L5. LDP views the RSVP LSP between Routers B and E as a single hop.

When the packet arrives at Router A, it enters the LSP established by LDP, and a label (L1) is pushed onto the packet. When the packet arrives at Router B, the label (L1) is swapped with another label (L2). Because the packet is entering the traffic-engineered LSP established by RSVP, a second label (L3) is pushed onto the packet.

This outer label (L3) is swapped with a new label (L4) at the intermediate router (C) within the RSVP LSP tunnel, and when the penultimate router (D) is reached, the top label is popped. Router E swaps the label (L2) with a new label (L5), and the penultimate router for the LDP-established LSP (F) pops the last label.

Figure 23: Swap and Push When LDP LSPs Are Tunneled Through RSVP LSPs

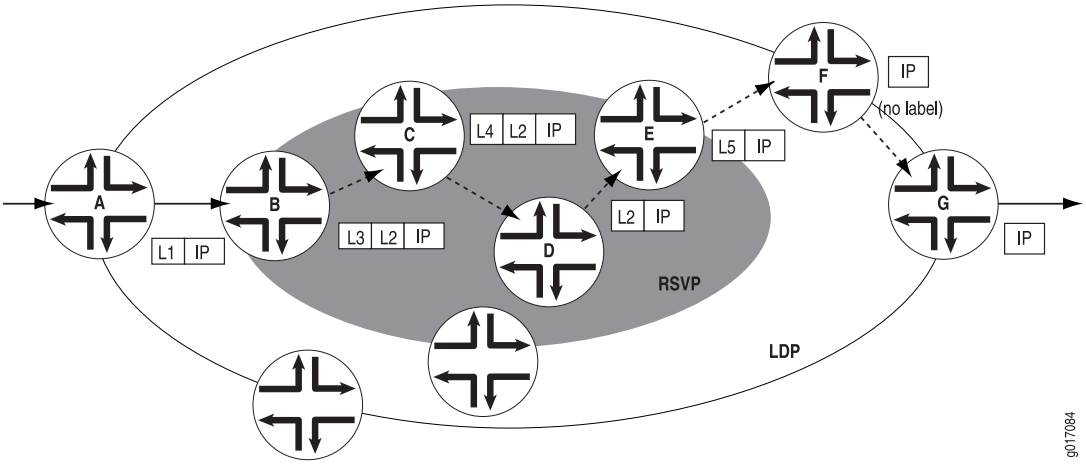
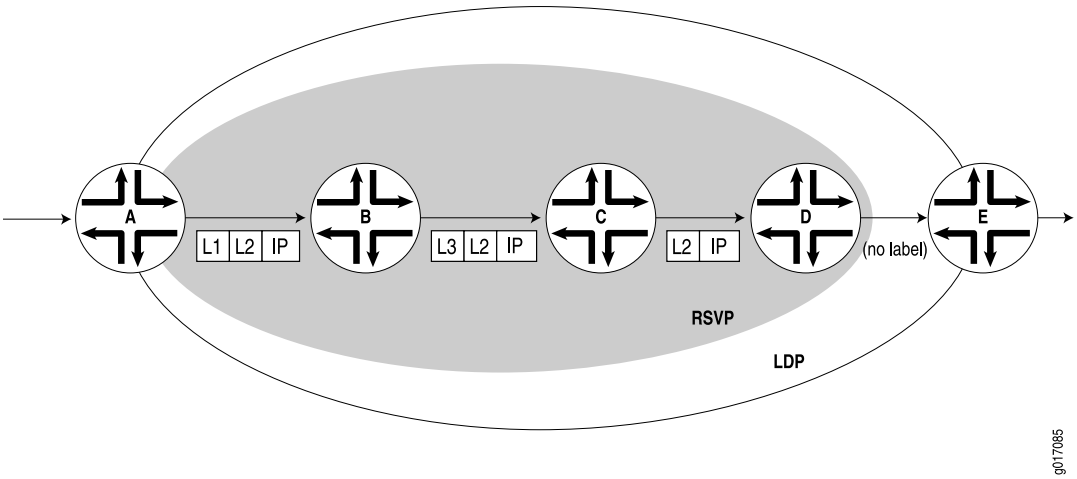


Figure 24 on page 333 depicts double push label operation (L1L2), which is used when the ingress router (A) of the LDP and the RSVP are the same router. Note that Router D is the penultimate hop for the LDP-established LSP, so L2 is popped from the packet by Router D.

Figure 24: Double Push When LDP LSPs Are Tunneled Through RSVP LSPs



LDP Message Types

LDP uses the message types described in the following sections to establish and remove mappings and to report errors. All LDP messages have a common structure that uses a type, length, and value (TLV) encoding scheme.

- Discovery Messages on page 333
- Session Messages on page 334
- Advertisement Messages on page 334
- Notification Messages on page 334

Discovery Messages

Discovery messages announce and maintain the presence of a router in a network. Routers indicate their presence in a network by sending hello messages periodically. Hello messages are transmitted as UDP packets to the LDP port at the group multicast address for all routers on the subnet.

LDP uses the following discovery procedures:

- Basic discovery—A router periodically sends LDP link hello messages through an interface. LDP link hello messages are sent as UDP packets addressed to the LDP discovery port. Receipt of an LDP link hello message on an interface identifies an adjacency with the LDP peer router.
- Extended discovery—LDP sessions between routers not directly connected are supported by LDP extended discovery. A router periodically sends LDP targeted hello messages to a specific address. Targeted hello messages are sent as UDP packets addressed to the LDP discovery port at the specific address. The targeted router decides whether to respond to or ignore the targeted hello message. A targeted router that chooses to respond does so by periodically sending targeted hello messages to the initiating router.

Session Messages

Session messages establish, maintain, and terminate sessions between LDP peers. When a router establishes a session with another router learned through the hello message, it uses the LDP initialization procedure over Transmission Control Protocol (TCP) transport. When the initialization procedure is completed successfully, the two routers are LDP peers and can exchange advertisement messages.

Advertisement Messages

Advertisement messages create, change, and delete label mappings for FECs. Requesting a label or advertising a label mapping to a peer is a decision made by the local router. In general, the router requests a label mapping from a neighboring router when it needs one and advertises a label mapping to a neighboring router when it wants the neighbor to use a label.

Notification Messages

Notification messages provide advisory information and signal error information. LDP sends notification messages to report errors and other events of interest. There are two kinds of LDP notification messages:

- Error notifications, which signal fatal errors. If a router receives an error notification from a peer for an LDP session, it terminates the LDP session by closing the TCP transport connection for the session and discarding all label mappings learned through the session.
- Advisory notifications, which pass information to a router about the LDP session or the status of some previous message received from the peer.

LDP Graceful Restart

LDP graceful restart enables a router whose LDP control plane is undergoing a restart to continue to forward traffic while recovering its state from neighboring routers. It also enables a router on which helper mode is enabled to assist a neighboring router that is attempting to restart LDP.

During session initialization, a router advertises its ability to perform LDP graceful restart or to take advantage of a neighbor performing LDP graceful restart by sending the graceful restart TLV. This TLV contains two fields relevant to LDP graceful restart: the reconnect time and the recovery time. The values of the reconnect and recovery times indicate the graceful restart capabilities supported by the router.

The reconnect time is configured in the JUNOS software as 60 seconds and is not user-configurable. When a router discovers that a neighboring router is restarting, it waits until the end of the recovery time before attempting to reconnect. The recovery time is the length of time a router waits for LDP to restart gracefully. The recovery time period begins when an initialization message is sent or received. This time period is also typically the length of time that a neighboring router maintains its information about the restarting router, allowing it to continue to forward traffic.

You can configure LDP graceful restart in both the master instance for the LDP protocol and for a specific routing instance. You can disable graceful restart at the global level for all protocols, at the protocol level for LDP only, and on a specific routing instance. LDP graceful restart is disabled by default, because at the global level, graceful restart is disabled by default. However, helper mode (the ability to assist a neighboring router attempting a graceful restart) is enabled by default.

The following are some of the behaviors associated with LDP graceful restart:

- Outgoing labels are not maintained in restarts. New outgoing labels are allocated.
- When a router is restarting, no label-map messages are sent to neighbors that support graceful restart until the restarting router has stabilized (label-map messages are immediately sent to neighbors that do not support graceful restart). However, all other messages (keepalive, address-message, notification, and release) are sent as usual. Distributing these other messages prevents the router from distributing incomplete information.
- Helper mode and graceful restart are independent. You can disable graceful restart in the configuration, but still allow the router to cooperate with a neighbor attempting to restart gracefully.

Chapter 15

LDP Configuration Guidelines

The Label Distribution Protocol (LDP) is instance-aware. To configure the LDP protocol, include the ldp statement:

```
ldp {
    explicit-null;
    (deaggregate | no-deaggregate);
    egress-policy policy-name;
    export [ policy-names ];
    import [ policy-names ];
    graceful-restart {
        disable;
        helper-disable;
        maximum-neighbor-recovery-time value;
        recovery-time value;
    }
    interface interface-name {
        apply-groups;
        disable;
        hello-interval seconds;
        hold-time seconds;
        transport-address (interface | router-id);
    }
    keepalive-interval seconds;
    keepalive-timeout seconds;
    log-updown {
        trap disable;
    }
    no-forwarding;
    policing {
        fec fec-address {
            ingress-traffic filter-name;
            transit-traffic filter-name;
        }
    }
    preference preference;
    session address {
        authentication-key authentication-key;
    }
    strict-targeted-hellos;
    traceoptions {
        apply-groups;
        file filename <replace> <size size> <files number> <no-stamp> <world-readable
            | no-world-readable>;
```

```
        flag flag <flag-modifier> <disable>;
    }
    track-igp-metric;
    traffic-statistics {
        file filename <replace> <size size> <files number> <world-readable |
            no-world-readable>;
        interval interval;
    }
    transport-address (interface | router-id);
}
```

For a list of hierarchy levels at which you can configure these statements, see the statement summary sections.

By default, LDP is disabled.

This chapter describes the minimum required LDP configuration and discusses the following configuration tasks:

- Minimum LDP Configuration on page 339
- Enabling and Disabling LDP on page 339
- Configuring the LDP Hello Interval on page 339
- Configuring the LDP Hold Time on page 340
- Configuring the LDP Keepalive Interval on page 340
- Configuring the LDP Keepalive Timeout on page 340
- Configuring LDP Route Preferences on page 341
- Configuring LDP Graceful Restart on page 341
- Configuring LDP Received-Label Filtering on page 343
- Configuring LDP Outbound-Label Filtering on page 345
- Configuring LDP Transport Address Control on page 347
- Configuring the LDP Egress Policy on page 347
- Configuring FEC Deaggregation on page 348
- Configuring Policers for LDP FECs on page 349
- Configuring LDP IPv4 FEC Filtering on page 350
- Configuring BFD for LDP LSPs on page 350
- Configuring ECMP-Aware BFD for RSVP LSPs on page 351
- Configuring LDP LSP Traceroute on page 352
- Collecting LDP Statistics on page 353
- Tracing LDP Protocol Traffic on page 355
- Configuring Miscellaneous LDP Properties on page 358

Minimum LDP Configuration

To enable LDP on a single interface, include the ldp statement and specify the interface using the interface statement. This is the minimum LDP configuration. All other LDP configuration statements are optional.

```
ldp {
    interface interface-name;
}
```

To enable LDP on all interfaces, specify all for *interface-name*.

For a list of hierarchy levels at which you can include these statements, see the statement summary sections.

Enabling and Disabling LDP

LDP is routing-instance-aware. To enable LDP on a specific interface, include the following statements:

```
ldp {
    interface interface-name;
}
```

For a list of hierarchy levels at which you can include these statements, see the statement summary sections.

To enable LDP on all interfaces, specify all for *interface-name*.

If you have configured interface properties on a group of interfaces and want to disable LDP on one of the interfaces, include the interface statement with the disable option:

```
interface interface-name {
    disable;
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section.

Configuring the LDP Hello Interval

LDP hello messages enable LDP nodes to discover one another and to detect the failure of a neighbor or of the link to the neighbor. Hello messages are sent periodically on all interfaces where LDP is enabled.

By default, LDP sends hello messages every 5 seconds for link hello messages and every 15 seconds for targeted hello messages. You cannot configure a time for the LDP hello interval that is greater than the LDP hold time. For more information, see “Configuring the LDP Hold Time” on page 340.

To modify how often LDP sends hello packets, include the hello-interval statement:

hello-interval *seconds*;

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Configuring the LDP Hold Time

The hold time determines how long an LDP node should wait for a hello message before declaring a neighbor to be down. This value is sent as part of a hello message so that each LDP node tells its neighbors how long to wait. The values sent by each neighbor do not have to match.

The hold time should normally be at least three times the hello interval. The default is 15 seconds for link hello messages and 45 seconds for targeted hello messages. However, it is possible to configure an LDP hold time that is close to the value for the hello interval.

NOTE: Configuring an LDP hold time that is close to the hello interval can cause the router to declare an LDP neighbor down that is still functioning normally. For more information, see "Configuring the LDP Hello Interval" on page 339.

To modify the hold time, include the hold-time statement:

hold-time *seconds*;

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Configuring the LDP Keepalive Interval

The keepalive interval determines how often a message is sent over the session to ensure that the keepalive timeout is not exceeded. If no other LDP traffic is sent over the session in this much time, a keepalive message is sent. The default is 10 seconds.

To modify the keepalive interval, include the keepalive-interval statement:

keepalive-interval *seconds*;

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Configuring the LDP Keepalive Timeout

After an LDP session is established, messages must be exchanged periodically to ensure that the session is still working. The keepalive timeout defines the amount of time that the neighbor LDP node waits before deciding that the session has failed. This value is usually set to at least three times the keepalive interval. The default is 30 seconds.

To modify the keepalive interval, include the keepalive-timeout statement:

```
keepalive-timeout seconds;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

The value configured for the keepalive-timeout statement is displayed as the hold time when you issue the show ldp session detail command.

Configuring LDP Route Preferences

When several protocols calculate routes to the same destination, route preferences are used to select which route is installed in the forwarding table. The route with the lowest preference value is selected. The preference value can be a number in the range 0 through 255. By default, LDP routes have a preference value of 9.

To modify the route preferences, include the preference statement:

```
preference preference;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Configuring LDP Graceful Restart

By default, graceful restart helper mode is enabled, but graceful restart is disabled. Thus, the default behavior of a router is to assist neighboring routers attempting a graceful restart, but not to attempt a graceful restart itself.

To configure LDP graceful restart, see the following sections:

- Enabling Graceful Restart on page 341
- Disabling LDP Graceful Restart or Helper Mode on page 342
- Configuring Recovery Time and Maximum Recovery Time on page 342

Enabling Graceful Restart

To enable LDP graceful restart, you also need to enable graceful restart on the router. To enable graceful restart, include the graceful-restart statement:

```
graceful-restart;
```

You can include this statement at the following hierarchy levels:

- [edit routing-options]
- [edit logical-systems *logical-system-name* routing-options]

The graceful-restart statement enables graceful restart for all protocols supporting this feature on the router. For more information about graceful restart, see the *JUNOS Routing Protocols Configuration Guide*.

By default, LDP graceful restart is enabled when you enable graceful restart at both the LDP protocol level and on all the routing instances. However, you can disable both LDP graceful restart and LDP graceful restart helper mode.

Disabling LDP Graceful Restart or Helper Mode

To disable LDP graceful restart and recovery, include the disable statement:

```
ldp {
   graceful-restart {
      disable;
   }
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

You can disable helper mode at the LDP protocols level only. You cannot disable helper mode for a specific routing instance. To disable LDP helper mode, include the helper-disable statement:

```
ldp {
   graceful-restart {
      helper-disable;
   }
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

The following LDP graceful restart configurations are possible:

- LDP graceful restart and helper mode are both enabled.
- LDP graceful restart is disabled but helper mode is enabled. A router configured in this way cannot restart gracefully but can help a restarting neighbor.
- LDP graceful restart and helper mode are both disabled. The router does not use LDP graceful restart or the graceful restart TLV sent in the initialization message. The router behaves as a router that cannot support LDP graceful restart.

A configuration error is issued if you attempt to enable graceful restart and disable helper mode.

Configuring Recovery Time and Maximum Recovery Time

The recovery time is the amount of time a router waits for LDP to restart gracefully. The recovery time period begins when an initialization message is sent or received. This period is also typically the amount of time that a neighboring router maintains its information about the restarting router, allowing it to continue to forward traffic.

To prevent a neighboring router from being adversely affected if it receives a false value for the recovery time from the restarting router, you can configure the maximum recovery time on the neighboring router. A neighboring router maintains its state

for the shorter of the two times. For example, router A is performing an LDP graceful restart. It has sent a recovery time of 900 seconds to neighboring router B. However, router B has its maximum recovery time configured at 400 seconds. Router B will only wait for 400 seconds before it purges its LDP information from router A.

To configure recovery time, include the recovery-time statement and the maximum-neighbor-recovery-time statement:

```
graceful-restart {
    maximum-neighbor-recovery-time seconds;
    recovery-time seconds;
}
```

For a list of hierarchy levels at which you can configure these statements, see the statement summary sections for these statements.

Configuring LDP Received-Label Filtering

You can filter received LDP label bindings, applying policies to accept or deny bindings advertised by neighboring routers. To configure received-label filtering, include the import statement:

```
import [ policy-names ];
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

The named policy (configured at the [edit policy-options] hierarchy level) is applied to all label bindings received from all LDP neighbors. All filtering is done with from statements. Table 11 on page 343 lists the only from operators that apply to LDP received-label filtering.

Table 11: from Operators That Apply to LDP Received-Label Filtering

from Operator	Description
interface	Matches on bindings received from a neighbor that is adjacent over the specified interface
neighbor	Matches on bindings received from the specified LDP router ID
next-hop	Matches on bindings received from a neighbor advertising the specified interface address
route-filter	Matches on bindings with the specified prefix

If a binding is filtered, it still appears in the LDP database, but is not considered for installation as part of a label-switched path (LSP).

Generally, applying policies in LDP can be used only to block the establishment of LSPs, not to control their routing. This is because the path that an LSP follows is

determined by unicast routing, and not by LDP. However, when there are multiple equal-cost paths to the destination through different neighbors, you can use LDP filtering to exclude some of the possible next hops from consideration. (Otherwise, LDP chooses one of the possible next hops at random.)

LDP sessions are not bound to interfaces or interface addresses. LDP advertises only per-router (not per-interface) labels; so if multiple parallel links exist between two routers, only one LDP session is established, and it is not bound to a single interface. When a router has multiple adjacencies to the same neighbor, take care to ensure that the filter does what is expected. (Generally, using next-hop and interface is not appropriate in this case.)

If a label has been filtered (meaning that it has been rejected by the policy and is not used to construct an LSP), it is marked as filtered in the database:

```
user@host> show ldp database
Input label database, 10.10.255.1:0–10.10.255.6:0
Label Prefix
3 10.10.255.6/32 (Filtered)
Output label database, 10.10.255.1:0–10.10.255.6:0
Label Prefix
3 10.10.255.1/32 (Filtered)
```

For more information about how to configure policies for LDP, see the *JUNOS Policy Framework Configuration Guide*.

Examples: Configuring Received-Label Filtering

Accept only /32 prefixes from all neighbors:

```
[edit]
protocols {
   ldp {
      import only-32;
      ...
   }
}
policy-options {
   policy-statement only-32 {
      term first {
         from {
            route-filter 0.0.0.0/0 upto /31;
         }
         then reject;
      }
      then accept;
   }
}
```

Accept 131.108/16 or longer from router ID 10.10.255.2 and accept all prefixes from all other neighbors:

```
[edit]
protocols {
   ldp {
```

```
        import nosy-neighbor;
        ...
    }
}
policy-options {
    policy-statement nosy-neighbor {
        term first {
            from {
                neighbor 10.10.255.2;
                route-filter 131.108.0.0/16 orlonger accept;
                route-filter 0.0.0.0/0 orlonger reject;
            }
        }
        then accept;
    }
}
```

Configuring LDP Outbound-Label Filtering

You can configure export policies to filter LDP outbound labels. You can filter outbound label bindings by applying routing policies to block bindings from being advertised to neighboring routers. To configure outbound label filtering, include the export statement:

```
export [policy-name];
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

The named export policy (configured at the [edit policy-options] hierarchy level) is applied to all label bindings transmitted to all LDP neighbors. The only from operator that applies to LDP outbound label filtering is route-filter, which matches bindings with the specified prefix. The only to operators that apply to outbound label filtering are the operators in Table 12 on page 345.

Table 12: to Operators for LDP Outbound-Label Filtering

to Operator	Description
interface	Matches on bindings sent to a neighbor that is adjacent over the specified interface
neighbor	Matches on bindings sent to the specified LDP router ID
next-hop	Matches on bindings sent to a neighbor advertising the specified interface address

If a binding is filtered, the binding is not advertised to the neighboring router, but it can be installed as part of an LSP on the local router. You can apply policies in LDP to block the establishment of LSPs, but not to control their routing. The path an LSP follows is determined by unicast routing, not by LDP.

LDP sessions are not bound to interfaces or interface addresses. LDP advertises only per-router (not per-interface) labels. If multiple parallel links exist between two routers, only one LDP session is established, and it is not bound to a single interface.

Do not use the next-hop and interface operators when a router has multiple adjacencies to the same neighbor.

Filtered labels are marked in the database:

```
user@host> show ldp database
Input label database, 10.10.255.1:0–10.10.255.3:0
Label Prefix
100007 10.10.255.2/32
3 10.10.255.3/32
Output label database, 10.10.255.1:0–10.10.255.3:0
Label Prefix
3 10.10.255.1/32
100001 10.10.255.6/32 (Filtered)
```

For more information about how to configure policies for LDP, see the *JUNOS Policy Framework Configuration Guide*.

Examples: Configuring Outbound-Label Filtering

Block transmission of 10.10.255.6/32 to all neighbors:

```
[edit protocols]
ldp {
   export block-one;
}
policy-options {
   policy-statement block-one {
      term first {
         from {
            route-filter 10.10.255.6/32 exact;
         }
         then reject;
      }
      then accept;
   }
}
```

Send only 131.108/16 or longer to router ID 10.10.255.2, and send all prefixes to all other routers:

```
[edit protocols]
ldp {
   export limit-lsps;
}
policy-options {
   policy-statement limit-lsps {
      term allow-one {
         from {
            route-filter 131.108.0.0/16 orlonger;
         }
```

```
            to {
                neighbor 10.10.255.2;
            }
            then accept;
        }
        term block-the-rest {
            to {
                neighbor 10.10.255.2;
            }
            then reject;
        }
        then accept;
    }
}
```

Configuring LDP Transport Address Control

You can control the transport address used by LDP. The transport address is the address used for the TCP session over which LDP is running. To configure transport address control, include the transport-address statement:

```
transport-address ( router-id | interface );
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

If you select router-id, the address of the router identifier is used as the transport address (unless otherwise configured, the router identifier is typically the same as the loopback address). If you select interface, the interface address is used as the transport address for any LDP sessions to neighbors that can be reached over that interface. Note that the router identifier is used as the transport address by default.

You cannot use transport-address interface when there are multiple parallel links to the same LDP neighbor, because the LDP specification requires that the same transport address be advertised on all interfaces to the same neighbor. If LDP detects multiple parallel links to the same neighbor, it disables interfaces to that neighbor one by one until the condition is cleared, either by disconnecting the neighbor on an interface or by configuring transport-address router-id.

Configuring the LDP Egress Policy

You can control the set of prefixes that are advertised into LDP and cause the router to be the egress router for those prefixes. By default, only the loopback address is advertised into LDP. To configure the set of prefixes from the routing table to be advertised into LDP, include the egress-policy statement:

```
egress-policy policy-name;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

NOTE: If you configure an egress policy for LDP that does not include the loopback address, it is no longer advertised in LDP. To continue to advertise the loopback address, you need to explicitly configure it as a part of the LDP egress policy.

The named policy (configured at the [edit policy-options] or the [edit logical-systems *logical-system-name* policy-options] hierarchy level) is applied to all routes in the routing table. Those routes that match the policy are advertised into LDP. You can control the set of neighbors to which those prefixes are advertised by using the export statement. Only from operators are considered; you can use any valid from operator. For more information, see the *JUNOS Routing Protocols Configuration Guide*.

Example: Configuring the LDP Egress Policy

Advertise all connected routes into LDP:

```
[edit protocols]
ldp {
   egress-policy connected-only;
}
policy-options {
   policy-statement connected-only {
      from {
         protocol direct;
      }
      then accept;
   }
}
```

Configuring FEC Deaggregation

When an LDP egress router advertises multiple prefixes, the prefixes are bound to a single label and aggregated into a single forwarding equivalence class (FEC). By default, LDP maintains this aggregation as the advertisement traverses the network.

By default, because an LSP cannot be split across multiple next hops and all the prefixes are bound into a single LSP, you cannot load-balance across equal-cost paths.

To change the default to load-balance across equal-cost paths, you need to deaggregate the FECs. Deaggregating the FECs causes each prefix to be bound to a separate label and become a separate LSP.

To configure deaggregated FECs, include the deaggregate statement:

```
deaggregate;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

For all LDP sessions, you can configure deaggregated FECs only globally.

Deaggregating a FEC allows the resulting multiple LSPs to be distributed across multiple equal-cost paths and distributes LSPs across the multiple next hops on the egress segments but installs only one next hop per LSP.

To aggregate FECs, include the no-deaggregate statement:

```
no-deaggregate;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

For all LDP sessions, you can configure aggregated FECs only globally.

Configuring Policers for LDP FECs

You can configure the JUNOS software to track and police traffic for LDP FECs. LDP FEC policers can be used to do any of the following:

- Track or police the ingress traffic for an LDP FEC.
- Track or police the transit traffic for an LDP FEC.
- Track or police LDP FEC traffic originating from a specific forwarding class.
- Track or police LDP FEC traffic originating from a specific virtual routing and forwarding (VRF) site.
- Discard false traffic bound for a specific LDP FEC.

To police traffic for an LDP FEC, you must first configure a filter. Specifically, you need to configure either the interface statement or the interface-set statement at the [edit firewall family *protocol-family* filter *filter-name* term *term-name* from] hierarchy level. The interface statement allows you to match the filter to a single interface. The interface-set statement allows you to match the filter to multiple interfaces.

For more information on how to configure the interface statement, the interface-set statement, and policers for LDP FECs, see the *JUNOS Policy Framework Configuration Guide*.

Once you have configured the filters, you need to include them in the policing statement configuration for LDP. To configure policers for LDP FECs, include the policing statement:

```
policing {
    fec fec-address {
        ingress-traffic filter-name;
        transit-traffic filter-name;
    }
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

The policing statement includes the following options:

- fec—Specify the FEC address for the LDP FEC you want to police.
- ingress-filter—Specify the name of the ingress traffic filter.
- transit-traffic—Specify the name of the transit traffic filter.

Configuring LDP IPv4 FEC Filtering

By default, when a targeted LDP session is established, the JUNOS software always exchanges both the IPv4 FECs and the Layer 2 circuit FECs over the targeted LDP session. For an LDP session to an indirectly connected neighbor, you might only want to export Layer 2 circuit FECs to the neighbor if the session was specifically configured to support Layer 2 circuits or VPLS.

In a mixed vendor network where all non-BGP prefixes are advertised into LDP, the LDP database can become large. For this type of environment, it can be useful to prevent the advertisement of IPv4 FECs over LDP sessions formed due to Layer 2 circuit or LDP VPLS configuration. Similarly, it can be useful to filter any IPv4 FECs received in this sort of environment.

If all the LDP neighbors associated with an LDP session are Layer 2 only, you can configure the JUNOS software to only advertise Layer 2 circuit FECs by configuring the l2-smart-policy statement. This feature also automatically filters out the IPv4 FECs received on this session. If you have configured an explicit export or import policy, this feature is disabled.

If one of the LDP session's neighbors is formed due to a discovered adjacency or if the adjacency is formed due to an LDP tunneling configuration on one or more RSVP LSPs, the IPv4 FECs are advertised and received using the default behavior.

To prevent LDP from exporting IPv4 FECs over LDP sessions with Layer 2 neighbors only and to filter out IPv4 FECs received over such sessions, include the l2-smart-policy statement:

```
l2-smart-policy;
```

For a list of hierarchy levels at which you can configure this statement, see the statement summary for this statement.

Configuring BFD for LDP LSPs

You can configure Bidirectional Forwarding Detection (BFD) for LDP LSPs. BFD can be turned on for all or a subset of LDP IPv4 FECs.

An error is logged whenever a BFD session for a path fails. The following shows how BFD for LDP LSP log messages might appear:

```
RPD_LDP_BFD_UP: LDP BFD session for FEC  10.255.16.14/32 is up
RPD_LDP_BFD_DOWN: LDP BFD session for FEC  10.255.16.14/32 is down
```

You can also configure BFD for RSVP LSPs, as described in “Configuring BFD for RSVP LSPs” on page 169.

