JUNOS™ Internet Software
for M-series and T-series Routing Platforms

MPLS Network Operations Guide
Log Reference

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

Part Number: 530-014170-01, Revision 1

JUNOS Internet Software for J-series, M-series, and T-series Routing Platforms MPLS Network Operations Guide Log Reference
Writing: Merisha Wazna
Editing: Sonia Saruba
Illustration: Merisha Wazna and Nathaniel Woodward
Cover design: Edmonds Design

Thanks to Tom Van Meter, Peter Moyer, Craig Pierantozzi, and Javed Syed for their help with the development of this book.

Revision History
14 September 2005—Revision 1

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.

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, 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. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

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 the Software on non-Juniper equipment where the Juniper documentation does not expressly permit installation on non-Juniper equipment; (j) use the 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 for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

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

Table of Contents

About This Guide

This preface provides the following guidelines for using the *JUNOS Internet Software for M-series and T-series Routing Platforms MPLS Network Operations Guide Log Reference* and related Juniper Networks, Inc., technical documents:

Objectives

This manual provides operational information helpful in monitoring router components and isolating potential problems. This manual is not directly related to any particular release of the JUNOS Internet software.

To obtain the most current version of this manual, refer to the product documentation page on the Juniper Networks Web site, which is located at http://www.juniper.net/.

Audience

This guide is designed for network administrators who are configuring and monitoring a Juniper Networks M-series or T-series routing platform in an MPLS network environment.

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.

Chapter Organization

Most chapters in this manual consist of a checklist at the beginning of the chapter listing the tasks and commands for monitoring the interface. The tasks and commands are then explained in step-by-step procedures.

Each step-by-step procedure consists of some or all of the following parts:

- Purpose—Describes what is affected if this task is not performed or what is accomplished with this task.
- What Is... —Describes a component (usually hardware).
- Step(s) To Take—Lists the steps in the task.
- Action—Describes an action to perform in order to complete the step.
- Sample Output—Presents sample output relevant to the procedure.
- What It Means—Describes or summarizes what is presented in the sample output.
- Symptom/Indications—Describes a problem with the software or hardware.
- See Also—Lists other topics related to this task.
- Alternative Actions—Describes other commands or ways of doing the task.
- Syntax—Describes the full syntax of the command or configuration statement. For an explanation of how to read the syntax statements, see “Documentation Conventions” on page xiii.

Documentation Conventions

Table 1 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.

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

Table 2: Text and Syntax Conventions

Convention	Element	Example
Bold sans serif typeface	Represents text that you type.	To enter configuration mode, type the configure command: user@host> **configure**
`Fixed-width typeface`	Represents output on the terminal screen.	`user@host> show chassis alarms` `No alarms currently active`
Italic typeface	■ 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 sans serif typeface	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*
Sans serif typeface	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*]

Convention	Element	Example

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

Related Juniper Networks Documentation

Table 3 lists the books included in the *Network Operations Guide* series.

Table 3: JUNOS Internet Software Network Operations Guides

Book	Description
JUNOS Internet Software for M-series and T-series Routing Platforms Network Operations Guides	
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 routers in the network, and using the layered MPLS troubleshooting model to investigate problems with an MPLS network.
MPLS Log Reference	Describes MPLS status and error messages that appear in the output of the show mpls lsp extensive command, how and when to configure Constrained Shortest Path First (CSPF) and Resource Reservation Protocol (RSVP) tracing, and how to examine a CSPF and RSVP failure in an example network.
Hardware	Describes tasks for monitoring M-series and T-series routing platforms.

Table 4 lists the software and hardware guides and release notes for Juniper Networks J-series, M-series, and T-series routing platforms and describes the contents of each document.

Table 4: Technical Documentation for J-series, M-series, and T-series Routing Platforms

Document	Description
JUNOS Internet Software for J-series, M-series, and T-series Routing Platforms Configuration Guides	
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.
Feature Guide	Provides a detailed explanation and configuration examples for several of the most complex features in the JUNOS software.
JUNOS-FIPS	(M-series and T-series routing platforms only) Provides an overview of JUNOS-FIPS 140-2 concepts and describes how to install and configure the JUNOS-FIPS software. Describes FIPS-related commands and how to configure, authorize, and zeroize the Adaptive Services (AS) II FIPS Physical Interface Card (PIC).
MPLS Applications	Provides an overview of traffic engineering concepts and describes how to configure traffic engineering protocols.
Multicast Protocols	Provides an overview of multicast concepts and describes how to configure multicast routing protocols.
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, forwarding options, and cflowd.
Routing Protocols	Provides an overview of routing concepts and describes how to configure routing, routing instances, and unicast routing protocols.
Services Interfaces	Provides an overview of the services interfaces functions of the JUNOS software and describes how to configure the services interfaces on the routing platform.
System Basics	Provides an overview of the JUNOS software and describes how to install and upgrade the software. This guide also describes how to configure system management functions and how to configure the chassis, including user accounts, passwords, and redundancy.
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	
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 protocols and policies, including firewall filters.

Document	Description
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 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 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.
JUNOScript API Configuration Reference	Provides a reference page for the configuration tags in the JUNOScript API.
JUNOScript API Operational Reference	Provides a reference page for the operational tags in the JUNOScript API.
JUNOS Configuration Scripting Guide	Provides an overview, instructions for using, and examples of the commit script feature of the JUNOS software. This guide explains how to enforce custom configuration rules defined in scripts that run at commit time. This guide also explains how to use commit script macros to provide simplified aliases for frequently used configuration statements.
JUNOS Comprehensive Index and Glossary	
Comprehensive Index and Glossary	Provides a complete index of all JUNOS software books and the *JUNOScript API Guide*. Also provides a comprehensive glossary.
JUNOScope Documentation	
JUNOScope Software User Guide	Describes the JUNOScope software 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.
J-series Services Router Documentation	
J-series Services Router Getting Started Guide	Provides an overview, basic instructions, and specifications for J-series Services Routers. The guide explains how to prepare your site for installation, unpack and install the router and its components, install licenses, and establish basic connectivity.
J-series Services Router Configuration Guide	Explains how to configure the interfaces on J-series Services Routers for basic IP routing with standard routing protocols. The guide also shows how to configure VPNs, configure and manage multicast networks, and apply routing techniques such as policies, firewall filters, IPSec tunnels, and service classification for safer, more efficient routing.
J-series Services Router Administration Guide	Shows how to manage users and operations, monitor network performance, upgrade software, and diagnose common problems on J-series Services Routers.
M-series and T-series 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 PICs. Each platform has its own PIC guide.

Document	Description
Release Notes	
JUNOS Release Notes	Summarize new features and known problems for a particular software release, provide corrections and updates to published JUNOS and JUNOScript 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 the supported PICs, and summarize known problems with the hardware and accompanying software. Each platform has its own release notes.
JUNOScope Software 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.
J-series Services Router Release Notes	Briefly describe the J-series Services Router features, identify known hardware problems, and provide upgrade and downgrade instructions.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. Send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at http://www.juniper.net/techpubs/docbug/docbugreport.html. 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

Requesting Support

For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

Part 1

Examining the LSP Event Log

This section provides examples of many MPLS status and error messages that appear in the LSP history log of the show mpls lsp extensive command output. The following types of messages are included:

Chapter 1

Understanding LSP Status Events

Label-switched path (LSP) status events occur in the history log of the show mpls lsp extensive command output, and provide detailed information that can help pinpoint the problem with an LSP. This chapter lists and describes many LSP status events. Descriptions generally include sample output of the LSP event, an explanation of what the event means, the possible cause of the event, and any possible actions that you can take. The LSP events are organized alphabetically. (See Table 5.)

Table 5: Checklist for Understanding LSP Status Events

Understanding LSP Status Events Tasks	Possible Action or Command
Displaying LSP Status Events on page 5	show mpls lsp extensive
1. Call Was Cleared by RSVP Event on page 7	Not applicable.
2. Change in Active Path Event on page 8	Not applicable.
3. Clear Call Event on page 8	Not applicable.
4. Deselected as Active Event on page 9	Analyze this event, and refer to events on either side of this event to determine the appropriate action.
5. Down Event on page 9	Analyze this event, and refer to events on either side of this event to determine the appropriate action.
6. Fast Reroute Detour Down Event on page 9	Analyze this event, and refer to events on either side of this event to determine the appropriate action.
7. Fast Reroute Detour Up Event on page 10	Not applicable.
8. Link Protection Down Event on page 11	Include the family mpls statement for all alternate paths for the LSP at the [edit interfaces type-*fpc/pic/port.unit*] hierarchy level.
9. Link Protection Up Event on page 12	Not applicable.
10.Originate Call Event on page 13	[edit protocols rsvp] set traceoptions file rsvp.log set traceoptions flag packets file show /var/log/rsvp.log
11.Originate Make-Before-Break Call Event on page 14	Not applicable.
12.Record Route Event on page 15	Not applicable.
13.ResvTear Received Event on page 15	Analyze this event, and refer to events on either side of this event to determine the appropriate action.
14.RSVP Disabled Event on page 16	[edit protocols] activate rsvp [edit protocols rsvp] set interface *type-fpc/pic/port*

Understanding LSP Status Events Tasks	Possible Action or Command
15.RSVP Error Event on page 16	[edit protocols] activate rsvp
16.Selected as Active Path Event on page 17	Not applicable.
17.Session Preempted Event on page 17	Not applicable.
18.Up Event on page 18	Not applicable.

Displaying LSP Status Events

Purpose Display extensive information about LSPs, including the 50 most recent history events and the reasons why an LSP might have failed.

Action To examine status messages, enter the following JUNOS command-line interface (CLI) operational mode command from the ingress router:

```
user@host> show mpls lsp extensive
```

Sample Output 1

```
user@R1# run show mpls lsp extensive
Ingress LSP: 1 sessions

10.0.0.6
  From: 10.0.0.1, State: Dn, ActiveRoute: 0, LSPname: R1-to-R6
  ActivePath: (none)
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
  Primary                   State: Dn
    Will be enqueued for recomputation in 3 second(s).
   68 Jan  5 10:02:56 CSPF failed: no route toward 10.0.0.6[9 times]
   67 Jan  5 09:58:33 Deselected as active
   66 Jan  5 09:58:33 CSPF failed: no route toward 10.0.0.6
   65 Jan  5 09:58:33 Clear Call
   64 Jan  5 09:58:33 Session preempted
   63 Jan  5 09:58:33 Down
   62 Jan  5 09:58:32 CSPF failed: no route toward 10.0.0.6[2 times]
   61 Jan  5 09:57:55 10.1.36.2: Explicit Route: wrong delivery
   60 Jan  5 09:57:34 CSPF failed: no route toward 10.0.0.6[2 times]
   59 Jan  5 09:57:28 CSPF: link down/deleted
10.1.36.1(R3.00/10.0.0.3)->10.1.36.2(R6.00/10.0.0.6)
   58 Jan  5 09:54:37 Selected as active path
   57 Jan  5 09:54:37 Record Route:  10.1.13.2 10.1.36.2
   56 Jan  5 09:54:37 Up
   55 Jan  5 09:54:37 Originate Call
   54 Jan  5 09:54:37 CSPF: computation result accepted
   53 Jan  4 18:11:28 CSPF failed: no route toward 10.0.0.6[2 times]
   52 Jan  4 18:10:44 Deselected as active
   51 Jan  4 18:10:44 CSPF failed: no route toward 10.0.0.6
   50 Jan  4 18:10:44 CSPF: link down/deleted
10.1.13.1(R1.00/10.0.0.1)->10.1.13.2(R3.00/10.0.0.3)
   49 Jan  4 18:10:44 RSVP Disabled
   48 Jan  4 18:10:44 RSVP error, subcode 4: protocol shutdown
   47 Jan  4 18:10:44 Down
   46 Jan  4 18:06:15 Up
   45 Jan  4 18:06:15 Down
   44 Jan  4 18:06:10 Selected as active path
   43 Jan  4 18:06:09 Record Route:  10.1.13.2 10.1.36.2
   42 Jan  4 18:06:09 Up
   41 Jan  4 18:06:09 Originate Call
   40 Jan  4 18:06:09 CSPF: computation result accepted
   39 Jan  4 18:05:40 CSPF failed: no route toward 10.0.0.6[2 times]
   38 Jan  4 18:04:57 Deselected as active
   37 Jan  4 18:04:57 CSPF failed: no route toward 10.0.0.6
   36 Jan  4 18:04:57 CSPF: link down/deleted
10.1.13.1(R1.00/10.0.0.1)->10.1.13.2(R3.00/10.0.0.3)
   35 Jan  4 18:04:57 CSPF failed: no route toward 10.0.0.6
   34 Jan  4 18:04:57 Clear Call
   33 Jan  4 18:04:57 Explicit Route: bad strict route
   32 Jan  4 18:04:57 No Route toward dest
   31 Jan  4 18:04:57 Down
```

```
   30 Dec 28 13:47:29 Selected as active path
   29 Dec 28 13:47:29 Record Route:  10.1.13.2 10.1.36.2
   28 Dec 28 13:47:29 Up
   27 Dec 28 13:47:29 Originate Call
   26 Dec 28 13:47:29 CSPF: computation result accepted
   25 Dec 28 13:46:59 CSPF failed: no route toward 10.0.0.6
   24 Dec 28 13:46:39 Deselected as active
   23 Dec 28 13:46:39 CSPF failed: no route toward 10.0.0.6
   22 Dec 28 13:46:39 Clear Call
   21 Dec 28 13:46:39 ResvTear received
   20 Dec 28 13:46:39 Down
   19 Dec 28 13:46:39 10.1.13.2: Session preempted
Created: Mon Dec 13 11:47:18 2004
Total 1 displayed, Up 0, Down 1
[...Output truncated...]
```

Sample Output 2

```
user@R1> show mpls lsp extensive
[...Output truncated...]
*Primary use-TOKYO       State: Up, No-decrement-ttl
    Received RRO:
         10.222.28.2(flag=0x9) 10.222.4.2(flag=0x1) 10.222.44.2
    7 Sep 20 18:13:45 Record Route: 10.222.28.2(flag=0x9)
10.222.4.2(flag=0x1) 10.222.44.2
    6 Sep 20 18:13:45 Record Route: 10.222.28.2(flag=0x9)
10.222.4.2 10.222.44.2
    5 Sep 20 18:13:45 Fast-reroute Detour Up
    4 Sep 20 18:13:42 Selected as active path
    3 Sep 20 18:13:42 Record Route: 10.222.28.2 10.222.4.2
10.222.44.2
    2 Sep 20 18:13:42 Up
    1 Sep 20 18:13:42 Originate Call
```

Sample Output 3

```
user@R1> show mpls lsp extensive
[...Output truncated...]
*Primary   long             State: Up, COS: 6
    Bandwidth per class: <ct0 20Mbps> <ct1 2Mbps> <ct2 3Mbps>
    OptimizeTimer: 250
    Reoptimization in 237 second(s).
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 50)
          10.35.38.2 S 192.168.135.29 S 10.35.39.1 S 10.35.40.2 S 10.35.41.1 S
    Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node
10=SoftPreempt):
          10.35.38.2 (flag=0x09) 192.168.135.29 (flag=0x10) 10.35.39.1
   (flag=0x01) 10.35.40.2 (flag=0x01) 10.35.41.1 (flag=0x01)
[...Output truncated...]
```

What It Means

Sample Output 1 from ingress router R1 shows extensive ingress LSP information, including LSP events that led to an LSP failure and the 50 most recent state events.

LSP events in bold are described in this chapter. Descriptions include sample output of the LSP event, an explanation of what the event means, the possible cause of the event, and any possible actions that you can take.

For completeness, events not included in this example output are also described in this chapter to show LSP events that did not occur in the example network configuration, but might occur in your network. The LSP events are organized alphabetically.

Sample Output 2 shows the state of the route received in the Received Record Route (Received RRO) created by fast reroute configurations in the network. The Received RRO indicates a series of hops. Each hop has an address followed by a flag. For more information on flags, see the *JUNOS MPLS Network Operations Guide*. In most cases, the Received RRO is the same as the computed Explicit Route Object (ERO).

Sample Output 3 shows a Computed ERO and a Received RRO. In this instance they are the same. However, if Received RRO is different from the Computed ERO, there is a topology change in the network, and the route is taking a detour.

Call Was Cleared by RSVP Event

LSP Event Call was cleared by RSVP

Sample Output

```
user@R1> show mpls lsp extensive
[...Output truncated...]
10.0.0.6
From: 10.0.0.1, State: Dn, ActiveRoute: 0, LSPname: R1-to-R6
ActivePath: (none)
LoadBalance: Random
Encoding type: Packet, Switching type: Packet, GPID: IPv4
Primary State: Dn
Will be enqueued for recomputation in 10 second(s).
11 Jan 26 14:58:32 CSPF failed: no route toward 10.0.0.6
10 Jan 26 14:58:25 Deselected as active
9 Jan 26 14:58:25 CSPF failed: no route toward 10.0.0.6
8 Jan 26 14:58:25 Call was cleared by RSVP
7 Jan 26 14:58:25 Session preempted
6 Jan 26 14:58:25 Down
[...Output truncated...]
```

What It Means This LSP event indicates that the Resource Reservation Protocol (RSVP) session corresponding to the LSP path was preempted and the corresponding RSVP state deleted.

Cause This LSP event is occurs when you issue the clear rsvp session command or trigger preemption of an RSVP session at the ingress router. Depending on the timer value, Constrained Shortest Path First (CSPF) recomputes the path and the LSP comes up again.

Change in Active Path Event

LSP Event Change in active path

Sample Output

```
user@R1> show mpls lsp extensive
[...Output truncated...]
13 Sep 19 00:02:20 Deselected as active
12 Sep 19 00:02:20 ResvTear received
11 Sep 19 00:02:20 Down
10 Sep 19 00:02:20 Change in active path
9 Sep 19 00:02:20
8 Sep 19 00:02:20 10.222.28.2: Explicit Route: bad strict routeChange in active
path
7 Sep 19 00:02:20 CSPF failed: no route toward 192.168.32.1
6 Sep 19 00:02:20 10.222.28.2: No Route toward dest
5 Sep 19 00:00:54 Selected as active path
4 Sep 19 00:00:54 Record Route: 10.222.28.2 10.222.4.2 10.222.44.2
3 Sep 19 00:00:54 Up
2 Sep 19 00:00:54 Originate Call
1 Sep 19 00:00:54 CSPF: computation result accepted
[...Output truncated...]
```

What It Means This LSP event indicates that even though the active physical path has changed, the LSP stays up. Because this network configuration has an alternate (fast-reroute) path available, the event is a Change in active path rather than a Session preempted event.

Cause The active path might have failed.

Clear Call Event

LSP Event Clear call

Sample Output

```
user@R1> show mpls lsp extensive
[...Output truncated...]
   65 Jan  5 09:58:33 Clear Call
   64 Jan  5 09:58:33 Session preempted
   63 Jan  5 09:58:33 Down
[...Output truncated...]
```

What It Means This LSP event indicates that the LSP was disconnected and restarted.

Cause The clear mpls lsp command was issued on the ingress router to disconnect existing RSVP sessions, release the routes and states associated with the LSP, and then start a new LSP. Issuing this command might impact traffic travelling along the LSP, because a time lag might occur between tearing down the old path and setting up a new path.

Deselected as Active Event

LSP Event Deselected as active

Sample Output

```
user@R1> show mpls lsp extensive
[...Output truncated...]
   Will be enqueued for recomputation in 18 second(s).
   53 Jan  4 18:11:28 CSPF failed: no route toward 10.0.0.6[2 times]
   52 Jan  4 18:10:44 Deselected as active
   51 Jan  4 18:10:44 CSPF failed: no route toward 10.0.0.6
   50 Jan  4 18:10:44 CSPF: link down/deleted
[...Output truncated...]
```

What It Means This LSP event indicates that the LSP is no longer the active path.

Cause Typically, other events, similar to those in lines 50 and 51, indicate the reason that the LSP is no longer the active path.

Action Refer to events on either side of this event to determine the appropriate action.