To enable BFD for LDP LSPs, include the oam and bfd-liveness-detection statements. You can enable BFD for all LDP LSPs on the router or just for the LDP LSPs associated with a specific FEC.

```
oam {
    bfd-liveness-detection {
        ecmp;
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        minimum-transmit-interval milliseconds;
        multiplier detection-time-multiplier;
    }
    fec fec-address;
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

The oam statement includes the following option:

- fec—Specify the FEC address.

The bfd-liveness-detection statement includes the following options:

- ecmp—Causes LDP to establish BFD sessions for all ECMP paths configured for the specified FEC. If you configure the ecmp option, you must also configure the periodic-traceroute statement for the specified FEC. If you do not do so, the commit fails. You can configure the periodic-traceroute statement at the global hierarchy level ([edit protocols ldp oam]) while only configuring the ecmp option for a specific FEC ([edit protocols ldp oam fec *address* bfd-liveness-detection]).
- minimum-interval—Specifies the minimum transmit and receive interval. If you configure the minimum-interval option, you do not need to configure the minimum-receive-interval option or the minimum-transmit-interval option.
- minimum-receive-interval—Specifies the minimum receive interval. The range is from 1 through 255,000 milliseconds.
- minimum-transmit-interval—Specifies the minimum transmit interval. The range is from 1 through 255,000 milliseconds.
- multiplier—Specifies the detection time multiplier. The range is from 1 through 255.

Configuring ECMP-Aware BFD for RSVP LSPs

When you configure BFD for a FEC, a BFD session is established for only one active local next-hop for the router. However, you can configure multiple BFD sessions, one for each FEC associated with a specific Equal Cost Multipath (ECMP) path. For this to function properly, you also need to configure LDP LSP periodic traceroute. (See “Configuring LDP LSP Traceroute” on page 352.) RSVP LSP traceroute is used to discover ECMP paths. A BFD session is initiated for each ECMP path discovered. Whenever a BFD session for one of the ECMP paths fails, an error is logged.

RSVP LSP traceroute is run periodically to check the integrity of the ECMP paths. The following might occur when a problem is discovered:

- If the latest RSVP LSP traceroute for a FEC differs from the previous traceroute, the BFD sessions associated with that FEC (the BFD sessions for address ranges that have changed from previous run) are brought down and new BFD sessions are initiated for the destination addresses in the altered ranges.
- If the RSVP LSP traceroute returns an error (for example, a timeout), all the BFD sessions associated with that FEC are torn down.

To configure RSVP to establish BFD sessions for all ECMP paths configured for the specified FEC, include the ecmp statement. If you configure the ecmp statement, you must also configure the periodic-traceroute statement for the specified FEC. If you do not do so, the commit fails. You can configure the periodic-traceroute statement at the global hierarchy level ([edit protocols ldp oam]) while only configuring the ecmp statement for a specific FEC ([edit protocols ldp oam fec *address* bfd-liveness-detection]).

```
ecmp;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Configuring LDP LSP Traceroute

The JUNOS software allows you to trace the route an LDP-signalled LSP follows. LDP LSP traceroute is based on RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*. This feature allows you to periodically trace all paths in a FEC. The FEC topology information is stored in a database accessible from the CLI.

A topology change does not automatically trigger a trace of an LDP LSP. However, you can manually initiate a traceroute. If the traceroute request is for an FEC that is currently in the database, the contents of the database are updated with the results.

The periodic traceroute feature applies to all FECs specified by the oam statement configured at the [edit protocols ldp] hierarchy level. To configure periodic LDP LSP traceroute, include the periodic-traceroute statement:

```
periodic-traceroute {
    disable;
    exp exp-value;
    fanout fanout-value;
    frequency minutes;
    paths number-of-paths;
    retries retry-attempts;
    source address;
    ttl ttl-value;
    wait seconds;
}
```

You can configure this statement at the following hierarchy levels:

- [edit protocols ldp oam]
- [edit protocols ldp oam fec *address*]

The periodic-traceroute statement includes the following options:

- exp—Specify the class of service to use when sending probes.
- fanout—Specify the maximum number of next hops to search per node.
- frequency—Specify the interval between traceroute attempts.
- paths—Specify the maximum number of paths to search.
- retries—Specify the number of attempts to send a probe to a specific node before giving up.
- source—Specify the IPv4 source address to use when sending probes.
- ttl—Specify the maximum time-to-live value. Nodes that are beyond this value are not traced.
- wait—Specify the wait interval before resending a probe packet.

Collecting LDP Statistics

LDP traffic statistics show the volume of traffic that has passed through a particular FEC on a router.

When you configure the traffic-statistics statement at the [edit protocols ldp] hierarchy level, the LDP traffic statistics are gathered periodically and written to a file. You can configure how often statistics are collected (in seconds) by using the interval option. The default collection interval is 5 minutes. You must configure an LDP statistics file; otherwise LDP traffic statistics are not gathered. If the LSP goes down, the LDP statistics are reset.

To collect LDP traffic statistics, include the traffic-statistics statement:

```
traffic-statistics {
   file filename <files number> <replace> <size size>
   <world-readable | no-world-readable>;
   interval interval;
   no-penultimate-hop;
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

This section includes the following topics:

- LDP Statistics Output on page 353
- Disabling LDP Statistics on the Penultimate-Hop Router on page 354
- LDP Statistics Limitations on page 355

LDP Statistics Output

The following is sample output from an LDP statistics file:

```
FEC                 Type       Packets     Bytes    Shared
10.255.350.448/32   Transit          0         0        No
                    Ingress          0         0        No
10.255.350.450/32   Transit          0         0       Yes
                    Ingress          0         0        No
10.255.350.451/32   Transit          0         0        No
                    Ingress          0         0        No
220.220.220.1/32    Transit          0         0       Yes
                    Ingress          0         0        No
220.220.220.2/32    Transit          0         0       Yes
                    Ingress          0         0        No
220.220.220.3/32    Transit          0         0       Yes
                    Ingress          0         0        No
May 28 15:02:05, read 12 statistics in  00:00:00 seconds
```

The following describes each column of data collected in the LDP statistics file:

- Bytes—Number of bytes of data passed by the FEC since its LSP came up.
- FEC—FEC for which LDP traffic statistics are collected.
- Packets—Number of packets passed by the FEC since its LSP came up.
- read—This number (which appears next to the date and time) might differ from the actual number of the statistics displayed. Some of the statistics are summarized before being displayed.
- Shared—A Yes value indicates that several prefixes are bound to the same label (for example, when several prefixes are advertised with an egress policy). The LDP traffic statistics for this case apply to all the prefixes and should be treated as such.
- Type—Type of traffic originating from a router, either Ingress (originating from this router) or Transit (forwarded through this router).

Disabling LDP Statistics on the Penultimate-Hop Router

Gathering LDP traffic statistics at the penultimate-hop router can consume excessive system resources, on next-hop routes in particular. This problem is exacerbated if you have configured the deaggregate statement in addition to the traffic-statistics statement. For routers reaching their limit of next-hop route usage, we recommend configuring the no-penultimate-hop option for the traffic-statistics statement:

```
traffic-statistics {
    no-penultimate-hop;
}
```

For a list of hierarchy levels at which you can configure the traffic-statistics statement, see the statement summary section for this statement.

NOTE: When you configure the no-penultimate-hop option, no statistics are available for the FECs that are the penultimate hop for this router.

Whenever you include or remove this option from the configuration, the LDP sessions are taken down and then restarted.

The following is sample output from an LDP statistics file showing routers on which the no-penultimate-hop option is configured:

```
FEC                 Type            Packets          Bytes       Shared
10.255.245.218/32   Transit               0              0           No
                    Ingress               4            246           No
10.255.245.221/32   Transit     statistics disabled
                    Ingress     statistics disabled
13.1.1.0/24         Transit     statistics disabled
                    Ingress     statistics disabled
13.1.3.0/24         Transit     statistics disabled
                    Ingress     statistics disabled
```

LDP Statistics Limitations

The following are issues related to collecting LDP statistics by configuring the traffic-statistics statement:

- You cannot clear the LDP statistics.
- If you shorten the specified interval, a new LDP statistics request is issued only if the statistics timer expires later than the new interval.
- A new LDP statistics collection operation cannot start until the previous one has finished. If the interval is short or if the number of LDP statistics is large, the time gap between the two statistics collections might be longer than the interval.

When an LSP goes down, the LDP statistics are reset.

Tracing LDP Protocol Traffic

The following sections describe how to configure the trace options to examine LDP protocol traffic:

- Tracing LDP Protocol Traffic at the Protocol and Routing Instance Levels on page 355
- Tracing LDP Protocol Traffic Within FEC on page 356
- Examples: Tracing LDP Protocol Traffic on page 357

Tracing LDP Protocol Traffic at the Protocol and Routing Instance Levels

To trace LDP protocol traffic, you can specify options in the global traceoptions statement at the [edit routing-options] hierarchy level, and you can specify LDP-specific options by including the traceoptions statement:

```
traceoptions {
   file filename <replace> <size size> <files number> <no-stamp> <world-readable |
      no-world-readable>;
   flag flag <flag-modifier> <disable>;
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Use the file statement to specify the name of the file that receives the output of the tracing operation. All files are placed in the directory /var/log. We recommend that you place LDP-tracing output in the file ldp-log.

The following trace flags display the operations associated with the sending and receiving of various LDP messages. Each can carry one or more of the following modifiers:

- address—Trace the operation of address and address withdrawal messages.
- binding—Trace label-binding operations.
- error—Trace error conditions.
- event—Trace protocol events.
- initialization—Trace the operation of initialization messages.
- label—Trace the operation of label request, label map, label withdrawal, and label release messages.
- notification—Trace the operation of notification messages.
- packet—Trace the operation of address, address withdrawal, initialization, label request, label map, label withdrawal, label release, notification, and periodic messages. This modifier is equivalent to setting the address, initialization, label, notification, and periodic modifiers.
- path—Trace label-switched path operations.
- periodic—Trace the operation of hello and keepalive messages.
- route—Trace the operation of route messages.
- state—Trace protocol state transitions.

Tracing LDP Protocol Traffic Within FEC

You can trace LDP protocol traffic within a specific FEC. You can filter LDP trace statements based on a FEC. The following trace flags are available for this purpose: route, path, and binding.

The following example illustrates how you might configure the LDP traceoptions statement to filter LDP trace statements based on a FEC:

```
[edit protocols ldp traceoptions]
flag route filter match-on fec policy "filter-policy-for-ldp-fec";
```

This feature has the following limitations:

- The filtering capability is only available for FECs composed of IP version 4 (IPv4) prefixes.
- Layer 2 circuit FECs cannot be filtered.
- When you configure both route tracing and filtering, Multiprotocol Label Switching (MPLS) routes are not displayed (they are blocked by the filter).
- Filtering is determined by the policy and the configured value for the match-on option. When configuring the policy, be sure that the default behavior is always reject.
- The only match-on option is fec. Consequently, the only type of policy you should include is a route-filter policy.

Examples: Tracing LDP Protocol Traffic

Trace LDP path messages in detail:

```
[edit]
protocols {
    ldp {
        traceoptions {
            file ldp size 10m files 5;
            flag path;
        }
    }
}
```

Trace all LDP outgoing messages:

```
[edit]
protocols {
    ldp {
        traceoptions {
            file ldp size 10m files 5;
            flag packets;
        }
    }
}
```

Trace all LDP error conditions:

```
[edit]
protocols {
    ldp {
        traceoptions {
            file ldp size 10m files 5;
            flag error;
        }
    }
}
```

Trace all LDP incoming messages and all label-binding operations:

```
[edit]
```

```
protocols {
    ldp {
        traceoptions {
            file ldp size 10m files 5 world-readable;
            flag packets receive;
            flag binding;
        }
        interface all {
        }
    }
}
```

Configuring Miscellaneous LDP Properties

The following sections describe how to configure a number of miscellaneous LDP properties:

- Configuring LDP to Use the IGP Route Metric on page 358
- Preventing Ingress Routes from Being Added to inet.0 on page 358
- Multiple-Instance LDP and Carrier-of-Carriers VPNs on page 359
- Configuring MPLS and LDP to Pop the Label on the Ultimate-Hop Router on page 359
- Enabling LDP over RSVP-Established LSPs on page 360
- Enabling LDP over RSVP-Established LSPs in Heterogeneous Networks on page 360
- Configuring the TCP MD5 Signature for an LDP Session on page 361
- Disabling SNMP Traps for LDP on page 361
- Enabling Strict Targeted Hellos on page 362
- Configuring LDP Synchronization with the IGP on page 362
- Configuring the Label Withdrawal Timer on page 363
- Ignoring the LDP Subnet Check on page 363

Configuring LDP to Use the IGP Route Metric

Use the track-igp-metric statement if you want the interior gateway protocol (IGP) route metric to be used for the LDP routes instead of the default LDP route metric (the default LDP route metric is 1).

To use the IGP route metric, include the track-igp-metric statement:

```
track-igp-metric;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Preventing Ingress Routes from Being Added to inet.0

By configuring the no-forwarding statement, you can prevent ingress routes from being added to the inet.0 routing table instead of the inet.3 routing table even if you

enabled the traffic-engineering bgp-igp statement at the [edit protocols mpls] or the [edit logical-systems *logical-system-name* protocols mpls] hierarchy level. By default, the no-forwarding statement is disabled.

To omit ingress routes from the inet.0 routing table, include the no-forwarding statement:

```
no-forwarding;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Multiple-Instance LDP and Carrier-of-Carriers VPNs

By configuring multiple LDP routing instances, you can use LDP to advertise labels in a carrier-of-carriers VPN from a service provider provider edge (PE) router to a customer carrier customer edge (CE) router. This is especially useful when the carrier customer is a basic Internet service provider (ISP) and wants to restrict full Internet routes to its PE routers. By using LDP instead of BGP, the carrier customer shields its other internal routers from the Internet. Multiple-instance LDP is also useful when a carrier customer wants to provide Layer 2 or Layer 3 VPN services to its customers.

For an example of how to configure multiple LDP routing instances for carrier-of-carriers VPNs, see the *JUNOS Feature Guide*.

Configuring MPLS and LDP to Pop the Label on the Ultimate-Hop Router

The default advertised label is label 3 (Implicit Null label). If label 3 is advertised, the penultimate-hop router removes the label and sends the packet to the egress router. If ultimate-hop popping is enabled, label 0 (IPv4 Explicit Null label) is advertised. Ultimate-hop popping ensures that any packets traversing an MPLS network include a label.

To configure ultimate-hop popping, include the explicit-null statement:

```
explicit-null;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

NOTE: Juniper Networks routers queue packets based on the incoming label. Routers from other vendors might queue packets differently. Keep this in mind when working with networks containing routers from multiple vendors.

For more information about labels, see “Label Description” on page 25 and “Label Allocation” on page 25.

Enabling LDP over RSVP-Established LSPs

You can run LDP over LSPs established by RSVP, effectively tunneling the LDP-established LSP through the one established by RSVP. To do so, enable LDP on the lo0.0 interface (see "Enabling and Disabling LDP" on page 339). You must also configure the LSPs over which you want LDP to operate by including the ldp-tunneling statement at the [edit protocols mpls label-switched-path *lsp-name*] hierarchy level:

```
[edit]
protocols {
   mpls {
      label-switched-path lsp-name {
         from source;
         to destination;
         ldp-tunneling;
      }
   }
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

For more information about tunneling LDP LSPs, see "Tunneling LDP LSPs in RSVP LSPs" on page 331.

Enabling LDP over RSVP-Established LSPs in Heterogeneous Networks

Some other vendors use an OSPF metric of 1 for the loopback address. Juniper Networks routers use an OSPF metric of 0 for the loopback address. This might require that you manually configure the RSVP metric when deploying LDP tunneling over RSVP LSPs in heterogeneous networks.

When a Juniper Networks router is linked to another vendor's router through an RSVP tunnel, and LDP tunneling is also enabled, by default the Juniper Networks router might not use the RSVP tunnel to route traffic to the LDP destinations downstream of the other vendor's egress router if the RSVP path has a metric of 1 larger than the physical OSPF path.

To ensure that LDP tunneling functions properly in heterogeneous networks, you can configure OSPF to ignore the RSVP LSP metric by including the ignore-lsp-metrics statement:

```
ignore-lsp-metrics;
```

You can configure this statement at the following hierarchy levels:

- [edit protocols ospf traffic-engineering shortcuts]
- [edit logical-systems *logical-system-name* protocols ospf traffic-engineering shortcuts]

To enable LDP over RSVP LSPs, you also still need to complete the procedure in "Enabling LDP over RSVP-Established LSPs" on page 360.

Configuring the TCP MD5 Signature for an LDP Session

You can configure an MD5 signature for an LDP TCP connection to protect against the introduction of spoofed TCP segments into LDP session connection streams.

A router using the MD5 signature option is configured with a password for each peer for which authentication is required. The password is stored encrypted.

LDP hello adjacencies can still be created even when peering interfaces are configured with different security signatures. However, the TCP session cannot be authenticated and is never established.

NOTE: If you apply an MD5 signature to an LDP interface with an established session, it drops the TCP connection and all the associated label bindings to the FEC entries for that session. The session regenerates the database information for that session once both interfaces agree on a common security method and password.

To configure an MD5 signature for an LDP TCP connection, include the session and authentication-key statement:

```
session address {
    authentication-key md5-authentication-key;
}
```

For a list of hierarchy levels at which you can include these statements, see the statement summary section for the session statement.

Use the session statement to configure the address for the remote end of the LDP session.

The *md5-authentication-key* (password) can be up to 69 characters long. Characters can include any ASCII strings. If you include spaces, enclose all characters in quotation marks.

Disabling SNMP Traps for LDP

Whenever an LDP LSP makes a transition from up to down, or down to up, the router sends a Simple Network Management Protocol (SNMP) trap. However, it is possible to disable the LDP SNMP traps on a router, logical system, or routing instance.

For information about the LDP SNMP traps and the proprietary LDP Management Information Base (MIB), see the *JUNOS Network Management Configuration Guide*.

To disable SNMP traps for LDP, specify the trap disable option for the log-updown statement:

```
log-updown {
    trap disable;
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Enabling Strict Targeted Hellos

This feature prevents LDP sessions from being established with remote neighbors that have not been specifically configured. If you configure the strict-targeted-hellos statement, an LDP peer will not respond to targeted hellos coming from a source that is not one of the configured remote neighbors. Configured remote neighbors can include:

- Endpoints of RSVP tunnels for which LDP tunneling is configured
- Layer 2 circuit neighbors

A hello from an unconfigured neighbor is ignored, and an error is logged (with the error traceoption flag) indicating the source. For example, if a targeted hello is received from 10.0.0.1, and no neighbor with this address is specifically configured, the following message is printed to the LDP log file:

```
LDP: Ignoring targeted hello from 10.0.0.1
```

To enable strict targeted hellos, include the strict-targeted-hellos statement:

```
strict-targeted-hellos;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Configuring LDP Synchronization with the IGP

LDP is a protocol for distributing labels in non-traffic-engineered applications. Labels are distributed along the best path determined by the IGP. If synchronization between LDP and the IGP is not maintained, the LSP goes down. When LDP is not fully operational on a given link (a session is not established and labels are not exchanged), the IGP advertises the link with the maximum cost metric. The link is not preferred but remains in the network topology.

LDP synchronization is supported only on active point-to-point interfaces and LAN interfaces configured as point-to-point under the IGP. LDP synchronization is not supported during graceful restart.

To advertise the maximum cost metric until LDP is operational for synchronization, include the ldp-synchronization statement:

```
ldp-synchronization {
    disable;
    hold-time seconds;
}
```

To disable synchronization, include the disable statement. To configure the time period to advertise the maximum cost metric for a link that is not fully operational, include the hold-time statement.

For a list of hierarchy levels at which you can configure this statement, see the statement summary section for this statement.

Configuring the Label Withdrawal Timer

The label withdrawal timer delays sending a label withdrawal message for a FEC to a neighbor. When an IGP link to a neighbor fails, the label associated with the FEC has to be withdrawn from all the upstream routers if the neighbor is the nexthop for the FEC. After the IGP converges and a label is received from a new nexthop, the label is readvertised to all the upstream routers. This is the typical network behavior. By delaying label withdrawal by a small amount of time (for example, until the IGP converges and the router receives a new label for the FEC from the downstream nexthop), the label withdrawal and sending a label mapping soon could be avoided. The label-withdrawal-delay statement allows you to configure this delay time. By default, the delay is 60 seconds.

If the router receives the new label before the timer runs out, the label withdrawal timer is canceled. However, if the timer runs out, the label for the FEC is withdrawn from all of the upstream routers.

By default, LDP waits for 60 seconds before withdrawing labels to avoid resignaling LSPs multiple times while the IGP is reconverging. To configure the label withdrawal delay time in seconds, include the label-withdrawal-delay statement:

```
label-withdrawal-delay seconds;
```

For a list of hierarchy levels at which you can configure this statement, see the statement summary section for this statement.

Ignoring the LDP Subnet Check

For JUNOS Release 8.4 and later releases, an LDP source address subnet check was added for the neighbor establishment procedure. The source address in the LDP link hello packet is matched against the interface address. This has caused an interoperability issue with some other vendor's equipment.

To allow Juniper Networks routers to ignore the subnet check, include the allow-subnet-mismatch statement:

```
allow-subnet-mismatch;
```

This statement can be included at the following hierarchy levels:

- [edit protocols ldp interface *interface-name*]
- [edit logical-systems *logical-system-name* protocols ldp interface *interface-name*]

Chapter 16

Summary of LDP Configuration Statements

This chapter provides a reference for each Label Distribution Protocol (LDP) configuration statement. The statements are organized alphabetically.

allow-subnet-mismatch

Syntax allow-subnet-mismatch;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp interface *interface-name*], [edit protocols ldp interface *interface-name*]

Release Information Statement introduced in JUNOS Release 9.3.

Description Ignore the LDP subnet check. For JUNOS Release 8.4 and later releases, an LDP source address subnet check was added for the neighbor establishment procedure. The source address in the LDP link hello packet is matched against the interface address.

Default The source address in the LDP link hello packet is matched against the interface address.

Usage Guidelines See "Ignoring the LDP Subnet Check" on page 363.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

authentication-key

Syntax authentication-key *md5-authentication-key*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp session *address*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp session *address*],
[edit protocols ldp session *address*],
[edit routing-instances *routing-instance-name* protocols ldp session *address*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Configure the MD5 authentication signature. The maximum length of the authentication signature is 69 characters.

Usage Guidelines See "Configuring the TCP MD5 Signature for an LDP Session" on page 361.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

bfd-liveness-detection

Syntax

```
bfd-liveness-detection {
    ecmp;
    minimum-interval milliseconds;
    minimum-receive-interval milliseconds;
    minimum-transmit-interval milliseconds;
    multiplier detection-time-multiplier;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols ldp oam],
[edit logical-systems *logical-system-name* protocols ldp oam fec *address*],
[edit protocols ldp oam],
[edit protocols ldp oam fec *address*]

Release Information

Statement introduced in JUNOS Release 7.6.
Support for the bfd-liveness-detection statement at the [edit protocols ldp oam fec *address*] hierarchy level and the ecmp option were added in JUNOS Release 9.0.

Description

Enable Bidirectional Forwarding Detection (BFD) for all MPLS LSPs or for just a specific LSP.

Options

minimum-interval—Minimum transmit and receive interval.
Range: 50 through 255,000 milliseconds
Default: 50

minimum-receive-interval—Minimum receive interval.
Range: 50 through 255,000 milliseconds
Default: 50

minimum-transmit-interval—Minimum transmit interval.
Range: 50 through 255,000 milliseconds
Default: 50

multiplier—Detection time multiplier.
Range: 50 through 255
Default: 3

The ecmp option is explained separately.

Usage Guidelines

See “Configuring BFD for LDP LSPs” on page 350.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

deaggregate

Syntax deaggregate | no-deaggregate;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp],
[edit protocols ldp],
[edit routing-instances *routing-instance-name* protocols ldp]

Release Information Statement introduced before JUNOS Release 7.4.

Description Control forwarding equivalence class (FEC) deaggregation on the router.

Default Deaggregation is disabled on the router.

Options deaggregate—Deaggregate FECs.

no-deaggregate—Aggregate FECs.

Usage Guidelines See "Configuring FEC Deaggregation" on page 348.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

disable

Syntax disable;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp graceful-restart],
[edit logical-systems *logical-system-name* protocols ldp interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* routing-options graceful-restart],
[edit protocols ldp graceful-restart],
[edit protocols ldp interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ldp interface *interface-name*],
[edit routing-instances *routing-instance-name* routing-options graceful-restart]

Release Information Statement introduced before JUNOS Release 7.4.

Description Explicitly disable LDP on an interface, or explicitly disable LDP graceful restart.

Default LDP is enabled on interfaces configured with the LDP interface statement. LDP graceful restart is automatically enabled when graceful restart is enabled under the [edit routing-options] hierarchy level.

Usage Guidelines See "Enabling and Disabling LDP" on page 339 and "Configuring LDP Graceful Restart" on page 341.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

ecmp

Syntax ecmp;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp oam bfd-liveness-detection],
[edit logical-systems *logical-system-name* protocols ldp oam fec *address* bfd-liveness-detection],
[edit protocols ldp oam bfd-liveness-detection],
[edit protocols ldp oam fec *address* bfd-liveness-detection]

Release Information Statement introduced in JUNOS Release 8.5.

Description Cause RSVP to establish BFD sessions for all ECMP paths configured for the specified FEC. If you configure the ecmp statement, you must also configure the periodic-traceroute statement for the specified FEC. If you do not do so, the commit fails. You can configure the periodic-traceroute statement at the global hierarchy level ([edit protocols ldp oam]) while only configuring the ecmp statement for a specific FEC ([edit protocols ldp oam fec *address* bfd-liveness-detection]).

Usage Guidelines See "Configuring ECMP-Aware BFD for RSVP LSPs" on page 351.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

egress-policy

Syntax egress-policy [*policy-names*]

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp],
[edit protocols ldp],
[edit routing-instances *routing-instance-name* protocols ldp]

Release Information Statement introduced before JUNOS Release 7.4.

Description Control the prefixes advertised into LDP.

Default Only the loopback address is advertised.

Options *policy-names*—Name of one or more routing policies.

Usage Guidelines See "Configuring the LDP Egress Policy" on page 347.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

explicit-null

Syntax explicit-null;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp],
[edit protocols ldp],
[edit routing-instances *routing-instance-name* protocols ldp]

Release Information Statement introduced before JUNOS Release 7.4.

Description Advertise label 0 to the egress router of a label-switched path (LSP).

Default If you do not include the explicit-null statement in the Multiprotocol Label Switching (MPLS) configuration, label 3 (implicit null) is advertised.

Usage Guidelines See "Configuring MPLS and LDP to Pop the Label on the Ultimate-Hop Router" on page 359.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

export

Syntax export [*policy-name*s];

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp],
[edit protocols ldp],
[edit routing-instances *routing-instance-name* protocols ldp]

Release Information Statement introduced before JUNOS Release 7.4.

Description Apply policy filters to outbound LDP label bindings. Filters are applied to all label bindings from all neighbors.

Options *policy-name*—Name of one or more routing policies.

Usage Guidelines See "Configuring LDP Outbound-Label Filtering" on page 345.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

graceful-restart

Syntax
```
graceful-restart {
    disable;
    helper-disable;
    maximum-neighbor-recovery-time value;
    recovery-time value;
}
```

Hierarchy Level
[edit logical-systems *logical-system-name* protocols ldp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp],
[edit protocols ldp],
[edit routing-instances *routing-instance-name* protocols ldp]

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable LDP graceful restart on the LDP master protocol instance or for a specific routing instance.

Usage Guidelines See "Configuring LDP Graceful Restart" on page 341.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

hello-interval

Syntax
```
hello-interval seconds;
```

Hierarchy Level
[edit logical-systems *logical-system-name* protocols ldp interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp interface *interface-name*],
[edit protocols ldp interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ldp interface *interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Control the rate at which hello messages are sent on the interface.

Options *seconds*—Length of time between hello packets.
Range: 1 through 65,535 seconds
Default: 5 seconds for link hello messages, 15 seconds for targeted hello messages

Usage Guidelines See "Configuring the LDP Hello Interval" on page 339.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

helper-disable

Syntax helper-disable;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp graceful-restart],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp graceful-restart],
[edit protocols ldp graceful-restart],
[edit routing-instances *routing-instance-name* protocols ldp graceful-restart]

Release Information Statement introduced before JUNOS Release 7.4.

Description Disable helper mode for LDP graceful restart. When helper mode is disabled, a router cannot help a neighboring router that is attempting to restart LDP.

Default Helper mode is enabled by default on all routing protocols (including LDP) that support graceful restart.

Usage Guidelines See "Configuring LDP Graceful Restart" on page 341.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

hold-time

Syntax hold-time *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp interface *interface-name*],
[edit protocols ldp interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ldp interface *interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify how long an LDP node should wait for a hello message before declaring a neighbor to be down. This value is sent as part of a hello message so that each LDP node tells its neighbors how long to wait.

Options *seconds*—Hold-time value.

Range: 1 through 65,535

Default: 15 seconds for link hello messages, 45 seconds for targeted hello messages

Usage Guidelines See "Configuring the LDP Hold Time" on page 340.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

ignore-lsp-metrics

Syntax ignore-lsp-metrics;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf traffic-engineering shortcuts],
[edit protocols ospf traffic-engineering shortcuts]

Release Information Statement introduced in JUNOS Release 7.5.

Description Cause OSPF to ignore the RSVP LSP metric.

Some other vendors use an OSPF metric of 1 for the loopback address. Juniper Networks routers use an OSPF metric of 0 for the loopback address. This can cause interoperability problems when you configure LDP tunneling over RSVP LSPs in heterogeneous networks.

Usage Guidelines See "Enabling LDP over RSVP-Established LSPs in Heterogeneous Networks" on page 360.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

import

Syntax import [*policy-name*s];

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp],
[edit protocols ldp],
[edit routing-instances *routing-instance-name* protocols ldp]

Release Information Statement introduced before JUNOS Release 7.4.

Description Apply policy filters to received LDP label bindings. Filters are applied to all label bindings from all neighbors.

Options *policy-name*—Name of one or more routing policies.

Usage Guidelines See "Configuring LDP Received-Label Filtering" on page 343.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

interface

Syntax
```
interface interface-name {
    disable;
    hello-interval seconds;
    hold-time seconds;
    transport-address (interface | loopback);
}
```

Hierarchy Level
```
[edit logical-systems logical-system-name protocols ldp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols
    ldp],
[edit protocols ldp],
[edit routing-instances routing-instance-name protocols ldp]
```

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable LDP on one or more router interfaces.

Default LDP is disabled on all interfaces.

Options *interface-name*—Name of an interface. To configure all interfaces, specify **all**.

The remaining statements are explained separately.

Usage Guidelines See "Enabling and Disabling LDP" on page 339.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

keepalive-interval

Syntax keepalive-interval *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp],
[edit protocols ldp],
[edit routing-instances *routing-instance-name* protocols ldp]

Release Information Statement introduced before JUNOS Release 7.4.

Description Set the keepalive interval value.

Options *seconds*—Keepalive value.
Range: 1 through 65,535
Default: 10 seconds

Usage Guidelines See "Configuring the LDP Keepalive Interval" on page 340.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

keepalive-timeout

Syntax keepalive-timeout *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp],
[edit protocols ldp],
[edit routing-instances *routing-instance-name* protocols ldp]

Release Information Statement introduced before JUNOS Release 7.4.

Description Set the keepalive timeout value. The keepalive timeout defines the amount of time that the neighbor LDP node waits before determining that the session has failed.

Options *seconds*—Keepalive timeout value.
Range: 1 through 65,535
Default: 30 seconds

Usage Guidelines See "Configuring the LDP Keepalive Timeout" on page 340.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

l2-smart-policy

Syntax l2-smart-policy;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp],
[edit protocols ldp],
[edit routing-instances *routing-instance-name* protocols ldp]

Release Information Statement introduced in JUNOS Release 8.4.

Description Prevent LDP from exporting IPv4 FECs over sessions with Layer 2 neighbors only. IPv4 FECs received over such sessions are filtered out.

Usage Guidelines See "Configuring LDP IPv4 FEC Filtering" on page 350.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

label-withdrawal-delay

Syntax label-withdrawal-delay *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp],
[edit protocols ldp],
[edit routing-instances *routing-instance-name* protocols ldp]

Release Information Statement introduced in JUNOS Release 9.1.

Description Delay the withdrawal of labels to reduce router workload during IGP convergence.

Options *seconds*—Configure the number of seconds to wait before withdrawing labels for the LDP LSPs.
Default: 60 seconds
Range: 0 through 300 seconds

Usage Guidelines See "Configuring the Label Withdrawal Timer" on page 363.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

ldp

Syntax ldp { ... }

Hierarchy Level [edit logical-systems *logical-system-name* protocols],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols],
[edit protocols],
[edit routing-instances *routing-instance-name* protocols]

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable LDP routing on the router.

You must include the ldp statement in the configuration to enable LDP on the router.

Default LDP is disabled on the router.

Usage Guidelines See "Minimum LDP Configuration" on page 339 and "Enabling and Disabling LDP" on page 339.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

ldp-synchronization

Syntax
```
ldp-synchronization {
    disable;
    hold-time seconds;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf interface *interface-name*],
[edit protocols ospf interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ospf interface *interface-name*]

Release Information Statement introduced in JUNOS Release 7.5.