Down Event

LSP Event Down

Sample Output

```
user@R1> show mpls lsp extensive
[...Output truncated...]
   48 Jan  4 18:10:44 RSVP error, subcode 4: protocol shutdown
   47 Jan  4 18:10:44 Down
   46 Jan  4 18:06:15 Up
   45 Jan  4 18:06:15 Down
[...Output truncated...]
```

What It Means This LSP event indicates the state of the LSP on January 4 at 1800 hours, 10 minutes, and 44 seconds. The LSP had failed or was down.

Action Refer to events on either side of the Down event to determine why the LSP was down.

Fast Reroute Detour Down Event

LSP Event Fast reroute detour down

Sample Output 1

```
user@R1> show mpls lsp extensive
[...Output truncated...]
10.0.0.6
  From: 10.0.0.1, State: Up, ActiveRoute: 0, LSPname: R1-R6-3
  ActivePath:  (primary)
  FastReroute desired
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
 *Primary                    State: Up
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 20)
 10.1.15.2 S 10.1.56.2 S
    Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node
10=SoftPreempt):
          10.1.15.2(flag=1) 10.1.56.2
```

```
    9 Feb 15 20:52:56 Fast-reroute Detour Up
    8 Feb 15 20:52:53 Fast-reroute Detour Down
    7 Feb 15 20:50:00 Record Route:  10.1.15.2(flag=1) 10.1.56.2
    6 Feb 15 20:50:00 Fast-reroute Detour Up
    5 Feb 15 20:49:57 Selected as active path
    4 Feb 15 20:49:57 Record Route:  10.1.15.2 10.1.56.2
    3 Feb 15 20:49:57 Up
    2 Feb 15 20:49:56 Originate Call
    1 Feb 15 20:49:56 CSPF: computation result accepted
  Created: Tue Feb 15 20:49:56 2005
Total 3 displayed, Up 3, Down 0
[...Output truncated...]
```

What It Means This LSP event applies only to detours on the router and indicates that the one-to-one (1:1) fast reroute detour to bypass the next downstream node is down.

Cause This LSP event is caused by a failure or configuration change that deletes or resignals the fast reroute detour path. For example, a detour path interface or primary link may be deactivated.

Action Analyze the status to determine if this is the required behavior. If this is not the required behavior, verify the surrounding LSP events to identify the cause of the problem.

Fast Reroute Detour Up Event

LSP Event Fast-reroute Detour Up

Sample Output 1

```
user@R1> show mpls lsp extensive
[...Output truncated...]
10.0.0.6
  From: 10.0.0.1, State: Up, ActiveRoute: 0, LSPname: R1-R6-3
  ActivePath:  (primary)
  FastReroute desired
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
 *Primary                    State: Up
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 20)
 10.1.15.2 S 10.1.56.2 S
    Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node
10=SoftPreempt):
          10.1.15.2(flag=1) 10.1.56.2
    7 Feb 15 20:50:00 Record Route:  10.1.15.2(flag=1) 10.1.56.2
    6 Feb 15 20:50:00 Fast-reroute Detour Up
    5 Feb 15 20:49:57 Selected as active path
    4 Feb 15 20:49:57 Record Route:  10.1.15.2 10.1.56.2
    3 Feb 15 20:49:57 Up
    2 Feb 15 20:49:56 Originate Call
    1 Feb 15 20:49:56 CSPF: computation result accepted
  Created: Tue Feb 15 20:49:57 2005
Total 3 displayed, Up 3, Down 0
[...Output truncated...]
```

Sample Output 2

```
[edit protocols mpls]
user@R1# show
label-switched-path R1-R6-3 {
    to 10.0.0.6;
    fast-reroute;
}
[...Output truncated...]
```

What It Means This LSP event only applies to detours on this route, and indicates that a fast reroute detour path is up. Sample Output 1 shows the fast reroute event. Sample Output 2 shows the configuration of fast reroute on ingress router R1.

Cause This LSP event is caused by the correct configuration of a one-to-one (1:1) fast reroute detour, resulting in the successful signaling of a fast reroute detour.

Action Not applicable.

Link Protection Down Event

LSP Event Link protection down

Sample Output 1

```
user@R1> show configuration protocols mpls
label-switched-path R1-to-R6 {
    to 10.0.0.6;
    link-protection;
}
interface fxp0.0 {
    disable;
}
interface all;
```

Sample Output

```
user@R1> show mpls lsp extensive
[...Output truncated...]
10.0.0.6
  From: 10.0.0.1, State: Up, ActiveRoute: 1, LSPname: R1-to-R6
  ActivePath:  (primary)
  Link protection desired
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
 *Primary                    State: Up
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 2)
 10.1.13.2 S 10.1.36.2 S
    Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node
10=SoftPreempt):
          10.1.13.2(flag=1 Label=101936) 10.1.36.2(Label=3)
   70 Feb 10 11:01:56 Link-protection Up
   69 Feb 10 11:01:56 Selected as active path
   68 Feb 10 11:01:56 Link-protection Down
   67 Feb 10 11:01:56 Link-protection Up
   66 Feb 10 11:01:56 Record Route:  10.1.13.2(flag=1 Label=101936)
10.1.36.2(Label=3)
   65 Feb 10 11:01:56 Up
   64 Feb 10 11:01:56 Originate Call
   63 Feb 10 11:01:56 CSPF: computation result accepted
   62 Feb 10 11:01:56 Clear Call
   61 Feb 10 11:01:56 Deselected as active
   60 Feb 10 11:01:56 Link-protection Down
   59 Feb 10 10:57:58 Record Route:  10.1.13.2(flag=1 Label=101920)
10.1.36.2(Label=3)
```

```
   58 Feb 10 10:57:56 Link-protection Up
   57 Feb 10 10:56:58 Selected as active path
   56 Feb 10 10:56:58 Record Route:  10.1.13.2(Label=101920) 10.1.36.2(Label=3)
   55 Feb 10 10:56:58 Up
   54 Feb 10 10:56:58 Originate Call
   53 Feb 10 10:56:58 CSPF: computation result accepted
   52 Feb 10 10:56:58 Clear Call
   51 Feb 10 10:56:58 Deselected as active
   50 Feb 10 10:56:58 Link-protection Down
   49 Feb 10 10:56:35 10.1.56.2: MPLS label allocation failure[2 times]
   48 Feb 10 10:48:32 Link-protection Up
   47 Feb 10 10:48:32 Selected as active path
[...Output truncated...]
```

What It Means Sample Output 1 shows the MPLS link-protection configuration on R1 for the LSP R1-to-R6.

Sample Output 2 shows that link protection came up and down several times. Link protection comes up when the LSP signals. Line 60 shows the result when RSVP is disabled on all alternate paths out of R6. Lines 68 to 70 are the result when the clear mpls lsp command is issued.

Cause This LSP event is caused by a failure or configuration change that deletes or resignals the bypass LSP. For example, you clear the LSP using the clear mpls lsp command, or you disable RSVP on all alternate paths for the LSP. The bypass LSP does not use the primary path, instead it looks for an alternate path.

Action Include the family mpls statement for all alternate paths for the LSP at the [edit interfaces type-fpc/pic/port.unit] hierarchy level.

Link Protection Up Event

LSP Event Link protection up

Sample Output

```
user@R1> show mpls lsp extensive
[...Output truncated...]
10.0.0.6
  From: 10.0.0.1, State: Up, ActiveRoute: 1, LSPname: R1-to-R6
  ActivePath:  (primary)
  Link protection desired
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
 *Primary                    State: Up
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 2)
 10.1.15.2 S 10.1.56.2 S
    Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node
10=SoftPreempt):
          10.1.15.2(flag=1 Label=100048) 10.1.56.2(Label=3)
   48 Feb 10 10:48:32 Link-protection Up
   47 Feb 10 10:48:32 Selected as active path
   46 Feb 10 10:48:32 Link-protection Down
   45 Feb 10 10:48:32 Link-protection Up
   44 Feb 10 10:48:32 Record Route:  10.1.15.2(flag=1 Label=100048)
```

```
10.1.56.2(Label=3)
   43 Feb 10 10:48:32 Up
   42 Feb 10 10:48:32 Originate Call
   41 Feb 10 10:48:32 CSPF: computation result accepted
   40 Feb 10 10:48:32 Clear Call
[...Output truncated...]
```

What It Means This LSP event indicates that the bypass LSP used to provide local protection (link or node protection) was successfully signaled at the first hop.

Action Not applicable.

Originate Call Event

LSP Event Originate call

Sample Output

```
user@R1> show mpls lsp extensive
[...Output truncated...]
   43 Jan  4 18:06:09 Record Route:  10.1.13.2 10.1.36.2
   42 Jan  4 18:06:09 Up
   41 Jan  4 18:06:09 Originate Call
   40 Jan  4 18:06:09 CSPF: computation result accepted
   39 Jan  4 18:05:40 CSPF failed: no route toward 10.0.0.6[2 times]
[...Output truncated...]
```

What It Means This LSP event indicates that the router is issuing an RSVP Path message.

Cause A Path message is transmitted by the ingress router toward the egress router to establish an LSP.

Action To analyze the contents of the Path message, enable RSVP tracing. To configure RSVP tracing, include the traceoptions statement at the [edit protocols rsvp] hierarchy level. 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. To examine the contents of the rsvp-log file, issue the file show /var/log/rsvp-log command. For more information about the output of the tracing operation, see "Examining the CSPF Log" on page 71. For more information about RSVP messages see the *JUNOS MPLS Applications Configuration Guide*.

Originate Make-Before-Break Call Event

LSP Event Originate make-before-break call

Sample Output

```
user@R1# run show mpls lsp extensive
Ingress LSP: 3 sessions

10.0.0.3
  From: 10.0.0.1, State: Up, ActiveRoute: 5, LSPname: R1-to-R3
  ActivePath:  (primary)
  LoadBalance: Random
  Metric: 1
  Autobandwidth
  MinBW: 155Mbps MaxBW: 155Mbps
  AdjustTimer: 300 secs AdjustThreshold: 10%
  Max AvgBW util: 392bps, Bandwidth Adjustment in 101 second(s).
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
 *Primary                    State: Up
    Bandwidth: 140Mbps
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 10)
 10.1.13.2 S
    Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node
10=SoftPreempt):
          10.1.13.2
   13 Feb 17 21:23:51 Manual Autobw adjustment failed
   12 Feb 17 21:23:51 CSPF failed: no route toward 10.0.0.3
   11 Feb 17 21:16:06 Record Route:  10.1.13.2
   10 Feb 17 21:16:06 Up
    9 Feb 17 21:16:06 Manual Autobw adjustment succeeded
    8 Feb 17 21:16:06 Originate make-before-break call
    7 Feb 17 21:16:06 CSPF: computation result accepted
    6 Feb 17 21:14:51 Selected as active path
    5 Feb 17 21:14:51 Record Route:  10.1.13.2
    4 Feb 17 21:14:51 Up
    3 Feb 17 21:14:51 Originate Call
    2 Feb 17 21:14:51 CSPF: computation result accepted
    1 Feb 17 21:14:22 CSPF failed: no route toward 10.0.0.3[4 times]
[...Output truncated...]
```

What It Means This LSP event indicates that a make-before-break operation is in progress, in which the label-switched router (LSR) signals a new path for the LSP and switches over to this path, tearing down the existing path.

Cause In an adaptive LSP, this LSP event is caused by a change in bandwidth or ERO. For an active LSP path, this LSP is caused by a change in reoptimization or autobandwidth adjustment.

Action Not applicable.

Record Route Event

LSP Event Record route

Sample Output

```
user@R1> show mpls lsp extensive
[...Output truncated...]
   10.1.36.1(R3.00/10.0.0.3)->10.1.36.2(R6.00/10.0.0.6)
   58 Jan  5 09:54:37 Selected as active path
   57 Jan  5 09:54:37 Record Route:  10.1.13.2 10.1.36.2
   56 Jan  5 09:54:37 Up
   55 Jan  5 09:54:37 Originate Call
[...Output truncated...]
```

What It Means This LSP event indicates that the recorded route for the session was taken from the Record Route Object (RRO). Address 10.1.13.2 is the IP address of the transit router R3, and address 10.1.36.2 is the IP address of the egress router.

ResvTear Received Event

LSP Event ResvTear received

Sample Output

```
user@R1> show mpls lsp extensive
[...Output truncated...]
    23 Dec 28 13:46:39 CSPF failed: no route toward 10.0.0.6
   22 Dec 28 13:46:39 Clear Call
   21 Dec 28 13:46:39 ResvTear received
   20 Dec 28 13:46:39 Down
   19 Dec 28 13:46:39 10.1.13.2: Session preempted
   18 Dec 28 13:42:07 Selected as active path
[...Output truncated...]
```

What It Means This LSP event indicates that an RSVP ResvTear message was received. ResvTear messages remove RSVP reservation states along a path. These messages travel upstream toward senders of the session. This message usually appears in the middle of a run of messages that tear the LSP down.

Cause In some cases, an ResvTear event is received because a router's reservation state times out. In other cases, when the downstream link fails, the upstream node must eliminate all RSVP states and initiates a ResvTear event. If you are running Fast ReRoute, the upstream node initiates a PathErr message, not a ResvTear message. It is beyond the scope of this document to include all possible reasons for an ResvTear event.

Action Analyze the status to determine if this is the required behavior. If this is not the required behavior, verify the surrounding LSP events to identify the cause of the problem.

RSVP Disabled Event

LSP Event RSVP disabled

Sample Output

```
user@R1> show mpls lsp extensive
[...Output truncated...]
   49 Jan  4 18:10:44 RSVP Disabled
   48 Jan  4 18:10:44 RSVP error, subcode 4: protocol shutdown
   47 Jan  4 18:10:44 Down
[...Output truncated...]
```

What It Means This LSP event indicates that the RSVP was specifically disabled, as opposed to not configured.

Cause This is a local router error message indicating that the RSVP protocol was either disabled at the [edit protocols] hierarchy level, or an interface was omitted from the RSVP configuration.

Action To enable the RSVP protocol if it was disabled, enter the activate rsvp command at the [edit protocols] hierarchy level. If an interface was omitted from the RSVP configuration, include the interface at the [edit protocols rsvp] hierarchy level

RSVP Error Event

LSP Event RSVP error

Sample Output 1

```
user@R1> show mpls lsp extensive
[...Output truncated...]
   50 Jan  4 18:10:44 CSPF: link down/deleted
10.1.13.1(R1.00/10.0.0.1)->10.1.13.2(R3.00/10.0.0.3)
   49 Jan  4 18:10:44 RSVP Disabled
   48 Jan  4 18:10:44 RSVP error, subcode 4: protocol shutdown
   47 Jan  4 18:10:44 Down
   46 Jan  4 18:06:15 Up
   45 Jan  4 18:06:15 Down
[...Output truncated...]
```

Sample Output 2

```
user@R1> show mpls lsp extensive
[...Output truncated...]
9 Jan 14 14:21:01 Deselected as active
8 Jan 14 14:21:01 10.0.22.2: RSVP error, subcode 4: protocol shutdown
7 Jan 14 14:21:01 ResvTear received
6 Jan 14 14:21:01 Down
5 Jan 14 12:35:16 Selected as active path
4 Jan 14 12:35:16 Record Route: 10.0.21.2 10.0.22.2 10.0.29.2
3 Jan 14 12:35:16 Up
2 Jan 14 12:35:16 Originate Call
1 Jan 14 12:35:16 CSPF: computation result accepted
[...Output truncated...]
```

What It Means This LSP event indicates that an RSVP error object was received and RSVP was disabled. For a list of error codes, see Table 21 on page 150. For more information on RSVP error codes, see RFC 2205, *Resource ReSerVation Protocol (RSVP), Version 1*, *Functional Specification,* or RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels*.

Cause Sample Output 1 shows that the protocol was disabled on the ingress router. Sample Output 2 shows that the router with the IP address 10.0.22.2 notified the ingress router that RSVP was disabled.

Action To bring the LSP back up, enable RSVP at the [edit protocols] hierarchy level.

Selected as Active Path Event

LSP Event Selected as active path

Sample Output

```
user@R1> show mpls lsp extensive
[...Output truncated...]
   44 Jan  4 18:06:10 Selected as active path
   43 Jan  4 18:06:09 Record Route:  10.1.13.2 10.1.36.2
[...Output truncated...]
```

What It Means This LSP event indicates that the LSP is up and selected as the active path. Conversely, an LSP can be up, but not active. See “Up Event” on page 18 for more information.

Session Preempted Event

LSP Event Session preempted

Sample Output 1

```
user@R1> show mpls lsp extensive
[...Output truncated...]
    21 Dec 28 13:46:39 ResvTear received
   20 Dec 28 13:46:39 Down
   19 Dec 28 13:46:39 10.1.13.2: Session preempted
   18 Dec 28 13:42:07 Selected as active path
   17 Dec 28 13:42:07 Record Route:  10.1.13.2 10.1.36.2
[...Output truncated...]
```

Sample Output 2

```
user@R1> show mpls lsp extensive
[...Output truncated...]
   66 Jan  5 09:58:33 CSPF failed: no route toward 10.0.0.6
   65 Jan  5 09:58:33 Clear Call
   64 Jan  5 09:58:33 Session preempted
   63 Jan  5 09:58:33 Down
   62 Jan  5 09:58:32 CSPF failed: no route toward 10.0.0.6[2 times]
61 Jan  5 09:57:55 10.1.36.2: Explicit Route: wrong delivery
   60 Jan  5 09:57:34 CSPF failed: no route toward 10.0.0.6[2 times]
   59 Jan  5 09:57:28 CSPF: link down/deleted
10.1.36.1(R3.00/10.0.0.3)->10.1.36.2(R6.00/10.0.0.6)
[...Output truncated...]
```

What It Means This LSP event indicates that the LSP session was taken over. Sample Output 1 shows the IP address (10.1.13.2) included with the event, indicating the IP address of the router that sent the message. Sample Output 2 does not include an IP address, indicating that the message originated on the ingress router.

Cause The state of the network might have changed, as shown in Sample Output 1, or an LSP with a higher priority might be using the bandwidth of the LSP.

Action Refer to the events preceding this event in the history log for more information on what might have caused the preemption. For example, in line 62, the CSPF failed message may indicate that you specified a disable constrained-path (no-cspf) LSP and an explicit route address that is strict and not directly connected. Additionally, the egress router might have changed its configuration, making the destination address unreachable.

Up Event

LSP Event Up

Sample Output

```
user@R1> show mpls lsp extensive
[...Output truncated...]
   48 Jan  4 18:10:44 RSVP error, subcode 4: protocol shutdown
   47 Jan  4 18:10:44 Down
   46 Jan  4 18:06:15 Up
   45 Jan  4 18:06:15 Down
[...Output truncated...]
```

What It Means This LSP event indicates the state of the LSP on January 4 at 1800 hours, 6 minutes, and 15 seconds. The LSP was able to forward traffic, but was not necessarily the active path, it was simply up. For example, an LSP can be up but not active when it is a secondary LSP configured with the standby statement at the [edit protocols mpls] hierarchy level. Similarly, a primary LSP may have failed while waiting for two retry intervals before the LSP reverts back from the secondary LSP to the primary LSP.

Chapter 2

Understanding General LSP Error Events

This chapter describes general label-switched path (LSP) error events that might occur in the output of the show mpls lsp extensive command. Various network configurations demonstrate LSP error events. Descriptions typically include sample output of the LSP event, an explanation of what the event means, the possible cause of the event, and any possible actions that you can take. (See Table 6.)

Table 6: Checklist for Understanding LSP Status Events

Understanding LSP Status Events Tasks	Possible Action or Command
Displaying General LSP Error Events on page 21	show mpls lsp extensive
1. Admission Control Failure Event on page 21	Not applicable.
2. Explicit Route: Bad Loose Route Event on page 22	Check the LSP configuration at the [edit protocols mpls] hierarchy level.
3. Explicit Route: Bad Strict Route Event on page 23	Examine the strict hop address, remove the no-cspf statement, or examine the path and verify that RSVP is enabled on each interface.
4. Explicit Route: Format Error Event on page 25	Analyze this event, and refer to events on either side to determine the appropriate action.
5. Explicit Route: Wrong Delivery Event on page 25	Take appropriate action: ■ Include the loopback (lo0) interface at the [edit protocols isis] hierarchy level. ■ Change the definition of the strict path at the [edit protocols mpls path path-name] hierarchy level. ■ Verify the validity of all IP addresses listed in the named path referenced by the LSP hop by hop.
6. Invalid Destination Address Event on page 26	Verify that the LSP destination address is not the local router's loopback address, and check that the addresses on the local router are correctly configured.
7. Invalid Filter for Policing Event on page 27	Not available.
8. MPLS Graceful Restart: Recovery Failed Event on page 27	Check the MPLS logs for more details about the failure.
9. MPLS Label Allocation Failure Event on page 28	Include interfaces at the [edit protocols mpls] hierarchy level, or include the family mpls statement at the [edit interfaces *type-fpc/pic/port*] hierarchy level.
10.Non-RSVP Capable Router Detected Event on page 28	Configure the router in question with RSVP.
11.No Route Toward Destination Event on page 29	Enable RSVP on the transit router's egress interface, or examine the IP configuration of the relevant router.
12.PathErr Received Event on page 30	Not available.

Understanding LSP Status Events Tasks	Possible Action or Command
13.Path MTU Change Event on page 30	Not available.
14.Path Name Undefined or Disabled Event on page 30	Define the named path.
15.Requested Bandwidth Unavailable Event on page 31	Lower the bandwidth of the ingress LSP or traffic-engineer other LSPs off the path.
16.Routing Loop Detected Event on page 32	Examine the strict hop addresses or examine the path in the ERO to determine the cause of the loop.
17.RSVP Error, Subcode 1: Bad Session Destination Address Event on page 33	Not available.
18.RSVP Error, Subcode 4: Protocol Shutdown Event on page 33	Check the RSVP configuration on the router in question.
19.RSVP Error, Subcode 6: No Non-lsp Route Event on page 34	Find the node with the error and confirm that the ERO route to the next hop takes an LSP next hop. Also, you can configure strict hops to avert the problem. For information about configuring strict hops, see the *JUNOS MPLS Applications Configuration Guide.*
20.TTL Expired Event on page 34	Not available.
21.Tunnel Local Repaired Event on page 35	Not available.
22.Unknown Object Class Event on page 36	Not available.
23.Unknown Object Type Event on page 36	Not available.
24.Unsupported Traffic Class Event on page 37	Not available.

Displaying General LSP Error Events

Purpose Display extensive information about LSPs, including the 50 most recent history events and the possible reasons why an LSP failed.

Action To examine error messages, enter the following JUNOS command-line interface (CLI) operational mode command from the ingress router:

```
user@host> show mpls lsp extensive
```

Sample Output

```
user@R1# run show mpls lsp extensive
Ingress LSP: 1 sessions

10.0.0.6
  From: 10.0.0.1, State: Dn, ActiveRoute: 0, LSPname: R1-to-R6
  ActivePath: (none)
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
  Primary                   State: Dn, No-decrement-ttl
    Bandwidth: 100Mbps
   14 Jan 21 15:43:39 Requested bandwidth unavailable[3 times]
   13 Jan 21 15:43:21 Deselected as active
   12 Jan 21 15:43:21 Requested bandwidth unavailable
   11 Jan 21 15:43:21 Clear Call
   10 Jan 21 15:42:32 Selected as active path
    9 Jan 21 15:42:32 Record Route:  10.1.12.2 10.1.26.2
    8 Jan 21 15:42:32 Up
[...Output truncated...]
```

What It Means The sample output from ingress router R1 is a section from the complete output. Typically, the output includes LSP events that led to an LSP failure and the 50 most recent state events. Only one example of a general LSP error event is displayed because it is impossible to provide all of the events described in this chapter in one sequence of log history. For a detailed description of this error event, see "Requested Bandwidth Unavailable Event" on page 31.

For completeness, events not generated by the example network used throughout this book are described to show LSP events that might occur in your network. The output for these events includes the prompt user@host rather than the usual user@R1 prompt.

Admission Control Failure Event

LSP Event Admission control failure

Sample Output Not available.

What It Means This LSP error event indicates that a Resource Reservation Protocol (RSVP) Admission control failure occurred along the LSP path. This event is logged because of on an error notification (PathErr message) received from RSVP for the label-switched path.

Cause This LSP event is caused by inadequate bandwidth on a link along the LSP path. The available bandwidth could not satisfy the requested traffic parameters and no other sessions were pre-emptied to accommodate this request.

Action This error event is not generated by Juniper Networks routers. However, when this event is received by a Juniper Networks router, it appears in the log output of the show mpls lsp extensive command.

Explicit Route: Bad Loose Route Event

LSP Event Explicit Route: bad loose route

Sample Output 1

```
user@R1# run show mpls lsp extensive
Ingress LSP: 1 sessions

10.0.0.6
  From: 10.0.0.1, State: Up, ActiveRoute: 0, LSPname: R1-R6-3
  ActivePath: R6-3-1 (secondary)
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
  Primary   R6-3              State: Dn
   10 Feb 15 21:21:58 Explicit Route: bad loose route[2 times]
    9 Feb 15 21:21:52 Deselected as active
    8 Feb 15 21:21:51 Explicit Route: bad loose route
    7 Feb 15 21:21:51 10.1.15.1: MPLS label allocation failure
    6 Feb 15 21:21:51 MPLS label allocation failure
    5 Feb 15 21:21:51 Down
    4 Feb 15 21:20:55 Selected as active path
    3 Feb 15 21:20:55 Record Route:  10.1.15.2 10.1.56.2
    2 Feb 15 21:20:55 Up
    1 Feb 15 21:20:55 Originate Call
 *Secondary R6-3-1           State: Up
    Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node 10=SoftPre-
empt):
          10.1.12.2 10.1.26.2
    4 Feb 15 21:21:52 Selected as active path
    3 Feb 15 21:21:52 Record Route:  10.1.12.2 10.1.26.2
    2 Feb 15 21:21:52 Up
    1 Feb 15 21:21:52 Originate Call
  Created: Tue Feb 15 21:20:55 2005
Total 3 displayed, Up 2, Down 1
```

Sample Output 2

```
user@R1# run show protocols mpls
label-switched-path R1-to-R6 {
    to 10.0.0.6;
    bandwidth 155;
    no-cspf;
    link-protection;
    primary to-R6;
}
label-switched-path R1-to-R6-2 {
    to 10.0.0.6;
    link-protection;
    auto-bandwidth {
        adjust-interval 300;
        minimum-bandwidth 1;
```

```
        maximum-bandwidth 1k;
    }
}
label-switched-path R1-R6-3 {
    to 10.0.0.6;
    no-cspf;  <--Allows a loose ERO
    primary R6-3;
    secondary R6-3-1;
}
path to-R6 {
    10.1.15.2 strict;
    10.1.56.2 strict;
}
path R6-3 {
    10.1.15.2 loose;   <--Loose ERO
}
path R6-3-1 {
    10.1.12.2;
}
interface fxp0.0 {
    disable;
}
interface all;
```

What It Means This LSP error event indicates that there is an error in the loose hop specified in the Explicit Route Object (ERO) of a Path message received by a label-switched router (LSR) along the LSP path, indicating an LSP setup failure.

Cause This LSP error event is caused by control plane unreachability or data plane incompatibility.

Action Check the LSP configuration at the [edit protocols mpls] hierarchy level.

Explicit Route: Bad Strict Route Event

LSP Event Explicit route: bad strict route

Sample Output 1

```
user@R1> show mpls lsp extensive
[...Output truncated...]
   36 Jan  4 18:04:57 CSPF: link down/deleted 10.1.13.1(R1.00/10.0.0.1)
->10.1.13.2(R3.00/10.0.0.3)
   35 Jan  4 18:04:57 CSPF failed: no route toward 10.0.0.6
   34 Jan  4 18:04:57 Clear Call
   33 Jan  4 18:04:57 Explicit Route: bad strict route
   32 Jan  4 18:04:57 No Route toward dest
   31 Jan  4 18:04:57 Down
[...Output truncated...]
```

Sample Output 2

```
user@host> show mpls lsp extensive
Ingress LSP: 34 sessions

10.172.2.99
From: 10.172.162.18, State: Up, ActiveRoute: 3726, LSPname:
dcr2.den_to_dcr1.chd_P
ActivePath: P1_dcr2.den_to_dcr1.chd (primary)
LoadBalance: Random
Metric: 25
```

```
Encoding type: Packet, Switching type: Packet, GPID: IPv4
*Primary P1_dcr2.den_to_dcr1.chd State: Up
Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node
10=SoftPreempt):
10.70.192.134
16 Jun 28 18:27:51 Selected as active path
15 Jun 28 18:27:51 Record Route: 10.70.192.134
14 Jun 28 18:27:51 Up
13 Jun 28 18:27:29 Deselected as active
12 Jun 28 18:27:28 No Route toward dest
11 Jun 28 18:27:28 Down
10 Jun 18 03:52:18 Selected as active path
9 Jun 18 03:52:18 Record Route: 10.70.192.134
8 Jun 18 03:52:18 Up
7 Jun 18 03:52:18 Originate Call
6 Jun 18 03:52:18 Clear Call
5 Jun 18 03:52:18 Deselected as active
4 Jun 18 02:56:25 Selected as active path
3 Jun 18 02:56:25 Record Route: 10.70.192.134
2 Jun 18 02:56:25 Up
1 Jun 18 02:56:25 Originate Call
Standby B1_dcr2.den_to_dcr1.chd State: Dn
18 Jun 29 12:49:21 10.70.192.26: Routing loop detected[4798 times]
17 Jun 27 00:53:42 10.70.192.77: Explicit Route: bad strict route[20 times]
16 Jun 27 00:39:49 204.70.192.26: Routing loop detected [3370 times]
[...Output truncated...]
```

What It Means This LSP event indicates that a poorly formed ERO was generated. Sample Outputs 1 and 2 show that this LSP event was caused by different situations described below.

Cause This LSP event can be caused by several factors:

- A strict hop address specified for an LSP on a link that does not have RSVP enabled.
- The no-cspf statement included in the LSP configuration.
- An error with the configuration of constraints on a Constrained Shortest Path First (CSPF) LSP generates the CSPF: No route towards dest message, followed by the Explicit Route: bad strict route event.
- An ERO that causes a routing loop. See Sample Output 2.

Action Examine the strict hop address, remove the no-cspf statement, or examine the path and verify that RSVP is enabled on each interface.

Explicit Route: Format Error Event

LSP Event Explicit route: format error

Sample Output

```
user@R1> show mpls lsp extensive
[...Output truncated...]
10.0.0.6
  From: 10.0.0.1, State: Dn, ActiveRoute: 0, LSPname: R1-to-R6
  ActivePath: (none)
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
  Primary   to-R6            State: Dn, No-decrement-ttl
    5 Jan 21 14:37:06 10.1.34.2: Explicit Route: format error[2 times]
    4 Jan 21 14:37:03 Originate Call
    3 Jan 21 14:37:03 Clear Call
[...Output truncated...]
```

What It Means This LSP event indicates an LSP setup failure in which a Path message error in the the ERO was received by a router along the LSP path.

Cause This LSP event can be caused by several factors:

- An incorrectly formed ERO in the RSVP Path message.
- A strict hop address specified in the middle of an ERO that is not contiguous.
- An unsupported subobject in the ERO of a router along the LSP path.
- The hop indicated by the RSVP hop object does not match the hop indicated by the ERO.

Action Examine the strict hop address configuration and make any necessary changes.

Explicit Route: Wrong Delivery Event

LSP Event Explicit route: wrong delivery

Sample Output 1

```
user@host> show mpls lsp extensive
[...Output truncated...]
Primary use-TOKYO State: Dn, No-decrement-ttl
   3 Sep 19 00:25:45 10.222.45.2: Explicit Route: wrong delivery
   2 Sep 19 00:25:34 No Route[8 times]
   1 Sep 19 00:23:01 Originate Call
[...Output truncated...]
```

Sample Output 2

```
user@host> show mpls lsp extensive
[...Output truncated...]
10.0.0.6
  From: 10.0.0.1, State: Dn, ActiveRoute: 0, LSPname: R1-to-R6
  ActivePath: (none)
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
  Primary   to-R6            State: Dn
   40 Jan 26 16:35:26 10.1.36.2: Explicit Route: wrong delivery[2 times]
   39 Jan 26 16:35:23 Originate Call
   38 Jan 26 16:35:23 Clear Call
[...Output truncated...]
```

Sample Output 3

```
user@R1> show configuration protocols mpls
label-switched-path R1-to-R6 {
    to 10.0.0.6;
    no-cspf;
    primary to-R6;
}
path to-R6 {
    10.1.13.2 strict;
    10.1.56.1 strict;      <<< IP address not directly connected to 10.1.13.2
    10.1.26.1 strict;
```

What It Means This LSP event indicates that a RSVP message with an ERO arrived at the wrong router, even though a strict route was specified. The receiving router determines that the address is inconsistent with the ERO, and generates the error message. Note that the IP address of the sending router precedes the error event; for example, 10.222.45.2 in Sample Output 1, and 10.1.36.2 in Sample Output 2.

Cause This LSP event can be caused by several factors:

- The loopback (lo0) interface on the ingress router is not configured at the [edit protocols isis] hierarchy level. After the loopback (lo0) interface is included in the Intermediate System-to-Intermediate System (IS-IS) configuration, and while IS-IS is forming adjacencies, an RSVP packet is forwarded to an incorrect destination, 10.222.45.2, as shown in Sample Output 1.

- A strict path is configured to a directly connected router, then another strict path is configured to an IP address that is not directly connected. For example, Sample Output 3 shows that the path to-R6 includes three IP addresses, one of which (10.1.56.1) is not directly connected to the other IP addresses in the path.

Action Take appropriate action. On the ingress router, include the loopback (lo0) interface at the [edit protocols isis] hierarchy level, change the definition of the strict path at the [edit protocols mpls path *path-name*] hierarchy level, or verify the validity of all IP addresses listed in the named path referenced by the LSP hop by hop.

Invalid Destination Address Event

LSP Event Invalid Dest addr

Sample Output

```
user@R1> show mpls lsp extensive
Ingress LSP: 1 sessions

10.0.0.1
  From: 10.0.0.1, State: Dn, ActiveRoute: 0, LSPname: R1-to-R6
  ActivePath: (none)
  LoadBalance: Random
  Metric: 100
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
  Primary                    State: Dn
    4 Apr 22 10:22:15 Invalid Dest Addr
    3 Apr 22 10:22:15 Originate Call
```

```
    2 Apr 22 10:22:15 Invalid Dest Addr
    1 Apr 22 10:22:15 Originate Call
  Created: Fri Apr 22 10:22:16 2005
Total 1 displayed, Up 0, Down 1
```

What It Means This LSP event indicates that the to address configured at the [edit protocols mpls labeled-switched-path *name*] hierarchy level is invalid.

Cause This LSP event is caused when the to address of the LSP is the loopback address of the ingress router. A contributing factor may be that the no-cspf statement is included in the LSP configuration.

Action Verify that the LSP destination address is not the local router's loopback address, and check that the addresses on the local router are correctly configured.

Invalid Filter for Policing Event

LSP Event Invalid filter for policing

Sample Output Not available. This LSP event indicates an abnormal condition and is difficult to recreate.

What It Means Although a policer was configured on the LSP, the corresponding firewall filter index was not found, indicating a failure in the routing protocol process (rpd) or the firewall process (dfwd).

Cause A possible cause is that the routing protocol process (rpd) or the firewall process (dfwd) were restarted in a situation in which the LSP was established.

Action Not available.

MPLS Graceful Restart: Recovery Failed Event

LSP Event MPLS graceful restart: recovery failed

Sample Output Not available.

What It Means This LSP event indicates unsuccessful recovery of an LSP path after graceful restart, resulting in potential traffic loss.

Cause This LSP event is caused by several factors:

- MPLS graceful restart procedures may have been aborted by this LSR.
- MPLS graceful restart is disabled, by configuration, during the recovery period.
- An MPLS LSP path is disabled either due to a configuration change or due to an error during the recovery period.
- CSPF computation failed for the restarted LSP path with parameters and constraints preserved across the restart.

- A signaling failure occurred and an RSVP PathErr was received on the LSP path signaled after a restart.
- A network failure occurred on some hop that the LSP was traversing during the recovery period.

Action Check the MPLS logs for more details about the failure.

MPLS Label Allocation Failure Event

LSP Event MPLS label allocation failure

Sample Output

```
user@R1> show mpls lsp extensive
[...Output truncated...]
   24 Jan 20 09:25:35 CSPF failed: no route toward 10.0.0.6
   23 Jan 20 09:25:35 Clear Call
   22 Jan 20 09:25:35 Deselected as active
   21 Jan 20 09:25:35 10.1.13.1: MPLS label allocation failure
   20 Jan 20 09:25:34 MPLS label allocation failure
   19 Jan 20 09:25:34 Down
[...Output truncated...]
```

What It Means This LSP event indicates that the MPLS protocol or the family mpls statement were not configured properly. When the LSP event is preceded by an IP address, the address is typically the router that has the MPLS configuration error.

Cause This LSP event is caused by the omission of interfaces at the [edit protocols mpls] hierarchy level or failure to configure the family mpls statement at the [edit interfaces *type-fpc/pic/port*] hierarchy level. The family mpls statement specifies to the interface ASICs to permit protocol code 0x8847 (unicast MPLS) into the router.

Action Include interfaces at the [edit protocols mpls] hierarchy level, or include the family mpls statement at the [edit interfaces *type-fpc/pic/port*] hierarchy level. You must configure the family mpls statement, in the same way that you must configure the family iso statement for IS-IS.

NOTE: Do not configure the family mpls statement on the loopback (lo0) interface.

Non-RSVP Capable Router Detected Event

LSP Event Non-RSVP capable router detected

Sample Output

```
user@host> show mpls lsp extensive
[...Output truncated...]
10.0.0.6
  From: 10.0.0.1, State: Dn, ActiveRoute: 0, LSPname: R1-to-R6
  ActivePath: (none)
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
  Primary                   State: Dn, No-decrement-ttl
   19 Jan 21 15:05:37 10.1.24.2: Non-RSVP capable router detected
   18 Jan 21 15:04:52 10.1.26.2: Non-RSVP capable router detected[4 times]
```

```
   17 Jan 21 15:04:34 Originate Call
   16 Jan 21 15:04:34 Clear Call
[...Output truncated...]
```

What It Means This LSP event indicates that a router, forwarding packets to the egress router, was not configured for RSVP.

Cause This LSP event might be caused when a router not configured for RSVP forwards an RSVP packet toward the egress router without decrementing the Send_TTL value in the RSVP common header. The next downstream router detects that the Send_TTL value and the IP_TTL value are different, and generates this LSP event. Note that two different routers generated the same error message at different times.

Action Configure the router in question with RSVP.

No Route Toward Destination Event

LSP Event No route toward destination

Sample Output 1

```
user@R1> show mpls lsp extensive
[...Output truncated...]
   35 Oct 26 22:48:36 Down
   34 Oct 26 22:48:29 CSPF failed: no route toward 10.0.0.1[4 times]
   33 Oct 26 22:47:25 CSPF: link down/deleted
10.1.13.2(R3.00/10.0.0.3)->10.1.13.1(R1.00/10.0.0.1)
   32 Oct 26 22:47:25 CSPF failed: no route toward 10.0.0.1
   31 Oct 26 22:47:25 10.1.36.1: No Route toward dest
   30 Oct 26 22:33:54 Selected as active path
   29 Oct 26 22:33:53 Record Route:  10.1.36.1 10.1.13.1
[...Output truncated...]
```

Sample Output 2

```
user@R1> show mpls lsp extensive
[...Output truncated...]
10.0.0.6
  From: 10.0.0.1, State: Dn, ActiveRoute: 0, LSPname: R1-to-R6
  ActivePath: (none)
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
  Primary                   State: Dn
    Will be enqueued for recomputation in 7 second(s).
   13 Oct 25 16:29:28 Deselected as active
   12 Oct 25 16:29:27 CSPF failed: no route toward 10.0.0.6
   11 Oct 25 16:29:27 CSPF: link down/deleted
10.1.13.1(R1.00/10.0.0.1)->10.1.13.2(R3.00/10.0.0.3)
   10 Oct 25 16:29:27 CSPF failed: no route toward 10.0.0.6
    9 Oct 25 16:29:27 Clear Call
    8 Oct 25 16:29:27 Explicit Route: bad strict route
    7 Oct 25 16:29:27 No Route toward dest
    6 Oct 25 16:29:27 Down
[...Output truncated...]
```

What It Means This LSP event indicates that the router at address 10.1.36.1 in Sample Output 1 does not have a route to the specified destination. Sample Output 2 shows that the local router, ingress router 10.0.0.1, does not have a route to the specified destination.