Description Enable synchronization by advertising the maximum cost metric until LDP is operational on the link.

Options The other statements are explained separately.

Usage Guidelines "Configuring LDP Synchronization with the IGP" on page 362

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

log-updown

Syntax
```
log-updown {
    trap disable;
}
```

Hierarchy Level
[edit logical-systems *logical-system-name* protocols ldp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp],
[edit protocols ldp],
[edit routing-instances *routing-instance-name* protocols ldp]

Release Information Statement introduced before JUNOS Release 7.4.

Description Disable LDP traps on the router, logical system, or routing instance.

Options trap disable—Disable LDP traps.
Default: LDP traps are enabled on the router.

Usage Guidelines See "Disabling SNMP Traps for LDP" on page 361.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

maximum-neighbor-recovery-time

Syntax
```
maximum-neighbor-recovery-time seconds;
```

Hierarchy Level
[edit logical-systems *logical-system-name* protocols ldp graceful-restart],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp graceful-restart],
[edit protocols ldp graceful-restart],
[edit routing-instances *routing-instance-name* protocols ldp graceful-restart]

Release Information Statement introduced before JUNOS Release 7.4. Statement changed from maximum-recovery-time to maximum-neighbor-recovery-time in JUNOS Release 9.1.

Description Specify the maximum amount of time to wait before giving up an attempt to gracefully restart.

Options *seconds*—Configure the maximum recovery time, in seconds.
Range: 120 through 1800 seconds
Default: 140 seconds

Usage Guidelines See "Configuring Recovery Time and Maximum Recovery Time" on page 342.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

no-deaggregate

See deaggregate.

no-forwarding

Syntax no-forwarding;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp],
[edit protocols ldp],
[edit routing-instances *routing-instance-name* protocols ldp]

Release Information Statement introduced before JUNOS Release 7.4.

Description Do not add ingress routes to the inet.0 routing table even if traffic-engineering bgp-igp (configured at the [edit protocols mpls] hierarchy level) is enabled.

Default The no-forwarding statement is disabled. Ingress routes are added to the inet.0 routing table instead of the inet.3 routing table when traffic-engineering bgp-igp is enabled.

Usage Guidelines See “Preventing Ingress Routes from Being Added to inet.0” on page 358.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

oam

Syntax

```
oam {
    bfd-liveness-detection {
        minimum-interval;
        minimum-receive-interval;
        minimum-transmit-interval;
        multiplier;
    }
    fec fec-address;
    periodic-traceroute {
        disable;
        exp exp-value;
        fanout fanout-value;
        frequency minutes;
        paths number-of-paths;
        retries retry-attempts;
        source address;
        ttl ttl-value;
        wait seconds;
    }
}
```

Hierarchy Level [edit protocols ldp]

Release Information Statement introduced in JUNOS Release 7.6.

Description Enable OAM for all of the LDP LSPs or for a specific LDP LSP.

Options fec*fec-address*—Specify the forwarding equivalence class (FEC) address.

The remaining statements are explained separately.

Usage Guidelines See “Configuring BFD for LDP LSPs” on page 350.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

periodic-traceroute

Syntax

```
periodic-traceroute {
    disable;
    exp exp-value;
    fanout fanout-value;
    frequency minutes;
    paths number-of-paths;
    retries retry-attempts;
    source address;
    ttl ttl-value;
    wait seconds;
}
```

Hierarchy Level [edit protocols ldp oam],
[edit protocols ldp oam fec *fec-address*]

Release Information Statement introduced in JUNOS Release 8.4.
Support added at the [edit protocols ldp oam] hierarchy level in JUNOS 9.0.

Description Enable tracing of forwarding equivalence classes (FECs) for LDP LSPs.

Options

disable—Disable tracing for a specific FEC. This option is available at the [edit protocols ldp oam fec *fec-address*] hierarchy level only.

exp—Specify the class of service to use when sending probes.
Default: 7
Range: 0 through 7

fanout—Specify the maximum number of next hops to search per node.
Default: 16
Range: 1 though 16

frequency—Specify the interval between traceroute attempts.
Default: 60 minutes
Range: 15 through 120 minutes

paths—Specify the maximum number of paths to search.
Default: 3
Range: 1 through 255

retries—Specify the number of attempts to send a probe to a specific node before giving up.
Default: 3
Range: 1 through 9

source—Specify the IPv4 source address to use when sending probes.

ttl—Specify the maximum time-to-live value. Nodes that are beyond this value are not traced.
Default: 64

Range: 1 through 255

wait—Specify the wait interval before resending a probe packet.
Default: 10 seconds
Range: 5 though 15 seconds

Usage Guidelines See "Configuring LDP LSP Traceroute" on page 352.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

policing

Syntax
```
policing {
    fec fec-address {
        ingress-traffic filter-name;
        transit-traffic filter-name;
    }
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp],
[edit protocols ldp],
[edit routing-instances *routing-instance-name* protocols ldp]

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable policing of forwarding equivalence classes (FECs) for LDP.

Options fec—Specify the address for the FEC.

ingress-traffic—Specify the name of the filter for policing ingress FEC traffic.

transit-traffic—Specify the name of the filter for policing transit FEC traffic.

Usage Guidelines See "Configuring Policers for LDP FECs" on page 349.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

preference

Syntax preference *preference*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp],
[edit protocols ldp interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ldp interface *interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Set the route preference level for LDP routes.

Options *preference*—Preferred value.
Range: 0 through 255
Default: 9

Usage Guidelines See "Configuring LDP Route Preferences" on page 341.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

recovery-time

Syntax recovery-time *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp graceful-restart],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp graceful-restart],
[edit protocols ldp graceful-restart],
[edit routing-instances *routing-instance-name* protocols ldp graceful-restart]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the amount of time a router waits for LDP to restart gracefully.

Options *seconds*—Configure the recovery time, in seconds.
Range: 120 through 1800 seconds
Default: 140 seconds

Usage Guidelines See "Configuring Recovery Time and Maximum Recovery Time" on page 342.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

session

Syntax
```
session address {
    authentication-key authentication-key;
}
```

Hierarchy Level
```
[edit logical-systems logical-system-name protocols ldp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols
    ldp],
[edit protocols ldp],
[edit routing-instances routing-instance-name protocols ldp]
```

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the LDP session to which you want to attach the Transmission Control Protocol (TCP) MD5 signature. Configure the address for the remote end of the LDP session.

The remaining statement is explained separately.

Usage Guidelines See "Configuring the TCP MD5 Signature for an LDP Session" on page 361.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

strict-targeted-hellos

Syntax
```
strict-targeted-hellos;
```

Hierarchy Level
```
[edit logical-systems logical-system-name protocols ldp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols
    ldp],
[edit protocols ldp],
[edit routing-instances routing-instance-name protocols ldp]
```

Release Information Statement introduced before JUNOS Release 7.4.

Description Prevents LDP sessions from being established with remote neighbors that have not been specifically configured. LDP peers will not respond to targeted hellos coming from a source that is not one of the configured remote neighbors.

Usage Guidelines See "Enabling Strict Targeted Hellos" on page 362.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

traceoptions

Syntax

```
traceoptions {
    file filename <replace> <size size> <files number> <no-stamp> <world-readable |
        no-world-readable>;
    flag flag <flag-modifier> <disable>;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols ldp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp],
[edit protocols ldp],
[edit routing-instances *routing-instance-name* protocols ldp]

Release Information

Statement introduced before JUNOS Release 7.4.

Description

LDP protocol-level trace options.

Default

The default LDP protocol-level trace options are inherited from the routing protocols **traceoptions** statement included at the **[edit routing-options]** hierarchy level.

Options

disable—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as **all**.

filename—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. We recommend that you place LDP tracing output in the file **ldp-log**.

files *number*—(Optional) Maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed *trace-file*.0, then *trace-file*.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.
Range: 2 through 1000
Default: 2 files

If you specify a maximum number of files, you must also include the **size** statement to specify the maximum file size.

flag—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements.

- **address**—Operation of address and address withdrawal messages
- **binding**—Label-binding operations
- **error**—Error conditions
- **event**—Protocol events
- **initialization**—Operation of initialization messages
- **label**—Operation of label request, label map, label withdrawal, and label release messages

- notification—Operation of notification messages
- packets—Equivalent to setting address, initialization, label, notification, and periodic flags
- path—Label-switched path operations
- periodic—Operation of hello and keepalive messages
- route—Operation of route messages
- state—Protocol state transitions

flag-modifier—(Optional) Modifier for the tracing flag. You can specify one or more of these modifiers:

- detail—Provide detailed trace information.
- disable—Disable this trace flag.
- filter—Filter to apply to this flag. The filter flag modifier can be applied only to the route, path, and binding flags. This flag modifier has the following options:
  - match-on—Match on argument specified. The match-on option has the following suboption: fec, a filter based on the FEC associated with the traced object.
  - policy *policy-name*—Specify the filter policy.
- receive—Packets being received.
- send—Packets being transmitted.

no-stamp—(Optional) Do not place timestamp information at the beginning of each line in the trace file.
Default: If you omit this option, timestamp information is placed at the beginning of each line of the tracing output.

no-world-readable—(Optional) Disallow any user to read the log file.

replace—(Optional) Replace an existing trace file if there is one.
Default: If you do not include this option, tracing output is appended to an existing trace file.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file*.0. When the *trace-file* again reaches this size, *trace-file*.0 is renamed *trace-file*.1 and *trace-file* is renamed *trace-file*.0. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.
Syntax: *x*k to specify KB, *x*m to specify MB, or *x*g to specify GB
Range: 10 KB through the maximum file size supported on your system
Default: 1 MB

If you specify a maximum file size, you must also include the files statement to specify the maximum number of files.

world-readable—(Optional) Allow any user to read the log file.

Usage Guidelines See "Tracing LDP Protocol Traffic" on page 355 and the *JUNOS Network Management Configuration Guide*.

Required Privilege Level routing and trace—To view this statement in the configuration.
routing-control and trace-control—To add this statement to the configuration.

track-igp-metric

Syntax track-igp-metric;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp],
[edit protocols ldp],
[edit routing-instances *routing-instance-name* protocols ldp]

Release Information Statement introduced before JUNOS Release 7.4.

Description Cause the IGP route metric to be used for the LDP routes instead of the default LDP route metric (the default LDP route metric is 1).

Usage Guidelines See "Configuring LDP to Use the IGP Route Metric" on page 358.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

traffic-statistics

Syntax

```
traffic-statistics {
    file filename <files number> <no-stamp> <replace> <size size> <world-readable |
        no-world-readable>;
    interval seconds;
    no-penultimate-hop;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols ldp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp],
[edit protocols ldp],
[edit routing-instances *routing-instance-name* protocols ldp]

Release Information

Statement introduced before JUNOS Release 7.4.

Description

LDP traffic statistics display the amount of traffic passed through a router for a particular FEC.

Options

file *filename*—Name of the file to receive the output of the LDP statistics operation. Enclose the name within quotation marks. All files are placed in the directory /var/log.

files *number*—(Optional) Maximum number of LDP statistics files. When a statistics file named *ldp-stat* reaches its maximum size, it is renamed *ldp-stat*.0, then *ldp-stat*.1, and so on, until the maximum number of LDP statistics files is reached. Then the oldest file is overwritten.
Range: 2 through 1000
Default: 2 files

If you specify a maximum number of files, you also must include the size statement to specify the maximum file size.

no-penultimate-hop—(Optional) Do not collect traffic statistics on the penultimate hop router.

no-world-readable—(Optional) Prevents all users from reading the log file.

replace—(Optional) Replace an existing statistics file, if there is one.
Default: If you do not include this option, LDP statistics output is appended to an existing statistics file.

size *size*—(Optional) Maximum size of each statistics file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a statistics file named *ldp-stat* reaches this size, it is renamed *ldp-stat*.0. When *ldp-stat* again reaches this size, *ldp-stat*.0 is renamed *ldp-stat*.1 and *ldp-stat* is renamed *ldp-stat*.0. This renaming scheme continues until the maximum number of statistics files is reached. Then the oldest statistics file is overwritten.
Syntax: *x*k to specify KB, *x*m to specify MB, or *x*g to specify GB
Range: 10 KB through the maximum file size supported on your system

Default: 1 MB

If you specify a maximum file size, you also must also include the files statement to specify the maximum number of files.

world-readable—(Optional) Enables log file access for all users.

interval *interval*—(Optional) Specifies the interval at which the statistics are polled and written to the file.
Default: 300 seconds (5 minutes)

Usage Guidelines See "Collecting LDP Statistics" on page 353.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

transport-address

Syntax transport-address (router-id | interface);

Hierarchy Level [edit logical-systems *logical-system-name* protocols ldp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ldp],
[edit protocols ldp interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols ldp interface *interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Allow control of the transport address used by LDP.

Default router-id

Options router-id—The router identifier is used as the transport address.

interface—The first IP address on the interface is used as the transport address.

Usage Guidelines See "Configuring LDP Transport Address Control" on page 347.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Part 5
CCC and TCC

- CCC and TCC Overview on page 393
- CCC and TCC Configuration Guidelines on page 397
- Summary of CCC and TCC Configuration Statements on page 421

Chapter 17

CCC and TCC Overview

This chapter includes the following sections:

- CCC Overview on page 393
- TCC Overview on page 394
- CCC and TCC Graceful Restart on page 394

CCC Overview

Circuit cross-connect (CCC) allows you to configure transparent connections between two circuits, where a circuit can be a Frame Relay data-link connection identifier (DLCI), an Asynchronous Transfer Mode (ATM) virtual circuit (VC), a Point-to-Point Protocol (PPP) interface, a Cisco High-Level Data Link Control (HDLC) interface, or a Multiprotocol Label Switching (MPLS) label-switched path (LSP). Using CCC, packets from the source circuit are delivered to the destination circuit with, at most, the Layer 2 address being changed. No other processing—such as header checksums, time-to-live (TTL) decrementing, or protocol processing—is done.

CCC circuits fall into two categories: logical interfaces, which include DLCIs, VCs, virtual local area network (VLAN) IDs, PPP and Cisco HDLC interfaces, and LSPs. The two circuit categories provide three types of cross-connect:

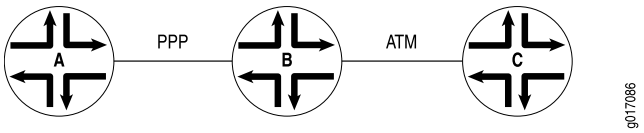
- Layer 2 switching—Cross-connects between logical interfaces provide what is essentially Layer 2 switching. The interfaces that you connect must be of the same type.
- MPLS tunneling—Cross-connects between interfaces and LSPs allow you to connect two distant interface circuits of the same type by creating MPLS tunnels that use LSPs as the conduit.
- LSP stitching—Cross-connects between LSPs provide a way to " stitch" together two label-switched paths, including paths that fall in two different traffic engineering database (TED) areas.

For Layer 2 switching and MPLS tunneling, the cross-connect is bidirectional, so packets received on the first interface are transmitted out the second interface, and those received on the second interface are transmitted out the first. For LSP stitching, the cross-connect is unidirectional.

TCC Overview

Translational cross-connect (TCC) is a switching concept that allows you to establish interconnections between a variety of Layer 2 protocols or circuits. It is similar to CCC. However, while CCC requires the same Layer 2 encapsulations on each side of a Juniper Networks router (such as PPP-to-PPP or Frame Relay-to-Frame Relay), TCC lets you connect different types of Layer 2 protocols interchangeably. Using TCC, combinations such as PPP-to-ATM (see Figure 25 on page 394) and Ethernet-to-Frame Relay connections are possible.

Figure 25: TCC Example



The Layer 2 circuits and encapsulation types that can be interconnected by TCC are:

- Ethernet
- Extended VLANs
- PPP
- HDLC
- ATM
- Frame Relay

TCC works by removing the Layer 2 header when frames enter the router and adding a different Layer 2 header on the frames before they leave the router. In Figure 25 on page 394, the PPP encapsulation is stripped from the frames arriving at Router B, and the ATM encapsulation is added before the frames are sent to Router C.

Note that all control traffic is terminated at the interconnecting router (Router B). Examples of traffic controllers include the Link Control Protocol (LCP) and the Network Control Protocol (NCP) for PPP, keepalives for HDLC, and Local Management Interface (LMI) for Frame Relay.

TCC functionality is different from standard Layer 2 switching. TCC only swaps Layer 2 headers. No other processing, such as header checksums, TTL decrementing, or protocol handling is performed. TCC is supported for IPv4 only.

You can configure TCC for interface switching and for Layer 2 VPNs. For more information about using TCC for virtual private networks (VPNs), see the *JUNOS VPNs Configuration Guide*.

CCC and TCC Graceful Restart

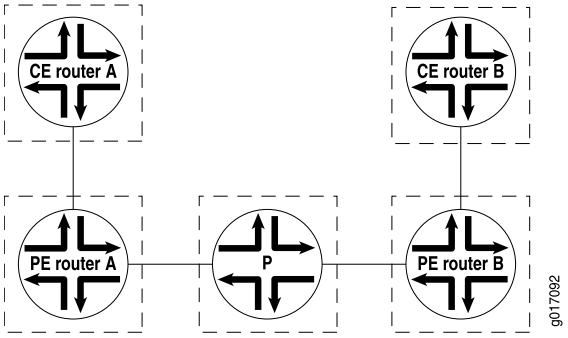
CCC and TCC graceful restart allows Layer 2 connections between customer edge (CE) routers to restart gracefully. These Layer 2 connections are configured with the

remote-interface-switch or lsp-switch statements. Because these CCC and TCC connections have an implicit dependency on RSVP LSPs, graceful restart for CCC and TCC uses the RSVP graceful restart capabilities.

RSVP graceful restart must be enabled on the PE routers and P routers to enable graceful restart for CCC and TCC. Also, because RSVP is used as the signaling protocol for signaling label information, the neighboring router must use helper mode to assist with the Resource Reservation Protocol (RSVP) restart procedures.

Figure 26 on page 395 illustrates how graceful restart might work on a CCC connection between two CE routers.

Figure 26: Remote Interface Switch Connecting Two CE Routers Using CCC



PE Router A is the ingress for the transmit LSP from PE Router A to PE Router B and the egress for the receive LSP from PE Router B to PE Router A. With RSVP graceful restart enabled on all the PE and P routers, the following occurs when PE router A restarts:

- PE Router A preserves the forwarding state associated with the CCC routes (those from CCC to MPLS and from MPLS to CCC).
- Traffic flows without disruption from CE router to CE router.
- After the restart, PE Router A preserves the label for the LSP for which PE Router A is the egress (the receive LSP, for example). The transmit LSP from PE Router A to PE Router B can derive new label mappings, but should not cause any traffic disruption.

Chapter 18

CCC and TCC Configuration Guidelines

This chapter includes the following sections:

- Configuring CCC on page 397
- Configuring TCC on page 411
- Configuring CCC and TCC Graceful Restart on page 417
- Configuring CCC Switching for Point-to-Multipoint LSPs on page 417

Configuring CCC

You can police (control) the amount of traffic flowing over CCC circuits. For more information, see the *JUNOS VPNs Configuration Guide*.

It is also possible to use the ping command to check the integrity of CCC LSPs. See "Pinging a CCC LSP" on page 171 for more information.

This section discusses the following circuit cross-connect (CCC) configuration tasks:

- Configuring Layer 2 Switching Cross-Connects on page 397
- Configuring MPLS LSP Tunnel Cross-Connects on page 405
- Configuring LSP Stitching Cross-Connects on page 409
- Transmitting Nonstandard BPDUs on page 411

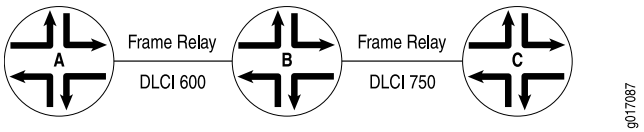
Configuring Layer 2 Switching Cross-Connects

Layer 2 switching cross-connects join logical interfaces to form what is essentially Layer 2 switching. The interfaces that you connect must be of the same type.

Figure 27 on page 398 illustrates a Layer 2 switching cross-connect. In this topology, Router A and Router C have Frame Relay connections to Router B, which is a Juniper Networks router. CCC allows you to configure Router B to act as a Frame Relay (Layer 2) switch.

To configure Router B to act as a Frame Relay switch, you configure a circuit from Router A to Router C that passes through Router B, effectively configuring Router B as a Frame Relay switch with respect to these routers. This configuration allows Router B to transparently switch packets (frames) between Router A and Router C without regard to the packets' contents or the Layer 3 protocols. The only processing that Router B performs is to translate DLCI 600 to 750.

Figure 27: Layer 2 Switching Cross-Connect



If the Router A–to–Router B and Router B–to–Router C circuits were PPP, for example, the Link Control Protocol and Network Control Protocol exchanges occur between Router A and Router C. These messages are handled transparently by Router B, allowing Router A and Router C to use various PPP options (such as header or address compression and authentication) that Router B might not support. Similarly, Router A and Router C exchange keepalives, providing circuit-to-circuit connectivity status.

You can configure Layer 2 switching cross-connects on PPP, Cisco HDLC, Frame Relay, Ethernet, and ATM circuits. In a single cross-connect, only like interfaces can be connected.

To configure Layer 2 switching cross-connects, you must configure the following on the router that is acting as the switch (Router B in Figure 27 on page 398):

- Defining the Encapsulation for Layer 2 Switching Cross-Connects on page 398
- Defining the CCC Connection for Layer 2 Switching Cross-Connects on page 402
- Configuring MPLS on page 403
- Example: Configuring Layer 2 Switching Cross-Connects on page 403

Defining the Encapsulation for Layer 2 Switching Cross-Connects

To configure Layer 2 switching cross-connects, configure the CCC encapsulation on the router that is acting as the switch (Router B in Figure 27 on page 398).

NOTE: You cannot configure families on CCC interfaces; that is, you cannot include the family statement at the [edit interfaces *interface-name* unit *logical-unit-number*] hierarchy level.

You can configure the following encapsulations for the Layer 2 switching cross-connect:

- ATM Encapsulation for Layer 2 Switching Cross-Connects on page 399
- Ethernet Encapsulation for Layer 2 Switching Cross-Connects on page 399
- Ethernet VLAN Encapsulation for Layer 2 Switching Cross-Connects on page 399
- Aggregated Ethernet Encapsulation for Layer 2 Switching Cross-Connects on page 401
- Frame Relay Encapsulation for Layer 2 Switching Cross-Connects on page 402
- PPP and Cisco HDLC Encapsulation for Layer 2 Switching Cross-Connects on page 402

ATM Encapsulation for Layer 2 Switching Cross-Connects

For ATM circuits, specify the encapsulation when configuring the virtual circuit (VC). Configure each VC as a circuit or a regular logical interface by including the following statements:

```
at-fpc/pic/port {
    atm-options {
        vpi vpi-identifier maximum-vcs maximum-vcs;
    }
    unit logical-unit-number {
        point-to-point; # Default interface type
        encapsulation encapsulation-type;
        vci vpi-identifier.vci-identifier;
    }
}
```

You can include these statements at the following hierarchy levels:

- [edit interfaces]
- [edit logical-systems *logical-system-name* interfaces]

Ethernet Encapsulation for Layer 2 Switching Cross-Connects

For Ethernet circuits, specify ethernet-ccc in the encapsulation statement. This statement configures the entire physical device. For these circuits to work, you must also configure a logical interface (unit 0).

Ethernet interfaces with standard Tag Protocol Identifier (TPID) tagging can use Ethernet CCC encapsulation. On M-series routing platforms, except the M320, one-port Gigabit Ethernet, two-port Gigabit Ethernet, four-port Gigabit Ethernet, and four-port Fast Ethernet Physical Interface Cards (PICs) can use Ethernet CCC encapsulation. On T-series platforms and M320 routers, one-port Gigabit Ethernet and two-port Gigabit Ethernet PICs installed in FPC2 can use Ethernet CCC encapsulation. When you use this encapsulation type, you can configure the ccc family only.

```
fe-fpc/pic/port {
    encapsulation ethernet-ccc;
    unit 0;
}
```

You can include these statements at the following hierarchy levels:

- [edit interfaces]
- [edit logical-systems *logical-system-name* interfaces]

Ethernet VLAN Encapsulation for Layer 2 Switching Cross-Connects

An Ethernet virtual LAN (VLAN) circuit can be configured using either the vlan-ccc or extended-vlan-ccc encapsulation. If you configure the extended-vlan-ccc encapsulation on the physical interface, you cannot configure the inet family on the logical interfaces. Only the ccc family is allowed. If you configure the vlan-ccc encapsulation on the

physical interface, both the inet and ccc families are supported on the logical interfaces. Ethernet interfaces in VLAN mode can have multiple logical interfaces.

For encapsulation type vlan-ccc, VLAN IDs from 512 through 4094 are reserved for CCC VLANs. For the extended-vlan-ccc encapsulation type, all VLAN IDs 1 and higher are valid. VLAN ID 0 is reserved for tagging the priority of frames.

NOTE: Some vendors use the proprietary TPIDs 0x9100 and 0x9901 to encapsulate a VLAN-tagged packet into a VLAN-CCC tunnel to interconnect a geographically separated metro Ethernet network. By configuring the extended-vlan-ccc encapsulation type, a Juniper Networks router can accept all three TPIDs (0x8100, 0x9100, and 0x9901).

Configure an Ethernet VLAN circuit with the vlan-ccc encapsulation as follows:

```
interfaces {
    type-fpc/pic/port {
        vlan-tagging;
        encapsulation vlan-ccc;
        unit logical-unit-number {
            encapsulation vlan-ccc;
            vlan-id vlan-id;
        }
    }
}
```

You can configure these statements at the following hierarchy levels:

- [edit logical-systems *logical-system-name* interfaces]
- [edit interfaces]

Configure an Ethernet VLAN circuit with the extended-vlan-ccc encapsulation statement as follows:

```
interfaces {
    type-fpc/pic/port {
        vlan-tagging;
        encapsulation extended-vlan-ccc;
        unit logical-unit-number {
            vlan-id vlan-id;
            family ccc;
        }
    }
}
```

You can configure these statements at the following hierarchy levels:

- [edit logical-systems *logical-system-name* interfaces]
- [edit interfaces]

Whether you configure the encapsulation as vlan-ccc or extended-vlan-ccc, you must enable VLAN tagging by including the vlan-tagging statement.

Aggregated Ethernet Encapsulation for Layer 2 Switching Cross-Connects

You can configure aggregated Ethernet interfaces for CCC connections and for Layer 2 virtual private networks (VPNs).

Aggregated Ethernet interfaces configured with VLAN tagging can be configured with multiple logical interfaces. The only encapsulation available for aggregated Ethernet logical interfaces is vlan-ccc. When you configure the vlan-id statement, you are limited to VLAN IDs 512 through 4094.

Aggregated Ethernet interfaces configured without VLAN tagging can be configured only with the ethernet-ccc encapsulation. All untagged Ethernet packets received are forwarded based on the CCC parameters.

To configure aggregated Ethernet interfaces for CCC connections, include the ae0 statement at the [edit interfaces] hierarchy level:

```
[edit interfaces]
ae0 {
   encapsulation (ethernet-cccextended-vlan-ccc | vlan-ccc);
   vlan-tagging;
   aggregated-ether-options {
      minimum-links links;
      link-speed speed;
   }
   unit logical-unit-number {
      encapsulation vlan-ccc;
      vlan-id identifier;
      family ccc;
   }
}
```

Be aware of the following limitations when configuring CCC connections over aggregated Ethernet interfaces:

- If you configured load balancing between child links, be aware that a different hash key is used to distribute packets among the child links. Standard aggregated interfaces have family inet configured. An IP version 4 (IPv4) hash key (based on the Layer 3 information) is used to distribute packets among the child links. A CCC connection over an aggregated Ethernet interface has family ccc configured instead. Instead of an IPv4 hash key, a Multiprotocol Label Switching (MPLS) hash key (based on the destination media access control [MAC] address) is used to distributed packets among the child links.
- The extended-vlan-ccc encapsulation is not supported on the 12-port Fast Ethernet PIC and the 48-port Fast Ethernet PIC.
- The JUNOS software does not support the Link Aggregation Control Protocol (LACP) when an aggregated interface is configured as a VLAN (with vlan-ccc encapsulation). LACP can be configured only when the aggregated interface is configured with the ethernet-ccc encapsulation.

For more information about how to configure aggregated Ethernet interfaces, see the *JUNOS Network Interfaces Configuration Guide*.

Frame Relay Encapsulation for Layer 2 Switching Cross-Connects

For Frame Relay circuits, specify the encapsulation when configuring the DLCI. Configure each DLCI as a circuit or a regular logical interface. The DLCI for regular interfaces must be from 1 through 511. For CCC interfaces, it must be from 512 through 4094.