Cause This LSP event is caused by different factors. The egress interface of a transit router might not have RSVP enabled, or IP reachability to the destination (either the egress router or the next address in the ERO) does not exist.

Action Enable RSVP on the transit router's egress interface, or examine the IP configuration of the relevant router.

PathErr Received Event

LSP Event PathErr received

Sample Output Not available.

What It Means This LSP error event indicates that an RSVP signaling error occurred along the LSP path and a PathErr message was sent back to the ingress LSR reporting the problem. If the failed link can be determined, depending on the RSVP signaling error reported, the failed link is not used while a new path is computed. This is an asynchronous event, occurring the first time the LSP is set up or after the LSP has been set up for some time.

Cause An RSVP signaling failure along the LSP path.

Action Not available.

Path MTU Change Event

LSP Event Path MTU change

Sample Output Not available.

What It Means This LSP event indicates that the RSVP path maximum transmission unit (MTU) value has changed and the MTU on the next hop was updated.

Cause Not available.

Action Not available.

Path Name Undefined or Disabled Event

LSP Event Path name undefined or disabled

Sample Output 1

```
user@host> show mpls lsp extensive
[...Output truncated...]
10.0.0.6
  From: 0.0.0.0, State: Dn, ActiveRoute: 0, LSPname: R1-to-R6
  ActivePath: (none)
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
  Primary   to-R6            State: Dn
        No computed ERO.
    1 Jan 26 16:40:49 Path name undefined or disabled[4 times]
[...Output truncated...]
```

Sample Output 2

```
user@host> show configuration protocols mpls
[...Output truncated...]
label-switched-path R1-to-R6 {
    to 10.0.0.6;
    primary to-R6;  <<< the path to-R6 is not defined
}
[...Output truncated...]
```

Sample Output 3

```
user@R1> show configuration protocols mpls
label-switched-path R1-to-R6 {
    to 10.0.0.6;
    primary to-R6;
}
path to-R6;     <<< the path is now defined
[...Output truncated...]
```

What It Means This LSP event indicates that the ingress router referenced a named path, but did not define it. The configuration was committed, but with a warning message.

Cause This LSP event is caused when you configure a primary LSP, primary/secondary LSP, or static LSP, and do not define the named path. For example, the LSP path primary to-R6 (shown in Sample Output 2), is not defined at the [edit protocols mpls] hierarchy level. RSVP does not signal this message.

Action Define the named path at the [edit protocols mpls] hierarchy level, as shown in Sample Output 3. For each path, specify some or all transit routers in the path, or leave the path empty, as shown in Sample Output 3. For more information on the configuration of named paths, see the *JUNOS MPLS Applications Configuration Guide*.

Requested Bandwidth Unavailable Event

LSP Event Requested Bandwidth Unavailable

Sample Output 1

```
user@R1> show mpls lsp extensive
[...Output truncated...]
10.0.0.6
  From: 10.0.0.1, State: Dn, ActiveRoute: 0, LSPname: R1-to-R6
  ActivePath: (none)
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
  Primary                   State: Dn, No-decrement-ttl
    Bandwidth: 100Mbps
   14 Jan 21 15:43:39 Requested bandwidth unavailable[3 times]
   13 Jan 21 15:43:21 Deselected as active
   12 Jan 21 15:43:21 Requested bandwidth unavailable
   11 Jan 21 15:43:21 Clear Call
   10 Jan 21 15:42:32 Selected as active path
    9 Jan 21 15:42:32 Record Route:  10.1.12.2 10.1.26.2
    8 Jan 21 15:42:32 Up
[...Output truncated...]
```

Sample Output 2:

```
user@R1> show mpls lsp extensive
10.0.0.6
  From: 10.0.0.1, State: Dn, ActiveRoute: 0, LSPname: R1-to-R6
  ActivePath: (none)
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
```

```
  Primary                    State: Dn, No-decrement-ttl
    Bandwidth: 100Mbps
   31 Jan 21 15:47:40 10.1.12.2: Requested bandwidth unavailable[2 times]
   30 Jan 21 15:47:37 Originate Call
   29 Jan 21 15:47:37 Clear Call
   28 Jan 21 15:47:37 Deselected as active
   27 Jan 21 15:45:12 Record Route:  10.1.12.2 10.1.26.2
   26 Jan 21 15:45:12 Up
[...Output truncated...]
```

What It Means This LSP event indicates that a router could not supply the requested bandwidth. Sample Output 1 was generated by the ingress router, while Sample Output 2 was generated by router 10.1.12.1, since the IP address precedes the LSP event.

Cause This LSP event is caused by the LSP requesting bandwidth that is not available in a router along the paths to the egress router.

Action Lower the bandwidth assignment of the ingress LSP below the amount of bandwidth available along the path to the egress router, or traffic-engineer other LSPs off the path that you want the ingress LSP to follow, freeing up the necessary bandwidth.

Routing Loop Detected Event

LSP Event Routing loop detected

Sample Output 1

```
user@R1> show mpls lsp extensive
[...Output truncated...]
10.0.0.6
  From: 10.0.0.1, State: Dn, ActiveRoute: 0, LSPname: R1-to-R6
  ActivePath: (none)
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
  Primary   to-R6            State: Dn, No-decrement-ttl
   10 Jan 21 14:40:19 10.1.12.1: Routing loop detected
    9 Jan 21 14:40:19 Originate Call
    8 Jan 21 14:40:19 Clear Call
    7 Jan 21 14:40:16 10.1.12.1: Routing loop detected
    6 Jan 21 14:40:16 Clear Call
[...Output truncated...]
```

What It Means This LSP error event indicates that the RSVP message has looped. The IP address of the router that detected the loop precedes the LSP event.

Cause The LSP error event is generated as part of a PathErr or ResvErr RSVP message when the packet goes through a router that is already listed in the Record Route Object (RRO). The RRO keeps a record of every address that the RSVP Path or Resv message transits.

Action Examine the strict hop addresses or examine the path in the ERO to determine the cause of the loop.

RSVP Error, Subcode 1: Bad Session Destination Address Event

LSP Event RSVP error, subcode 1: Bad sess dst addr

Sample Output Not available.

What It Means This LSP error event is a Juniper Networks proprietary error that indicates failure of the RSVP session destination address at the egress LSR.

Cause This LSP error event can be caused by a number of situations. For example, the RSVP session destination is a link, and that link is down.

Action Not available.

RSVP Error, Subcode 4: Protocol Shutdown Event

LSP Event RSVP error, subcode 4: protocol shutdown

Sample Output

```
user@R1> show mpls lsp extensive
Ingress LSP: 1 sessions

10.0.0.6
  From: 10.0.0.1, State: Dn, ActiveRoute: 0, LSPname: R1-to-R6
  ActivePath: (none)
  LoadBalance: Random
  Metric: 100
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
  Primary                    State: Dn
    Will be enqueued for recomputation in 27 second(s).
   164 May 10 18:50:50 CSPF failed: no route toward 10.0.0.6[3 times]
   163 May 10 18:49:52 Clear Call
   162 May 10 18:49:52 CSPF: link down/deleted:
10.1.36.1(R3.00/10.0.0.3)->10.1.36.2(R6.00/10.0.0.6)
   161 May 10 18:49:52 Deselected as active
   160 May 10 18:49:52 10.1.13.2: RSVP error, subcode 4: protocol shutdown
   159 May 10 18:49:52 ResvTear received
   158 May 10 18:49:52 Down
   157 May 10 18:48:19 Selected as active path
   156 May 10 18:48:19 Record Route:  10.1.13.2 10.1.36.2
   155 May 10 18:48:19 Up
[...Output truncated...]
  Created: Fri Apr 29 10:38:54 2005
Total 1 displayed, Up 0, Down 1
```

What It Means This LSP event is a Juniper Networks proprietary error and indicates that the RSVP control plane on an LSR along the path is terminated.

Cause This LSP event is caused when you disable an RSVP configuration, restart the routing protocol process (rpd), or load a new image on an LSR along the LSP path.

Action Check the RSVP configuration on the router in question.

RSVP Error, Subcode 6: No Non-lsp Route Event

LSP Event RSVP error, subcode 6: No non-lsp route

Sample Output

```
user@host> show mpls lsp extensive
Ingress LSP: 1 sessions

192.168.28.1
From: 192.168.0.1, State: Dn, ActiveRoute: 0, LSPname: sj-to-lo
ActivePath: (none)
LoadBalance: Random
Encoding type: Packet, Switching type: Packet, GPID: IPv4
Primary State: Dn
87 Sep 18 08:23:12 Deselected as active
86 Sep 18 08:23:12 RSVP error, subcode 6: No non-lsp route
85 Sep 18 08:23:12 Down
84 Sep 18 08:23:12 RSVP error, subcode 6: No non-lsp route
83 Sep 18 08:23:07 Selected as active path
82 Sep 18 08:23:07 Record Route: 10.0.1.1 10.0.24.2 10.0.29.1
81 Sep 18 08:23:07 Up
80 Sep 18 08:22:27 Deselected as active
79 Sep 18 08:22:27 RSVP error, subcode 6: No non-lsp route
78 Sep 18 08:22:27 Down
77 Sep 18 08:22:27 RSVP error, subcode 6: No non-lsp route
76 Sep 18 08:22:22 Selected as active path
75 Sep 18 08:22:22 Record Route: 10.0.1.1 10.0.24.2 10.0.29.1
74 Sep 18 08:22:22 Up
[...Output truncated...]
```

What It Means This LSP event indicates that RSVP Path messages for one LSP are tunneled into another RSVP LSP along the LSP path. Non-adjacent RSVP signaling is not currently supported on Juniper Networks LSRs, resulting in a path setup failure. This error is reported only by a Juniper Networks LSR.

Cause This LSP event is most likely to occur when an LSP configured with the no-cspf statement and loose hops is in a Multiprotocol Label Switching (MPLS) network configured with interior gateway protocol (IGP) shortcuts or LSP advertisements.

Action Find the node with the error and confirm that the ERO route to the next hop takes an LSP next hop. Also, you can configure strict hops to avert the problem. For information about configuring strict hops, see the *JUNOS MPLS Applications Configuration Guide*.

TTL Expired Event

LSP Event TTL expired

Sample Output Not available.

What It Means This LSP error event indicates that the time to live (TTL) in the RSVP header of a received Path message is zero.

Cause Not available.

Action Not available.

Tunnel Local Repaired Event

LSP Event Tunnel local repaired

Sample Output

```
10.0.0.6
  From: 10.0.0.1, State: Up, ActiveRoute: 0, LSPname: R1-R6-3
  ActivePath:  (primary)
  FastReroute desired
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
 *Primary                    State: Up
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 20)
 10.1.12.2 S 10.1.26.2 S
    Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node
10=SoftPreempt):
          10.1.12.2(flag=1) 10.1.26.2
   24 Feb 15 20:56:12 Record Route:  10.1.12.2(flag=1) 10.1.26.2
   23 Feb 15 20:56:11 Fast-reroute Detour Up
   22 Feb 15 20:56:09 Record Route:  10.1.12.2 10.1.26.2
   21 Feb 15 20:56:09 Up
   20 Feb 15 20:56:09 CSPF: computation result accepted
   19 Feb 15 20:56:09 CSPF: link down/deleted
10.1.15.1(R1.00/10.0.0.1)->10.1.15.2(R5.00/10.0.0.5)
   18 Feb 15 20:56:09 Record Route:  10.1.12.2 10.1.26.2
   17 Feb 15 20:56:09 Up
   16 Feb 15 20:56:08 CSPF: computation result accepted
   15 Feb 15 20:56:08 Tunnel local repaired
   14 Feb 15 20:56:08 CSPF: computation result accepted
   13 Feb 15 20:56:08 10.1.15.1: MPLS label allocation failure
   12 Feb 15 20:56:08 MPLS label allocation failure
   11 Feb 15 20:56:08 Record Route:  10.1.13.2 10.1.36.2
   10 Feb 15 20:56:08 Down
    9 Feb 15 20:52:56 Fast-reroute Detour Up
    8 Feb 15 20:52:53 Fast-reroute Detour Down
    7 Feb 15 20:50:00 Record Route:  10.1.15.2(flag=1) 10.1.56.2
    6 Feb 15 20:50:00 Fast-reroute Detour Up
    5 Feb 15 20:49:57 Selected as active path
    4 Feb 15 20:49:57 Record Route:  10.1.15.2 10.1.56.2
    3 Feb 15 20:49:57 Up
    2 Feb 15 20:49:56 Originate Call
    1 Feb 15 20:49:56 CSPF: computation result accepted
  Created: Tue Feb 15 20:49:56 2005
Total 3 displayed, Up 2, Down 1
```

What It Means This LSP error event indicates to the head-end (ingress) router that a local protection path was used when a link or node failed along the protected LSP path. Also, the LSR received a PathErr message from RSVP for the label-switched path.

Cause This LSP error event is caused by a network failure along an LSP path that is locally protected with either a bypass LSP or fast reroute detour. In this case, the failure occurred when the primary link was deactivated, resulting in the fast reroute detour repairing the tunnel.

Action Not available.

Unknown Object Class Event

LSP Event Unknown object class

Sample Output Not available. This LSP event indicates an abnormal condition and is difficult to recreate.

What It Means This LSP error event indicates that the LSR received a PathErr message from RSVP for the label-switched path.

Cause This LSP error event is caused when an LSR along the LSP path receives an RSVP object with a class number that is unsupported by the LSR.

Action Not available.

Unknown Object Type Event

LSP Event Unknown Object type: recovery label

Sample Output

```
user@R1> show mpls lsp extensive
Ingress LSP: 1 sessions

10.0.0.6
  From: 10.0.0.1, State: Up, ActiveRoute: 0, LSPname: R1-to-R6
  ActivePath:  (primary)
  LoadBalance: Random
  Metric: 100
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
 *Primary                    State: Up
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 20)
 10.1.15.2 S 10.1.56.2 S
    Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node
10=SoftPreempt):
          10.1.15.2 10.1.56.2
   17 Mar 29 20:36:07 Selected as active path
   16 Mar 29 20:36:07 Record Route:  10.1.15.2 10.1.56.2
   15 Mar 29 20:36:07 Up
   14 Mar 29 20:36:07 Originate Call
   13 Mar 29 20:36:07 CSPF: computation result accepted
   12 Mar 29 20:35:37 CSPF failed: no route toward 10.0.0.6
   11 Mar 29 20:35:37 Clear Call
   10 Mar 29 20:35:37 Deselected as active
    9 Mar 29 20:35:37 Session preempted
    8 Mar 29 20:35:37 Down
    7 Mar 29 20:34:49 10.1.15.2: Unknown Object type:recovery label
    6 Mar 29 20:29:09 Selected as active path
    5 Mar 29 20:29:09 Record Route:  10.1.15.2 10.1.56.2
```

What It Means This LSP error event indicates that the LSR received a PathErr message from RSVP for the label-switched path.

Cause This LSP event is caused when an LSR receives an RSVP object with a class type that the LSR does not support.

Action Not available.

Unsupported Traffic Class Event

LSP Event Unsupported traffic class

Sample Output Not available. This LSP event indicates an abnormal condition and is difficult to recreate.

What It Means This LSP error event is a Juniper Networks proprietary error, indicating that a Diffserv-traffic engineering (TE) LSP was signaled with one or more traffic classes with values greater than the four traffic classes currently supported.

Cause Not available.

Action Not available.

Chapter 3

Understanding CSPF Events

This chapter lists and describes Constrained Shortest Path First (CSPF) events that occur in the output of the show mpls lsp extensive command, including sample output of the label-switched path (LSP) event, an explanation of what the event means, the possible cause of the event, and any possible actions that you can take to remedy the situation. (See Table 7.)

Table 7: Checklist for Understanding CSPF Events

Understanding CSPF Events Tasks	Possible Action or Command
Displaying CSPF Events on page 40	show mpls lsp extensive
1. CSPF Failed: No Route Toward Event on page 41	show ted database detail Determine if there is a route to the destination. [edit protocols mpls label-switched-path *lsp-path-name*] no-cspf
2. CSPF: Link Down/Deleted Event on page 42	Investigate possible causes for the link failure.
3. CSPF: Computation Result Accepted Event on page 43	Not applicable.
4. CSPF: Computation Result Ignored Event on page 43	Not applicable.
5. CSPF: Could Not Determine Self Event on page 44	Take appropriate action: ■ Enable traffic engineering ■ Configure the family iso statement or address statement ■ Include interfaces at the [edit interfaces], [edit protocols mpls], or [edit protocols isis] hierarchy level
6. CSPF: Can't Find Non-Overlapping Path Event on page 45	Not applicable.
7. CSPF: Reroute Due to Re-Optimization Event on page 45	Not applicable.
8. Retry Limit Exceeded Event on page 46	clear mpls lsp
9. CSPF Failed: Empty Route Event on page 47	Enter the correct IP address at the [edit protocols mpls label-switched-path *lsp-path-name*] hierarchy level.

Displaying CSPF Events

Purpose The ingress router determines the physical path for each LSP by applying a CSPF algorithm to the information in the traffic engineering database (TED). CSPF is a shortest-path-first (SPF) algorithm that has been modified to take into account specific restrictions when calculating the shortest path across a network. Links that do not comply with the restrictions are removed from the tree and cannot be factored into the resulting SPF calculations. When compliant routes cannot be found, the output of the CSPF algorithm is a CSPF event or error message that can appear in the output of the show mpls lsp extensive command.

Action To display CSPF messages, enter the following JUNOS command-line interface (CLI) operational mode command from the ingress router:

```
user@host> show mpls lsp extensive
```

Sample Output

```
user@R1# run show mpls lsp extensive
Ingress LSP: 1 sessions

10.0.0.6
  From: 10.0.0.1, State: Dn, ActiveRoute: 0, LSPname: R1-to-R6
  ActivePath: (none)
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
  Primary                   State: Dn
    Will be enqueued for recomputation in 3 second(s).
   68 Jan  5 10:02:56 CSPF failed: no route toward 10.0.0.6[9 times]
   67 Jan  5 09:58:33 Deselected as active
   66 Jan  5 09:58:33 CSPF failed: no route toward 10.0.0.6
   65 Jan  5 09:58:33 Clear Call
   64 Jan  5 09:58:33 Session preempted
   63 Jan  5 09:58:33 Down
   62 Jan  5 09:58:32 CSPF failed: no route toward 10.0.0.6[2 times]
   61 Jan  5 09:57:55 10.1.36.2: Explicit Route: wrong delivery
   60 Jan  5 09:57:34 CSPF failed: no route toward 10.0.0.6[2 times]
   59 Jan  5 09:57:28 CSPF: link down/deleted
10.1.36.1(R3.00/10.0.0.3)->10.1.36.2(R6.00/10.0.0.6)
   58 Jan  5 09:54:37 Selected as active path
   57 Jan  5 09:54:37 Record Route:  10.1.13.2 10.1.36.2
   56 Jan  5 09:54:37 Up
   55 Jan  5 09:54:37 Originate Call
   54 Jan  5 09:54:37 CSPF: computation result accepted
[...Output truncated...]
```

What It Means The sample output from ingress router R1 shows extensive ingress LSP information, including LSP events that led to an LSP failure, with the most recent events at the top. The last line before the history log begins indicates the length of time the router waits before attempting to re-signal the LSP, three seconds in this instance.

LSP events in bold are described in this chapter. Descriptions include sample output of the LSP event, an explanation of what the event means, the possible cause of the event, and any possible actions that you can take.

For completeness, events not included in this example output are also described in this chapter to show LSP events that did not occur in the example network configuration, but might occur in your network. The output for these events includes the prompt user@host rather than the usual user@R1 prompt.

CSPF Failed: No Route Toward Event

LSP Event CSPF failed: no route toward *ip-address*

Sample Output

```
user@R1> show mpls lsp extensive
[...Output truncated...]
Will be enqueued for recomputation in 3 second(s).
   68 Jan  5 10:02:56 CSPF failed: no route toward 10.0.0.6[9 times]
   67 Jan  5 09:58:33 Deselected as active
   66 Jan  5 09:58:33 CSPF failed: no route toward 10.0.0.6
[...Output truncated...]
```

What It Means This LSP event indicates that the CSPF calculation on the ingress router R1 failed to find a route to the destination, in this case the egress router.

Cause The CSPF calculation to the destination can fail for many reasons, and failures occur frequently. The failures include, but are not limited to:

- A downstream node not configured for the Resource Reservation Protocol (RSVP) or Multiprotocol Label Switching (MPLS).
- The family mpls statement not configured on routers along the LSP path.
- The loopback (lo0) interface not configured at the [edit protocols isis] hierarchy level on the ingress or egress routers
- A faulty Explicit Route Object (ERO) that causes a loop or contains a bad address.

This event always includes an address it cannot reach. The listed address may be the LSP egress address, an ERO address, or an intermediate address.

Action Determine if the node is listed in the traffic engineering database with the show ted database detail command. If necessary, compare the LSP constraints of all links that lead to the address to determine if there is a route to the destination.

NOTE: The CSPF algorithm prunes the database of links that do not comply with LSP constraints, then computes the shortest path from the remaining links.

A ping to an address that is unreachable by CSPF follows the interior gateway protocol (IGP) shortest path, not the CSPF constraints. Therefore, using the ping command to verify the connection does not provide information about why CSPF failed.

To verify whether the problem is a constraint issue, configure your LSP with the no-cspf statement at the [edit protocols mpls label-switched-path *lsp-path-name*] hierarchy level, then determine if the router signals the LSP successfully. If it does, the traffic engineering database contains links that do not comply with your constraints for the LSP.

The CSPF algorithm follows these steps to select a path:

1. Compute 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. Prune the traffic engineering database of all links that are not full duplex and do not have sufficient reservable bandwidth.
3. If the LSP configuration includes the include statement, prune all links that do not share any included colors.
4. If the LSP configuration includes the exclude statement for the LSP, prune all links that contain excluded colors and do not contain a color.
5. Find the shortest path towards 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, choose the path whose last-hop address is the same as the LSP's destination.
7. If several equal-cost paths remain, select the path with the fewest number of hops.
8. If several equal-cost paths remain, apply the CSPF load-balancing rule configured on the LSP (least-fill, most-fill, or random).

CSPF: Link Down/Deleted Event

LSP Event CSPF: link down/deleted

Sample Output

```
user@R1> show mpls lsp extensive
[...Output truncated...]
60 Jan  5 09:57:34 CSPF failed: no route toward 10.0.0.6[2 times]
   59 Jan  5 09:57:28 CSPF: link down/deleted
10.1.36.1(R3.00/10.0.0.3)->10.1.36.2(R6.00/10.0.0.6)
[...Output truncated...]
```

What It Means This LSP event indicates that the traffic engineering database no longer includes this link.

Cause The link probably failed.

Action Investigate possible causes for the link failure. For more information on checking the physical layer, see the *JUNOS MPLS Network Operations Guide*.

CSPF: Computation Result Accepted Event

LSP Event CSPF: computation result accepted

Sample Output

```
user@R1> show mpls lsp extensive
[...Output truncated...]
  57 Jan  5 09:54:37 Record Route:  10.1.13.2 10.1.36.2
   56 Jan  5 09:54:37 Up
   55 Jan  5 09:54:37 Originate Call
   54 Jan  5 09:54:37 CSPF: computation result accepted
[...Output truncated...]
```

What It Means This LSP event indicates that CSPF pruned the traffic engineering database of noncompliant links and found a shortest path. CSPF generated an ERO, which was then passed to the RSVP.

CSPF: Computation Result Ignored Event

LSP Event CSPF: computation result ignored

Sample Output

```
user@host> show mpls lsp extensive
[...Output truncated...]
34 May  8 13:27:39 CSPF failed: no route toward 10.11.2.10
   33 May  8 13:27:39 CSPF: link down/deleted
0.0.0.0(eagle.04/0.0.0.0)->0.0.0.0(papst.00/10.255.11.215)
   32 May  8 13:27:12 CSPF: computation result ignored[16 times]
   31 May  8 13:19:35 Record Route:  10.11.1.9(flag=9 Label=100064)
10.11.1.2(flag=9 Label=100048) 10.11.2.1(flag=1 Label=100048)
[...Output truncated...]
```

What It Means This LSP event indicates that during reoptimization, a CSPF path computation for a potential optimal path is performed. Various checks are carried out to evaluate whether the new path is better than the existing one. If the new path is not considered to be better, the CSPF computation results for the new path are ignored and the new path is not signaled.

Cause There can be various reasons for ignoring computation of a potential optimal path:

- The optimization is purely metric based, so switching to the new path could increase bandwidth congestion on links.
- Switching to the new path could cause preemption.
- The metric of the new path is higher than that of the existing path.
- The metric is the same on the new and existing paths, but the number of hops in the new path is higher than on the existing path.

CSPF: Could Not Determine Self Event

LSP Event CSPF: could not determine self

Sample Output 1

```
user@host# run show ted database extensive
TED database: 10 ISIS nodes
9 INET nodes NodeID: HongKong.00(192.168.16.1)
Type: ---, Age: 148 secs, LinkIn: 1, LinkOut: 0
```

Sample Output 2

```
user@R1# run show ted database detail
TED database: 6 ISIS nodes 6 INET nodes
NodeID: R1.00(10.0.0.1)
  Type: ---, Age: 654 secs, LinkIn: 3, LinkOut: 0
NodeID: R2.00(10.0.0.2)
  Type: Rtr, Age: 642 secs, LinkIn: 3, LinkOut: 4
  Protocol: IS-IS(2)
```

Sample Output 3

```
user@host> show mpls lsp extensive
[...Output truncated...]
192.168.32.1
  From: 0.0.0.0, State: Dn, ActiveRoute: 0, LSPname: HK->AM
  ActivePath: (none)
  FastReroute desired
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
  Primary use-TOKYO State: Dn, No-decrement-ttl
  Will be enqueued for recomputation in 22 second(s).
  1 Sep 19 00:16:22 CSPF: could not determine self
[...Output truncated...]
```

What It Means This LSP event indicates that the traffic engineering database cannot determine the address of the local router. Sample Outputs 1 and 2 show the entry in the traffic engineering database where the node entry Type: — does not indicate a type of router (Rtr) or pseudonode (Net) address. Since the node does not know what type it is, it cannot know its own address.

Cause This LSP event can be caused by several factors. Traffic engineering might not be configured for OSPF, the loopback (lo0) interface might not have the family ISO or an ISO address configured, or the loopback interface might not be included at the [edit interfaces] hierarchy level.

Note that in Sample Output 3, the source address of the LSP is 0.0.0.0 since the node does not know its own address. When the From address is 0.0.0.0, it can indicate that interfaces are not included at the [edit protocols mpls] or the [edit protocols isis] hierarchy level.

Action Take the corrective action appropriate to the situation: enable traffic engineering, configure the family iso statement or address statement, or include interfaces at the [edit interfaces], [edit protocols mpls], or [edit protocols isis] hierarchy level.

CSPF: Can't Find Non-Overlapping Path Event

LSP Event CSPF: Can't find non-overlapping path to *ip-address*

Sample Output

```
user@host> show mpls lsp extensive
[...Output truncated...]
Standby    test1           State: Dn
     Bandwidth: 80Mbps
     Will be enqueued for recomputation in 22 second(s).
     1 Apr 9 21:10:47 CSPF: Can't find non-overlapping path to 10.0.3.4[2 times]
  Created: Wed Apr 9 20:40:16 2003
Total 1 displayed, Up 1, Down 0
[...Output truncated...]
```

What It Means This LSP event indicates that CSPF needed to compute an alternate path that did not intersect any other path.

Cause This error appears when running the adaptive feature to run shared explicit (SE)-style reservations, where no nonoverlapping paths are possible.

CSPF: Reroute Due to Re-Optimization Event

LSP Event CSPF: Reroute due to re-optimization

Sample Output

```
user@host> show mpls lsp extensive
[...Output truncated...]
9 Dec 11 17:32:35  Up
    8 Dec 11 17:32:35  Clear Call
    7 Dec 11 17:32:35  CSPF: computation result accepted
    6 Dec 11 17:32:35  CSPF: Reroute due to re-optimization
    5 Dec 11 17:28:29  CSPF: computation result ignored
    4 Dec 11 17:24:23  Record Route:  10.35.38.2 S 192.168.135.29 S
10.35.39.1 S 10.35.40.2 S 10.35.41.1 S
    3 Dec 11 17:24:23  Up
[...Output truncated...]
```

What It Means This LSP event indicates that CSPF found an optimal path for LSP traffic, and switched over to the new path.

Cause This is a periodic or one-time reoptimization event.

Retry Limit Exceeded Event

LSP Event Retry limit exceeded

Sample Output 1

```
user@R1> show mpls lsp extensive
[...Output truncated...]
10.0.0.6
  From: 10.0.0.1, State: Dn, ActiveRoute: 0, LSPname: R1-to-R6
  ActivePath: (none)
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
  Primary                  State: Dn
    RetryCount: 13
    RetryLimit: 1
   12 Jan 14 15:39:30 Clear Call
   11 Jan 14 15:39:30 Retry limit exceeded
   10 Jan 14 15:39:10 10.1.12.1: MPLS label allocation failure[11 times]
[...Output truncated...]
```

Sample Output 2

```
user@R1> show mpls lsp extensive
[...Output truncated...]
10.0.0.6
  From: 10.0.0.1, State: Dn, ActiveRoute: 0, LSPname: R1-to-R6
  ActivePath: (none)
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
  Primary                  State: Dn
   14 Jan 14 15:44:07 10.1.12.1: MPLS label allocation failure[3 times]
   13 Jan 14 15:43:58 Originate Call
   12 Jan 14 15:39:30 Clear Call
   11 Jan 14 15:39:30 Retry limit exceeded
   10 Jan 14 15:39:10 10.1.12.1: MPLS label allocation failure[11 times]
[...Output truncated...]
```

What It Means This LSP event indicates that the number of CSPF path computations for a particular path exceeded a configured retry limit. After this point, the path is not recomputed or signaled, unless the user intervenes.

Cause The number of CSPF path computations for an LSP path exceeded the configured non-zero retry limit. Sample Output 1 shows that a configured retry limit of 1 was exceeded by the retry count of 13.

Action Enter the clear mpls lsp command to disconnect and restart the LSP. Sample Output 2 shows that events 13 and 14 were generated after the clear mpls lsp command was issued. This operation disconnects existing RSVP sessions on the ingress router, releases the routes and states associated with the LSPs, and starts a new LSP. Issuing this command might impact traffic travelling along the LSP, because of a time lag that can occur between the old path being torn down and the new path being set up.

CSPF Failed: Empty Route Event

LSP Event CSPF failed: empty route

Sample Output

```
user@R1> show mpls lsp extensive
[...Output truncated...]
From: 10.0.0.1, State: Dn, ActiveRoute: 0, LSPname: R1-to-R6
  ActivePath: (none)
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
  Primary                   State: Dn
    Will be enqueued for recomputation in 23 second(s).
    1 Jan 13 12:59:47 CSPF failed: empty route 10.0.0.1
  Created: Thu Jan 13 12:59:48 2005
Total 1 displayed, Up 0, Down 1
[...Output truncated...]
```

What It Means This LSP event indicates that the destination route for the LSP is incorrect.

Cause The IP address in the to statement at the [edit protocols mpls label-switched-path *lsp-path-name*] hierarchy level is incorrectly configured as the loopback (lo0) interface of this router itself, as indicated by the From address (10.0.0.1) which is identical to the empty route address (10.0.0.1).

Action Enter the correct IP address for the egress router at the [edit protocols mpls label-switched-path *lsp-path-name*] hierarchy level.

Chapter 4

Understanding Autobandwidth Events

Multiprotocol Label Switching (MPLS) autobandwidth automatically adjusts the bandwidth size of an MPLS traffic-engineered tunnel based on the actual traffic flowing through the tunnel. Autobandwidth success and failure is logged in the output of the show mpls lsp extensive command. For more information on autobandwidth, see the *JUNOS MPLS Applications Configuration Guide*.

This chapter lists and describes autobandwidth events that occur in the output of the show mpls lsp extensive command, including sample output of the label-switched path (LSP) event, an explanation of what the event means, the possible cause of the event, and any specific actions that you can take to remedy the situation. (See Table 8.)

Table 8: Checklist for Understanding Autobandwidth Events

Understanding Autobandwidth Events Tasks	Possible Action or Command
Displaying Autobandwidth Events on page 50	show mpls lsp extensive
Manual Autobandwidth Adjustment on page 53	
1. Manual Autobandwidth Adjustment Failed Event on page 53	Take the corrective action appropriate to the situation: ■ Verify the MPLS and RSVP configurations on all available paths to the LSP endpoint. ■ Check available bandwidth on alternate paths using the show rsvp interface command.
2. Manual Autobandwidth Adjustment Succeeded Event on page 54	Not applicable.
Automatic Autobandwidth Adjustment on page 56	
1. Automatic Autobandwidth Adjustment Failed Event on page 56	Take action appropriate to the situation: ■ Verify the MPLS and RSVP configurations on all available paths to the LSP endpoint. ■ Check available bandwidth on alternate paths using the show rsvp interface command.
2. Automatic Autobandwidth Adjustment Succeeded Event on page 58	Not applicable.

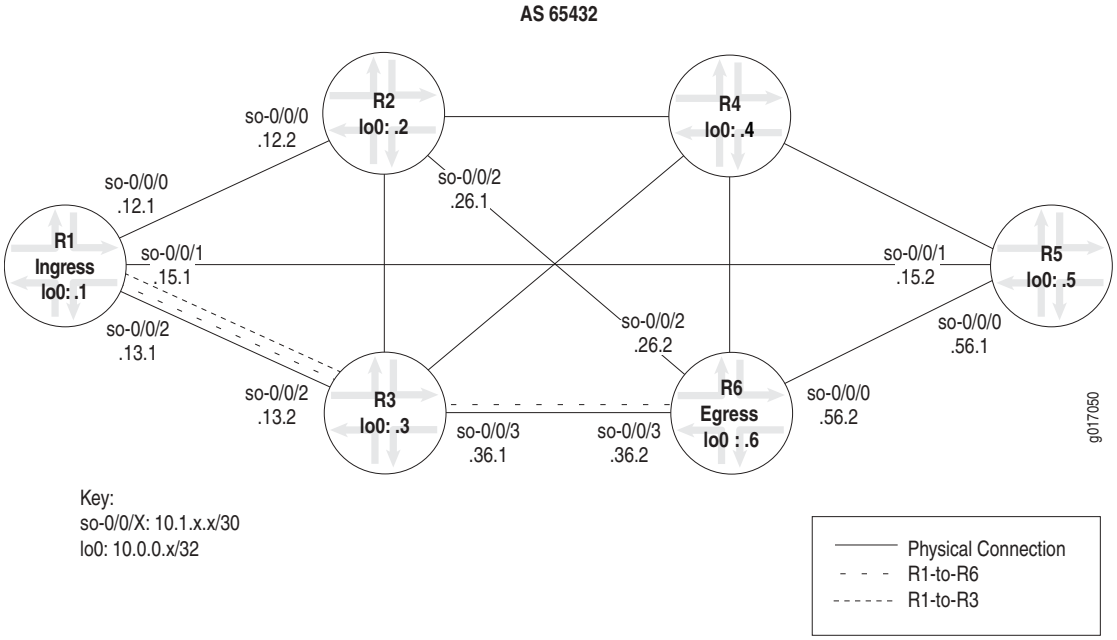
Displaying Autobandwidth Events

Purpose Automatic autobandwidth allocation allows an MPLS tunnel to automatically adjust its bandwidth allocation based on the volume of traffic flowing through the tunnel. Bandwidth allocation is adjusted according to a specified time interval when current maximum average bandwidth usage is compared with the allocated bandwidth for the LSP. If the bandwidth needs adjustment, a path with the new adjusted bandwidth is computed. The LSP's traffic is routed through the new path and the old path is removed.

Manual autobandwidth adjustment is used on the active LSP path when you do not wish to wait for the specified time interval to trigger an autobandwidth adjustment. The minimum specified time interval is 5 minutes (300 seconds) for MPLS LSP automatic bandwidth allocation adjustment. For more information on configuring autobandwidth, see the *JUNOS MPLS Applications Configuration Guide*.

Autobandwidth success and failure is logged in the output of the show mpls lsp extensive command. Figure 1 illustrates the example MPLS network used in this chapter to demonstrate autobandwidth LSP events.

Figure 1: MPLS Network Topology Configured with Autobandwidth



The MPLS network in Figure 1 illustrates a router-only network with SONET interfaces that consists of the following components:

- A full-mesh interior BGP (IBGP) topology, using AS 65432.
- MPLS is enabled on all routers.
- Autobandwidth is configured on ingress router R1.

- To produce the autobandwidth events, Resource Reservation Protocol (RSVP) is disabled on interfaces that could provide an alternate route for the LSP.
- A policy is configured on ingress router R1 that advertises new routes into the network.
- An LSP is established between routers R1 and R3, R1-to-R3.
- An LSP is established between router R1 and R6, R1-to-R6.

The network shown in Figure 1 is a BGP full-mesh network. Since route reflectors and confederations are not used to propagate BGP learned routes, each router must have a BGP session with every other router running BGP.

Action To display autobandwidth events, enter the following JUNOS command-line interface (CLI) operational mode command from the ingress router:

```
user@host> show mpls lsp extensive
```

Sample Output 1

```
user@R1# run show mpls lsp extensive
Ingress LSP: 3 sessions

10.0.0.3
  From: 10.0.0.1, State: Up, ActiveRoute: 5, LSPname: R1-to-R3
  ActivePath:  (primary)
  LoadBalance: Random
  Metric: 1
  Autobandwidth
  MinBW: 155Mbps MaxBW: 155Mbps
  AdjustTimer: 300 secs AdjustThreshold: 10%
  Max AvgBW util: 392bps, Bandwidth Adjustment in 101 second(s).
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
 *Primary                    State: Up
    Bandwidth: 140Mbps
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 10)
 10.1.13.2 S
    Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node
10=SoftPreempt):
          10.1.13.2
   13 Feb 17 21:23:51 Manual Autobw adjustment failed
   12 Feb 17 21:23:51 CSPF failed: no route toward 10.0.0.3
   11 Feb 17 21:16:06 Record Route:  10.1.13.2
   10 Feb 17 21:16:06 Up
    9 Feb 17 21:16:06 Manual Autobw adjustment succeeded
    8 Feb 17 21:16:06 Originate make-before-break call
    7 Feb 17 21:16:06 CSPF: computation result accepted
    6 Feb 17 21:14:51 Selected as active path
    5 Feb 17 21:14:51 Record Route:  10.1.13.2
    4 Feb 17 21:14:51 Up
    3 Feb 17 21:14:51 Originate Call
    2 Feb 17 21:14:51 CSPF: computation result accepted
    1 Feb 17 21:14:22 CSPF failed: no route toward 10.0.0.3[4 times]
[...Output truncated...]
```

Sample Output 2

```
user@R1> show configuration protocols mpls
statistics {
    file auto-bw.log;
    interval 5;
    auto-bandwidth;
}
label-switched-path R1-to-R6 {
    to 10.0.0.6;
    auto-bandwidth {
        adjust-interval 300;
        adjust-threshold 10;
        minimum-bandwidth 5m;
        maximum-bandwidth 80m;
    }
}
label-switched-path R1-to-R3 {
    to 10.0.0.3;
    auto-bandwidth {
        adjust-interval 300;
        adjust-threshold 10;
        minimum-bandwidth 155m;
        maximum-bandwidth 155m;
    }
}
```

What It Means

Sample Output 1 from ingress router R1 shows extensive ingress LSP information, including LSP events that led to an LSP failure, with the most recent events at the top.

The autobandwidth LSP events in bold are described in this chapter. Descriptions include sample output of the LSP event, an explanation of what the event means, the possible cause of the event, and any specific actions that you can take.

For completeness, autobandwidth events not included in this example output are also described in this chapter.