```
interfaces {
    type-fpc/pic/port {
        unit logical-unit-number {
            point-to-point; # Default interface type
            encapsulation encapsulation-type;
            dlci dlci-identifier;
        }
    }
}
```

You can configure these statements at the following hierarchy levels:

- [edit logical-systems *logical-system-name* interfaces]
- [edit interfaces]

PPP and Cisco HDLC Encapsulation for Layer 2 Switching Cross-Connects

For PPP and Cisco HDLC circuits, specify the encapsulation in the encapsulation statement. This statement configures the entire physical device. For these circuits to work, you must configure a logical interface (unit 0).

```
interfaces type-fpc/pic/port {
    encapsulation encapsulation-type;
    unit 0;
}
```

You can configure these statements at the following hierarchy levels:

- [edit logical-systems *logical-system-name* interfaces *type-fpc/pic/port*]
- [edit interfaces *type-fpc/pic/port*]

Defining the CCC Connection for Layer 2 Switching Cross-Connects

To configure Layer 2 switching cross-connects, define the connection between the two circuits by including the interface-switch statement. You configure this connection on the router that is acting as the switch (Router B in Figure 27 on page 398). The connection joins the interface that comes from the circuit's source to the interface that leads to the circuit's destination. When you specify the interface names, include the logical portion of the name, which corresponds to the logical unit number. The cross-connect is bidirectional, so packets received on the first interface are transmitted out the second interface, and those received on the second interface are transmitted out the first.

```
interface-switch connection-name {
    interface interface-name.unit-number;
    interface interface-name.unit-number;
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols connections]
- [edit logical-systems *logical-system-name* protocols connections]

Configuring MPLS

For Layer 2 switching cross-connects to work, you must configure MPLS by including the interface statement. The following is a minimal MPLS configuration:

```
interface (interface-name | all);
```

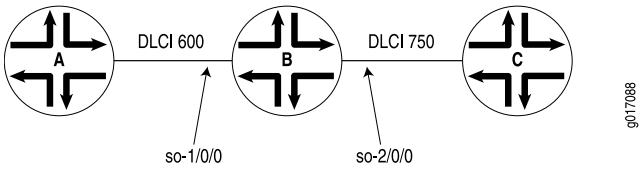
You can include this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

Example: Configuring Layer 2 Switching Cross-Connects

Configure a full-duplex Layer 2 switching cross-connect between Router A and Router C, using a Juniper Networks router, Router B, as the virtual switch. See the topology in Figure 28 on page 403 and Figure 29 on page 404.

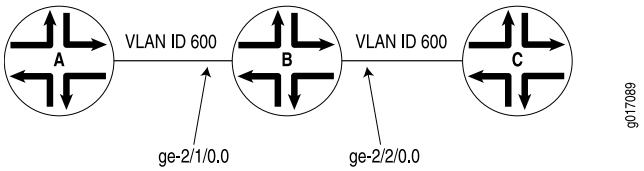
Figure 28: Topology of a Frame Relay Layer 2 Switching Cross-Connect




```
[edit]
interfaces {
    so-1/0/0 {
        encapsulation frame-relay-ccc;
        unit 1 {
            point-to-point;
            encapsulation frame-relay-ccc;
            dlci 600;
        }
    }
    so-2/0/0 {
        encapsulation frame-relay-ccc;
        unit 2 {
            point-to-point;
            encapsulation frame-relay-ccc;
            dlci 750;
```

```
    }
  }
}
protocols {
  connections {
    interface-switch router-a-router-c {
      interface so-1/0/0.1;
      interface so-2/0/0.2;
    }
  }
  mpls {
    interface all;
  }
}
```

Figure 29: Sample Topology of a VLAN Layer 2 Switching Cross-Connect



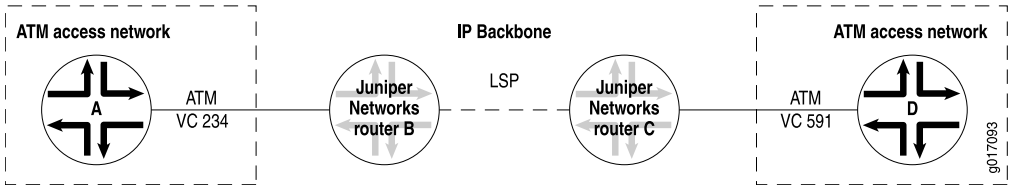

```
[edit]
interfaces {
  ge-2/1/0 {
    vlan-tagging;
    encapsulation vlan-ccc;
    unit 0 {
      encapsulation vlan-ccc;
      vlan-id 600;
    }
  }
  ge-2/2/0 {
    vlan-tagging;
    encapsulation vlan-ccc;
    unit 0 {
      encapsulation vlan-ccc;
      vlan-id 600;
    }
    unit 1 {
      family inet {
        vlan-id 1;
        address 10.9.200.1/24;
      }
    }
  }
}
protocols {
  mpls {
    interface all;
  }
  connections {
    interface-switch layer2-sw {
      interface ge-2/1/0.0;
```

```
            interface ge-2/2/0.0;
        }
    }
}
```

Configuring MPLS LSP Tunnel Cross-Connects

MPLS tunnel cross-connects between interfaces and LSPs allow you to connect two distant interface circuits of the same type by creating MPLS tunnels that use LSPs as the conduit. The topology in Figure 30 on page 405 illustrates an MPLS LSP tunnel cross-connect. In this topology, two separate networks, in this case ATM access networks, are connected through an IP backbone. CCC allows you to establish an LSP tunnel between the two domains. With LSP tunneling, you tunnel the ATM traffic from one network across a SONET backbone to the second network by using an MPLS LSP.

Figure 30: MPLS LSP Tunnel Cross-Connect



When traffic from Router A (VC 234) reaches Router B, it is encapsulated and placed into an LSP, which is sent through the backbone to Router C. At Router C, the label is removed, and the packets are placed onto the ATM permanent virtual circuit (PVC) (VC 591) and sent to Router D. Similarly, traffic from Router D (VC 591) is sent over an LSP to Router B, then placed on VC 234 to Router A.

You can configure LSP tunnel cross-connect on PPP, Cisco HDLC, Frame Relay, and ATM circuits. In a single cross-connect, only like interfaces can be connected.

When you use MPLS tunnel cross-connects to support IS-IS, you must ensure that the LSP's maximum transmission unit (MTU) can, at a minimum, accommodate a 1492-octet IS-IS protocol data unit (PDU) in addition to the link-level overhead associated with the technology being connected.

For the tunnel cross-connects to work, the IS-IS frame size on the edge routers (Routers A and D in Figure 30 on page 405) must be smaller than the LSP's MTU.

NOTE: Frame size values do not include the frame checksum sequence (FCS) or delimiting flags.

To determine the LSP MTU required to support IS-IS, use the following calculation:

IS-IS MTU (minimum 1492, default 1497) + frame overhead + 4 (MPLS shim header) = Minimum LSP MTU

The framing overhead varies based on the encapsulation being used. The following lists the IS-IS encapsulation overhead values for various encapsulations:

- ATM
  - AAL5 multiplex—8 bytes (RFC 1483)
  - VC multiplex—0 bytes
- Frame Relay
  - Multiprotocol—2 bytes (RFCs 1490 and 2427)
  - VC multiplex—0 bytes
- HDLC—4 bytes
- PPP—4 bytes
- VLAN—21 bytes (802.3/LLC)

For IS-IS to work over VLAN-CCC, the LSP's MTU must be at least 1513 bytes (or 1518 for 1497-byte PDUs). If you increase the size of a Fast Ethernet MTU above the default of 1500 bytes, you might need to explicitly configure jumbo frames on intervening equipment.

To modify the MTU, include the mtu statement when configuring the logical interface family at the [edit interfaces *interface-name* unit *logical-unit-number* encapsulation *family*] hierarchy level. For more information about setting the MTU, see the *JUNOS Network Interfaces Configuration Guide*.

To configure an LSP tunnel cross-connect, you must configure the following on the interdomain router (Router B in Figure 30 on page 405):

- Defining the CCC Encapsulation for LSP Tunnel Cross-Connects on page 406
- Defining the CCC Connection for LSP Tunnel Cross-Connects on page 408
- Example: Configuring LSP Tunnel Cross-Connects on page 408

Defining the CCC Encapsulation for LSP Tunnel Cross-Connects

To configure LSP tunnel cross-connects, you must configure the CCC encapsulation on the ingress and egress routers (Router B and Router C, respectively, in Figure 30 on page 405).

NOTE: You cannot configure families on CCC interfaces; that is, you cannot include the family statement at the [edit interfaces *interface-name* unit *logical-unit-number*] hierarchy level.

For PPP or Cisco HDLC circuits, include the encapsulation statement to configure the entire physical device. For these circuits to work, you must configure logical unit 0 on the interface.

```
type-fpc/pic/port {
    encapsulation (ppp-ccc | cisco-hdlc-ccc);
```

```
    unit 0;
}
```

You can include these statements at the following hierarchy levels:

- [edit protocols interfaces]
- [edit logical-systems *logical-system-name* protocols interfaces]

For ATM circuits, specify the encapsulation when configuring the VC by including the following statements. For each VC, you configure whether it is a circuit or a regular logical interface.

```
at-fpc/pic/port {
    atm-options {
        vpi vpi-identifier maximum-vcs maximum-vcs;
    }
    unit logical-unit-number {
        point-to-point; # Default interface type
        encapsulation atm-ccc-vc-mux;
        vci vpi-identifier.vci-identifier;
    }
}
```

You can include these statements at the following hierarchy levels:

- [edit protocols interfaces]
- [edit logical-systems *logical-system-name* protocols interfaces]

For Frame Relay circuits, include the following statements to specify the encapsulation when configuring the DLCI. For each DLCI, you configure whether it is a circuit or a regular logical interface. The DLCI for regular interfaces must be in the range 1 through 511. For CCC interfaces, it must be in the range 512 through 1022.

```
type-fpc/pic/port {
    encapsulation frame-relay-ccc;
    unit logical-unit-number {
        point-to-point; # default interface type
        encapsulation frame-relay-ccc;
        dlci dlci-identifier;
    }
}
```

You can include these statements at the following hierarchy levels:

- [edit protocols interfaces]
- [edit logical-systems *logical-system-name* protocols interfaces]

For more information about the **encapsulation** statement, see the *JUNOS Network Interfaces Configuration Guide*.

Defining the CCC Connection for LSP Tunnel Cross-Connects

To configure LSP tunnel cross-connects, include the remote-interface-switch statement to define the connection between the two circuits on the ingress and egress routers (Router B and Router C, respectively, in Figure 30 on page 405). The connection joins the interface or LSP that comes from the circuit's source to the interface or LSP that leads to the circuit's destination. When you specify the interface name, include the logical portion of the name, which corresponds to the logical unit number. For the cross-connect to be bidirectional, you must configure cross-connects on two routers.

```
remote-interface-switch connection-name {
   interface interface-name.unit-number;
   transmit-lsp label-switched-path;
   receive-lsp label-switched-path;
}
```

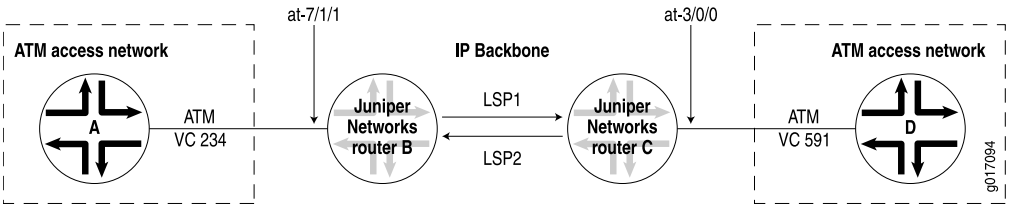
You can include these statements at the following hierarchy levels:

- [edit protocols connections]
- [edit logical-systems *logical-system-name* protocols connections]

Example: Configuring LSP Tunnel Cross-Connects

Configure a full-duplex MPLS LSP tunnel cross-connect from Router A to Router D, passing through Router B and Router C. See the topology in Figure 31 on page 408.

Figure 31: Example Topology of MPLS LSP Tunnel Cross-Connect



On Router B:

```
[edit]
interfaces {
   at-7/1/1 {
      atm-options {
         vpi 1 maximum-vcs 600;
      }
      unit 1 {
         point-to-point; # default interface type
         encapsulation atm-ccc-vc-mux;
         vci 1.234;
      }
   }
}
protocols {
   connections {
```

```
        remote-interface-switch router-b-to-router-c {
            interface at-7/1/1.1;
            transmit-lsp lsp1;
            receive-lsp lsp2;
        }
    }
}
```

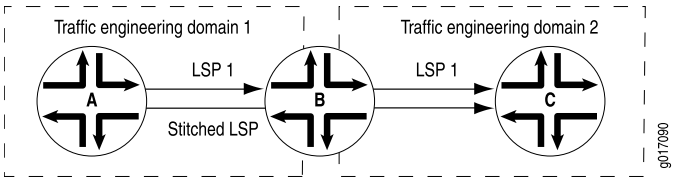
On Router C:

```
[edit]
interfaces {
    at-3/0/0 {
        atm-options {
            vpi 2 maximum-vcs 600;
        }
        unit 2 {
            point-to-point; # default interface type
            encapsulation atm-ccc-vc-mux;
            vci 2.591;
        }
    }
}
protocols {
    connections {
        remote-interface-switch router-b-to-router-c {
            interface at-3/0/0.2;
            transmit-lsp lsp2;
            receive-lsp lsp1;
        }
    }
}
```

Configuring LSP Stitching Cross-Connects

LSP stitching cross-connects "stitch" together LSPs to join two LSPs. For example, they stitch together LSPs that fall in two different TED areas. The topology in Figure 32 on page 409 illustrates an LSP stitching cross-connect. In this topology, the network is divided into two traffic engineering domains. CCC allows you to establish an LSP between the two domains by stitching together LSPs from the two domains. For LSP stitching to work, the LSPs must be dynamic LSPs, not static.

Figure 32: LSP Stitching Cross-Connect



Without LSP stitching, a packet traveling from Router A to Router C is encapsulated on Router A (the ingress router for the first LSP), decapsulated on Router B (the egress router), and then reencapsulated on Router B (the ingress router for the second LSP).

With LSP stitching, you connect LSP1 and LSP2 into a single, stitched LSP, which means that the packet is encapsulated once (on Router A) and decapsulated once (on Router C).

You can use LSP stitching to create a seamless LSP for LSPs carrying any kind of traffic.

To configure LSP stitching cross-connects, configure the two LSPs that you are stitching together on the two ingress routers. Then on the interdomain router (Router B in Figure 32 on page 409), you define the connection between the two LSPs. The connection joins the LSP that comes from the connection's source to the LSP that leads to the connection's destination.

```
protocols {
   connections {
      lsp-switch connection-name {
         transmit-lsp label-switched-path;
         receive-lsp label-switched-path;
      }
   }
}
```

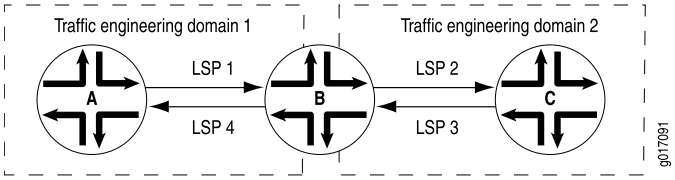
You can configure these statements at the following hierarchy levels:

- [edit logical-systems *logical-system-name* protocols connections]
- [edit protocols connections]

Example: Configuring LSP Stitching Cross-Connects

Configure a full-duplex LSP stitching cross-connect between Router A and Router C. To do this, you configure Router B, which is the interdomain router. See the topology in Figure 33 on page 410.

Figure 33: Example Topology of LSP Stitching Cross-Connect




```
[edit]
protocols {
   connections interface-switch {
      lsp-switch router-a-to-router-c {
         transmit-lsp lsp2;
         receive-lsp lsp1;
      }
   }
   connections {
      lsp-switch router-c-to-router-a {
         receive-lsp lsp3;
```

```
            transmit-lsp lsp4;
        }
    }
}
```

Transmitting Nonstandard BPDUs

CCC protocol (and Layer 2 Circuit and Layer 2 VPN) configurations can transmit nonstandard bridge protocol data units (BPDUs) generated by other vendors' equipment. This is the default behavior on all supported PICs and requires no additional configuration.

The following PICs are supported on T-series and M320 routers:

- 1-port Gigabit Ethernet PIC
- 2-port Gigabit Ethernet PIC
- 4-port Gigabit Ethernet PIC
- 10-port Gigabit Ethernet PIC

Configuring TCC

This section describes how to configure translational cross-connect (TCC). Extensive examples on how to configure TCC for interface switching and for Layer 2.5 VPNs are available in the *JUNOS Feature Guide*.

To configure TCC, you must perform the following tasks on the router that is acting as the switch:

- Defining the Encapsulation for the Layer 2 Switching TCCs on page 411
- Defining the Connection for the Layer 2 Switching TCC on page 415
- Configuring MPLS on page 416

Defining the Encapsulation for the Layer 2 Switching TCCs

To begin configuring a Layer 2 switching TCC, configure the TCC encapsulation on the desired interfaces of the router that is acting as the switch.

NOTE: You cannot configure standard protocol families on TCC or CCC interfaces. Only the CCC family is allowed on CCC interfaces, and only the TCC family is allowed on TCC interfaces.

You can configure the following types of circuits and encapsulations:

- PPP and Cisco HDLC Encapsulation for Layer 2 Switching TCCs on page 412
- ATM Encapsulation for Layer 2 Switching TCCs on page 412
- Frame Relay Encapsulation for Layer 2 Switching TCCs on page 413
- Ethernet Encapsulation for Layer 2 Switching TCCs on page 413

- Ethernet Extended VLAN Encapsulation for Layer 2 Switching TCCs on page 414
- ARP Configuration for Ethernet TCC Encapsulations on page 415

For Ethernet circuits and Ethernet extended VLAN circuits, you also need to configure the Address Resolution Protocol (ARP). See "ARP Configuration for Ethernet TCC Encapsulations" on page 415.

PPP and Cisco HDLC Encapsulation for Layer 2 Switching TCCs

For PPP and Cisco HDLC circuits, specify the encapsulation in the encapsulation statement at the [edit interfaces] hierarchy level. This statement configures the entire physical device. For these circuits to work, you must configure the logical interface unit 0.

To configure PPP and Cisco HDLC circuits, include the following statements:

```
type-fpc/pic/port {
    encapsulation (ppp-tcc | cisco-hdlc-tcc);
    unit 0;
}
```

You can include these statements at the following hierarchy levels:

- [edit protocols interfaces]
- [edit logical-systems *logical-system-name* protocols interfaces]

ATM Encapsulation for Layer 2 Switching TCCs

Specify the encapsulation type for ATM circuits when configuring the virtual circuit (VC). Specify whether each VC is a circuit or a regular logical interface.

Configure ATM circuits for TCC as follows:

```
interfaces {
    at-fpc/pic/port {
        atm-options {
            vpi vpi-identifier maximum-vcs maximum-vcs;
        }
        unit logical-unit-number {
            point-to-point;
            encapsulation (atm-tcc-vc-mux | atm-tcc-snap);
            vci vpi-identifier.vci-identifier;
        }
    }
}
```

You can configure these statements at the following hierarchy levels:

- [edit logical-systems *logical-system-name* protocols interfaces]
- [edit protocols interfaces]

Frame Relay Encapsulation for Layer 2 Switching TCCs

Specify the encapsulation type for Frame Relay circuits when configuring the data-link connection identifier (DLCI). You configure each DLCI as a circuit or a regular logical interface. The DLCI for regular interfaces must be in the range from 1 through 511. For TCC and CCC interfaces, it must be in the range from 512 through 1022.

Configure Frame Relay circuits for TCC as follows:

```
interfaces {
   encapsulation frame-relay-tcc;
   type-fpc/pic/port {
      unit logical-unit-number {
         point-to-point;
         encapsulation frame-relay-tcc;
         dlci dlci-identifier;
      }
   }
}
```

You can configure these statements at the following hierarchy levels:

- [edit logical-systems *logical-system-name* protocols interfaces]
- [edit protocols interfaces]

Ethernet Encapsulation for Layer 2 Switching TCCs

Specify the encapsulation type for Ethernet TCC circuits in the encapsulation statement. This statement configures the entire physical device. You must also specify a proxy address and a remote address statically at the [edit interfaces *interface-name* unit *unit-number* family tcc] hierarchy level.

The difference between the remote address and the proxy address is that the former is associated with the TCC switching router's Ethernet neighbor and the latter is associated with the TCC router's other neighbor connected by the unlike link. The remote statement requires that you configure both the IP address and the media access control (MAC) address for the Ethernet neighbor. The proxy statement requires the IP address for the non-Ethernet neighbor.

One-port Gigabit Ethernet, two-port Gigabit Ethernet, four-port Gigabit Ethernet, and four-port Fast Ethernet PICs can use Ethernet TCC encapsulation.

Configure Ethernet circuits for TCC as follows:

```
interfaces
ethernet-interface- type-fpc/pic/port {
   encapsulation ethernet-tcc;
   unit 0 {
      family tcc {
         proxy {
            inet-address address;
         }
         remote {
```

```
            inet-address address;
            mac-address mac-address;
          }
        }
      }
    }
```

You can configure these statements at the following hierarchy levels:

- [edit logical-systems *logical-system-name* protocols interfaces]
- [edit protocols interfaces]

For Ethernet circuits, you also need to configure the ARP. See "ARP Configuration for Ethernet TCC Encapsulations" on page 415.

Ethernet Extended VLAN Encapsulation for Layer 2 Switching TCCs

Specify the encapsulation type for Ethernet extended VLAN circuits in the encapsulation statement. This statement configures the entire physical device. You must also enable VLAN tagging. Ethernet interfaces in VLAN mode can have multiple logical interfaces. For encapsulation type extended-vlan-tcc, all VLAN IDs from 0 through 4094 are valid, up to a maximum of 1024 VLANs. As with Ethernet circuits, you must also specify a proxy address and a remote address at the [edit interfaces *interface-name* unit *logical-unit-number* family tcc] hierarchy level.

Configure Ethernet extended VLAN circuits for TCC as follows:

```
interfaces {
  ethernet-interface-type-fpc/pic/port {
    vlan-tagging;
    encapsulation extended-vlan-tcc;
    unit 0 {
      vlan-id 600;
      family tcc;
      proxy {
        inet-address address;
      }
      remote {
        inet-address address;
        mac-address mac-address;
      }
    }
  }
}
```

You can configure these statements at the following hierarchy levels:

- [edit logical-systems *logical-system-name* protocols interfaces]
- [edit protocols interfaces]

For Ethernet extended VLAN circuits, you also need to configure the ARP. See "ARP Configuration for Ethernet TCC Encapsulations" on page 415.

ARP Configuration for Ethernet TCC Encapsulations

All Ethernet TCC and Ethernet extended VLAN TCC encapsulations require that you also configure the ARP. Since TCC simply removes one Layer 2 header and adds another, the default form of dynamic ARP is not supported. To retain the functionality of ARP for Ethernet networks, you must configure static ARP.

You configure the arp statement at the [edit interfaces *interface-number* unit *unit-number* family inet address *ip-address*] hierarchy level. Since you already specified remote and proxy addresses on the router performing TCC switching, you must apply the static ARP statement to the Ethernet-type interfaces of the routers that connect to the TCC-switched router. The arp statement must contain the IP address and the MAC address of the remotely connected neighbor by use of the unlike Layer 2 protocol on the far side of the TCC switching router.

Configure static ARP as follows:

```
interfaces {
   ethernet-interface-type-fpc/pic/port {
      unit 0 {
         family inet {
            address ip-address {
               arp ip-address mac mac-address;
            }
         }
      }
   }
}
```

You can configure these statements at the following hierarchy levels:

- [edit logical-systems *logical-system-name* protocols interfaces]
- [edit protocols interfaces]

Defining the Connection for the Layer 2 Switching TCC

You must configure the connection between the two circuits of the Layer 2 switching TCC on the router acting as the switch. The connection joins the interface coming from the circuit's source to the interface leading to the circuit's destination. When you specify the interface names, include the logical portion of the name, which corresponds to the logical unit number. The cross-connect is bidirectional, so packets received on the first interface are transmitted from the second interface, and those received on the second interface are transmitted from the first.

To configure a connection for a local interface switch, include the following statements:

```
interface-switch connection-name {
   interface interface-name.unit-number;
}
lsp-switch connection-name {
   transmit-lsp lsp-number;
   receive-lsp lsp-number;
```

```
}
```

You can include these statements at the following hierarchy levels:

- [edit protocols connections]
- [edit logical-systems *logical-system-name* protocols connections]

To configure a connection for a remote interface switch, include the following statements:

```
remote-interface-switch connection-name {
    interface interface-name.unit-number;
    interface interface-name.unit-number;
    transmit-lsp lsp-number;
    receive-lsp lsp-number;
}
```

You can include these statements at the following hierarchy levels:

- [edit protocols connections]
- [edit logical-systems *logical-system-name* protocols connections]

Configuring MPLS

For a Layer 2 switching cross-connect to function, you need to configure MPLS.

To configure MPLS on an interface, configure a logical interface using the unit statement:

```
unit logical-unit-number;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name*]
- [edit logical-systems *logical-system-name* interfaces *interface-name*]

To enable MPLS, include the interface statement:

```
interface (interface-name | all);
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls]
- [edit logical-systems *logical-system-name* protocols mpls]

NOTE: LSP link protection does not support TCC.

Configuring CCC and TCC Graceful Restart

To enable CCC and TCC graceful restart, include the graceful-restart statement:

```
graceful-restart;
```

You can include this statement at the following hierarchy levels:

- [edit routing-options]
- [edit logical-systems *logical-system-name* routing-options]

The graceful-restart statement enables graceful restart for all protocols supporting this feature on the router. For more information about graceful restart, see the *JUNOS Routing Protocols Configuration Guide*.

CCC and TCC graceful restart depend on RSVP graceful restart. If you disable RSVP graceful restart, CCC and TCC graceful restart will not work. For more information about RSVP graceful restart, see "RSVP Graceful Restart" on page 266 and "Configuring RSVP Graceful Restart" on page 286.

Configuring CCC Switching for Point-to-Multipoint LSPs

You can configure CCC to switch traffic from interfaces to point-to-multipoint LSPs. This feature is useful for handling multicast or broadcast traffic (for example, a digital video stream).

To configure CCC switching for point-to-multipoint LSPs, you do the following:

- On the ingress provider edge (PE) router, you configure CCC to switch traffic from an incoming interface to a point-to-multipoint LSP.
- On the egress PE, you configure CCC to switch traffic from an incoming point-to-multipoint LSP to an outgoing interface.

The CCC connection for point-to-multipoint LSPs is unidirectional.

For more information on point-to-multipoint LSPs, see "Point-to-Multipoint LSPs" on page 47 and "Point-to-Multipoint LSP Configuration Guidelines" on page 143.

To configure a CCC connection for a point-to-multipoint LSP, complete the steps in the following sections:

- Configuring the Point-to-Multipoint LSP Switch on the Ingress PE Router on page 417
- Configuring the Point-to-Multipoint LSP Switch on the Egress PE Router on page 418

Configuring the Point-to-Multipoint LSP Switch on the Ingress PE Router

To configure the ingress PE router with a CCC switch for a point-to-multipoint LSP, configure the p2mp-transmit-switch statement.