Sample Output 2 shows the configuration of autobandwidth on ingress router R1. LSP R1-to-R3 is configured with 155 MB of bandwidth, and LSP R1-to-R6 is configured with 5 MB of bandwidth. The autobandwidth failure events described in this chapter are created as follows:

- RSVP is disabled on all links except for the links used for the LSP.
- Traffic is sent along LSP R1-to-R6.
- The adjust interval for the LPS R1-to-R3 expires, resulting in no valid usable paths, except for the existing path configured with 155 MB of bandwidth.

Manual Autobandwidth Adjustment

Purpose Manual autobandwidth adjustment is used on the active LSP path when you wish to trigger an autobandwidth adjustment before the next specified automatic bandwidth adjustment.

NOTE: Request for manual autobandwidth adjustment is a feature introduced in JUNOS software Release 7.0.

To manually trigger a bandwidth allocation adjustment, 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. Once you execute the request mpls lsp adjust-autobandwidth 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 set bandwidth value determined during the validation process.

For more information on configuring autobandwidth, see the *JUNOS MPLS Applications Configuration Guide*.

Autobandwidth success and failure is logged in the output of the show mpls lsp extensive command. The following manual autobandwidth adjustment events are included in this section:

- Manual Autobandwidth Adjustment Failed Event on page 53
- Manual Autobandwidth Adjustment Succeeded Event on page 54

Manual Autobandwidth Adjustment Failed Event

LSP Event Manual Autobw adjustment failed

Sample Output

```
user@R1> show mpls lsp extensive
Ingress LSP: 3 sessions

10.0.0.3
  From: 10.0.0.1, State: Up, ActiveRoute: 5, LSPname: R1-to-R3
  ActivePath:  (primary)
  LoadBalance: Random
  Metric: 1
  Autobandwidth
  MinBW: 155Mbps MaxBW: 155Mbps
  AdjustTimer: 300 secs AdjustThreshold: 10%
  Max AvgBW util: 392bps, Bandwidth Adjustment in 101 second(s).
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
 *Primary                    State: Up
    Bandwidth: 140Mbps
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 10)
 10.1.13.2 S
    Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node
10=SoftPreempt):
          10.1.13.2
   13 Feb 17 21:23:51 Manual Autobw adjustment failed
```

```
   12 Feb 17 21:23:51 CSPF failed: no route toward 10.0.0.3
   11 Feb 17 21:16:06 Record Route:  10.1.13.2
   10 Feb 17 21:16:06 Up
[...Output truncated...]
```

What It Means This LSP event indicates that autobandwidth adjustment was triggered manually for the LSP using the request mpls lsp adjust-autobandwidth name *name* command. This adjustment failed, and the LSP continued on the existing path with its current bandwidth. Manual autobandwidth adjustment is a JUNOS Release 7.0 feature that enables you to issue the request mpls lsp adjust-autobandwidth name *name* command to manually adjust the bandwidth.

Cause This LSP event is caused by a Constrained Shortest Path First (CSPF) computation failure or a signaling failure on the new path. When you issue the request mpls lsp adjust-autobandwidth name *name* command, the current maximum average bandwidth usage is compared to 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, traffic on the LSP is routed through the new path and the old path is removed in a make-before-break fashion. If the attempt fails, the traffic on the LSP continues to use its current path.

Action Take the corrective action appropriate to the situation:

- Verify the MPLS and RSVP configurations on all available paths to the LSP endpoint. For more information on verifying the MPLS and RSVP configurations, see the *JUNOS MPLS Network Operations Guide*.
- Check available bandwidth on alternate paths using the show rsvp interface command. If not enough bandwidth is available on any available paths, adjust the minimum-bandwidth parameter for the LSP in order to establish or adjust the priority to allow the LSP to preempt another LSP of lesser priority. For an LSP to be preempted, its hold priority must be lower than the LSP you are trying to establish.

Manual Autobandwidth Adjustment Succeeded Event

LSP Event Manual Autobw adjustment succeeded

Sample Output

```
user@R1> show mpls lsp extensive
[...Output truncated...]
user@R1> request mpls lsp adjust-autobandwidth name R1-to-R6

user@R1> show mpls lsp extensive
Ingress LSP: 3 sessions

10.0.0.6
  From: 10.0.0.1, State: Up, ActiveRoute: 4, LSPname: R1-to-R6
  ActivePath:  (primary)
  LoadBalance: Random
  Metric: 1
  Autobandwidth
  MinBW: 5Mbps MaxBW: 80Mbps
  AdjustTimer: 300 secs AdjustThreshold: 10%
  Max AvgBW util: 736bps, Bandwidth Adjustment in 65 second(s).
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
 *Primary                    State: Up
```

```
    Bandwidth: 5Mbps
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 20)
 10.1.13.2 S 10.1.36.2 S
    Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node
10=SoftPreempt):
          10.1.13.2 10.1.36.2
   11 Feb 17 21:16:22 Record Route:  10.1.13.2 10.1.36.2
   10 Feb 17 21:16:22 Up
    9 Feb 17 21:16:22 Manual Autobw adjustment succeeded
    8 Feb 17 21:16:22 Originate make-before-break call
    7 Feb 17 21:16:22 CSPF: computation result accepted
    6 Feb 17 21:14:51 Selected as active path
    5 Feb 17 21:14:51 Record Route:  10.1.13.2 10.1.36.2
    4 Feb 17 21:14:51 Up
    3 Feb 17 21:14:51 Originate Call
    2 Feb 17 21:14:51 CSPF: computation result accepted
    1 Feb 17 21:14:22 CSPF failed: no route toward 10.0.0.6[4 times]
[...Output truncated...]
```

What It Means This LSP event indicates that the autobandwidth adjustment is triggered manually for the LSP using the request mpls lsp adjust-autobandwidth command. A new path for the LSP with the adjust bandwidth is successfully computed and signaled, resulting in the LSP (and traffic) switching over to the new adjusted path

Cause When the CLI command to trigger the manual adjustment is issued, the autobandwidth adjustment validation runs. The current maximum average bandwidth usage is compared to 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 in a make-before-break fashion. If the attempt fails, the LSP continues to use its current path.

Action No action needed. Manual autobandwidth adjustment succeeded.

Automatic Autobandwidth Adjustment

Purpose Automatic autobandwidth allocation allows an MPLS tunnel to automatically adjust its bandwidth allocation based on the volume of traffic flowing through the tunnel. Bandwidth allocation is adjusted according to a specified time interval. At the end of the time interval specified at the [edit protocols mpls label-switched-path auto-bandwidth] hierarchy level, 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.

For more information on configuring autobandwidth, see the *JUNOS MPLS Applications Configuration Guide*.

Autobandwidth success and failure is logged in the output of the show mpls lsp extensive command. The following manual autobandwidth adjustment events are included in this section:

- Automatic Autobandwidth Adjustment Failed Event on page 56
- Automatic Autobandwidth Adjustment Succeeded Event on page 58

Automatic Autobandwidth Adjustment Failed Event

LSP Event Autobw adjustment failed

Sample Output 1

```
user@R1> show configuration protocols mpls
statistics {
    file auto-bw.log;
    interval 5;
    auto-bandwidth;
}
label-switched-path R1-to-R6 {
    to 10.0.0.6;
    auto-bandwidth {
        adjust-interval 300;
        adjust-threshold 10;
        minimum-bandwidth 5m;
        maximum-bandwidth 80m;
    }
}
label-switched-path R1-to-R3 {
    to 10.0.0.3;
    auto-bandwidth {
        adjust-interval 300;
        adjust-threshold 10;
        minimum-bandwidth 155m;
        maximum-bandwidth 155m;
    }
}
```

Sample Output

```
user@R1> show mpls lsp extensive
Ingress LSP: 3 sessions

10.0.0.3
  From: 10.0.0.1, State: Up, ActiveRoute: 5, LSPname: R1-to-R3
  ActivePath:  (primary)
  LoadBalance: Random
  Metric: 1
  Autobandwidth
  MinBW: 155Mbps MaxBW: 155Mbps
  AdjustTimer: 300 secs AdjustThreshold: 10%
  Max AvgBW util: 192bps, Bandwidth Adjustment in 219 second(s).
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
 *Primary                    State: Up
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 10)
 10.1.13.2 S
    Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node
10=SoftPreempt):
          10.1.13.2
    7 Feb 17 15:41:12 Autobw adjustment failed
    6 Feb 17 15:41:12 CSPF failed: no route toward 10.0.0.3
    5 Feb 17 15:36:23 Selected as active path
    4 Feb 17 15:36:23 Record Route:  10.1.13.2
    3 Feb 17 15:36:23 Up
    2 Feb 17 15:36:23 Originate Call
    1 Feb 17 15:36:23 CSPF: computation result accepted
  Created: Thu Feb 17 15:36:23 2005
[...Output truncated...]
```

What It Means This LSP event indicates that a periodic (timer-based) autobandwidth adjustment for the LSP is triggered at the end of the adjust interval. The adjustment fails, and the LSP stays up on the existing path with its current bandwidth.

Cause Adjustment failure may be due to a path CSPF computation failure with the adjust bandwidth or a signaling failure on the new path.

At the end of the time interval specified at the [edit protocols mpls label-switched-path auto-bandwidth] hierarchy level, the current maximum average bandwidth usage is compared to 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.

Action Take action appropriate to the situation:

- Verify the MPLS and RSVP configuration on all available paths to the LSP endpoint.
- Check available bandwidth on alternate paths using the show rsvp interface command. If not enough bandwidth is available on any available paths, adjust the minimum-bandwidth parameter for the LSP in order to establish or adjust the priority to allow the LSP to preempt another LSP of lesser priority. For an LSP to be preempted, its hold priority must be lower than the LSP you are trying to establish.

Automatic Autobandwidth Adjustment Succeeded Event

LSP Event Autobw adjustment succeeded

Sample Output 1

```
user@R1> show configuration protocols mpls
statistics {
    file auto-bw.log;
    interval 5;
    auto-bandwidth;
}
label-switched-path R1-to-R6 {
    to 10.0.0.6;
    auto-bandwidth {
        adjust-interval 300;
        adjust-threshold 10;
        minimum-bandwidth 10m;
        maximum-bandwidth 80m;
    }
}
```

Sample Output 2

```
user@host> show mpls lsp extensive
[...Output truncated...]
Ingress LSP: 1 sessions

10.0.0.6
  From: 10.0.0.1, State: Up, ActiveRoute: 0, LSPname: R1-to-R6
  ActivePath:  (primary)
  LoadBalance: Random
  Autobandwidth
  MinBW: 10Mbps MaxBW: 80Mbps
  AdjustTimer: 300 secs AdjustThreshold: 10%
  Max AvgBW util: 0bps, Bandwidth Adjustment in 282 second(s).
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
 *Primary                    State: Up
    Bandwidth: 10Mbps
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 20)
 10.1.13.2 S 10.1.36.2 S
    Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node
10=SoftPreempt):
          10.1.13.2 10.1.36.2
    9 Feb 17 14:41:12 Record Route:  10.1.13.2 10.1.36.2
    8 Feb 17 14:41:12 Up
    7 Feb 17 14:41:12 Autobw adjustment succeeded
    6 Feb 17 14:41:12 CSPF: computation result accepted
    5 Feb 17 14:36:29 Selected as active path
    4 Feb 17 14:36:29 Record Route:  10.1.13.2 10.1.36.2
    3 Feb 17 14:36:29 Up
    2 Feb 17 14:36:29 Originate Call
    1 Feb 17 14:36:29 CSPF: computation result accepted
  Created: Thu Feb 17 14:36:29 2005
Total 1 displayed, Up 1, Down 0
[...Output truncated...]
```

What It Means This LSP event indicates that a periodic (timer-based) autobandwidth adjustment for the LSP is triggered at the end of the adjust interval. A new path for the LSP, with the adjusted bandwidth, is successfully computed and signaled. The LSP (and traffic) switches over to the new adjusted path.

Cause At the end of the time interval specified at the [edit protocols mpls label-switched-path auto-bandwidth] hierarchy level, the current maximum average bandwidth usage is compared to 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.

Action No action required. Automatic autobandwidth adjustment succeeded.

Chapter 5
Understanding DiffServ-Aware Traffic-Engineered LSP Events

This chapter lists and describes label-switched path (LSP) events that might occur in the output of the show mpls lsp extensive command for Differentiated-Services-Aware (DiffServ) traffic-engineered LSPs. Descriptions typically include sample output of the LSP event, an explanation of what the event means, the possible cause of the event, and any possible actions that you can take. (See Table 9.)

Table 9: Checklist for Understanding DiffServ-Aware Traffic-Engineered LSP Events

Understanding DiffServ-Aware Traffic Engineered LSP Events Tasks	Possible Action or Command
Displaying DiffServ-Aware Traffic-Engineered LSP Events on page 62	
1. Unsupported Traffic Class Event on page 63	Not available.
2. Traffic Class Value Out of Allowed Range Event on page 63	Not available.
3. The Combination of Setup Priority and Traffic Class Is Not One of the Configured TE Classes Event on page 63	Correct the configuration depending on supported traffic engineering classes.
4. The Combination of Hold Priority and Traffic Class Is Not One of the Configured TE Classes Event on page 64	Correct the configuration depending on supported traffic engineering classes.

Displaying DiffServ-Aware Traffic-Engineered LSP Events

Purpose A DiffServ-aware traffic-engineered LSP is configured with a bandwidth reservation for a specific class type, and carries traffic for a single class type. On the packets, the class type is specified by the experimental (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, instead of being signaled in Resource Reservation Protocol (RSVP).

The class type must be configured consistently across the DiffServ domain, and 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 forwarding classes and class of service, see the *JUNOS Class of Service Configuration Guide*. For more information about differentiated services, see RFC 3270, *Multi-Protocol Label Switching (MPLS) Support of Differentiated Services*.

When the configuration of a DiffServ-aware traffic-engineered LSP is incorrect, an even or error message might occur in the output of the show mpls lsp extensive command.

Action To display LSP events that can occur with a Diff-Serv-aware LSP, enter the following JUNOS command-line interface (CLI) operational mode command from the ingress router:

```
user@host> show mpls lsp extensive
```

Sample Output Not available.

Unsupported Traffic Class Event

LSP Event Unsupported traffic class

Sample Output Not available.

What It Means This LSP error event is a Juniper Networks proprietary error indicating that a Diffserv traffic engineering LSP was signaled with one or more traffic classes with values greater than the 4 traffic classes currently supported by the JUNOS software.

Cause Not available.

Action Not available.

Traffic Class Value Out of Allowed Range Event

LSP Event Traffic class value out of allowed range

Sample Output Not available.

What It Means This LSP error event is a Juniper Networks proprietary error indicating that a single class, IETF-style DiffServ traffic engineering LSP was signaled with a traffic class value of zero, which is invalid.

Cause Not available.

Action Not available.

The Combination of Setup Priority and Traffic Class Is Not One of the Configured TE Classes Event

LSP Event The combination of setup-priority and traffic class is not one of the configured TE-classes

Sample Output Not available.

What It Means This LSP error event is a Juniper Networks proprietary error that indicates the setup priority signaled in the Path message for the LSP does not match the supported Diffserv traffic engineering classes configured on a label-switching router (LSR) along the LSP path.

Cause This LSP error event is caused by incorrect configuration of the LSP setup priority on the ingress LSR, or the incorrect configuration of a DiffServ traffic engineering class on an LSR along the LSP path.

Action Correct the configuration depending on the supported traffic engineering classes.

The Combination of Hold Priority and Traffic Class Is Not One of the Configured TE Classes Event

LSP Event The combination of hold priority and traffic class is not one of the configured traffic engineering classes

Sample Output Not available.

What It Means This LSP event is a Juniper Networks proprietary error indicating that the hold priority signaled in the Path message for the LSP does not match the supported DiffServ traffic engineering classes configured on an LSR along the LSP path.

Cause This LSP event is caused by the incorrect configuration of the LSP hold priority at the ingress LSR, or the incorrect configuration of the DiffServ traffic engineering class on an LSR along the LSP path.

Action Correct the configuration depending on the supported traffic engineering classes.

Chapter 6
Understanding GMPLS Events

This chapter describes Generalized Multiprotocol Label Switching (GMPLS) error events that might occur in the output of the show mpls lsp extensive command. Descriptions typically include sample output of the label-switched path (LSP) event, an explanation of what the event means, the possible cause of the event, and any possible actions that you can take. (See Table 10.)

Table 10: Checklist for Understanding GMPLS Events

Understanding GMPLS Events Tasks	Possible Action or Command
Displaying GMPLS Events on page 66	show mpls lsp extensive
1. RSVP Error, Subcode 7, Signal Type Does Not Match Link Encoding Event on page 67	Make sure that the configured bandwidth and the encoding type of the traffic engineering link match in the LSP configuration.
2. RSVP Error, Subcode 8, Tspec Invalid for Encoding/Switching Type Requested Event on page 67	Not available.
3. Unacceptable Label Value Event on page 67	Not available
4. Unsupported Encoding Type Event on page 68	Not available.
5. Unsupported Switching Type Event on page 68	Not available.
6. Update LSP Encoding Type Event on page 68	Not available.

Displaying GMPLS Events

Purpose GMPLS generalizes MPLS by defining labels for switching varying types of Layer 1, Layer 2, or Layer 3 traffic. LSPs must start and end on links with the same switching capability. For example, routers can establish packet-switched LSPs with other routers. LSPs might be carried over a Time-Division Multiplexing (TDM)-switched LSP between SONET add/drop multiplexers (ADMs), which in turn might be carried over a lambda-switched LSP. GMPLS signaling requires strict paths, and you must disable Constrained Shortest Path First (CSPF) with the no-cspf statement. For more information on GMPLS, see the *JUNOS MPLS Applications Configuration Guide.*

When the configuration of an GMPLS LSP is incorrect, an event or error message can appear in the output of the show mpls lsp extensive command.

Action To display GMPLS events, enter the following JUNOS command-line interface (CLI) operational mode command from the ingress router:

```
user@host> show mpls lsp extensive
```

Sample Output

```
user@host> show mpls lsp extensive
Ingress LSP: 1 sessions

10.255.255.40
  From: 10.255.255.35, State: Up, ActiveRoute: 0, LSPname: gmpls-lsp1
  Bidirectional
  ActivePath: path-lsp1 (primary)
  LoadBalance: Random
  Signal type: STM-1
  Encoding type: SDH/SONET, Switching type: Fiber, GPID: PPP
 *Primary   path-lsp1             State: Up
    Bandwidth: 155.52Mbps
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 2)
          10.35.100.1 S 10.35.150.1 S 10.35.200.1 S
    Received RRO:
          10.35.100.1 10.35.150.1 10.35.200.1
    7 Nov  7 15:47:11  Selected as active path
    6 Nov  7 15:47:11  Record Route:  10.35.100.1 10.35.150.1 10.35.200.1
    5 Nov  7 15:47:11  Up
    4 Nov  7 15:47:11  Update LSP Encoding Type
    3 Nov  7 15:47:11  Originate Call
    2 Nov  7 15:47:11  CSPF: computation result accepted
    1 Nov  7 15:46:41  CSPF failed: no route toward 10.255.255.40
  Created: Thu Nov  7 15:46:38 2002
Total 1 displayed, Up 1, Down 0
[...Output truncated...]
```

What It Means The sample output from ingress router R1 shows extensive ingress LSP information, including LSP events that led to an LSP failure, with the most recent events at the top. The last line before the history log begins indicates the length of time the router waits before attempting to re-signal the LSP, three seconds in this instance.

LSP events in bold are described in this chapter. Descriptions include sample output of the LSP event, an explanation of what the event means, the possible cause of the event, and any possible actions that you can take.

For completeness, events not included in this example output are also described in this chapter to show LSP events that did not occur in the example network configuration, but might occur in your network. The output for these events includes the prompt user@host rather than the usual user@R1 prompt.

RSVP Error, Subcode 7, Signal Type Does Not Match Link Encoding Event

LSP Event RSVP error, subcode 7, signal-type does not match link encoding

Sample Output Not available

What It Means This LSP error event is a Juniper Networks proprietary error reported for GMPLS LSPs when the configured signal bandwidth does not match the encoding type of the traffic engineering link selected on the first hop.

Cause The signal bandwidth is misconfigured with the encoding type of the traffic engineering link.