To specify a name for the ingress CCC switch, include the p2mp-transmit-switch statement:

```
p2mp-transmit-switch point-to-multipoint-transmit-switch-name;
```

You can include this statement at the following hierarchy levels:

- [edit protocols connections]
- [edit logical-systems *logical-system-name* protocols connections]

To specify the name of the ingress interface, include the input-interface statement:

```
input-interface input-interface-name.unit-number;
```

You can include this statement at the following hierarchy levels:

- [edit protocols connections p2mp-transmit-switch *point-to-multipoint-transmit-switch-name*]
- [edit logical-systems *logical-system-name* protocols connections p2mp-transmit-switch *point-to-multipoint-transmit-switch-name*]

To specify the name of the transmitting point-to-multipoint LSP, include the transmit-p2mp-lsp statement:

```
transmit-p2mp-lsp transmitting-point-to-multipoint-lsp;
```

You can include this statement at the following hierarchy levels:

- [edit protocols connections p2mp-transmit-switch *point-to-multipoint-transmit-switch-name*]
- [edit logical-systems *logical-system-name* protocols connections p2mp-transmit-switch *point-to-multipoint-transmit-switch-name*]

Configuring the Point-to-Multipoint LSP Switch on the Egress PE Router

To configure the CCC switch for a point-to-multipoint LSP on the egress PE router, include the p2mp-receive-switch statement.

To specify a name for the egress CCC switch, include the p2mp-receive-switch statement:

```
p2mp-receive-switch point-to-multipoint-transmit-switch-name;
```

You can include this statement at the following hierarchy levels:

- [edit protocols connections]
- [edit logical-systems *logical-system-name* protocols connections]

You can specify multiple egress interfaces for the egress CCC switch by including the output-interface option:

output-interface [*input-interface-name*.*unit-number*];

You can include this option at the following hierarchy levels:

- [edit protocols connections p2mp-receive-switch *point-to-multipoint-transmit-switch-name*]
- [edit logical-systems *logical-system-name* protocols connections p2mp-receive-switch *point-to-multipoint-transmit-switch-name*]

To specify the name of the receiving point-to-multipoint LSP, include the receive-p2mp-lsp option:

receive-p2mp-lsp *transmitting-point-to-multipoint-lsp*;

You can include this option at the following hierarchy levels:

- [edit protocols connections p2mp-transmit-switch *point-to-multipoint-transmit-switch-name*]
- [edit logical-systems *logical-system-name* protocols connections p2mp-transmit-switch *point-to-multipoint-transmit-switch-name*]

Chapter 19

Summary of CCC and TCC Configuration Statements

This chapter provides a reference for each circuit cross-connect (CCC) configuration statement. The statements are organized alphabetically.

connections

Syntax

```
connections {
    interface-switch connection-name {
        interface interface-name.unit-number;
    }
    lsp-switch connection-name {
        transmit-lsp label-switched-path;
        receive-lsp label-switched-path;
    }
    p2mp-receive-switch {
        output-interface [ interface-name.unit-number ];
        receive-p2mp-lsp receiving-point-to-multipoint-lsp;
    }
    p2mp-transmit-switch {
        input-interface input-interface-name.unit-number;
        transmit-p2mp-lsp transmitting-point-to-multipoint-lsp;
    }
    remote-interface-switch connection-name {
        interface interface-name.unit-number;
        receive-lsp label-switched-path;
        transmit-lsp label-switched-path;
    }
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols],
[edit protocols]

Release Information Statement introduced before JUNOS Release 7.4.

Description Define the connection between two circuits in a CCC connection.

Options The statements are explained separately.

Usage Guidelines See "CCC and TCC Configuration Guidelines" on page 397 and the *JUNOS Network Interfaces Configuration Guide*.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

encapsulation

See the following sections:

- encapsulation (Logical Interface) on page 424
- encapsulation (Physical Interface) on page 427

encapsulation (Logical Interface)

Syntax encapsulation (atm-ccc-cell-relay | atm-ccc-vc-mux | atm-tcc-vc-mux | atm-cisco-nlpid | atm-mlppp-llc | atm-nlpid | atm-ppp-llc | atm-ppp-vc-mux | atm-snap | atm-tcc-snap | atm-vc-mux | ether-over-atm-llc | ether-vpls-over-atm-llc | frame-relay-ccc | frame-relay-ppp | frame-relay-tcc | gre-fragmentation | multilink-frame-relay-end-to-end | multilink-ppp | ppp-over-ether | ppp-over-ether-over-atm-llc | vlan-ccc | vlan-ccc | vlan-vpls);

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number*],
[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Logical link-layer encapsulation type.

Options atm-ccc-cell-relay—Use ATM cell-relay encapsulation.

atm-ccc-vc-mux—Use ATM VC multiplex encapsulation on circuit cross-connect (CCC) circuits. When you use this encapsulation type, you can configure the family ccc only.

atm-cisco-nlpid—Use Cisco ATM NLPID encapsulation. When you use this encapsulation type, you can configure the family inet only.

atm-mlppp-llc—For ATM2 IQ interfaces only, use Multilink PPP over ATM adaptation layer 5 (AAL5) logical link control (LLC). For this encapsulation type, your router must be equipped with a Link Services PIC.

atm-nlpid—Use ATM NLPID encapsulation. When you use this encapsulation type, you can configure the family inet only.

atm-ppp-llc—For ATM2 IQ interfaces only, use PPP over ATM adaptation layer 5 (AAL5) logical link control (LLC) encapsulation.

atm-ppp-vc-mux—For ATM2 IQ interfaces only, use PPP over ATM adaptation layer 5 (AAL5) multiplex encapsulation.

atm-snap—Use ATM SNAP encapsulation.

atm-tcc-snap—Use ATM SNAP encapsulation on translational cross-connect (TCC) circuits.

atm-tcc-vc-mux—Use ATM VC multiplex encapsulation on translational cross-connect (TCC) circuits. When you use this encapsulation type, you can configure the family tcc only.

atm-vc-mux—Use ATM VC multiplex encapsulation. When you use this encapsulation type, you can configure the family inet only.

ether-over-atm-llc—For interfaces that carry IPv4 traffic, use Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure multipoint interfaces.

ether-vpls-over-atm-llc—For ATM intelligent queuing interfaces only, use the Ethernet VPLS over ATM LLC encapsulation to bridge Ethernet interfaces and ATM interfaces over a VPLS routing instance (as described in RFC 2684). Packets from the ATM interfaces are converted to standard ENET2/802.3 encapsulated Ethernet frames with the FCS field removed.

frame-relay-ccc—Use Frame Relay encapsulation on CCC circuits. When you use this encapsulation type, you can configure the family ccc only.

frame-relay-ppp—Use Frame Relay encapsulation on PPP circuits.

frame-relay-tcc—Use Frame Relay encapsulation on TCC circuits for connecting unlike media. When you use this encapsulation type, you can configure the family tcc only.

gre-fragmentation—For adaptive services interfaces only, use GRE fragmentation encapsulation to enable fragmentation of IPv4 packets in GRE tunnels. This encapsulation clears the don't fragment (DF) bit in the packet header. If the packet's size exceeds the tunnel's MTU value, the packet is fragmented before encapsulation.

multilink-frame-relay-end-to-end—Use Multilink Frame Relay (MLFR) FRF.15 encapsulation. This encapsulation is used only on multilink and link services interfaces and their constituent T1 or E1 interfaces.

multilink-ppp—Use Multilink Point-to-Point Protocol (MLPPP) encapsulation. This encapsulation is used only on multilink and link services interfaces and their constituent T1 or E1 interfaces.

ppp-over-ether—For underlying Ethernet interfaces on J-series Services Routers only, use PPP over Ethernet encapsulation. When you use this encapsulation type, you cannot configure the interface address. Instead, you configure the interface address on the PPP interface. For more information, see the *J-series Services Router Advanced WAN Access Configuration Guide*.

ppp-over-ether-over-atm-llc—For underlying ATM interfaces on J-series Services Routers only, use PPP over Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure the interface address. Instead, you configure the interface address on the PPP interface. For more information, see the *J-series Services Router Advanced WAN Access Configuration Guide*.

vlan-ccc—Use Ethernet virtual local area network (VLAN) encapsulation on CCC circuits. When you use this encapsulation type, you can configure the family ccc only.

vlan-tcc—Use Ethernet VLAN encapsulation on TCC circuits. When you use this encapsulation type, you can configure the family tcc only.

vlan-vpls—Use Ethernet VLAN encapsulation on virtual private LAN service (VPLS) circuits.

Usage Guidelines See "Defining the Encapsulation for Layer 2 Switching Cross-Connects" on page 398, "Defining the CCC Encapsulation for LSP Tunnel Cross-Connects" on page 406, and "Defining the Encapsulation for the Layer 2 Switching TCCs" on page 411. For more information about how to configure interfaces, see the *JUNOS Network Interfaces Configuration Guide*.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

encapsulation (Physical Interface)

Syntax encapsulation (atm-ccc-cell-relay | atm-pvc | cisco-hdlc | cisco-hdlc-ccc | cisco-hdlc-tcc | ethernet-ccc | ethernet-over-atm | ethernet-tcc | ethernet-vpls | extended-frame-relay-ccc | extended-frame-relay-tcc | extended-vlan-ccc | extended-vlan-tcc | extended-vlan-vpls | flexible-ethernet-services | flexible-frame-relay | frame-relay | frame-relay-ccc | frame-relay-tcc | frame-relay-port-ccc | multilink-frame-relay-uni-nni | ppp | ppp-ccc | ppp-tcc | vlan-ccc | vlan-vpls);

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Physical link-layer encapsulation type.

Default PPP encapsulation.

Options atm-ccc-cell-relay—Use ATM cell-relay encapsulation.

atm-pvc—Use ATM PVC encapsulation.

cisco-hdlc—Use Cisco-compatible HDLC framing.

cisco-hdlc-ccc—Use Cisco-compatible HDLC framing on CCC circuits.

cisco-hdlc-tcc—Use Cisco-compatible HDLC framing on TCC circuits for connecting unlike media.

ethernet-ccc—Use Ethernet CCC encapsulation on Ethernet interfaces that must accept packets carrying standard TPID values.

ethernet-over-atm—As defined in RFC 1483, this encapsulation type allows ATM interfaces to connect to devices that support only bridged-mode protocol data units (PDUs). The JUNOS software does not completely support bridging, but accepts BPDU packets as a default gateway. If you use the router as an edge device, then the router acts as a default gateway. It accepts Ethernet LLC/SNAP frames with IP or ARP in the payload and drops the rest. For packets destined the Ethernet LAN, a route lookup is done by use of the destination IP address. If the route lookup yields a full address match, the packet is encapsulated with an LLC/SNAP and MAC header, and the packet is forwarded to the ATM interface.

ethernet-tcc—For interfaces that carry IPv4 traffic, use Ethernet TCC encapsulation on interfaces that must accept packets carrying standard TPID values. Ethernet TCC is not currently supported on Fast Ethernet 48-port PICs.

ethernet-vpls—Use Ethernet VPLS encapsulation on Ethernet interfaces that have VPLS enabled and that must accept packets carrying standard TPID values.

extended-frame-relay-ccc—Use Frame Relay encapsulation on CCC circuits. This encapsulation type allows you to dedicate DLCIs 1 through 1022 to CCC.

extended-frame-relay-tcc—Use Frame Relay encapsulation on TCC circuits to connect unlike media. This encapsulation type allows you to dedicate DLCIs 1 through 1022 to TCC.

extended-vlan-ccc—Use extended VLAN encapsulation on CCC circuits with Gigabit Ethernet and four-port Fast Ethernet interfaces that must accept packets carrying 802.1Q values.

extended-vlan-tcc—For interfaces that carry IPv4 traffic, use extended VLAN encapsulation on TCC circuits with Gigabit Ethernet interfaces on which you want to use 802.1Q tagging. Extended Ethernet TCC is not currently supported on Fast Ethernet 48-port PICs.

extended-vlan-vpls—Use extended VLAN VPLS encapsulation on Ethernet interfaces that have VLAN 802.1Q tagging and VPLS enabled and that must accept packets carrying TPIDs 0x8100, 0x9100, and 0x9901.

flexible-ethernet-services—For Gigabit Ethernet intelligent queuing interfaces only, use flexible Ethernet services encapsulation when you want to configure multiple per-unit Ethernet encapsulations. This encapsulation type allows you to configure any combination of routed, TCC, CCC, and VPLS encapsulations on a single physical port.

flexible-frame-relay—For intelligent queuing interfaces only, use flexible Frame Relay encapsulation when you want to configure multiple per-unit Frame Relay encapsulations. This encapsulation type allows you to configure any combination of TCC, CCC, or standard Frame Relay encapsulations on a single physical port. Also, each logical interface can have any DLCI value in the range 1 through 1022.

frame-relay—Use Frame Relay encapsulation.

frame-relay-ccc—Use plain Frame Relay encapsulation or Frame Relay encapsulation on circuit cross-connect (CCC) circuits.

frame-relay-tcc—Use Frame Relay encapsulation on TCC circuits to connect unlike media.

frame-relay-port-ccc—Use Frame Relay port CCC encapsulation to transparently carry all the DLCIs between two CE routers without explicitly configuring each DLCI on the two PE routers with Frame Relay transport. When you use this encapsulation type, you can configure the family ccc only.

multilink-frame-relay-uni-nni—Use MLFR user-to-network (UNI) network-to-network (NNI) encapsulation. This encapsulation is used only on link services interfaces functioning as FRF.16 bundles and their constituent T1 or E1 interfaces.

ppp—Use serial PPP encapsulation.

ppp-ccc—Use serial PPP encapsulation on CCC circuits. When you use this encapsulation type, you can configure the family ccc only.

ppp-tcc—Use serial PPP encapsulation on TCC circuits for connecting unlike media. When you use this encapsulation type, you can configure the family tcc only.

vlan-ccc—Use Ethernet VLAN encapsulation on CCC circuits.

vlan-vpls—Use VLAN VPLS encapsulation on Ethernet interfaces with VLAN tagging and VPLS enabled. Interfaces with VLAN VPLS encapsulation accept packets carrying standard TPID values only.

Usage Guidelines See "Defining the Encapsulation for Layer 2 Switching Cross-Connects" on page 398, "Defining the CCC Encapsulation for LSP Tunnel Cross-Connects" on page 406, and "Defining the Encapsulation for the Layer 2 Switching TCCs" on page 411. For more information about how to configure interfaces, see the *JUNOS Network Interfaces Configuration Guide*.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

interface-switch

Syntax
```
interface-switch connection-name {
    interface interface-name.unit-number;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols connections],
[edit protocols connections]

Release Information Statement introduced before JUNOS Release 7.4.

Description Configure Layer 2 switching cross-connects. The cross-connect is bidirectional, so packets received on the first interface are transmitted out the second interface, and those received on the second interface are transmitted out the first.

For Layer 2 switching cross-connects to work, you must also configure MPLS.

Options *connection-name*—Connection name.

interface *interface-name.unit-number*—Interface name. Include the logical portion of the name, which corresponds to the logical unit number.

Usage Guidelines See "Defining the CCC Connection for Layer 2 Switching Cross-Connects" on page 402.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration

lsp-switch

Syntax

```
lsp-switch connection-name {
    transmit-lsp label-switched-path;
    receive-lsp label-switched-path;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols connections], [edit protocols connections]

Release Information Statement introduced before JUNOS Release 7.4.

Description Configure Layer 2 switching cross-connects.

Options *connection-name*—Connection name.

receive-lsp *label-switched-path*—Name of the LSP from the connection's source.

transmit-lsp *label-switched-path*—Name of the LSP to the connection's destination.

Usage Guidelines See "CCC and TCC Configuration Guidelines" on page 397, "Configuring LSP Stitching Cross-Connects" on page 409, and "Defining the Connection for the Layer 2 Switching TCC" on page 415.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

p2mp-receive-switch

Syntax

```
p2mp-receive-switch point-to-multipoint-switch-name {
    output-interface [ interface-name.unit-number ];
    receive-p2mp-lsp receiving-point-to-multipoint-lsp;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols connections], [edit protocols connections]

Release Information Statement introduced before JUNOS Release 7.4.

Description Configure the CCC switch for a point-to-multipoint LSP on the egress PE router.

Options *point-to-multipoint-switch-name*—Point-to-multipoint CCC receive switch name.

output-interface *interface-name.unit-number*—Name of the egress interfaces for the point-to-multipoint LSP traffic. You can configure multiple output interfaces.

receive-p2mp-lsp *receiving-point-to-multipoint-lsp*—Name of the point-to-multipoint LSP that is switched to the output interface.

Usage Guidelines See "Configuring the Point-to-Multipoint LSP Switch on the Egress PE Router" on page 418.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

p2mp-transmit-switch

Syntax

```
p2mp-transmit-switch point-to-multipoint-transmit-switch-name {
    input-interface interface-name.unit-number;
    transmit-p2mp-lsp interface-name.unit-number;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols connections], [edit protocols connections]

Release Information Statement introduced before JUNOS Release 7.4.

Description Configure the CCC switch for the point-to-multipoint LSP on the ingress PE router.

Options

point-to-multipoint-transmit-switch-name—Point-to-multipoint CCC transmit switch name.

input-interface *input-interface-name.unit-number*—Specify the name of the interface carrying incoming traffic to be switched to the point-to-multipoint LSP.

transmit-p2mp-lsp *transmitting-point-to-multipoint-lsp*—Specify the name of the point-to-multipoint LSP carrying traffic to the CCC switch on the egress PE router.

Usage Guidelines See "Configuring the Point-to-Multipoint LSP Switch on the Ingress PE Router" on page 417.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

remote-interface-switch

Syntax

```
remote-interface-switch connection-name {
    interface interface-name.unit-number;
    transmit-lsp label-switched-path;
    receive-lsp label-switched-path;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols connections], [edit protocols connections]

Release Information Statement introduced before JUNOS Release 7.4.

Description Configure MPLS LSP tunnel cross-connects.

Options *connection-name*—Connection name.

interface *interface-name.unit-number*—Interface name. Include the logical portion of the name, which corresponds to the logical unit number.

receive-lsp *label-switched-path*—Name of the LSP from the connection's source.

transmit-lsp *label-switched-path*—Name of the LSP to the connection's destination.

Usage Guidelines See "CCC and TCC Configuration Guidelines" on page 397 and "Configuring MPLS LSP Tunnel Cross-Connects" on page 405.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Part 6
GMPLS

- GMPLS Overview on page 437
- GMPLS Configuration Guidelines on page 443
- RSVP LSP Hierarchy Configuration Guidelines on page 459
- Summary of GMPLS Configuration Statements on page 465

Chapter 20

GMPLS Overview

Generalized Multiprotocol Label Switching (GMPLS) is the next-generation implementation of Multiprotocol Label Switching (MPLS). GMPLS extends the functionality of MPLS to include a wider range of label-switched path (LSP) options for a variety of network devices.

This chapter includes the following topics:

- GMPLS Standards on page 437
- Terms and Acronyms on page 438
- Overview on page 439
- GMPLS Operation on page 440
- GMPLS and OSPF on page 441
- GMPLS and CSPF on page 441
- GMPLS Features on page 441

GMPLS Standards

The JUNOS software supports the following IETF RFC and Internet drafts related to GMPLS:

- RFC 3471, *Generalized Multi-Protocol Label Switching (GMPLS)-Signaling Functional Description* (generalized label request [bandwidth encoding only], generalized label [suggested label only], bidirectional LSPs [upstream label only], and control channel separation)
- RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions* (only Section 9, “Fault Handling”)
- RFC 4206, *Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)*
- Internet draft draft-ietf-ccamp-gmpls-routing-09.txt, *Routing Extensions in Support of Generalized MPLS* (expires April 2004)

- Internet draft draft-ietf-ccamp-gmpls-rsvp-te-ason-02.txt, *Generalized MPLS (GMPLS) RSVP-TE Signaling in support of Automatically Switched Optical Network (ASON)* (expires January 2005)
- Internet draft draft-ietf-ccamp-gmpls-sonet-sdh-08.txt, *Generalized Multi-Protocol Label Switching Extensions for SONET and SDH Control* (expires August 2003), (SUKLM labels and SONET traffic parameters only)
- Internet draft draft-ietf-ccamp-lmp-10.txt, *Link Management Protocol (LMP)* (expires April 2004)
- Internet draft draft-ietf-ccamp-ospf-gmpls-extensions-04.txt, *OSPF Extensions in Support of Generalized MPLS* (expires August 2002), (except Link Local/Remote Identifiers, Link Protection Type, Shared Risk Link Group (SRLG), and Implications of Graceful Restart)

The interface switching capability descriptor described in Section 6.4 is implemented; however, it is currently packet-switch capable only.

- Internet draft draft-ietf-mpls-bundle-04.txt, *Link Bundling in MPLS Traffic Engineering*

To access RFCs and drafts, go to the IETF Web site at http://www.ietf.org/.

Terms and Acronyms

The following is a list of GMPLS-related terms:

- Generalized Multiprotocol Label Switching (GMPLS)—An extension to MPLS that allows data from multiple layers to be switched over label-switched paths (LSPs). GMPLS LSP connections are possible between similar Layer 1, Layer 2, and Layer 3 devices.
- Forwarding adjacency—A forwarding path for sending data between GMPLS-enabled devices.
- GMPLS label—Layer 3 identifiers, fiber port, time-division multiplexing (TDM) time slot, or dense wavelength-division multiplexing (DWDM) wavelength of a GMPLS-enabled device used as a next-hop identifier.
- GMPLS LSP types—The four types of GMPLS LSPs are:
  - Fiber-switched capable (FSC)—LSPs are switched between two fiber-based devices, such optical cross-connects (OXCs) that operate at the level of individual fibers.
  - Lambda-switched capable (LSC)—LSPs are switched between two DWDM devices, such as such as OXCs that operate at the level of individual wavelengths.
  - TDM-switched capable (TDM)—LSPs are switched between two TDM devices, such as SONET ADMs.
  - Packet-switched capable (PSC)—LSPs are switched between two packet-based devices, such as routers or ATM switches.

- Link Management Protocol—A protocol used to define a forwarding adjacency between peers and to maintain and allocate resources on the traffic engineering links.
- Traffic engineering link—A logical connection between GMPLS-enabled devices. Traffic engineering links can have addresses or IDs and are associated with certain resources or interfaces. They also have certain attributes (encoding-type, switching capability, bandwidth, and so on). The logical addresses can be routable, although this is not required because they are acting as link identifiers. Each traffic engineering link represents a forwarding adjacency between a pair of devices.

Overview

Traditional MPLS is designed to carry Layer 3 IP traffic using established IP-based paths and associating these paths with arbitrarily assigned labels. These labels can be configured explicitly by a network administrator, or can be dynamically assigned by means of a protocol such as the Label Distribution Protocol (LDP) or the Resource Reservation Protocol (RSVP).

GMPLS generalizes MPLS in that it defines labels for switching varying types of Layer 1, Layer 2, or Layer 3 traffic. GMPLS nodes can have links with one or more of the following switching capabilities:

- Fiber-switched capable (FSC)
- Lambda-switched capable (LSC)
- Time-division multiplexing (TDM) switched-capable (TSC)
- Packet-switched capable (PSC)

Label-switched paths (LSPs) must start and end on links with the same switching capability. For example, routers can establish packet-switched LSPs with other routers. The LSPs might be carried over a TDM-switched LSP between SONET add/drop multiplexers (ADMs), which in turn might be carried over a lambda-switched LSP.

The result of this extension of the MPLS protocol is an expansion in the number of devices that can participate in label switching. Lower-layer devices, such as OXCs and SONET ADMs, can now participate in GMPLS signaling and set up paths to transfer data. A router can participate in signaling optical paths across a transport network.

Two service models determine the visibility that a client node (a router, for example) has into the optical core or transport network. The first is through a user-to-network interface (UNI), which is often referred to as the overlay model. The second is known as the peer model. Juniper Networks supports both models.

NOTE: There is not necessarily a one-to-one correspondence between a physical interface and a GMPLS interface. If a GMPLS connection uses a nonchannelized physical connector, the GMPLS label can use the physical port ID. However, the label for channelized interfaces often is based on a channel or time slot. Consequently, it is best to refer to GMPLS labels as identifiers for a resource on a traffic engineering link.

To establish LSPs, GMPLS uses the following mechanisms:

- An out-of-band control channel and a data channel—RSVP messages for LSP setup are sent over an out-of-band control network. Once the LSP setup is complete and the path is provisioned, the data channel is up and can be used to carry traffic. The Link Management Protocol (LMP) is used to define and manage the data channels between a pair of nodes. You can optionally use LMP to establish and maintain LMP control channels between peers running the same JUNOS software release.
- RSVP-TE extensions for GMPLS—RSVP-TE is already designed to signal the setup of packet LSPs. This has been extended for GMPLS to be able to request path setup for various kinds of LSPs (nonpacket) and request labels like wavelengths, time slots, and fibers as label objects.
- Bidirectional LSPs—Data can travel both ways between GMPLS devices over a single path, so nonpacket LSPs are signaled to be bidirectional.

GMPLS Operation

The basic functionality of GMPLS requires close interaction between RSVP and LMP. It works in the following sequence:

1. LMP notifies RSVP of the new entities:
   - Traffic engineering link (forwarding adjacency)
   - Resources available for the traffic engineering link
   - Control peer
2. GMPLS extracts the LSP attributes from the configuration and requests RSVP to signal one or more specific paths, which are specified by the traffic engineering link addresses.
3. RSVP determines the local traffic engineering link, corresponding control adjacency and active control channel, and transmission parameters (such as IP destination). It requests that LMP allocate a resource from the traffic engineering link with the specified attributes. If LMP finds a resource matching the attributes, label allocation succeeds. RSVP sends a PathMsg hop by hop until it reaches the target router.
4. When the target router receives the PathMsg, RSVP again requests that LMP allocate a resource based on the signaled parameters. If label allocation succeeds, the router sends back a ResvMsg.
5. If the signaling is successful, a bidirectional optical path is provisioned.

GMPLS and OSPF

You can configure the Open Shortest Path First (OSPF) protocol for GMPLS. OSPF is an interior gateway protocol (IGP) that routes packets within a single autonomous system (AS). OSPF uses link-state information to make routing decisions.

GMPLS and CSPF

GMPLS introduces extra constraints for computing paths for GMPLS LSPs that use CSPF. These additional constraints affect the following link attributes:

- Signal type (minimum LSP bandwidth)
- Encoding type
- Switching type

These new constraints are populated in the traffic engineering database (TED) with the exchange of an interface-switching capability descriptor type length value (TLV) through an IGP.

The ignored constraints that are exchanged through the interface switching capability descriptor include:

- Maximum LSP bandwidth
- Maximum transmission unit (MTU)

The CSPF path computation is the same as in non-GMPLS environments, except that the links are also limited by GMPLS constraints.

Each link can have multiple interface-switching capability descriptors. All the descriptors are checked before a link is rejected.

The constraints are checked in the following order:

1. The signal type configured for the GMPLS LSP signifies the amount of bandwidth requested. If the desired bandwidth is less than the minimum LSP bandwidth, the interface-switching descriptor is rejected.
2. The encoding type of the link for the ingress and the egress interfaces should match. The encoding type is selected and stored at the ingress node after all the constraints are satisfied by the link and is used to select the link on the egress node.
3. The switching type of the links of the intermediate switches should match that of the GMPLS LSP specified in the configuration.

GMPLS Features

The JUNOS software includes the following GMPLS functionality:

- An out-of-band control plane makes it possible to signal LSP path setup.
- RSVP-TE extensions support additional objects beyond Layer 3 packets, such as ports, time slots, and wavelengths.
- The LMP protocol creates and maintains a database of traffic engineering links and peer information. Only the static version of this protocol is supported in the JUNOS software. You can optionally configure LMP to establish and maintain LMP control channels between peers running the same JUNOS software release.
- Bidirectional LSPs are required between devices.
- Several GMPLS label types that are defined in RFC 3471, *Generalized MPLS —Signaling Functional Description*, such as MPLS, Generalized, SONET/SDH, Suggested, and Upstream, are supported. Generalized labels do not contain a type field, because the nodes should know from the context of their connection what type of label to expect.
- Traffic parameters facilitate GMPLS bandwidth encoding and SONET/SDH formatting.
- Other supported attributes include interface identification and errored interface identification, UNI-style signaling, and secondary LSP paths.

Chapter 21

GMPLS Configuration Guidelines

Although you can configure the GMPLS-related statements at the [edit logical-systems *logical-system-name*] hierarchy level, GMPLS is not supported on logical routers.

To configure GMPLS, you must complete the following tasks:

- Configuring LMP on page 443
- Configuring MPLS LSPs for GMPLS on page 453
- Gracefully Tearing Down GMPLS LSPs on page 456

Configuring LMP

You need to configure the Link Management Protocol (LMP) to define the data channel connection and the control channel connection between devices. Include the following statements at the [edit protocols link-management] hierarchy level:

```
[edit protocols link-management]
peer peer-name {
    address address;
    control-channel control-channel-name;
    lmp-control-channel control-channel-interface {
        remote-address ip-address;
    }
    lmp-protocol {
        hello-interval milliseconds;
        hello-dead-interval milliseconds;
        retransmission-interval milliseconds;
        retry-limit number;
        passive;
    }
    te-link te-link-name;
}
te-link te-link-name {
    disable;
    interface interface-name {
        disable;
        local-address ip-address;
        remote-address ip-address;
        remote-id id-number;
    }
    label-switched-path lsp-name;
    local-address ip-address;
```

```
    remote-address ip-address;
    remote-id id-number;
  }
  traceoptions {
    file filename <files number> <no-stamp> <replace> <size size>
    <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
  }
```

The sections that follow describe how to configure LMP:

- Configuring LMP Traffic Engineering Links on page 444
- Configuring LMP Peers on page 446
- Configuring Peer Interfaces in RSVP and OSPF on page 451
- Configuring MPLS Paths for GMPLS on page 452
- Tracing LMP Traffic on page 452

Configuring LMP Traffic Engineering Links

An LMP traffic engineering link acts as a data channel connection between GMPLS devices.

To configure a traffic engineering link, include the **te-link** statement at the **[edit protocols link-management]** hierarchy level:

```
[edit protocols link-management]
te-link te-link-name {
  disable;
  interface interface-name {
    local-address ip-address;
    remote-address ip-address;
    remote-id id-number;
  }
  label-switched-path lsp-name;
  local-address ip-address;
  remote-address ip-address;
  remote-id id-number;
}
```

Complete the procedures in the following sections to configure an LMP traffic engineering link:

- Configuring the Local IP Address for the Traffic Engineering Link on page 445
- Configuring the Remote IP Address for the Traffic Engineering Link on page 445
- Configuring the Remote ID for the Traffic Engineering Link on page 445

When you configure a traffic engineering link that contains interfaces for an LMP peer, you must also configure a control channel. However, no control channel is required for a traffic engineering link that contains an LSP. For information on configuring control channels, see “Configuring LMP Peers” on page 446.

Configuring the Local IP Address for the Traffic Engineering Link

Use the local-address statement to configure the local IP address associated with the traffic engineering link.

We recommend that you configure an IP address subnet for your traffic engineering link addresses that is different from the subnet configured for your physical interfaces. This configuration enables you to identify which addresses are physical and which addresses belong to the traffic engineering link.

To configure the local IP address for the traffic engineering link, include the local-address statement:

```
te-link te-link-name {
    interface interface-name {
        local-address ip-address;
    }
    local-address ip-address;
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Configuring the Remote IP Address for the Traffic Engineering Link

You need to specify the address of the remote end of the data channel for each traffic engineering link. Use the remote-address statement to configure the remote IP address.

We recommend that you configure an IP address subnet for your traffic engineering link addresses that is different from the subnet configured for your physical interfaces. This enables you to identify which addresses are physical and which addresses belong to the traffic engineering link.

To configure the remote IP address for the traffic engineering link, include the remote-address statement:

```
te-link te-link-name {
    interface interface-name {
        remote-address ip-address;
    }
    remote-address ip-address;
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Configuring the Remote ID for the Traffic Engineering Link

The local ID for the traffic engineering link is automatically assigned by LMP. The port identifier and labels for the interfaces (resources) in the traffic engineering link are also assigned automatically. However, you need to explicitly configure the remote ID for the traffic engineering link and the remote ID traffic engineering link interface.

The remote ID for the interface must be based on the post-ID assignment of the peer node. The remote IDs are needed for static mapping of remote labels to local labels.

Before you can obtain the remote IDs for the traffic engineering link and traffic engineering link interface on the peer node, you must first configure the LMP peer, as described in "Configuring LMP Peers" on page 446. Once you have configured the LMP peer, you can obtain the traffic engineering link local ID and interface local ID by issuing the show link-management te-link command. Once you have these IDs, you can configure them as the remote IDs on the peer node.

To configure the remote ID for a traffic engineering link and for the traffic engineering link interface, include the remote-id statement:

```
te-link te-link-name {
    interface interface-name {
        remote-id id-number;
    }
    remote-id id-number;
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Configuring LMP Peers

You need to configure network peers for GMPLS. A peer is a network device that your router communicates with when setting up the control and data channels. The peer is often an optical cross-connect (OXC).

To configure an LMP peer name, include the peer statement at the [edit protocols link-management] hierarchy level:

```
peer peer-name {
    address ip-address;
    control-channel control-channel-interface;
    lmp-control-channel control-channel-interface {
        remote-address ip-address;
    }
    lmp-protocol {
        hello-interval milliseconds;
        hello-dead-interval milliseconds;
        retransmission-interval milliseconds;
        retry-limit number;
        passive;
    }
    te-link te-link-name;
}
```

The following sections describe how to configure the other statements needed for an LMP peer:

- Configuring the LMP Peer ID on page 447
- Configuring the Control Channel Interface on page 447
- Configuring the LMP Control Channel Interface for the Peer on page 447

- Configuring the Remote IP Address for the LMP Control Channel on page 448
- Configuring the Hello Message Attributes for the LMP Control Channel on page 448
- Configuring Message Attributes for the LMP Control Channel on page 449
- Configuring the Local Peer to Wait for the Remote Peer on page 450
- Configuring the Traffic Engineering Link for the LMP Peer on page 450
- Disabling the Traffic Engineering Link for the LMP Peer on page 450

Configuring the LMP Peer ID

To configure the LMP peer ID, include the address statement at the [edit protocols link-management peer *peer-name*] hierarchy level. The default value for the LMP peer ID is the loopback address.

```
[edit protocols link-management peer peer-name]
address ip-address;
```

Configuring the Control Channel Interface

You must configure one or more control channels between the LMP peers. The control channels must travel across either a point-to-point link or a tunnel.

To configure an interface for the control channel, include the control-channel statement at the [edit protocols link-management peer *peer-name*] hierarchy level:

```
[edit protocols link-management peer peer-name]
control-channel control-channel-interface;
```

You can configure a generic routing encapsulation (GRE) interface for the control channel. This type of interface does not require a Tunnel PIC.

NOTE: You can configure GRE interfaces only for GMPLS control channels. GRE interfaces are not supported or configurable for other applications. For more information, see the *JUNOS Network Interfaces Configuration Guide*.

Configuring the LMP Control Channel Interface for the Peer

In an environment that uses LMP to establish and maintain an LMP control channel between peers, you can configure a number of attributes associated with LMP. To configure the interface to be associated with the LMP control channel for the peer, include the lmp-control-channel statement:

```
lmp-control-channel control-channel-interface;
```

You can configure this statement at the following hierarchy levels:

- [edit protocols link-management peer *peer-name*]
- [edit logical-systems *logical-system-name* protocols link-management peer *peer-name*]

You can configure a generic routing encapsulation (GRE) interface for the LMP control channel. This type of interface does not require a Tunnel PIC.

NOTE: You can configure GRE interfaces only for GMPLS control channels. GRE interfaces are not supported or configurable for other applications. For more information, see the *JUNOS Network Interfaces Configuration Guide*.

When this LMP control channel interface comes up, the peers use LMP to negotiate channel parameters and configure the control channel.

The local peer repeatedly sends a Config message to the remote peer. The Config message contains the local control channel ID, the local peer's node ID, a message ID, and a CONFIG object that includes hello message attributes (the hello interval and the hello dead interval).

The channel is activated when the remote peer responds with a ConfigAck message. The remote peer does so only when its own configured hello interval and hello dead interval match the values in the received Config message or the default values. If these values do not match, the remote peer responds with a ConfigNack message. The local peer logs this event and resends the Config message until the message retry limit is reached. When the message retry limit is reached, the local peer logs that event and restarts the configuration process.

Configuring the Remote IP Address for the LMP Control Channel

You need to specify the address of the remote end of the LMP control channel.

To configure the remote IP address for the LMP control channel, include the remote-address statement:

```
remote-address address;
```

You can configure this statement at the following hierarchy levels:

- [edit protocols link-management peer *peer-name* lmp-control-channel *control-channel-interface*]
- [edit logical-systems *logical-system-name* protocols link-management peer *peer-name* lmp-control-channel *control-channel-interface*]

Configuring the Hello Message Attributes for the LMP Control Channel

Hello messages are exchanged between LMP peers to maintain the control channel after LMP has activated the control channel. The LMP control channel is considered to be up only when the hello negotiation is successful. Successful negotiation consists of the local peer sending a hello message to the remote peer and receiving a hello message in response.

The LMP peers continue to exchange hello messages after the LMP control channel is up in order to maintain the channel.

The hello interval specifies the interval between periodic hello messages. The hello dead interval specifies how long the local peer waits for a hello response before it declares the LMP control channel to be down. When the channel goes down, the local peer restarts the LMP control channel negotiation and configuration process.

You can specify a hello interval from 150 through 300,000 milliseconds. The default hello interval is 150 milliseconds.

You can specify a hello dead interval from 500 through 300,000 milliseconds. The default hello dead interval is 500 milliseconds.

To configure the attributes for hello messages exchanged between LMP peers, include the hello-interval and hello-dead-interval statements:

```
hello-interval milliseconds;
hello-dead-interval milliseconds;
```

You can configure these statements at the following hierarchy levels:

- [edit protocols link-management peer *peer-name* lmp-protocol]
- [edit logical-systems *logical-system-name* protocols link-management peer *peer-name* lmp-protocol]

When an LMP control channel comes up after a successful exchange of hello messages between LMP peers, LMP uses link property correlation to verify the traffic engineering and data link information on both sides of a link. To do so, the local peer sends a LinkSummary message for each traffic engineering link governed by the LMP control channel. The LinkSummary message contains information that characterizes the traffic engineering link and each data link in the traffic engineering link.

The local peer continues sending a LinkSummary message for each link until the remote peer responds with a LinkSummaryAck message or until the message retry limit is reached. When the message retry limit is reached, the local peer logs that event and restarts the link property correlation process.

When the remote peer receives a LinkSummary message, it examines its own link information. If this information agrees with that in the LinkSummary message, the remote peer responds with a LinkSummaryAck message. If the information is different, the remote peer responds with a LinkSummaryNack message.

Configuring Message Attributes for the LMP Control Channel

You can configure message attributes that control the exchange of LMP Config and LinkSummary messages. The retransmission interval specifies the interval between resubmitted LMP messages. The retry limit specifies how many times LMP sends a message before restarting the process.

You can specify a retransmission interval from 500 through 300,000 milliseconds. The default retransmission interval is 500 milliseconds.

You can specify a retry limit from 3 through 1000 attempts. The default number of retry attempts is three.

To configure attributes governing the exchange of LMP messages between peers, include the retransmission-interval and retry-limit statements:

```
retransmission-interval milliseconds;
retry-limit number;
```

You can configure these statements at the following hierarchy levels:

- [edit protocols link-management peer *peer-name* lmp-protocol]
- [edit logical-systems *logical-system-name* protocols link-management peer *peer-name* lmp-protocol]

Configuring the Local Peer to Wait for the Remote Peer

You can specify that the local peer does not initiate LMP negotiation. Instead, the local peer waits for the remote peer to configure the LMP control channel.

To configure the local peer to wait for the remote peer to configure the LMP control channel, include the passive statement:

```
passive;
```

You can configure this statement at the following hierarchy levels:

- [edit protocols link-management peer *peer-name* lmp-protocol]
- [edit logical-systems *logical-system-name* protocols link-management peer *peer-name* lmp-protocol]

Configuring the Traffic Engineering Link for the LMP Peer

To specify the name of a traffic engineering link to be associated with this peer, include the te-link statement at the [edit protocols link-management peer *peer-name*] hierarchy level:

```
[edit protocols link-management peer peer-name]
te-link te-link-name;
```

For information on how to configure a traffic engineering link, see "Configuring LMP Traffic Engineering Links" on page 444.

Disabling the Traffic Engineering Link for the LMP Peer

To disable a specific traffic engineering link, include the disable statement:

```
disable;
```

You can configure this statement at the following hierarchy levels:

- [edit protocols link-management te-link *te-link-name*]
- [edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name*]

Configuring Peer Interfaces in RSVP and OSPF

After you have configured the LMP peers, add the peer interfaces to RSVP and OSPF. The peer interface name must match the peer name configured in LMP. Once the peer interfaces are added to the protocols, the traffic engineering link local and remote addresses can be signaled and advertised to peers like any other interface enabled for RSVP and OSPF. These addresses act as virtual interfaces for GMPLS.

NOTE: When adding the virtual peer interfaces to RSVP and OSPF, do not configure the corresponding physical control channel interface in either protocol. If you include the interface all statement, you must disable the RSVP and OSPF protocols manually on the control channel interface.

To configure peer interfaces in RSVP and OSPF, complete the procedures in the following sections:

- Configuring Peer Interfaces in RSVP on page 451
- Configuring Peer Interfaces in OSPF on page 451
- Configuring the Hello Interval for Peer Interfaces on page 452

Configuring Peer Interfaces in RSVP

To configure RSVP signaling for LMP peers, configure the LMP peer interface by including the peer-interface statement at the [edit protocols rsvp] hierarchy level:

```
[edit protocols rsvp]
peer-interface peer-interface-name {
    (aggregate | no-aggregate);
    authentication-key key;
    disable;
    hello-interval seconds;
    (reliable | no-reliable);
}
```

The statements configured at the [edit protocols rsvp peer-interface *peer-interface-name*] hierarchy level have the same functionality as the statements configured at the [edit protocols rsvp interface *interface-name*] hierarchy level.

Configuring Peer Interfaces in OSPF

To configure OSPF routing for LMP peers, configure the name of the LMP peer by including the peer-interface statement at the [edit protocols ospf area *area-number*] hierarchy level:

```
[edit protocols ospf area area-number]
peer-interface peer-interface-name {
    dead-interval seconds;
    disable;
    hello-interval seconds;
    retransmit-interval seconds;
    transit-delay seconds;
```

```
}
```

For information on how to configure OSPF statements, see the *JUNOS Routing Protocols Configuration Guide*.

Configuring the Hello Interval for Peer Interfaces

Hello packets are used to indicate to neighboring routers that the peer interface is still up and running. The hello interval must be the same for all routers on a shared logical IP network. You can specify a hello interval from 1 through 255 seconds. The default hello interval is normally 10 seconds. For nonbroadcast networks, the default hello interval is 120 seconds.

To specify how often the router sends hello packets out the peer interface, configure the hello-interval statement:

```
hello-interval seconds;
```

You can configure this statement at the following hierarchy levels:

- [edit logical-systems *logical-system-name* protocols ospf area *area-number* peer-interface *peer-interface-name*]
- [edit protocols ospf area *area-number* peer-interface *peer-interface-name*]

Configuring MPLS Paths for GMPLS

As part of the configuration for GMPLS, you need to establish a Multiprotocol Label Switching (MPLS) path for each unique device connected through GMPLS. Configure the traffic engineering link remote address as the address at the [edit protocols mpls path *path-name*] hierarchy level. Constrained Shortest Path First (CSPF) is supported so you can choose either the strict or loose option with the address.

See “Configuring LMP” on page 443 for information about how to obtain a traffic engineering link remote address.

To configure the MPLS path, include the path statement at the [edit protocols mpls] hierarchy level:

```
[edit protocols mpls]
path path-name {
   next-hop-address (strict | loose);
}
```

For information about how to configure MPLS paths, see “Creating a Named Path” on page 58.

Tracing LMP Traffic

To trace LMP protocol traffic, include the traceoptions statement at the [edit protocols link-management] hierarchy level:

```
[edit protocols link-management]
```

```
traceoptions {
   file filename <files number> <no-stamp> <replace> <size size> <world-readable |
      no-world-readable>;
   flag flag <flag-modifier> <disable>;
}
```

Use the file statement to specify the name of the file that receives the output of the tracing operation. All files are placed in the directory /var/log.

The following trace flags display the operations associated with the sending and receiving of various LMP messages:

- all—Trace all available operations
- hello-packets—Trace hello packets on any LMP control channel
- init—Output from the initialization messages
- packets—Trace all packets other than hello packets on any LMP control channel
- parse—Operation of the parser
- process—Operation of the general configuration
- route-socket—Operation of route socket events
- routing—Operation of the routing protocols
- server—Server processing operations
- show—Servicing operations for show commands
- state—Trace state transitions of the LMP control channels and traffic engineering links

Each flag can carry one or more of the following flag modifiers:

- detail—Provide detailed trace information
- receive—Packets being received
- send—Packets being transmitted

Configuring MPLS LSPs for GMPLS

To enable the proper GMPLS switching parameters, configure the label-switched path (LSP) attributes that are appropriate for your network connection. The default value for switching-type is psc-1, which is also appropriate for standard MPLS.

To configure the LSP attributes, include the lsp-attributes statement at the [edit protocols mpls label-switched-path *lsp-name*] hierarchy level:

```
[edit protocols mpls label-switched-path lsp-name]
lsp-attributes {
   encoding-type type;
   gpid gpid;
   signal-bandwidth type;
   switching-type type;
```

```
}
```

If you include the no-cspf statement in the label-switched path configuration, you must also configure primary and secondary paths, or the configuration cannot be committed.

The following sections describe how to configure each of the LSP attributes for a GMPLS LSP:

- Configuring the Encoding Type on page 454
- Configuring the GPID on page 454
- Configuring the Signal Bandwidth Type on page 455
- Configuring GMPLS Bidirectional LSPs on page 455
- Allowing Non-Packet GMPLS LSPs to Establish Paths Through a JUNOS-based Router on page 455

Configuring the Encoding Type

You need to specify the encoding type of the payload carried by the LSP. It can be any of the following:

- ethernet—Ethernet
- packet—Packet
- pdh—Plesiochronous digital hierarchy (PDH)
- sonet-sdh—SONET/SDH

The default value is packet.

To configure the encoding type, include the encoding-type statement at the [edit protocols mpls label-switched-path *lsp-name* lsp-attributes] hierarchy level:

```
[edit protocols mpls label-switched-path lsp-name lsp-attributes]
encoding-type type;
```

Configuring the GPID

You need to specify the type of payload carried by the LSP. The payload is the type of packet underneath the MPLS label. The payload is specified by the generalized payload identifier (GPID).

You can specify the GPID with any of the following values:

- hdlc—High-Level Data Link Control (HDLC)
- ethernet—Ethernet
- ipv4—Internet Protocol version 4 (default)
- pos-scrambling-crc-16—For interoperability with other vendors' equipment
- pos-no-scrambling-crc-16—For interoperability with other vendors' equipment

- pos-scrambling-crc-32—For interoperability with other vendors' equipment
- pos-no-scrambling-crc-32—For interoperability with other vendors' equipment
- ppp—Point-to-Point Protocol (PPP)

To configure the GPID, include the gpid statement at the [edit protocols mpls label-switched-path *lsp-name* lsp-attributes] hierarchy level:

```
[edit protocols mpls label-switched-path lsp-name lsp-attributes]
gpid gpid;
```

Configuring the Signal Bandwidth Type

The signal bandwidth type is the encoding used for path computation and admission control. To configure the signal bandwidth type, include the signal-bandwidth statement at the [edit protocols mpls label-switched-path *lsp-name* lsp-attributes] hierarchy level:

```
[edit protocols mpls label-switched-path lsp-name lsp-attributes]
signal-bandwidth type;
```

Configuring GMPLS Bidirectional LSPs

Because MPLS and GMPLS use the same configuration hierarchy for LSPs, it is helpful to know which LSP attributes control LSP functionality. Standard MPLS packet-switched LSPs are unidirectional, whereas GMPLS nonpacket LSPs are bidirectional.

If you use the default packet-switching type of psc-1, your LSP becomes unidirectional. To enable a GMPLS bidirectional LSP, you must select a non-packet-switching type option, such as lambda, fiber, or ethernet. Include the switching-type statement at the [edit protocols mpls label-switched-path *lsp-name* lsp-attributes] hierarchy level:

```
[edit protocols mpls label-switched-path lsp-name lsp-attributes]
switching-type (lambda | fiber | ethernet);
```

Allowing Non-Packet GMPLS LSPs to Establish Paths Through a JUNOS-based Router

You can allow non-packet GMPLS LSPs to establish paths through JUNOS-based routers by setting the A-bit in the Admin Status object. When an ingress router sends an RSVP PATH message with the Admin Status A-bit set, an external device (not a JUNOS software-based router) can either perform a Layer 1 path setup test or help bring up an optical cross-connect.

When set, the A-bit in the Admin Status object indicates the administrative down status for an LSP. This feature is used specifically by non-packet GMPLS LSPs. It does not affect control path setup or data forwarding for packet LSPs.

The JUNOS software does not distinguish between the control path setup and data path setup. Other nodes along the network path use RSVP PATH signaling using the A-bit in a meaningful way.

To configure the Admin Status object for a GMPLS LSP, include the admin-down statement:

```
admin-down;
```

You can include this statement at the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name*]
- [edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]

Gracefully Tearing Down GMPLS LSPs

You can gracefully tear down nonpacket GMPLS LSPs. An LSP that is torn down abruptly, a common process in a packet-switched network, can cause stability problems in non-packet-switched networks. To maintain the stability of non-packet-switched networks, it might be necessary to tear down LSPs gracefully.

The following sections describe how to tear down GMPLS LSPs gracefully:

- Temporarily Deleting a GMPLS LSP on page 456
- Permanently Deleting a GMPLS LSP on page 456
- Configuring the Graceful Deletion Timeout Interval on page 457

Temporarily Deleting a GMPLS LSP

You can gracefully tear down a GMPLS LSP using the clear rsvp session gracefully command.

This command gracefully tears down an RSVP session for a nonpacket LSP in two passes. In the first pass, the Admin_Status object is signaled along the path to the endpoint of the LSP. During the second pass, the LSP is taken down. Using this command, the LSP is taken down temporarily. After the appropriate interval, the GMPLS LSP is resignaled and then reestablished.

The clear rsvp session gracefully command has the following properties:

- It only works on the ingress and egress routers of the RSVP session. If used on a transit router, it has the same behavior as the clear rsvp session command.
- It only works for nonpacket LSPs. If used with packet LSPs, it has the same behavior as the clear rsvp session command.

For more information, see the *JUNOS Routing Protocols and Policies Command Reference*.

Permanently Deleting a GMPLS LSP

When you disable an LSP in the configuration, the LSP is permanently deleted. By configuring the disable statement, you can disable a GMPLS LSP permanently. If the LSP being disabled is a nonpacket LSP, then the graceful LSP tear-down procedures

that use the Admin_Status object are used. If the LSP being disabled is a packet LSP, then the regular signaling procedures for LSP deletion are used.

To disable a GMPLS LSP, include the disable statement at any of the following hierarchy levels:

- [edit protocols mpls label-switched-path *lsp-name*]—Disables the LSP.
- [edit protocols link-management te-link *te-link-name*]—Disables a traffic engineering link.
- [edit protocols link-management te-link *te-link-name* interface *interface-name*]—Disables an interface used by a traffic engineering link.

Configuring the Graceful Deletion Timeout Interval

The router that initiates the graceful deletion procedure for an RSVP session waits for the graceful deletion timeout interval to ensure that all routers along the path (especially the ingress and egress routers) have prepared for the LSP to be taken down.

The ingress router initiates the graceful deletion procedure by sending the Admin_Status object in the Path message with the D bit set. The ingress router expects to receive an Resv message with the D bit set from the egress router. If the ingress router does not receive this message within the time specified by the graceful deletion timeout interval, it initiates a forced tear-down of the LSP by sending a PathTear message.

To configure the graceful deletion timeout interval, include the graceful-deletion-timeout statement at the [edit protocols rsvp] hierarchy level. You can configure a time from between 1 through 300 seconds. The default value is 30 seconds.

```
graceful-deletion-timeout seconds;
```

You can configure this statement at the following hierarchy levels:

- [edit protocols rsvp]
- [edit logical-systems *logical-system-name* protocols rsvp]

You can use the show rsvp version command to determine the current value configured for the graceful deletion timeout.

Chapter 22

RSVP LSP Hierarchy Configuration Guidelines

This chapter provides an overview and describes how to configure the Resource Reservation Protocol (RSVP) label-switched path (LSP) hierarchy. The RSVP LSP hierarchy allows you to tunnel multiple RSVP LSPs over a single RSVP LSP.

The RSVP LSP hierarchy is described in the following sections:

- RSVP LSP Hierarchy Standard on page 459
- RSVP LSP Hierarchy Terminology on page 459
- RSVP LSP Hierarchy Overview on page 460
- Configuring the RSVP LSP Hierarchy on page 460

RSVP LSP Hierarchy Standard

For more information on how the RSVP LSP hierarchy functions, see RFC 4206, *Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)*.

RSVP LSP Hierarchy Terminology

The following terminology is used to describe functionality related to the RSVP LSP hierarchy:

- Forwarding adjacency LSP—An RSVP LSP used to tunnel other RSVP LSPs; forms the basis for a forwarding adjacency.
- Forwarding adjacency—A traffic engineering link created by a forwarding adjacency LSP. You can create a forwarding adjacency between two routers in a network by configuring a forwarding adjacency LSP. Forwarding adjacencies can only be statically configured. However, you can configure Open Shortest Path First (OSPF) to advertise the forwarding adjacency to other routers. When an RSVP LSP traverses a forwarding adjacency, existing Multiprotocol Label Switching (MPLS) features such as fast reroute continue to function.

RSVP LSP Hierarchy Overview

The following sections provide an overview of how the RSVP LSP hierarchy function:

- RSVP LSP Hierarchy on page 460
- Advertising the Forwarding Adjacency with OSPF on page 460

RSVP LSP Hierarchy

Forwarding adjacencies are configured and managed as point-to-point traffic engineering links using statements configured at the [protocols link-management] hierarchy level. For the forwarding adjacency to function properly, you also need to make RSVP aware of the forwarding adjacency by configuring the corresponding peer interface at the [edit protocols rsvp] hierarchy level.

Although forwarding adjacency LSPs are configured and managed as traffic engineering links on the local router, it is not necessary to advertise these traffic engineering links to other routers in the network. However, if you want to automatically forward MPLS traffic over the forwarding adjacency or want other routers to compute paths over the forwarding adjacency, you must configure OSPF to advertise the forwarding adjacency to the other routers in the network and add the forwarding adjacency to the traffic engineering database (TED). OSPF is the only supported interior gateway protocol (IGP).

Advertising the Forwarding Adjacency with OSPF

Once a forwarding adjacency LSP and the corresponding traffic engineering link you have configured, you can configure OSPF to advertise the forwarding adjacency. Unlike regular traffic engineering links, OSPF hellos are not exchanged between the forwarding adjacency LSP endpoints and therefore no routing adjacency is created between the forwarding adjacency endpoints. If you issue a show ospf neighbor command on an ingress forwarding adjacency, the command displays the egress router of the forwarding adjacency LSP as a neighbor. However, no real OSPF adjacency is established (no OSPF hellos are exchanged) between the ingress and egress routers. For display purposes only, OSPF creates a pseudo neighbor corresponding to the peer.

You can configure forwarding adjacencies over existing MPLS networks. A forwarding adjacency LSP is signaled as a regular MPLS LSP without generalized MPLS (GMPLS) extensions. When the forwarding adjacency LSP is advertised as a traffic engineering link in OSPF, the corresponding traffic engineering link in OSPF is also advertised as a regular MPLS traffic engineering link without GMPLS extensions.

Configuring the RSVP LSP Hierarchy

The following sections describe how to configure the RSVP LSP hierarchy:

- Configuring an RSVP LSP on page 461
- Configuring a Forwarding Adjacency on page 461

- Configuring RSVP for a Forwarding Adjacency on page 462
- Advertising a Forwarding Adjacency Using OSPF on page 463

Configuring an RSVP LSP

To configure a standard RSVP LSP on the ingress router to be used as the forwarding adjacency LSP, see "Configuring an LSP" on page 62. This LSP requires no special configuration to function as a forwarding adjacency LSP.

Configuring a Forwarding Adjacency

A forwarding adjacency is a type of GMPLS traffic engineering link. It requires that you configure local and remote addresses to identify the link. A forwarding adjacency is associated with a specific peer router. You could configure multiple forwarding adjacencies to the same peer router.

To configure a forwarding adjacency, you need to configure the te-link statement at the [edit protocols link-management] hierarchy level:

```
[edit protocols link-management]
te-link te-link-name {
    label-switched-path lsp-name;
    local-address ip-address;
    remote-address ip-address;
}
```

For more information on how to configure GMPLS traffic engineering links, see "Configuring LMP Traffic Engineering Links" on page 444.

NOTE: Do not configure the control channel for a forwarding adjacency peer router. Configuring a control channel causes the commit to fail.

The following sections describe how to configure the te-link statement for a forwarding adjacency:

- Configuring the Local IP Address for the Forwarding Adjacency on page 461
- Configuring the Remote IP Address for the Forwarding Adjacency on page 462
- Configuring the LSP for the Forwarding Adjacency on page 462

Configuring the Local IP Address for the Forwarding Adjacency

To configure the local IP address for the forwarding adjacency, include the local-address statement:

```
local-address ip-address;
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Configuring the Remote IP Address for the Forwarding Adjacency

The address of the peer router is the node ID for the forwarding adjacency LSP egress node. You configure this node ID for the forwarding adjacency using the remote-address statement:

```
remote-address ip-address;
```

You can include this statement at the following hierarchy levels:

- [edit protocols link-management te-link *te-link-name*],
- [edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name*]

Configuring the LSP for the Forwarding Adjacency

To configure a router to function as a forwarding adjacency, specify the LSP configured in "Configuring an RSVP LSP" on page 461 using the label-switched-path statement at the [edit protocols link-management te-link *te-link-name*] hierarchy level:

```
label-switched-path label-switched-path-name;
```

You can specify this statement at the following hierarchy levels:

- [edit protocols link-management te-link *te-link-name*]
- [edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name*]

Configuring RSVP for a Forwarding Adjacency

For the forwarding adjacency to function properly, RSVP must be made aware of it. Do this by specifying the name of the peer interface corresponding to the link-management peer associated with the forwarding adjacency. Configuring the peer-interface statement at the [edit protocols rsvp] hierarchy level allows RSVP to use all of the traffic engineering links configured for that peer. You can also configure RSVP control-plane parameters such as the hello interval and refresh reduction.