Action Make sure that the configured bandwidth and the encoding type of the traffic engineering link match in the LSP configuration.

RSVP Error, Subcode 8, Tspec Invalid for Encoding/Switching Type Requested Event

LSP Event RSVP error, subcode 8, Tspec invalid for encoding/switching type requested

Sample Output Not available.

What It Means This LSP error event is a Juniper Networks proprietary error reported for GMPLS LSPs as a result of validation of the signaled traffic parameters against the generalized label request for the LSP.

Cause An incorrect Sender Tspec is used with a particular LSP switching or encoding type.

Action Not available.

Unacceptable Label Value Event

LSP Event Unacceptable label value event

Sample Output Not available.

What It Means This LSP error event indicates that the label value signaled in either the Path or Resv message was unacceptable to a label-switched router (LSR) along the LSP path.

Cause For GMPLS LSPs, this LSP error event is generated by incorrect label mapping configured on one of the LSRs, or by deletion of a resource that was being used by an LSP.

Action Not available.

Unsupported Encoding Type Event

LSP Event Unsupported encoding type

Sample Output Not available.

What It Means This LSP error event indicates that the LSP encoding type requested in the generalized label request for a GMPLS LSP is unsupported on the corresponding selected traffic engineering link.

Cause Not available.

Action Not available.

Unsupported Switching Type Event

LSP Event Unsupported switching type

Sample Output Not available.

What It Means This LSP error event indicates that the switching type requested in the generalized label request for a GMPLS LSP is unsupported on the corresponding selected TE link.

Cause Not available.

Action Not available.

Update LSP Encoding Type Event

LSP Event Update Encoding Type

Sample Output

```
user@host> show mpls lsp extensive
Ingress LSP: 1 sessions

10.255.255.40
  From: 10.255.255.35, State: Up, ActiveRoute: 0, LSPname: gmpls-lsp1
  Bidirectional
  ActivePath: path-lsp1 (primary)
  LoadBalance: Random
  Signal type: STM-1
  Encoding type: SDH/SONET, Switching type: Fiber, GPID: PPP
 *Primary   path-lsp1             State: Up
    Bandwidth: 155.52Mbps
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 2)
          10.35.100.1 S 10.35.150.1 S 10.35.200.1 S
    Received RRO:
          10.35.100.1 10.35.150.1 10.35.200.1
```

```
    7 Nov  7 15:47:11  Selected as active path
    6 Nov  7 15:47:11  Record Route:  10.35.100.1 10.35.150.1 10.35.200.1
    5 Nov  7 15:47:11  Up
    4 Nov  7 15:47:11  Update LSP Encoding Type
    3 Nov  7 15:47:11  Originate Call
    2 Nov  7 15:47:11  CSPF: computation result accepted
    1 Nov  7 15:46:41  CSPF failed: no route toward 10.255.255.40
  Created: Thu Nov  7 15:46:38 2002
Total 1 displayed, Up 1, Down 0
```

What It Means This LSP event indicates that the encoding type was updated based on the traffic engineering link selected as the first hop.

Cause This LSP event occurs when the encoding type is not configured on a non-packet LSP. In this case, the encoding type is derived from the traffic engineering link that was selected as the first hop.

Action Not available.

Part 2

Examining the CSPF Log

This section describes how and when to configure Constrained Shortest Path First (CSPF) tracing on a network, and provides information about the output for the traceoptions command.

The following information is covered:

Chapter 7

Configuring CSPF Tracing

The chapter describes how and when to configure Multiprotocol Label Switching (MPLS) Constrained Shortest Path First (CSPF) tracing. With each flag that you configure, more granular information about CSPF calculations is provided by the CSPF log file output. (See Table 11.)

Table 11: Checklist for Configuring CSPF Tracing

Configuring CSPF Tracing Tasks	Possible Action or Command
Understanding CSPF on page 74	
Configuring CSPF Tracing on page 76	[edit] edit protocols mpls [edit protocols mpls] set traceoptions file *filename* set traceoptions flag cspf set traceoptions flag cspf-link set traceoptions flag cspf-node show commit
Examining the CSPF Log File on page 77	
1. Trace Only CSPF Computations on page 78	[edit protocols mpls] run monitor start *filename* run show log *filename*
2. Trace Nodes Visited During CSPF Computations on page 79	[edit protocols mpls] run monitor start *filename* run show log *filename*
3. Trace Links Visited During CSPF Computations on page 81	[edit protocols mpls] run monitor start *filename* run show log *filename* show ted database

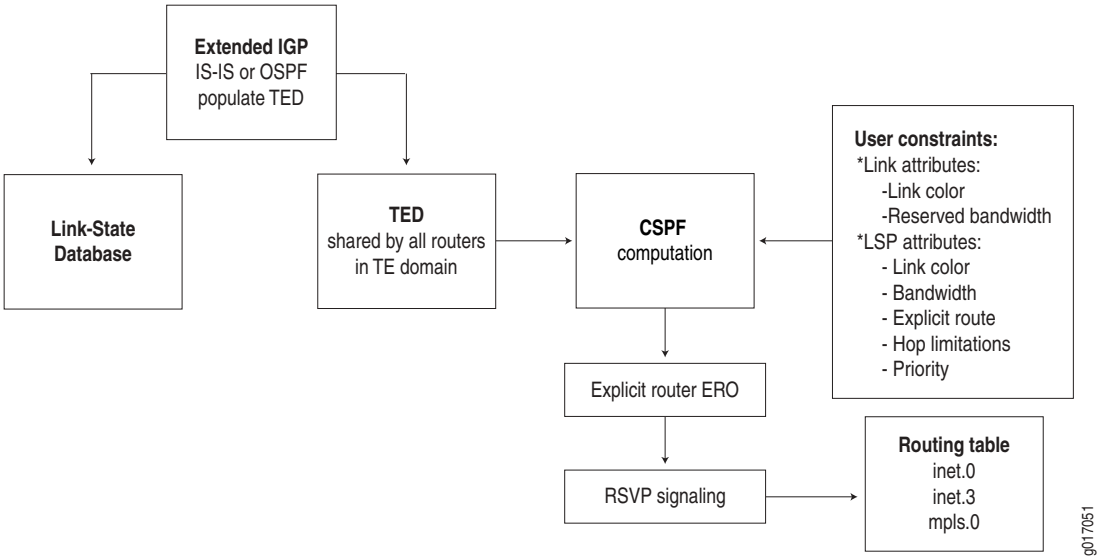
Understanding CSPF

Purpose CSPF is a link-state algorithm used in computing paths for label-switched paths (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 attempts to minimize congestion by balancing the network load.

After pruning paths that do not meet the configured constraints from the shortest-path-first (SPF) tree, CSPF derives the best available path based on the information in the traffic engineering database (TED). Based on the best available path, CSPF produces a strict Explicit Route Object (ERO) which the Resource Reservation Protocol (RSVP) uses to signal the LSP.

The CSPF algorithm is a modified version of the SPF algorithm used within the link-state databases of Intermediate System-to-Intermediate System (IS-IS) and Open Shortest Path First (OSPF) protocols. CSPF operates on the traffic engineering database, which is constructed through extensions to IS-IS and OSPF. Figure 2 illustrates the various components that contribute to the CSPF computation.

Figure 2: CSPF Components



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 traffic engineering database of all 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, and the other from Router A to the egress router.

6. If several paths have equal cost, chooses the path whose last-hop address is the same as the LSP's destination.

7. If several equal-cost paths remain, selects the path 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).

The result of the above steps is a strict-hop ERO that details each hop along the calculated path. The ERO is passed to the RSVP protocol process, where it is used to signal and establish the LSP in the network.

Steps To Take To determine how and when to configure and examine MPLS CSPF tracing, follow these steps:

1. Configuring CSPF Tracing on page 76

2. Examining the CSPF Log File on page 77

Configuring CSPF Tracing

Purpose When the output of the show mpls lsp extensive command indicates that the CSPF algorithm has failed, configuring CSPF tracing on the ingress router can often provide more information about the problem.

Action On the ingress router, to configure a log file and specify MPLS tracing flags, follow these steps:

1. In configuration mode, go to the following hierarchy level:

   ```
   [edit]
   user@host# edit protocols mpls
   ```

2. Configure a log file:

   ```
   [edit protocols mpls]
   user@host# set traceoptions file filename
   ```

3. Depending on your situation, specify all or one of the following CSPF-specific tracing flags:

   ```
   [edit protocols mpls]
   user@host# set traceoptions flag cspf
   user@host# set traceoptions flag cspf-link
   user@host# set traceoptions flag cspf-node
   ```

4. Verify and commit the configuration:

   ```
   user@host# show
   user@host# commit
   ```

Sample Output

```
[edit protocols mpls]
user@R1# show
traceoptions {
    file cspf;
    flag cspf;
    flag cspf-link;
    flag cspf-node;
}
label-switched-path R6-to-R1 {
    to 10.0.0.1;
}
interface so-0/0/0.0;
interface so-0/0/1.0;
interface so-0/0/2.0;
interface so-0/0/3.0;
```

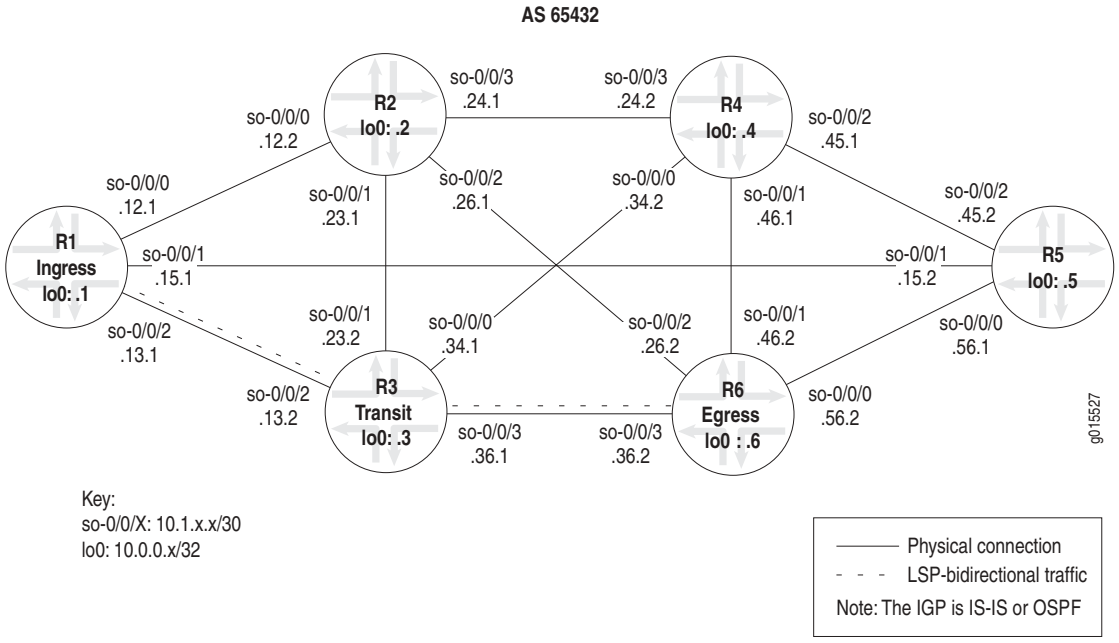
What It Means The sample output shows a typical CSPF tracing configuration. The log file cpsf contains all the information gathered for each configured flag. Each flag provides slightly different information about CSPF computations. The cspf flag traces CSPF computations only; the cspf-link flag traces links visited during CSPF computations, and the cspf-node flag traces nodes visited during CSPF computations. See “Examining the CSPF Log File” on page 77 for information about examining a CSPF log file.

Examining the CSPF Log File

Purpose The CSPF log file provides useful information about the steps taken by the CSPF algorithm to calculate the shortest path from the ingress router to the egress router. The following steps and output illustrate the CSPF algorithm in the successful establishment of an LSP. With each flag that you configure, starting with the cspf flag, then the cspf-node flag, and finally the cspf-link flag, more granular information about CSPF calculations is provided by the output in the CSPF log file configured to gather the information.

Figure illustrates the example network topology used in this section. The example MPLS network uses IS-IS Level 2 and a policy to create traffic. However, IS-IS Level 1 or an OSPF area can be used and the policy omitted if the network has existing Border Gateway Protocol (BGP) traffic.

Figure 3: MPLS Network Topology



The MPLS network in Figure is a router-only network with SONET interfaces that consist of the following components:

- A full-mesh interior BGP (IBGP) topology, using AS 65432
- MPLS and RSVP enabled on all routers
- A send-statics policy on routers R1 and R6 that allows a new route to be advertised into the network
- Two unidirectional LSPs between R1 and R6, which allow bidirectional traffic

See the *JUNOS MPLS Network Operations Guide* for information on configuring an MPLS network. The ingress router R1 is configured with CSPF tracing, and the output examined in the following three steps is taken from R1.

Steps To Take To examine the CSPF log file, follow these steps:

1. Trace Only CSPF Computations on page 78
2. Trace Nodes Visited During CSPF Computations on page 79
3. Trace Links Visited During CSPF Computations on page 81

Step 1: Trace Only CSPF Computations

Purpose The cspf flag provides an overview of the CSPF computations performed and the resulting ERO for the LSP. Details about nodes or links visited during CSPF computations are not included in this log file.

Action To run trace CSPF computations and examine the CSPF log file, enter the following JUNOS command-line interface (CLI) commands:

```
[edit protocols mpls]
user@R1# run monitor start filename
user@R1# run show log filename
```

NOTE: To stop monitoring CSPF, issue the monitor stop command. If you are working in configuration mode, issue the run monitor stop command.

Sample Output 1

```
[edit protocols mpls]
user@R1# show
traceoptions {
    file cspf;
    flag cspf;
}
label-switched-path R6-to-R1 {
    to 10.0.0.1;
}
interface so-0/0/0.0;
interface so-0/0/1.0;
interface so-0/0/2.0;
interface so-0/0/3.0;
```

Sample Output 2

```
[edit protocols mpls]

user@R1> show log cspf
Apr 29 11:35:59 trace_on: Tracing to "/var/log/cspf" started
Apr 29 13:22:52 RPD_MPLS_LSP_DOWN: MPLS LSP R1-to-R6 down on primary()
Apr 29 13:22:52 RPD_MPLS_PATH_DOWN: MPLS path down on LSP R1-to-R6
Apr 29 13:22:52 CSPF adding path R1-to-R6(primary) to CSPF queue 1
Apr 29 13:22:52 CSPF creating CSPF job
Apr 29 13:22:52
Apr 29 13:22:52 CSPF for path R1-to-R6(primary), begin at R1.00, starting
Apr 29 13:22:52         bandwidth: CT0=0bps; setup priority: 0; random
Apr 29 13:22:52 CSPF final destination 10.0.0.6
Apr 29 13:22:52 CSPF starting from R1.00 (10.0.0.1) to 10.0.0.6, hoplimit 254
Apr 29 13:22:52 CSPF Reached target
Apr 29 13:22:52 CSPF completed in 0.000106s
Apr 29 13:22:52 CSPF ERO for R1-to-R6(primary) (2 hops)
Apr 29 13:22:52         node 10.1.15.2/32
Apr 29 13:22:52         node 10.1.56.2/32
Apr 29 13:22:52 CSPF for R1-to-R6 done!
```

```
Apr 29 13:22:52 RPD_MPLS_PATH_UP: MPLS path up on LSP R1-to-R6
Apr 29 13:22:52 RPD_MPLS_LSP_UP: MPLS LSP R1-to-R6 up on primary() Route 10.1.15.2 10.1.56.2
monitor stop
```

What It Means Sample Output 1 shows the configuration of the cspf file and cspf flag at the [edit protocols mpls traceoptions] hierarchy level. See "Configuring CSPF Tracing" on page 76 for steps to configure CSPF tracing.

Sample Output 2 shows the contents of the cspf file in the /var/log/ directory on ingress router R1. The cspf file contains the CSPF computations obtained when the cspf flag is configured at the [edit protocols mpls traceoptions] hierarchy level and after the run monitor start cspf and run show log cspf commands were issued.

Each line of output describes the steps taken by the CSPF algorithm to calculate the shortest path between the ingress and egress routers. The result of the CSPF algorithm is formed into a strict-hop ERO that details each hop along the calculated path. For example, the ERO for the LSP R1-to-R6 contains two hops that pass through nodes 10.1.15.2/32 and 10.1.56.2.32. When the ERO is completed, CSPF for R1-to-R6 done!, the ERO is passed to the RSVP protocol process, where it is used for signaling and establishing the LSP in the network. The output shows RPD_MPLS_LSP_UP, indicating that the LSP was established successfully.

Step 2: Trace Nodes Visited During CSPF Computations

Purpose The configuration of the cspf-node flag provides details in the log file about the nodes visited during CSPF computations. The node information is in addition to the overview information provided by the cspf flag. Details about links visited during CSPF computations are not included in the log file.

Action To trace nodes visited during CSPF computations and to examine the CSPF log file, enter the following JUNOS CLI commands:

```
[edit protocols mpls]
user@R1# run monitor start filename
user@R1# run show log filename
```

NOTE: To stop monitoring CSPF, issue the monitor stop command. If you are working in configuration mode, as shown in the sample output, issue the run monitor stop command.

Sample Output 1

```
[edit protocols mpls]
user@R1# show
traceoptions {
    file cspf-node1;
    flag cspf;
    flag cspf-node;
}
label-switched-path R6-to-R1 {
    to 10.0.0.1;
}
interface so-0/0/0.0;
interface so-0/0/1.0;
interface so-0/0/2.0;
interface so-0/0/3.0;
```

Sample Output 2

```
[edit protocols mpls]
user@R1# run show log cspf-node1 | no-more
Apr 29 13:39:08 trace_on: Tracing to "/var/log/cspf-node1" started
Apr 29 13:40:43 RPD_MPLS_LSP_DOWN: MPLS LSP R1-to-R6 down on primary()
Apr 29 13:40:43 RPD_MPLS_PATH_DOWN: MPLS path down on LSP R1-to-R6
Apr 29 13:40:43 CSPF adding path R1-to-R6(primary) to CSPF queue 1
Apr 29 13:40:43 CSPF creating CSPF job
Apr 29 13:40:43
Apr 29 13:40:43 CSPF for path R1-to-R6(primary), begin at R1.00, starting
Apr 29 13:40:43         bandwidth: CT0=0bps; setup priority: 0; random
Apr 29 13:40:43 CSPF final destination 10.0.0.6
Apr 29 13:40:43 CSPF starting from R1.00 (10.0.0.1) to 10.0.0.6, hoplimit 254
Apr 29 13:40:43     Node R1.00 (10.0.0.1) metric 0, hops 0, avail 32000 32000 32000 32000
Apr 29 13:40:43     Node R3.00 (10.0.0.3) metric 10, hops 1, avail 32000 32000 32000 32000
Apr 29 13:40:43     Node R5.00 (10.0.0.5) metric 10, hops 1, avail 32000 32000 32000 32000
Apr 29 13:40:43     Node R2.00 (10.0.0.2) metric 10, hops 1, avail 32000 32000 32000 32000
Apr 29 13:40:43     Node R4.00 (10.0.0.4) metric 20, hops 2, avail 32000 32000 32000 32000
Apr 29 13:40:43     Node R6.00 (10.0.0.6) metric 20, hops 2, avail 32000 32000 32000 32000
Apr 29 13:40:43 CSPF Reached target
Apr 29 13:40:43 CSPF completed in 0.000304s
Apr 29 13:40:43 CSPF ERO for R1-to-R6(primary) (2 hops)
Apr 29 13:40:43         node 10.1.12.2/32
Apr 29 13:40:43         node 10.1.26.2/32
Apr 29 13:40:43 CSPF for R1-to-R6 done!
Apr 29 13:40:43 RPD_MPLS_PATH_UP: MPLS path up on LSP R1-to-R6
Apr 29 13:40:43 RPD_MPLS_LSP_UP: MPLS LSP R1-to-R6 up on primary() Route 10.1.12.2 10.1.26.2
[...Output truncated...]
```

```
[edit protocols mpls]
user@R1# run monitor stop
```

What It Means Sample Output 1 shows the configuration of the cspf-node file, cspf flag and cspf-node flag at the [edit protocols mpls traceoptions] hierarchy level. See "Configuring CSPF Tracing" on page 76 for steps to configure CSPF tracing.