To configure RSVP to recognize a forwarding adjacency, include the peer-interface statement:

```
peer-interface peer-interface-name {
    disable;
    (aggregate | no-aggregate);
    authentication-key key;
    hello-interval seconds;
    (reliable | no-reliable);
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols rsvp]
- [edit logical-systems *logical-system-name* protocols rsvp]

For more information on how to configure the peer-interface statement, see "Configuring Peer Interfaces in RSVP and OSPF" on page 451.

Advertising a Forwarding Adjacency Using OSPF

You can allow other routers to dynamically signal paths over a forwarding adjacency LSP by configuring OSPF. This configuration is optional.

If you configure OSPF to advertise a forwarding adjacency LSP, the LSP is added to the traffic engineering database on each router in the traffic engineering domain. Because the forwarding adjacency LSP is unidirectional, the corresponding traffic engineering link (forwarding adjacency) is also unidirectional. The forwarding adjacency LSP appears as a standard traffic engineering database half-link to all routers in the traffic engineering domain.

CSPF performs a bidirectional link check to ensure that traffic can flow in both directions. CSPF checks for a reverse link, either the exact reverse forwarding adjacency or another reverse link. If there is no reverse link from the forwarding adjacency LSP egress router to the forwarding adjacency LSP ingress router, the CSPF check fails.

CSPF might find another parallel reverse link. However, the LSP cannot function properly over the forwarding adjacency unless you have explicitly configured a corresponding forwarding adjacency LSP to handle the traffic flowing in the opposite direction on the forwarding adjacency LSP egress router.

To advertise the traffic engineering properties of a forwarding adjacency to a specific peer router, include the peer-interface statement:

```
peer-interface peer-interface-name {
    dead-interval seconds;
    disable;
    hello-interval seconds;
    retransmit-interval seconds;
    transit-delay seconds;
}
```

You can configure this statement at the following hierarchy levels:

- [edit logical-systems *logical-system-name* protocols ospf area *area-name*]
- [edit protocols ospf area *area-name*]

For more information on how to configure the peer-interface statement, see "Configuring Peer Interfaces in RSVP and OSPF" on page 451.

Chapter 23

Summary of GMPLS Configuration Statements

This chapter provides a reference for each Generalized Multiprotocol Label Switching (GMPLS) configuration statement. The statements are organized alphabetically.

address

Syntax address *ip-address*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management peer *peer-name*], [edit protocols link-management peer *peer-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the ID of the peer.

Default The loopback address is advertised.

Options *ip-address*—IP address of the peer.

Usage Guidelines See "Configuring the LMP Peer ID" on page 447.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

admin-down

See admin-down

control-channel

Syntax control-channel *control-channel-interface*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management peer *peer-name*], [edit protocols link-management peer *peer-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the control channel interface for the peer.

Options *control-channel-interface*—Name of the control channel interface.

Usage Guidelines See "Configuring LMP Peers" on page 446.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

dead-interval

Syntax dead-interval *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-number* peer-interface *peer-interface-name*],
[edit protocols ospf area *area-number* peer-interface *peer-interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify how long Open Shortest Path First (OSPF) and OSPF version 3 (OSPFv3) wait before declaring that a neighboring router is unavailable. This is an interval during which the router receives no hello packets from the neighbor.

Options *seconds*—Interval to wait.
Range: 1 through 65,535
Default: 40 seconds (four times the hello interval)

Usage Guidelines See "Configuring Peer Interfaces in RSVP and OSPF" on page 451.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics hello-interval

disable

See the following sections:

- disable (for GMPLS) on page 467
- disable (for OSPF) on page 467

disable (for GMPLS)

Syntax disable;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name*],
[edit protocols link-management te-link *te-link-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Disable a traffic engineering link.

Default The configured object is enabled (operational) unless explicitly disabled.

Usage Guidelines See "Disabling the Traffic Engineering Link for the LMP Peer" on page 450.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

disable (for OSPF)

Syntax disable;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-number* peer-interface *peer-interface-name*],
[edit protocols ospf area *area-number* peer-interface *peer-interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Disable an OSPF peer interface.

Default The configured object is enabled (operational) unless explicitly disabled.

Usage Guidelines See "Configuring Peer Interfaces in RSVP and OSPF" on page 451.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

hello-dead-interval

Syntax hello-dead-interval *milliseconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management peer *peer-name* lmp-protocol],
[edit protocols link-management peer *peer-name* lmp-protocol]

Release Information Statement introduced in JUNOS Release 8.0.

Description Specify how long the Link Management Protocol (LMP) waits before declaring the control channel to be dead. This is an interval during which the router receives no LMP hello packets from the neighbor on a control that is active or up.

Options *seconds*—Interval to wait before declaring the control channel to be dead.
Range: 500 through 300,000
Default: 500 milliseconds (three times the hello interval)

Usage Guidelines See "Configuring the Hello Message Attributes for the LMP Control Channel" on page 448.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics hello-interval

hello-interval

See the following sections:

- hello-interval (for LMP) on page 469
- hello-interval (for OSPF) on page 470

hello-interval (for LMP)

Syntax hello-interval *milliseconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management peer *peer-name* lmp-protocol],
[edit protocols link-management peer *peer-name* lmp-protocol]

Release Information Statement introduced in JUNOS Release 8.1.

Description Specify how often the router sends Link Management Protocol (LMP) hello packets.

Options *seconds*—Length of time between hello packets.
Range: 150 through 300,000
Default: 150 milliseconds

Usage Guidelines See "Configuring the Hello Message Attributes for the LMP Control Channel" on page 448.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics hello-dead-interval

hello-interval (for OSPF)

Syntax hello-interval *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-number* peer-interface *peer-interface-name*],
[edit protocols ospf area *area-number* peer-interface *peer-interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify how often the router sends hello packets out the peer interface. The hello interval must be the same for all routers on a shared logical IP network.

Options *seconds*—Length of time between hello packets.
Range: 1 through 255
Default: 10 seconds; 120 seconds (nonbroadcast networks)

Usage Guidelines See "Configuring Peer Interfaces in RSVP and OSPF" on page 451.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics dead-interval.

interface

Syntax interface *interface-name*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name*],
[edit protocols link-management te-link *te-link-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the egress router interface.

Options *interface-name*—Name of the interface to the egress router.

Usage Guidelines See "Configuring LMP" on page 443.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

label-switched-path

Syntax label-switched-path *lsp-name*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name*], [edit protocols link-management te-link *te-link-name*]

Release Information Statement introduced in JUNOS Release 7.4.

Description Specify the LSP to be used by the forwarding adjacency.

Options *lsp-name*—Name of the LSP.

Usage Guidelines See "Configuring a Forwarding Adjacency" on page 461.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

link-management

Syntax link-management { ... }

Hierarchy Level [edit logical-systems *logical-system-name* protocols], [edit protocols]

Release Information Statement introduced before JUNOS Release 7.4.

Description Enable Link Management Protocol (LMP) on the router.

Usage Guidelines See "Configuring LMP" on page 443.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

lmp-control-channel

Syntax
```
lmp-control-channel control-channel-interface {
    remote-address ip-address;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management peer *peer-name*], [edit protocols link-management peer *peer-name*]

Release Information Statement introduced in JUNOS Release 8.1.

Description Specify the Link Management Protocol (LMP) control channel interface for the peer.

Options *control-channel-interface*—Name of the control channel interface.

The remaining statement is described separately in this chapter.

Usage Guidelines See "Configuring the LMP Control Channel Interface for the Peer" on page 447.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

lmp-protocol

Syntax
```
lmp-protocol {
    hello-interval milliseconds;
    hello-dead-interval milliseconds;
    retransmission-interval milliseconds;
    retry-limit number;
    passive;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management peer *peer-name*], [edit protocols link-management peer *peer-name*]

Release Information Statement introduced in JUNOS Release 8.1.

Description Configure attributes of Link Management Protocol (LMP) to establish and maintain the LMP control channel for the peer.

Options The statements are described separately in this chapter.

Usage Guidelines See "Configuring LMP Peers" on page 446.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

local-address

Syntax local-address *ip-address*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name*],
[edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name* interface *interface-name*],
[edit protocols link-management te-link *te-link-name*],
[edit protocols link-management te-link *te-link-name* interface *interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the local IP address associated with the traffic engineering link.

Options *local-address*—Local IP address of the traffic engineering link.

Usage Guidelines See "Configuring the Local IP Address for the Traffic Engineering Link" on page 445 and "Configuring the Local IP Address for the Forwarding Adjacency" on page 461.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

passive

Syntax passive;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management peer *peer-name* lmp-protocol],
[edit protocols link-management peer *peer-name* lmp-protocol]

Release Information Statement introduced in JUNOS Release 8.1.

Description Specify the router to not configure the Link Management Protocol (LMP) control channels, but to wait for the remote peer to configure the LMP control channels.

Usage Guidelines See "Configuring the Local Peer to Wait for the Remote Peer" on page 450.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

peer

Syntax

```
peer peer-name {
    address ip-address;
    control-channel control-channel-interface;
    lmp-control-channel control-channel-interface;
    lmp-protocol {
        hello-interval milliseconds;
        hello-dead-interval milliseconds;
        retransmission-interval milliseconds;
        retry-limit number;
        passive;
    }
    te-link te-link-name;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management],
[edit protocols link-management]

Release Information Statement introduced before JUNOS 7.4. For JUNOS 8.1, the lmp-protocol statement and sub-statements were added.

Description Configure a network peer.

Options *peer-name*—Name of the network peer.

The remaining statements are described separately in this chapter.

Usage Guidelines See “Configuring LMP Peers” on page 446.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

peer-interface

See the following sections:

- peer-interface (for OSPF) on page 475
- peer-interface (for RSVP) on page 475

peer-interface (for OSPF)

Syntax

```
peer-interface peer-interface-name {
    dead-interval seconds;
    disable;
    hello-interval seconds;
    retransmit-interval seconds;
    transit-delay seconds;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-id*],
[edit protocols ospf area *area-id*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Configure the control channel. The peer interface name is the same as the peer interface name configured under LMP.

Usage Guidelines See "Configuring Peer Interfaces in RSVP and OSPF" on page 451 and "Advertising a Forwarding Adjacency Using OSPF" on page 463.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics *JUNOS Routing Protocols Configuration Guide*

peer-interface (for RSVP)

See peer-interface in "Summary of RSVP Configuration Statements" on page 297.

remote-address

See the following sections:

- remote-address (for LMP Control Channel) on page 476
- remote-address (for LMP Traffic Engineering) on page 476

remote-address (for LMP Control Channel)

Syntax remote-address *ip-address*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management peer *peer-name* lmp-control-channel *control-channel-interface*],
[edit protocols link-management peer *peer-name* lmp-control-channel *control-channel-interface*]

Release Information Statement introduced in JUNOS Release 8.1.

Description Specify the remote IP address for the Link Management Protocol (LMP) control channel interface.

Options *ip-address*—Remote IP address mapped to the LMP control channel interface.

Usage Guidelines See "Configuring the Remote IP Address for the LMP Control Channel" on page 448.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

remote-address (for LMP Traffic Engineering)

Syntax remote-address *ip-address*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name*],
[edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name* interface *interface-name*],
[edit protocols link-management te-link *te-link-name*],
[edit protocols link-management te-link *te-link-name* interface *interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the remote IP address for the traffic engineering link.

Options *ip-address*—Remote IP address mapped to the traffic engineering link.

Usage Guidelines See "Configuring the Remote IP Address for the Traffic Engineering Link" on page 445 and "Configuring the Remote IP Address for the Forwarding Adjacency" on page 462.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

remote-id

Syntax remote-id *id-number*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name*],
[edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name* interface *interface-name*],
[edit protocols link-management te-link *te-link-name*],
[edit protocols link-management te-link *te-link-name* interface *interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify the ID assigned to a traffic engineering link or an interface (resource) on the peer node.

Options *id-number*—ID number for the remote device.

Usage Guidelines See "Configuring the Remote ID for the Traffic Engineering Link" on page 445.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

retransmission-interval

Syntax retransmission-interval *milliseconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management peer *peer-name* lmp-protocol],
[edit protocols link-management peer *peer-name* lmp-protocol]

Release Information Statement introduced in JUNOS Release 8.1.

Description Specify how often Link Management Protocol (LMP) sends Config and LinkSummary messages on the LMP control channel.

Options *milliseconds*—Length of time between Config messages.
Range: 500 through 300,000
Default: 500 milliseconds

Usage Guidelines See "Configuring Message Attributes for the LMP Control Channel" on page 449.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics retry-limit.

retransmit-interval

Syntax retransmit-interval *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-number* peer-interface *peer-interface-name*],
[edit protocols ospf area *area-number* peer-interface *peer-interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Specify how long the router waits to receive a link-state acknowledgment packet before retransmitting link-state advertisements to a peer interface's neighbors.

Options *seconds*—Interval to wait for a link-state acknowledgment packet.
Range: 1 through 65,535
Default: 5 seconds

Usage Guidelines See "Configuring Peer Interfaces in RSVP and OSPF" on page 451.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

retry-limit

Syntax retry-limit *number*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management peer *peer-name* lmp-protocol],
[edit protocols link-management peer *peer-name* lmp-protocol]

Release Information Statement introduced in JUNOS Release 8.1.

Description Specify how many times the Link Management Protocol (LMP) sends Config and LinkSummary messages on the LMP control channel without receiving an appropriate acknowledgment before it logs a message and restarts the LMP control channel configuration process.

Options *number*—Maximum number of times messages are sent without receiving an acknowledgment.
Range: 3 through 1000
Default: 3

Usage Guidelines See "Configuring Message Attributes for the LMP Control Channel" on page 449.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics retransmission-interval.

te-link

Syntax

```
te-link te-link-name {
    disable;
    interface interface-name {
        disable;
        local-address ip-address;
        remote-address ip-address;
        remote-id id-number;
    }
    local-address ip-address;
    remote-address ip-address;
    remote-id id-number;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management],
[edit logical-systems *logical-system-name* protocols link-management peer *peer-name*],
[edit protocols link-management],
[edit protocols link-management peer *peer-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Represent a collection of physical ports or time slots. Assign a traffic engineering link to the specified network peer.

Options *te-link-name*—Name of the collection of physical ports or the name of the time slots.

disable—Disable the traffic engineering link or an interface to a traffic engineering link.

The other statements are described separately in this chapter.

Usage Guidelines See "Configuring LMP Traffic Engineering Links" on page 444.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

traceoptions

Syntax

```
traceoptions {
   file filename <files number> <no-stamp> <replace> <size size> <world-readable |
      no-world-readable>;
   flag flag <flag-modifier> <disable>;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management],
[edit protocols link-management]

Release Information Statement introduced before JUNOS Release 7.4. For JUNOS 8.1, the hello-packets, packets, and state flags were added.

Description Trace options for the LMP protocol.

Options disable—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as all.

filename—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log.

files *number*—(Optional) Maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed *trace-file*.0, then *trace-file*.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.
Range: 2 through 1000
Default: 2 files

If you specify a maximum number of files, you must also include the size statement to specify the maximum file size.

flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.

- all—Trace all available operations
- hello-packets—Trace hello packets on any LMP control channel
- init—Output from the initialization messages
- packets—Trace all packets other than hello packets on any LMP control channel
- parse—Operation of the parser
- process—Operation of the general configuration
- route-socket—Operation of route socket events
- routing—Operation of the routing protocols
- server—Server processing operations
- show—show command servicing operations

- state—Trace state transitions of the LMP control channels and traffic engineering links

flag-modifier—(Optional) Modifier for the tracing flag. You can specify one or more of these modifiers:

- detail—Provide detailed trace information
- receive—Packets being received
- send—Packets being transmitted

no-stamp—(Optional) Do not place timestamp information at the beginning of each line in the trace file.
Default: If you omit this option, timestamp information is placed at the beginning of each line of tracing output.

no-world-readable—(Optional) Prevents all users from reading the log file.

replace—(Optional) Replace an existing trace file if there is one.
Default: If you do not include this option, tracing output is appended to an existing trace file.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file*.0. When the *trace-file* again reaches this size, *trace-file*.0 is renamed *trace-file*.1 and *trace-file* is renamed *trace-file*.0. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.
Syntax: *x*k to specify KB, *x*m to specify MB, or *x*g to specify GB
Range: 10 KB through the maximum file size supported on your system
Default: 1 MB

If you specify a maximum file size, you must also include the files statement to specify the maximum number of files.

world-readable—(Optional) Enables log file access for all users.

Usage Guidelines See "Tracing LMP Traffic" on page 452 and the *JUNOS Network Management Configuration Guide*.

Required Privilege Level routing and trace—To view this statement in the configuration.
routing-control and trace-control—To add this statement to the configuration.

transit-delay

Syntax transit-delay *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-number* peer-interface *peer-interface-name*],
[edit protocols ospf area *area-number* peer-interface *peer-interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Set the estimated time required to transmit a link-state update on the peer interface. When calculating this time, you should account for transmission and propagation delays.

Options *seconds*—Estimated time.
Range: 1 through 65,535
Default: 1 second

Usage Guidelines See "Configuring Peer Interfaces in RSVP and OSPF" on page 451.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Part 7
Indexes

- Index on page 485
- Index of Statements and Commands on page 501

Index

Symbols

#, comments in configuration statements.....xxxv
( ), in syntax descriptions.....xxxv
< >, in syntax descriptions.....xxxv
[ ], in configuration statements.....xxxv
{ }, in configuration statements.....xxxv
| (pipe), in syntax descriptions.....xxxv

A

adaptive rerouting.....94, 175
adaptive statement.....175
    usage guidelines.....94
address (tracing flag).....386
address statement
    LMP.....465
        usage guidelines.....447
addresses
    associating with LSPs.....73, 204
    egress router address.....66, 246
    ingress router.....68, 198
adjust-interval statement.....176
    usage guidelines.....83
adjust-threshold statement.....176
    usage guidelines.....84
adjust-threshold-overflow-limit statement.....177
    usage guidelines.....85
Admin Status object, GMPLS.....455
admin-down statement.....177
    configuration guidelines.....455
admin-group statement
    bypass LSPs.....297
    configuration
        bypass LSPs.....281
    LSPs.....179
    MPLS interfaces.....178
admin-groups statement.....180
    usage guidelines.....89
administrative groups
    admin-groups statement.....180
    configuration.....89
    exclude statement.....194
    fast reroute.....72
    include-all statement.....201
    include-any statement.....203
advertisement messages, LDP.....334
advertisement-hold-time statement.....180
    usage guidelines.....100
aggregate statement
    RSVP.....298
        usage guidelines.....274
aggregated Ethernet interfaces.....401
aggregated interfaces.....37
aggregation, RSVP.....298
all (tracing flag).....247
    LMP.....480
    RSVP.....323
allocation of labels.....25
allow-fragmentation statement.....181
    usage guidelines.....290
allow-subnet-mismatch statement.....365
    usage guidelines.....363
ARP configuration.....415
associate-backup-pe-groups statement.....181
    usage guidelines.....149
ATM
    circuits.....398, 407
ATM encapsulation
    Layer 2 TCC.....412
authentication
    RSVP.....276, 299
authentication-key statement
    LDP.....366
        usage guidelines.....361
    RSVP.....299
        usage guidelines.....276
auto-bandwidth statement.....182
    usage guidelines.....82
auto-policing statement.....183
    usage guidelines.....164
automatic bandwidth allocation.....47, 182
    bandwidth monitoring.....86
    LSPs.....81
    manually trigger.....87
    threshold.....84
automatic policers, LSPs.....164

B

backup paths....32
backup-pe-group statement....184
bandwidth
  LSP paths....98
  RSVP reservations....322
bandwidth model....119
bandwidth oversubscription
  overview....122
bandwidth statement
  fast reroute....185
    usage guidelines....72
  link protection....300
    usage guidelines....282
  LSPs
    usage guidelines....129
  multiclass LSPs....185
    usage guidelines....132
  RSVP....300
  signaled LSPs....185
    usage guidelines....98
bandwidth update threshold....277
bandwidth-model statement....186
  usage guidelines....119
bandwidth-percent statement....187
  usage guidelines....130, 133
BFD
  ECMP paths....351
  fast reroute....170
  LDP LSPs....350
  revert timer....233
  RSVP LSPs....169
bfd-liveness-detection statement
  LDP LSPs....367
    usage guidelines....350
  RSVP LSPs....188
    usage guidelines....169
BGP
  destinations....38
binding (tracing flag)....386
braces, in configuration statements....xxxv
brackets
  angle, in syntax descriptions....xxxv
  square, in configuration statements....xxxv
branch LSPs....144
bypass LSPs....280
  administrative groups....281
  bandwidth....282
  bandwidth subscription....285
  class-of-service....282
  CSPF, disabling....284
  explicit paths....285
  hop limit....283
  maximum number....283
  multiple....264
  node protection, disabling....284
  optimization interval....284
  priority and preemption....286
  types....265
bypass statement....301
  usage guidelines....280

C

CCC
  aggregated Ethernet....401
  BPDUs, nonstandard....411
  encapsulation
    Ethernet CCC....399
  example configurations....403, 408, 410
  graceful restart
    configuration....417
    overview....394
  Layer 2 switching cross-connects
    configuration....397
    overview....393
  LSP stitching cross-connects....393, 409
  MPLS tunneling
    cross-connects....393, 405, 408, 433
  overview....393
  ping CCC LSPs....171
  point-to-multipoint LSPs....417, 431, 432
  traffic policing....397
Cisco HDLC circuits....398
Cisco HDLC encapsulation
  Layer 2 switching cross-connect....411
class types
  bandwidth subscription....126
class-of-service statement
  bypass LSPs....302
    usage guidelines....282
  ingress routers....189
    usage guidelines....135
  signaled LSPs....189
    usage guidelines....92
  static LSPs....189
    usage guidelines....139
colored links....72, 89, 180
comments, in configuration statements....xxxv
connection (tracing flag)....247
connection-detail (tracing flag)....247
connections statement....422
  complete hierarchy under....10
  TCC
    usage guidelines....415
Constrained Shortest Path First algorithm *See* CSPF algorithm

constrained-path LSPs
computation
CSPF algorithm....29
disabling....88, 216
overview....29
example configurations....103
overview....28
scope....29
control-channel statement....466
usage guidelines....447
conventions
text and syntax....xxxiv
CoS....119
CoS requests....253
CoS values....91
cross-connect, circuit *See* CCC
cspf (tracing flag)....247
CSPF algorithm
fate-sharing....61
offline path computation....6, 31
online path computation....29
disabling....88, 216
overview....5
cspf-link (tracing flag)....247
cspf-node (tracing flag)....247
curly braces, in configuration statements....xxxv
customer support....xliii
contacting JTAC....xliii

D

damping
LSP transitions....100
dead-interval statement....466
usage guidelines....451
deaggregate statement....368
usage guidelines....348
default route
MPLS....101
default-route statement....190
usage guidelines....101
description statement
MPLS....190
usage guidelines....71
detail (tracing flag modifier)
LDP....387
LMP....481
RSVP....324
detours *See* fast reroute
Differentiated Services
bandwidth model....119
extended MAM....119
LSPs....116
MAM....119
RDM....119
diffserv-te statement....191
usage guidelines....118
disable (tracing flag modifier)....387
disable option to traceoptions statement
LDP....386
LMP....480
RSVP....323
disable statement
GMPLS....467
usage guidelines....450
LDP....369
usage guidelines....339
link protection....303
usage guidelines....278
MPLS....192
usage guidelines....88
OSPF....467
usage guidelines....451
RSVP....303
usage guidelines....271
RSVP graceful restart....303
usage guidelines....286
discard statement
MPLS....192
usage guidelines....139
discovery messages, LDP....333
distinct reservations....259
documentation set
comments on....xliii
double-push statement....193
usage guidelines....135
DSCP
MPLS-tagged packets....167
dynamic LSP metric....75

E

ECMP paths
BFD....351
ecmp statement....370
usage guidelines....351
egress policy, loopback address....347
egress routers
example configuration....140
overview....27
signaled LSPs....66
static LSPs....138, 205
egress-policy statement....370
usage guidelines....347
empty paths....223
encapsulation
CCC....397
TCC....411

encapsulation statement
Layer 2 switching cross-connect....423
usage guidelines....398
LSP tunnel cross-connect....423
usage guidelines....406
TCC....423
usage guidelines....411
encoding-type statement....193
usage guidelines....454
error (tracing flag)
LDP....386
MPLS....247
RSVP....323
Ethernet extended VLAN TCC, ARP configuration....415
Ethernet TCC
ARP configuration....415
ethernet-ccc encapsulation type....399
event (tracing flag)
LDP....386
RSVP....323
exclude statement....194
administrative groups
usage guidelines....89
fast reroute
usage guidelines....72
EXP and IP precedence bits....168
EXP bits....26, 91, 93, 160
DSCP values....167
rewrite....167
EXP rewrite rule....93
expand-loose-hop statement....195
usage guidelines....154
experimental bits *See* EXP bits
Explicit Null label....25
Explicit Route object....6
explicit routes....5
explicit senders, RSVP....259
explicit-null statement
LDP....371
usage guidelines....359
MPLS....196
usage guidelines....151
RSVP....196
usage guidelines....291
explicit-path LSPs
computation, disabling....88, 216
configuring....142
example configurations....103
overview....28
scope....29
export statement....371
usage guidelines....345
extended MAM....119, 186

F

facility backup....263
failed LSPs
fast reroute....42, 71, 185, 196
standby secondary paths....42
fast reroute....263
BFD....170
configuring....196
multiclass LSPs....133
overview....42, 71
path optimization....72
path optimization overview....46
PFE fast reroute....72, 287
traffic-engineered LSPs....130
fast-reroute optimize-timer statement....304
usage guidelines....72
fast-reroute statement....196
fate-sharing
CSPF algorithm....61
example configuration....61
overview....32
signaled LSPs....59, 197
fate-sharing statement....197
usage guidelines....59
FECs....329
FF (reservation style)....259
filtering received labels....343, 374
fixed-filter reservation style....259
font conventions....xxxiv
forwarding *See* MPLS
forwarding adjacency
configuration....461
LSP....462
OSPF configuration....463
peer router address....462
RSVP configuration....462
forwarding equivalence classes *See* FECs
forwarding next hop....40
Frame Relay circuits....402, 407
Frame Relay encapsulation
Layer 2 TCC....413
from statement
MPLS....198
usage guidelines....68

G

Generalized Multiprotocol Label Switching *See* GMPLS
GMPLS
Admin Status object....455
configuration....443
configuration statements....465
graceful deletion timeout interval....457
graceful LSP teardown....456
non-packet LSPs....455
overview....437

permanent LSP deletion....456
RSVP LSP hierarchy....459
temporary LSP deletion....456
gpid statement....199
usage guidelines....453
graceful deletion timeout interval....457
graceful restart
LDP....372
point-to-multipoint LSPs....146
RSVP....305
graceful teardown, GMPLS LSPs....456
graceful-deletion-timeout statement....304
usage guidelines....457
graceful-restart (tracing flag)....248
graceful-restart statement
LDP....372
usage guidelines....341
RSVP....305
usage guidelines....286
GRE tunnels....106
groups
administrative....72, 89, 180, 194, 201, 203

H

headers, MPLS and IPv4....168
hello interval
LDP....339, 372
RSVP....276, 306
hello messages....333
hello packets
RSVP....256
hello-dead-interval statement....468
usage guidelines....448
hello-interval statement
LDP....372
usage guidelines....339
LMP....469
usage guidelines....448
OSPF....469
usage guidelines....452
RSVP....306
usage guidelines....276
hello-packets (tracing flag)
LMP....480
helper-disable statement
LDP....373
usage guidelines....341
RSVP
usage guidelines....286
hold priority....95
hold time
LDP....340, 373
signaled LSPs....100, 180
hold-time statement
LDP....373
usage guidelines....340
hop-limit statement....200, 306
usage guidelines....98, 283
host routes....38, 73
hot-standby state....99

I

icmp-tunneling statement....200
usage guidelines....112
icons defined, notice....xxxiv
IEEE 802.p rewrite rule....93
ignore-lsp-metrics statement....374
usage guidelines....360
IGP
advertising LSPs....36
destinations....39
shortcuts
enabling....34
LSP metrics....75
overview....33
qualified LSPs....34
routing tables....35
uses of....35
Implicit Null label....25
import statement
LDP....374
usage guidelines....343
include statement
fast reroute
usage guidelines....72
include-all statement....201
administrative groups
usage guidelines....89
include-any statement....203
administrative groups
usage guidelines....89
inet option to static-path statement....135, 240
inet.0 routing table
IGP shortcuts....35
MPLS....40
inet.3 routing table
IGP shortcuts....35
MPLS....40
routes, installing....73
information distribution, traffic engineering....5
ingress routers
address configuration....68, 198
configuring for static LSPs....135
example configurations....103, 137
overview....27
path connection retry information....74, 232
init (tracing flag)
LMP....480

initialization (tracing flag).....386
install statement
MPLS.....204
usage guidelines.....73
Integrity object.....255
inter-area traffic engineering.....154
interface (from operator, LDP).....343
interface statement
LDP.....375
usage guidelines.....339
LMP.....470
usage guidelines.....443
RSVP.....307
usage guidelines.....271
static LSPs.....205
usage guidelines.....138
interface-switch statement.....429
Layer 2 switching cross-connects
usage guidelines.....402
usage guidelines.....402
interfaces
aggregated.....37
interior gateway protocol *See* IGP
intermediate routers
configuring for static LSPs.....138, 205
example configurations.....139
intraregion LSPs.....35
IP packets over aggregated interfaces.....37
IPv4 Explicit Null label.....25
IPv6
Implicit Null label.....25
tunneling over MPLS.....108
VPNs.....111
ipv6-tunneling statement.....206
usage guidelines.....111

K

keep multiplier, RSVP.....289, 308
keep-multiplier statement.....308
usage guidelines.....289
keepalive-interval statement.....376
usage guidelines.....340
keepalive-timeout statement.....376
usage guidelines.....340
keepalives
interval.....340, 376
timeout.....340, 376

L

l2-smart-policy statement.....377
usage guidelines.....350
label (tracing flag).....386
Label Distribution Protocol *See* LDP
label filtering.....343, 374
Label object.....6
Label Request object.....6
label-map statement.....206
usage guidelines.....138
label-switched paths *See* LSPs
label-switched-path statement
GMPLS.....471
MPLS.....207
usage guidelines.....62
MPLS with RSVP.....207
usage guidelines.....271
usage guidelines.....462
label-withdrawal-delay statement.....377
usage guidelines.....363
labels
allocation.....25
numerical ranges.....25
operations.....27, 331
overview.....21
properties.....135
reserved labels.....25
stacks.....25
swapping.....4
values.....25
Layer 2 switching
MPLS.....416
TCC.....415
Layer 2 switching cross-connect
CCC connections.....402
CCC encapsulation.....398
configuration.....397
configuring MPLS.....403
example configuration.....403
overview.....393
TCC encapsulation.....411
Layer 2 VPNs
aggregated Ethernet.....401
LDP
carrier-of-carriers VPNs.....359
configuration statements.....365
configuring.....375, 378
disabling.....339, 369
egress policy.....347
enabling.....339
example configuration
received label filtering.....344
tracing.....357
Explicit Null label.....291, 359
FEC policers.....349
graceful restart.....334, 341, 372
hello interval.....339, 372
hello messages.....333
hold time.....340, 373
Implicit Null label.....291, 359
Internet drafts.....329
JUNOS implementation.....330

keepalive
interval....340, 376
timeout....340, 376
label operations....331
message types....333
metrics....358
minimum configuration....339
multiple instances....359
operations....330
overview....329
policy filters....374
received label filtering....343, 374
RFC....329
route preferences....341, 384
standards....329
synchronization with the IGP....362
targeted hello messages....333
tracing operation of....355, 386
tunneling through RSVP LSPs....100, 209, 331, 360
ultimate-hop popping....291, 359, 371
ldp statement....378
complete hierarchy under....11
usage guidelines....339
ldp-synchronization statement....378
usage guidelines....362
ldp-tunneling statement....209
usage guidelines....360
least-fill statement....210
usage guidelines....76
least-fill tie-breaking rule....31, 76, 230
link attributes considered by CSPF algorithm....29
link coloring....72, 89, 180
link protection....263, 278
bypass LSPs
administrative groups....281
multiple bypass LSPs....283
RSVP....263
link-layer protocols....23
link-management statement....471
complete hierarchy under....12
usage guidelines....443
link-protection statement....210, 309
usage guidelines....146, 278, 279
LMP
peer network device configuration....446
tracing protocol operations....480
tracing protocol traffic....452
traffic engineering links....443
lmp (tracing flag)....323
lmp-control-channel statement....472
usage guidelines....447
lmp-protocol statement....472
load balancing
IP header....49
LSPs....77
MPLS labels....49
without CSPF....79
load-balance statement....311
usage guidelines....287
local-address statement
link management....473
usage guidelines....445
usage guidelines....461
log-updown statement
LDP....379
usage guidelines....361
MPLS....211
usage guidelines....159
logical-router *See* logical-system
logical-routers *See* logical-systems
loopback address, egress policy....347
loose explicit routes....5, 142
LSP graceful teardown....456
LSP metric....154
lsp-attributes statement....212
usage guidelines....453
lsp-switch statement....430
usage guidelines....409
lsping (tracing flag)....248
LSPs
adaptive rerouting....94, 175
administrative groups
admin-group statement....178
admin-groups statement....180
configuring....89
exclude statement....194
fast reroute....72
advertising in IGPs....36
associating addresses....73, 204
attributes considered by CSPF algorithm....29
automatic bandwidth allocation....182
bandwidth
maximum bounds....83
minimum bounds....83
BFD configuration....169
bypass....278
configuration statements....62, 207
configuring....129
constrained-path *See* constrained-path LSPs
CoS values....91
creating....62
damping LSP transitions....100
description, textual....71
differentiated service aware....116
egress routers....66, 138, 140, 205
example configurations....103
explicit-path *See* explicit-path LSPs
failure of....42
fast reroute....42, 71, 185, 196
fate-sharing....32, 59, 197

forwarding next hops
selecting....40
hold time....100, 180
host routes....38
IGP shortcuts....33
ingress routers....68, 198
intermediate routers....138, 205
intraregion LSPs....35
LDP tunneling....100
load balancing....77
without CSPF....79
metrics....75, 213
MPLS routers, configuring....62
multiple bypass....264
named paths....58, 223
OAM configuration....169
overview....4, 24
packet traversal....4, 28
path
bandwidth....98
calculation....3
connection retry information....74, 232
length....98, 200
pings....170
policing....162
preemption....95, 228
preference levels....91, 226
primary....68, 227
priorities....95, 228
recording routes....91
reoptimization....96, 220, 221
router functions....27
routing options....7
RSVP-signaled....28
scope of....29
secondary....68, 236
signaled *See* signaled LSPs
soft preemption....80
standby secondary paths....42
standby state....99, 239
static *See* static LSPs
stitching cross-connects....393, 409
text description....190
tie-breaking rules....31, 76, 230
traffic engineering, configuring....152
TTL decrementing, disabling....79, 217, 218
tunnel cross-connects, MTU....406
tunneling through RSVP LSPs....209, 331, 360

M

MAM....119, 186
manuals
comments on....xliii
max-bypasses statement....312
usage guidelines....283
maximum-bandwidth statement....212
usage guidelines....83
maximum-neighbor-recovery-time statement....379
usage guidelines....342
MD5 authentication....276
messages
LDP message types....333
MPLS system log....159, 211
Resv, RSVP....257
ResvConfirm, RSVP....258
ResvErr, RSVP....258
ResvTear, RSVP....258
RSVP message types....257
RSVP PathErr....101
RSVP refresh....289
metric statement
MPLS....213
usage guidelines....75
metrics
dynamic LSP metric....75
LDP tracking IGP....358
static LSP metric....75, 213
minimum-bandwidth statement....213
usage guidelines....83
monitor-bandwidth statement....214
usage guidelines....86
most-fill statement....214
usage guidelines....76
most-fill tie-breaking rule....31, 76, 214
MPLS....3
aggregated interfaces....37
automatic bandwidth allocation....182
backbones, packet traversal....4, 28
BFD....169
BGP destinations....38
configuration statements....51
configuring....55
CoS values....91
default route....101
DSCP and EXP values....167
exception monitoring....101
EXP bits....26, 91, 93, 160
Explicit Null label....151
fast reroute....42, 71, 185, 196
firewall filter....160
GRE tunnels....106
IGP and BGP destinations....39
Implicit Null label....151
IPv4 packet headers....168
IPv6....108
label range....25
Layer 2 switching TCC....416
link-layer protocols supported....23
load balancing....49
LSP tunnel cross-connects....405
MTU....406

LSPs *See* LSPs
OAM....169
overview....21
packets over aggregated interfaces....37
ping
Layer 3 VPNs....172
LSP end points....171
LSPs....170
routing tables....40
RSVP *See* RSVP
signaled LSPs *See* signaled LSPs
SNMP traps....159, 211
soft preemption....80
standards supported....21
standby secondary paths....42
static....135, 205
static LSPs *See* static LSPs
statistics....82
statistics output....158
system log messages....159, 211
tracing protocol operations....172, 247
traffic engineering....154
overview....24
traffic protection....42
traffic statistics....158, 241
tunneling
CCC connection....408, 433
CCC encapsulation....406
example configurations....408
overview....393, 405
tunnels for IPv6....108
ultimate-hop popping....151, 196
See also LDP, LSPs, RSVP, traffic engineering database
mpls statement
Layer 2 switching cross-connect....214
usage guidelines....403
MPLS....214
complete hierarchy under....12
usage guidelines....55
mpls.0 routing table....40
MTU signaling, in RSVP....260
mtu-signaling statement....215
usage guidelines....290
multicast
RPF check policy....147
multiclass LSPs
bandwidth subscription....126
configuring....132
fast reroute....133
multiple bypass LSPs....264, 280, 282, 283
Multiple Push (label operation)....27

N

named paths
empty paths....223
example configuration....59
overview....58
neighbor (from operator, LDP)....343
next hop (from operator, LDP)....343
next hops
selecting....40
next-hop bypass LSP....265
next-hop statement....215
next-next-hop bypass LSP....265
no-adjacency-down-notification statement....312
configuration guidelines....292
no-aggregate statement....298
usage guidelines....274
no-cspf statement....216, 313
usage guidelines....88, 284
no-decrement-ttl statement....217
no-forwarding statement....380
usage guidelines....358
no-install-to-address statement....218
usage guidelines....67
no-neighbor-down-notification statement....313
usage guidelines....292
no-node-protection statement
usage guidelines....284
no-p2mp-sublsp statement....314
usage guidelines....149
no-propagate-ttl statement....218
no-record statement....231
usage guidelines....91
no-reliable statement....320
usage guidelines....275
no-stamp option to traceoptions statement
LMP....481
no-trap statement....219
usage guidelines....160
no-world-readable option to traceoptions statement
LDP....387
LMP....481
MPLS....248
RSVP....324
node protection....263, 265
node-link-protection statement....314
usage guidelines....278
notice icons defined....xxxiv
notification (tracing flag)....387
notification messages
LDP....334

O

oam statement
LDP LSPs....381
usage guidelines....350
RSVP LSPs....220
usage guidelines....169
OAM, MPLS....169
offline path calculation....6, 31
one-to-one backup....263
operations on labels....27
optimize-aggressive statement....220
usage guidelines....96
optimize-timer statement
bypass LSPs....315
usage guidelines....284
MPLS....221
usage guidelines....96
optimizing LSPs....96, 220, 221
OSPF
hello interval....469
inter-area traffic engineering....154
link-state
advertisements....478
LSP metric advertisement....154
router dead interval....466
outgoing MTU value in RSVP
determining....262

P

p2mp statement....222
usage guidelines....143, 144
p2mp-lsp-next-hop statement....222
usage guidelines....140
p2mp-receive-switch statement....431
usage guidelines....418
p2mp-transmit-switch statement....432
usage guidelines....417
packet forwarding component
traffic engineering....4
packet headers, MPLS and IPv4....168
packet traversal on LSPs....4, 28
packets (tracing flag)
LDP....387
LMP....480
RSVP....323
parentheses, in syntax descriptions....xxxv
parser (tracing flag)
LMP....480
passive statement....473
usage guidelines....450
path
bandwidth, LSP....98
calculation
constrained-path computation....88, 216
CSPF algorithm....5, 29
offline path computation....6, 31
routing options....7
tie-breaking rules....31, 76, 230
connection retry information....74, 232
length, LSP....98, 200
selection component, traffic engineering....5
path (tracing flag)
LDP....387
RSVP....323
path messages, RSVP....257
path optimization
fast reroute....72
path selection....70
path statement
MPLS....223
RSVP....316
usage guidelines....285
path-mtu statement....224, 290
PathErr messages....101, 258
pathtear (tracing flag)....323
PathTear messages, RSVP....258
peer network device configuration....446
peer statement
LMP....474
usage guidelines....446
peer-interface statement
OSPF....475
usage guidelines....451
RSVP....317
usage guidelines....451
usage guidelines....462, 463
periodic (tracing flag)....387
periodic-traceroute statement....382
usage guidelines....351, 352
permanent GMPLS LSP deletion....456
PFE fast reroute....72, 287
ping
Layer 3 VPNs....172
LSP end point....171
LSPs....170
P2MP LSP....171
PLP bit....92
point-to-multipoint LSPs
branch LSPs....144
dynamic paths....144
static paths....145
CCC....417
configuration....143
graceful restart....146
link protection....146
overview....47
RPF check policy....147
static routes....140
ultimate-hop popping....293
policers
LDP FECs....349

policing.....162, 164, 397
policing filter statement
usage guidelines.....162
policing statement.....224, 383
usage guidelines.....164, 349
policy filters, LDP.....374
Pop (label operation).....27
pop statement
MPLS.....225
usage guidelines.....139
PPP circuits
Layer 2 switching cross-connects.....398
preemption
LSPs.....80
RSVP sessions.....290
signaled LSPs.....95, 228
preemption statement.....318
usage guidelines.....290
preference levels
LDP routes.....341, 384
signaled LSPs.....91, 226
static LSPs.....135, 139
preference statement
LDP.....384
usage guidelines.....341
signaled LSPs.....226
usage guidelines.....91
static LSPs.....226
usage guidelines (egress router).....139
usage guidelines (ingress router).....135
primary LSPs.....68, 227
primary paths
revert timer.....69
revert timer, BFD.....233
selection.....70
primary statement
MPLS.....227
usage guidelines.....68
priorities
signaled LSPs.....95, 228
priority statement
MPLS.....228
usage guidelines.....95
RSVP.....319
usage guidelines.....286
process (tracing flag).....480
Push (label operation).....27
push statement
MPLS.....229

R

random statement.....230
usage guidelines.....76
random tie-breaking rule.....31, 76, 230
RDM.....119, 186
receive (tracing flag modifier)
LDP.....387
LMP.....481
RSVP.....324
received label filtering.....374
Record Route object.....91
record statement.....231
usage guidelines.....91
recording routes.....91
recovery-time statement.....384
usage guidelines.....342
refresh messages, RSVP.....289
refresh reduction, RSVP.....259
refresh time, RSVP.....289
refresh-time statement.....320
usage guidelines.....289
reject statement.....231
usage guidelines.....139
reliable statement.....320
usage guidelines.....275
remote-address statement.....476
control channel management
usage guidelines.....448
usage guidelines.....445, 462
remote-id statement
link management.....477
usage guidelines.....445
remote-interface-switch statement.....433
usage guidelines.....408
reoptimizing LSPs.....96, 220, 221
replace option to traceoptions statement
LDP.....387
LMP.....481
MPLS.....248
RSVP.....324
requests, CoS.....253
rerouting LSPs
adaptive rerouting.....94, 175
fast reroute.....42, 71, 185, 196
reservation styles.....259
reserved labels.....25
reserving network resources *See* RSVP
resource classes.....72, 89
Resource Reservation Protocol *See* RSVP
resv (tracing flag).....323
Resv messages, RSVP.....257
ResvConfirm messages, RSVP.....258
ResvErr messages, RSVP.....258
resvtear (tracing flag).....324
ResvTear messages, RSVP.....258
retransmission-interval statement.....477
usage guidelines.....449
retransmit-interval statement.....478
usage guidelines.....451
retry information.....74, 232

retry-limit statement....232, 478
usage guidelines....74, 449
retry-timer statement....232
usage guidelines....74
revert-timer statement....233
usage guidelines....69
rewrite rules....93
IEEE 802.p and MPLS CoS....93
MPLS and VPNs....168
route (tracing flag)....324
LDP....387
route preferences
LDP....341, 384
signaled LSPs....91, 226
route-socket (tracing flag)
LMP....480
Router Alert label....25
routers
egress *See* egress routers
ingress *See* ingress routers
label operations....27
LSP functions....27
transit....27
routes
recording....91
route preferences....91, 226, 341, 384
routing (tracing flag)....480
routing options, traffic engineering....7
routing tables
host routes, installing....73, 204
IGP shortcuts....35
inet.0....35, 40
inet.3....35, 40, 73
MPLS....40
mpls.0....40
rpf-check-policy statement....234
configuration guidelines....147
RSVP....3
aggregation....298
authentication....276, 299
bandwidth
reserving....322
update threshold....277
BFD....169
configuration statements....269
configuration, minimum....271
disabling....271
ECMP-aware BFD....351
enabling....100, 271
example configurations....272, 295
Explicit Null label....291
graceful restart....266, 305
hello interval....276, 306
hello packets....256
IGP hello packets....256
Implicit Null label....291
JUNOS implementation....255
keep multiplier....308
link protection....278
load balancing....287
message types....257
MPLS, configuring with RSVP....271
MTU signaling in....260
overview....253
PathErr messages....101
preemption....290
reservation styles....259
RFC draft documents....254
sessions....255, 271
signaled LSPs....28, 100
signaling extensions....6
timers....289, 320
timers, hello packets....256
tracing protocol traffic....294, 323
tunneling LDP LSPs through RSVP LSPs....209, 331, 360
ultimate-hop popping....291, 293
unnumbered interfaces....278
See also LDP
RSVP LSP hierarchy....459
configuration....460
overview....460
RSVP refresh reduction
configuration....273
overview....259
rsvp statement....321
complete hierarchy under....16
usage guidelines....271
rsvp-error-hold-time statement....235
usage guidelines....101

S

scope of LSPs....29
SE (reservation style)....259
secondary
LSPs....68, 99, 236
paths....42
revert timer....69
selection....70
secondary statement....236
usage guidelines....68
select statement....237
usage guidelines....70
send (tracing flag modifier)
LDP....387
LMP....481
RSVP....324
server (tracing flag)....480
session messages, LDP....334
session statement....385
usage guidelines....361

sessions, RSVP....255, 271
setup priority, signaled LSPs....95
shared explicit reservation style....259
shared reservations....259
show (tracing flag)
LMP....480
signal-bandwidth statement....237
usage guidelines....453
signaled LSPs....223
adaptive rerouting....94, 175
administrative groups
admin-group statement....178
admin-groups statement....180
configuring....89
exclude statement....194
fast reroute....72
associating addresses....73, 204
configuration statements....62, 207
constrained-path computation
disabling....88, 216
CoS values....91
creating....62
damping LSP transitions....100
egress router address....66, 246
example configurations....103
fast reroute....71, 185, 196
fate-sharing....59, 197
hold time....100, 180
ingress router address....68, 198
LDP tunneling....100
load balancing without CSPF....79
metrics....75, 213
MPLS routers, configuring....62
named paths....58
overview....57
path
bandwidth....98
connection retry information....74, 232
length....98, 200
preemption....95, 228
preference levels....91, 226
primary....68, 227
priorities....95, 228
recording routes....91
reoptimization....96, 220, 221
RSVP *See* RSVP
secondary....68, 236
standby state....99, 239
tie-breaking rules....31, 76, 230
TTL decrementing....79, 217, 218
signaling component, traffic engineering....6
signaling extensions, RSVP....6
size option to traceoptions statement
LMP....481
smart-optimize-timer statement....238
usage guidelines....97
SNMP traps
MPLS....159, 211
soft-preemption statement
MPLS....238
usage guidelines....80
RSVP....321
usage guidelines....80
special labels....25
stacked labels....25
standby secondary paths....42
standby state, signaled LSPs....99, 239
standby statement....239
usage guidelines....99
state (tracing flag)
LDP....387
LMP....481
MPLS....248
RSVP....324
static LSPs
configuring....135
egress routers....138, 140, 205
ingress routers....135
intermediate routers....138, 205
overview....28
static LSP metric....75, 213
static MPLS....135
static routes
point-to-multipoint LSPs....140
static-path statement....240
usage guidelines....135
statistics
MPLS traffic....158, 241
output file....158
statistics statement....241
usage guidelines....158
strict explicit routes....5, 142
strict-targeted-hellos statement....385
usage guidelines....362
subscribing to bandwidth....322
subscription statement....322
usage guidelines....126
summary LSA....154
support, technical *See* technical support
Swap (label operation)....27
Swap and Push (label operation)....27
swap statement
MPLS....242
usage guidelines....139
swap-push statement
MPLS....243
switching-type statement....244
usage guidelines....453
syntax conventions....xxxiv
system log messages
MPLS....159, 211

T

targeted hello messages....333
TCC
  configuration....411
  connections....415
  encapsulation....411
  graceful restart
    configuration....417
    overview....394
  Layer 2 switching....411
  overview....394
te-class-matrix statement....245
  usage guidelines....120
te-link statement....479
  LMP traffic engineering link
    usage guidelines....444
  traffic engineering link associated with peer
    usage guidelines....450
  usage guidelines....461
technical support
  contacting JTAC....xliii
temporary GMPLS LSP deletion....456
tie-breaking rules, path calculation....31, 76, 230
timer (tracing flag)
  MPLS....248
timers
  RSVP....289, 320
to statement
  MPLS....246
    usage guidelines....66
traceoptions statement
  LDP....386
    usage guidelines....355
  LMP....480
    usage guidelines....452
  MPLS....247
    usage guidelines....172
  RSVP....323
    usage guidelines....294
tracing flag modifiers
  detail
    LDP....387
    LMP....481
    RSVP....324
  disable....387
  receive
    LDP....387
    LMP....481
    RSVP....324
  send
    LDP....387
    LMP....481
    RSVP....324
tracing flags
  address....386
  all....247
    LMP....480
    RSVP....323
  binding....386
  connection....247
  connection-detail....247
  cspf....247
  cspf-link....247
  cspf-node....247
  error
    LDP....386
    MPLS....247
    RSVP....323
  event
    LDP....386
    RSVP....323
  graceful-restart....248
  hello-packets
    LMP....480
  init
    LMP....480
  initialization....386
  label....386
  lmp....323
  lsping....248
  notification....387
  packets
    LDP....387
    LMP....480
    RSVP....323
  parse
    LMP....480
  path
    LDP....387
    RSVP....323
  pathtear....323
  periodic 387
  process....480
  resv....323
  resvtear....324
  route....324
    LDP....387
  route-socket
    LMP....480
  routing....480
  server....480
  show
    LMP....480
  state
    LDP....387
    LMP....481

MPLS....248
RSVP....324
timer
MPLS....248
tracing operations
LDP....355, 386
LMP....452, 480
MPLS....172, 247
RSVP....294, 323
track-igp-metric statement....388
usage guidelines....358
traffic
policing....397
protection, MPLS....42
statistics....158, 241
traffic engineering
BGP destinations....38
fate-sharing....32
IGP and BGP destinations....39
IGP shortcuts....33
information distribution component....5
inter-area, OSPF....154
links....443
LSP metric advertisement....154
overview....3, 24
packet-forwarding component....4
path-selection component....5
routing options....7
signaling component....6
TED accuracy....101
traffic engineering database....29
accuracy....101
bandwidth update threshold....277
traffic-engineered LSPs
fast reroute....130
traffic-engineering statement
bgp-igp option....152
bgp-igp-both-ribs option....153
MPLS....249
usage guidelines....152
mpls-forwarding option....153
traffic-statistics statement....389
usage guidelines....353
transit routers....27
transit-delay statement....482
usage guidelines....451
transitions
advertising....100, 180
damping....100
translational cross-connect *See* TCC
transport-address statement....390
usage guidelines....347
traps, SNMP *See* SNMP traps
triple-push statement....250
usage guidelines....135
TTL decrementing
disabling....79, 217, 218
tunnel-services statement....325
usage guidelines....293
tunneling, MPLS
CCC encapsulation....406
example configurations....408
overview....393, 405
RSVP LSPs....209, 331, 360
RSVP LSPs, heterogeneous networks....360

U

ultimate-hop popping....151
point-to-multipoint LSPs....293
unnumbered interfaces, RSVP....278
unstable LSPs
fate-sharing *See* fate-sharing
update-threshold statement....325
usage guidelines....277

W

wildcard filter (WF) reservation style....259
wildcard senders, RSVP....259
world-readable option to statistics statement
MPLS....241, 242
world-readable option to traceoptions statement
LDP....388
LMP....481
MPLS....248
RSVP....324

Index of Statements and Commands

A

adaptive statement....175
address statement
    LMP....465
adjust-interval statement....176
adjust-threshold statement....176
adjust-threshold-overflow-limit statement....177
admin-down statement....177
admin-group statement
    bypass LSPs....297
    LSPs....179
    MPLS interfaces....178
admin-groups statement....180
advertisement-hold-time statement....180
aggregate statement
    RSVP....298
allow-fragmentation statement....181
allow-subnet-mismatch statement....365
associate-backup-pe-groups statement....181
authentication-key statement
    LDP....366
    RSVP....299
auto-bandwidth statement....182
auto-policing statement....183

B

backup-pe-group statement....184
bandwidth statement
    fast reroute....185
    link protection....300
    multiclass LSPs....185
    RSVP....300
    signaled LSPs....185
bandwidth-model statement....186
bandwidth-percent statement....187
bfd-liveness-detection statement
    LDP LSPs....367
    RSVP LSPs....188
bypass statement....301

C

class-of-service statement
    bypass LSPs....302
    ingress routers....189
    signaled LSPs....189
    static LSPs....189
connections statement....422
control-channel statement....466

D

dead-interval statement....466
deaggregate statement....368
default-route statement....190
description statement
    MPLS....190
diffserv-te statement....191
disable statement
    GMPLS....467
    LDP....369
    link protection....303
    MPLS....192
    OSPF....467
    RSVP....303
    RSVP graceful restart....303
discard statement
    MPLS....192
double-push statement....193

E

ecmp statement....370
egress-policy statement....370
encapsulation statement
    Layer 2 switching cross-connect....423
    LSP tunnel cross-connect....423
    TCC....423
encoding-type statement....193
exclude statement....194
expand-loose-hop statement....195
explicit-null statement
    LDP....371
    MPLS....196
    RSVP....196

export statement....371

F

fast-reroute optimize-timer statement....304
fast-reroute statement....196
fate-sharing statement....197
from statement
    MPLS....198

G

gpid statement....199
graceful-deletion-timeout statement....304
graceful-restart statement
    LDP....372
    RSVP....305

H

hello-dead-interval statement....468
hello-interval statement
    LDP....372
    LMP....469
    OSPF....469
    RSVP....306
helper-disable statement
    LDP....373
hold-time statement
    LDP....373
hop-limit statement....200, 306

I

icmp-tunneling statement....200
ignore-lsp-metrics statement....374
import statement
    LDP....374
include-all statement....201
include-any statement....203
install statement
    MPLS....204
interface statement
    LDP....375
    LMP....470
    RSVP....307
    static LSPs....205
interface-switch statement....429
ipv6-tunneling statement....206

K

keep-multiplier statement....308
keepalive-interval statement....376
keepalive-timeout statement....376

L

l2-smart-policy statement....377
label-map statement....206
label-switched-path statement
    GMPLS....471
    MPLS....207
label-withdrawal-delay statement....377
ldp statement....378
ldp-synchronization statement....378
ldp-tunneling statement....209
least-fill statement....210
link-management statement....471
link-protection statement....210, 309
lmp-control-channel statement....472
lmp-protocol statement....472
load-balance statement....311
local-address statement
    link management....473
log-updown statement
    LDP....379
    MPLS....211
lsp-attributes statement....212
lsp-switch statement....430

M

max-bypasses statement....312
maximum-bandwidth statement....212
maximum-neighbor-recovery-time statement....379
metric statement
    MPLS....213
minimum-bandwidth statement....213
monitor-bandwidth statement....214
most-fill statement....214
mpls statement
    Layer 2 switching cross-connect....214
    MPLS....214
mtu-signaling statement....215

N

next-hop statement....215
no-adjacency-down-notification statement....312
no-cspf statement....216, 313
no-decrement-ttl statement....217
no-forwarding statement....380
no-install-to-address statement....218
no-neighbor-down-notification statement....313
no-p2mp-sublsp statement....314
no-propagate-ttl statement....218
no-trap statement....219
node-link-protection statement....314

O

oam statement
    LDP LSPs....381
    RSVP LSPs....220
optimize-aggressive statement....220
optimize-timer statement
    bypass LSPs....315
    MPLS....221

P

p2mp statement....222
p2mp-lsp-next-hop statement....222
p2mp-receive-switch statement....431
p2mp-transmit-switch statement....432
passive statement....473
path statement
    MPLS....223
    RSVP....316
path-mtu statement....224, 290
peer statement
    LMP....474
peer-interface statement
    OSPF....475
    RSVP....317
periodic-traceroute statement....382
policing statement....224, 383
pop statement
    MPLS....225
preemption statement....318
preference statement
    LDP....384
    signaled LSPs....226
    static LSPs....226
primary statement
    MPLS....227
priority statement
    MPLS....228
    RSVP....319
push statement
    MPLS....229

R

random statement....230
record statement....231
recovery-time statement....384
refresh-time statement....320
reject statement....231
reliable statement....320
remote-address statement....476
remote-id statement
    link management....477
remote-interface-switch statement....433
retransmission-interval statement....477
retransmit-interval statement....478
retry-limit statement....232, 478
retry-timer statement....232
revert-timer statement....233
rpf-check-policy statement....234
rsvp statement....321
rsvp-error-hold-time statement....235

S

secondary statement....236
select statement....237
session statement....385
signal-bandwidth statement....237
smart-optimize-timer statement....238
soft-preemption statement
    MPLS....238
    RSVP....321
standby statement....239
static-path statement....240
statistics statement....241
strict-targeted-hellos statement....385
subscription statement....322
swap statement
    MPLS....242
swap-push statement
    MPLS....243
switching-type statement....244

T

te-class-matrix statement....245
te-link statement....479
to statement
    MPLS....246
traceoptions statement
    LDP....386
    LMP....480
    MPLS....247
    RSVP....323
track-igp-metric statement....388
traffic-engineering statement
    MPLS....249
traffic-statistics statement....389
transit-delay statement....482
transport-address statement....390
triple-push statement....250
tunnel-services statement....325

U

update-threshold statement....325