Sample Output 2 shows the contents of the cspf-node file in the /var/log/ directory on ingress router R1. The cspf-node file contains the CSPF computations logged when the cspf and cspf-node flags are configured at the [edit protocols mpls traceoptions] hierarchy level and after the run monitor start cspf and run show log cspf commands are issued.

Each line of output describes the steps taken by the CSPF algorithm to calculate the shortest path between the ingress and egress routers. Because the cspf-node flag is configured, the output shows the nodes visited during the calculations performed by the CSPF algorithm. For example, all nodes in the network shown in Figure on page 77 are included.

The result of the CSPF algorithm is formed into a strict-hop ERO. For example, the ERO for the LSP R1-to-R6 contains two hops that pass through nodes 10.1.12.2/32 and 10.1.26.2.32. When the ERO is completed, CSPF for R1-to-R6 done!, the ERO is passed to the RSVP protocol process, where it is used for signaling and establishing the LSP in the network. The output shows RPD_MPLS_LSP_UP, indicating that the LSP was established successfully.

Step 3: Trace Links Visited During CSPF Computations

Purpose The configuration of the cspf-link flag provides details in the log file about the links visited during CSPF computations. The link information is in addition to the overview information provided by the cspf flag, and the node information provided by the cpsf-node flag.

Action To run trace links visited during CSPF computations and examine the CSPF log file, enter the following JUNOS CLI commands:

```
[edit protocols mpls]
user@R1# run monitor start filename
user@R1# run show log filename
user@R1# run show ted database
```

NOTE: To stop monitoring CSPF, issue the monitor stop command. If you are working in configuration mode, as shown in the sample output, issue the run monitor stop command.

Sample Output 1

```
[edit protocols mpls]
user@R1# show
traceoptions {
    file cspf-link;
    flag cspf;
    flag cspf-link;
}
label-switched-path R6-to-R1 {
    to 10.0.0.1;
}
interface so-0/0/0.0;
interface so-0/0/1.0;
interface so-0/0/2.0;
interface so-0/0/3.0;
```

Sample Output 2

```
[edit protocols mpls]
user@R1# run show log cspf-link | no-more
Apr 29 13:29:52 trace_on: Tracing to "/var/log/cspf-link" started
Apr 29 13:30:27 RPD_MPLS_LSP_DOWN: MPLS LSP R1-to-R6 down on primary()
Apr 29 13:30:27 RPD_MPLS_PATH_DOWN: MPLS path down on LSP R1-to-R6
Apr 29 13:30:27 CSPF adding path R1-to-R6(primary) to CSPF queue 1
Apr 29 13:30:27 CSPF creating CSPF job
Apr 29 13:30:27
Apr 29 13:30:27 CSPF for path R1-to-R6(primary), begin at R1.00, starting
Apr 29 13:30:27 bandwidth: CT0=0bps; setup priority: 0; random
Apr 29 13:30:27 CSPF final destination 10.0.0.6
Apr 29 13:30:27 CSPF starting from R1.00 (10.0.0.1) to 10.0.0.6, hoplimit 254
Apr 29 13:30:27   Node R1.00 (10.0.0.1) metric 0, hops 0, avail 32000 32000 32000 32000
Apr 29 13:30:27      Link 10.1.13.1->10.1.13.2(R3.00/10.0.0.3) metric 10 color 0x00000000 bw 155.52Mbps
Apr 29 13:30:27       Reverse Link for 10.1.13.1->10.1.13.2 is 10.1.13.2->10.1.13.1
Apr 29 13:30:27       link's interface switch capability descriptor #1
Apr 29 13:30:27         encoding: Packet, switching: Packet
Apr 29 13:30:27       link passes constraints
Apr 29 13:30:27      Link 10.1.12.1->10.1.12.2(R2.00/10.0.0.2) metric 10 color 0x00000000 bw 155.52Mbps
Apr 29 13:30:27       Reverse Link for 10.1.12.1->10.1.12.2 is 10.1.12.2->10.1.12.1
Apr 29 13:30:27       link's interface switch capability descriptor #1
Apr 29 13:30:27        encoding: Packet, switching: Packet
Apr 29 13:30:27       link passes constraints
```

```
Apr 29 13:30:27      Link 10.1.15.1->10.1.15.2(R5.00/10.0.0.5) metric 10 color 0x00000000 bw 155.52Mbps
Apr 29 13:30:27       Reverse Link for 10.1.15.1->10.1.15.2 is 10.1.15.2->10.1.15.1
Apr 29 13:30:27       link's interface switch capability descriptor #1
Apr 29 13:30:27        encoding: Packet, switching: Packet
Apr 29 13:30:27       link passes constraints
Apr 29 13:30:27     Node R3.00 (10.0.0.3) metric 10, hops 1, avail 32000 32000 32000 32000
Apr 29 13:30:27      Link 10.1.13.2->10.1.13.1(R1.00/10.0.0.1) metric 10 color 0x00000000 bw 155.52Mbps
Apr 29 13:30:27       skipped: end point already visited
Apr 29 13:30:27      Link 10.1.34.1->10.1.34.2(R4.00/10.0.0.4) metric 10 color 0x00000000 bw 155.52Mbps
Apr 29 13:30:27       Reverse Link for 10.1.34.1->10.1.34.2 is 10.1.34.2->10.1.34.1
Apr 29 13:30:27       link's interface switch capability descriptor #1
Apr 29 13:30:27        encoding: Packet, switching: Packet
Apr 29 13:30:27       link passes constraints
Apr 29 13:30:27      Link 10.1.23.2->10.1.23.1(R2.00/10.0.0.2) metric 10 color 0x00000000 bw 155.52Mbps
Apr 29 13:30:27       Reverse Link for 10.1.23.2->10.1.23.1 is 10.1.23.1->10.1.23.2
Apr 29 13:30:27       link's interface switch capability descriptor #1
Apr 29 13:30:27        encoding: Packet, switching: Packet
Apr 29 13:30:27       link passes constraints
Apr 29 13:30:27       metric: 20 vs 10; hops: 2 vs 1; avail: 32000 32000 32000 32000
Apr 29 13:30:27      Link 10.1.36.1->10.1.36.2(R6.00/10.0.0.6) metric 10 color 0x00000000 bw 155.52Mbps
Apr 29 13:30:27       Reverse Link for 10.1.36.1->10.1.36.2 is 10.1.36.2->10.1.36.1
Apr 29 13:30:27       link's interface switch capability descriptor #1
Apr 29 13:30:27        encoding: Packet, switching: Packet
Apr 29 13:30:27       link passes constraints
Apr 29 13:30:27     Node R5.00 (10.0.0.5) metric 10, hops 1, avail 32000 32000 32000 32000
Apr 29 13:30:27      Link 10.1.15.2->10.1.15.1(R1.00/10.0.0.1) metric 10 color 0x00000000 bw 155.52Mbps
Apr 29 13:30:27       skipped: end point already visited
Apr 29 13:30:27      Link 10.1.45.2->10.1.45.1(R4.00/10.0.0.4) metric 10 color 0x00000000 bw 155.52Mbps
Apr 29 13:30:27       Reverse Link for 10.1.45.2->10.1.45.1 is 10.1.45.1->10.1.45.2
Apr 29 13:30:27       link's interface switch capability descriptor #1
Apr 29 13:30:27        encoding: Packet, switching: Packet
Apr 29 13:30:27       link passes constraints
Apr 29 13:30:27       metric: 20 vs 20; hops: 2 vs 2; avail: 32000 32000 32000 32000
Apr 29 13:30:27       Better path: random wins
Apr 29 13:30:27      Link 10.1.56.1->10.1.56.2(R6.00/10.0.0.6) metric 10 color 0x00000000 bw 155.52Mbps
Apr 29 13:30:27       Reverse Link for 10.1.56.1->10.1.56.2 is 10.1.56.2->10.1.56.1
Apr 29 13:30:27       link's interface switch capability descriptor #1
Apr 29 13:30:27        encoding: Packet, switching: Packet
Apr 29 13:30:27       link passes constraints
Apr 29 13:30:27       metric: 20 vs 20; hops: 2 vs 2; avail: 32000 32000 32000 32000
Apr 29 13:30:27       Old path is better
Apr 29 13:30:27   Node R2.00 (10.0.0.2) metric 10, hops 1, avail 32000 32000 32000 32000
Apr 29 13:30:27      Link 10.1.12.2->10.1.12.1(R1.00/10.0.0.1) metric 10 color 0x00000000 bw 155.52Mbps
Apr 29 13:30:27       skipped: end point already visited
Apr 29 13:30:27      Link 10.1.23.1->10.1.23.2(R3.00/10.0.0.3) metric 10 color 0x00000000 bw 155.52Mbps
Apr 29 13:30:27       skipped: end point already visited
Apr 29 13:30:27      Link 10.1.24.1->10.1.24.2(R4.00/10.0.0.4) metric 10 color 0x00000000 bw 155.52Mbps
Apr 29 13:30:27       Reverse Link for 10.1.24.1->10.1.24.2 is 10.1.24.2->10.1.24.1
Apr 29 13:30:27       link's interface switch capability descriptor #1
Apr 29 13:30:27        encoding: Packet, switching: Packet
Apr 29 13:30:27       link passes constraints
Apr 29 13:30:27       metric: 20 vs 20; hops: 2 vs 2; avail: 32000 32000 32000 32000
Apr 29 13:30:27       Old path is better
Apr 29 13:30:27      Link 10.1.26.1->10.1.26.2(R6.00/10.0.0.6) metric 10 color 0x00000000 bw 155.52Mbps
Apr 29 13:30:27       Reverse Link for 10.1.26.1->10.1.26.2 is 10.1.26.2->10.1.26.1
Apr 29 13:30:27       link's interface switch capability descriptor #1
Apr 29 13:30:27        encoding: Packet, switching: Packet
Apr 29 13:30:27       link passes constraints
Apr 29 13:30:27       metric: 20 vs 20; hops: 2 vs 2; avail: 32000 32000 32000 32000
Apr 29 13:30:27       Old path is better
Apr 29 13:30:27   Node R4.00 (10.0.0.4) metric 20, hops 2, avail 32000 32000 32000 32000
Apr 29 13:30:27      Link 10.1.34.2->10.1.34.1(R3.00/10.0.0.3) metric 10 color 0x00000000 bw 155.52Mbps
Apr 29 13:30:27       skipped: end point already visited
```

```
Apr 29 13:30:27      Link 10.1.24.2->10.1.24.1(R2.00/10.0.0.2) metric 10 color 0x00000000 bw 155.52Mbps
Apr 29 13:30:27       skipped: end point already visited
Apr 29 13:30:27      Link 10.1.45.1->10.1.45.2(R5.00/10.0.0.5) metric 10 color 0x00000000 bw 155.52Mbps
Apr 29 13:30:27       skipped: end point already visited
Apr 29 13:30:27      Link 10.1.46.1->10.1.46.2(R6.00/10.0.0.6) metric 10 color 0x00000000 bw 155.52Mbps
Apr 29 13:30:27       Reverse Link for 10.1.46.1->10.1.46.2 is 10.1.46.2->10.1.46.1
Apr 29 13:30:27       link's interface switch capability descriptor #1
Apr 29 13:30:27        encoding: Packet, switching: Packet
Apr 29 13:30:27       link passes constraints
Apr 29 13:30:27       metric: 30 vs 20; hops: 3 vs 2; avail: 32000 32000 32000 32000
Apr 29 13:30:27     Node R6.00 (10.0.0.6) metric 20, hops 2, avail 32000 32000 32000 32000
Apr 29 13:30:27 CSPF Reached target
Apr 29 13:30:27 CSPF completed in 0.001880s
Apr 29 13:30:27 CSPF ERO for R1-to-R6(primary) (2 hops)
Apr 29 13:30:27         node 10.1.13.2/32
Apr 29 13:30:27         node 10.1.36.2/32
Apr 29 13:30:27 CSPF for R1-to-R6 done!
Apr 29 13:30:27 RPD_MPLS_PATH_UP: MPLS path up on LSP R1-to-R6
Apr 29 13:30:27 RPD_MPLS_LSP_UP: MPLS LSP R1-to-R6 up on primary() Route 10.1.13.2 10.1.36.2
```

Sample Output 3

```
user@R1# run show ted database | no-more
TED database: 6 ISIS nodes 6 INET nodes
ID                            Type Age(s) LnkIn LnkOut Protocol
R1.00(10.0.0.1)               Rtr     148     3      3 IS-IS(2)
    To: R3.00(10.0.0.3), Local: 10.1.13.1, Remote: 10.1.13.2
    To: R5.00(10.0.0.5), Local: 10.1.15.1, Remote: 10.1.15.2
    To: R2.00(10.0.0.2), Local: 10.1.12.1, Remote: 10.1.12.2
ID                            Type Age(s) LnkIn LnkOut Protocol
                                                       OSPF(0.0.0.0)
    To: R3.00(10.0.0.3), Local: 10.1.13.1, Remote: 10.1.13.2
    To: R5.00(10.0.0.5), Local: 10.1.15.1, Remote: 10.1.15.2
    To: R2.00(10.0.0.2), Local: 10.1.12.1, Remote: 10.1.12.2
ID                            Type Age(s) LnkIn LnkOut Protocol
R2.00(10.0.0.2)               Rtr     580     4      4 IS-IS(2)
    To: R1.00(10.0.0.1), Local: 10.1.12.2, Remote: 10.1.12.1
    To: R3.00(10.0.0.3), Local: 10.1.23.1, Remote: 10.1.23.2
    To: R4.00(10.0.0.4), Local: 10.1.24.1, Remote: 10.1.24.2
    To: R6.00(10.0.0.6), Local: 10.1.26.1, Remote: 10.1.26.2
ID                            Type Age(s) LnkIn LnkOut Protocol
                                                       OSPF(0.0.0.0)
    To: R1.00(10.0.0.1), Local: 10.1.12.2, Remote: 10.1.12.1
    To: R3.00(10.0.0.3), Local: 10.1.23.1, Remote: 10.1.23.2
    To: R4.00(10.0.0.4), Local: 10.1.24.1, Remote: 10.1.24.2
    To: R6.00(10.0.0.6), Local: 10.1.26.1, Remote: 10.1.26.2
ID                            Type Age(s) LnkIn LnkOut Protocol
R3.00(10.0.0.3)               Rtr     390     4      4 IS-IS(2)
    To: R1.00(10.0.0.1), Local: 10.1.13.2, Remote: 10.1.13.1
    To: R4.00(10.0.0.4), Local: 10.1.34.1, Remote: 10.1.34.2
    To: R2.00(10.0.0.2), Local: 10.1.23.2, Remote: 10.1.23.1
    To: R6.00(10.0.0.6), Local: 10.1.36.1, Remote: 10.1.36.2
ID                            Type Age(s) LnkIn LnkOut Protocol
                                                       OSPF(0.0.0.0)
    To: R1.00(10.0.0.1), Local: 10.1.13.2, Remote: 10.1.13.1
    To: R4.00(10.0.0.4), Local: 10.1.34.1, Remote: 10.1.34.2
    To: R2.00(10.0.0.2), Local: 10.1.23.2, Remote: 10.1.23.1
    To: R6.00(10.0.0.6), Local: 10.1.36.1, Remote: 10.1.36.2
ID                            Type Age(s) LnkIn LnkOut Protocol
R4.00(10.0.0.4)               Rtr     677     4      4 IS-IS(2)
    To: R3.00(10.0.0.3), Local: 10.1.34.2, Remote: 10.1.34.1
    To: R5.00(10.0.0.5), Local: 10.1.45.1, Remote: 10.1.45.2
    To: R2.00(10.0.0.2), Local: 10.1.24.2, Remote: 10.1.24.1
    To: R6.00(10.0.0.6), Local: 10.1.46.1, Remote: 10.1.46.2
ID                            Type Age(s) LnkIn LnkOut Protocol
```

```
                                                        OSPF(0.0.0.0)
    To: R3.00(10.0.0.3), Local: 10.1.34.2, Remote: 10.1.34.1
    To: R5.00(10.0.0.5), Local: 10.1.45.1, Remote: 10.1.45.2
    To: R2.00(10.0.0.2), Local: 10.1.24.2, Remote: 10.1.24.1
    To: R6.00(10.0.0.6), Local: 10.1.46.1, Remote: 10.1.46.2
ID                           Type Age(s) LnkIn LnkOut Protocol
R5.00(10.0.0.5)              Rtr     609     3      3 IS-IS(2)
    To: R1.00(10.0.0.1), Local: 10.1.15.2, Remote: 10.1.15.1
    To: R4.00(10.0.0.4), Local: 10.1.45.2, Remote: 10.1.45.1
    To: R6.00(10.0.0.6), Local: 10.1.56.1, Remote: 10.1.56.2
ID                           Type Age(s) LnkIn LnkOut Protocol
                                                        OSPF(0.0.0.0)
    To: R1.00(10.0.0.1), Local: 10.1.15.2, Remote: 10.1.15.1
    To: R4.00(10.0.0.4), Local: 10.1.45.2, Remote: 10.1.45.1
    To: R6.00(10.0.0.6), Local: 10.1.56.1, Remote: 10.1.56.2
ID                           Type Age(s) LnkIn LnkOut Protocol
R6.00(10.0.0.6)              Rtr     633     4      4 IS-IS(2)
    To: R3.00(10.0.0.3), Local: 10.1.36.2, Remote: 10.1.36.1
    To: R4.00(10.0.0.4), Local: 10.1.46.2, Remote: 10.1.46.1
    To: R5.00(10.0.0.5), Local: 10.1.56.2, Remote: 10.1.56.1
    To: R2.00(10.0.0.2), Local: 10.1.26.2, Remote: 10.1.26.1
ID                           Type Age(s) LnkIn LnkOut Protocol
                                                        OSPF(0.0.0.0)
    To: R3.00(10.0.0.3), Local: 10.1.36.2, Remote: 10.1.36.1
    To: R4.00(10.0.0.4), Local: 10.1.46.2, Remote: 10.1.46.1
    To: R5.00(10.0.0.5), Local: 10.1.56.2, Remote: 10.1.56.1
    To: R2.00(10.0.0.2), Local: 10.1.26.2, Remote: 10.1.26.1
```

What It Means Sample Output 1 shows the configuration of the cspf-link file, cspf flag, and cspf-link flag at the [edit protocols mpls traceoptions] hierarchy level. See "Configuring CSPF Tracing" on page 76 for steps to configure CSPF tracing.

Sample Output 2 shows the contents of the cspf-link file in the /var/log/ directory on ingress router R1. The cspf-link file contains the CSPF computations logged when the cspf and cspf-link flags are configured at the [edit protocols mpls traceoptions] hierarchy level and after the run monitor start cspf and run show log cspf commands are issued.

Each line of output describes the steps taken by the CSPF algorithm to calculate the shortest path between the ingress and egress routers. Because the cspf-link flag is configured, the output shows the node and link information included in the calculations performed by the CSPF algorithm. For example, R1 (ingress router) has three links with three possible paths to the egress router (R6), Link 10.1.13.1->10.1.13.2, Link 10.1.12.1->10.1.12.2, and Link 10.1.15.1->10.1.15.2. In this instance, the CSPF algorithm selects the 10.1.13.1->10.1.13.2 link as the shortest path to the egress router.

The result of the CSPF algorithm is formed into a strict-hop ERO. For example, the ERO for the LSP R1-to-R6 contains two hops that pass through nodes 10.1.13.2/32 and 10.1.36.2.32. When the ERO is completed, CSPF for R1-to-R6 done!, the ERO is passed to the RSVP protocol process, where it is used for signaling and establishing the LSP in the network. The output shows RPD_MPLS_LSP_UP, indicating that the LSP was established successfully

Sample Output 3 shows a brief summary of the contents of the traffic engineering database. (For more detailed information, use the detail or extensive options.) When CSPF tracing is configured, the contents of the specified CSPF log file should correlate to the contents of the traffic engineering database; that is, the links shown in the output for the show log *filename* command should also appear in the output for the show ted database command. In the example network shown in Figure on page 77, the six nodes and all links associated with those nodes appear in the output of both commands.

The traffic engineering database is built through link–state routing protocol extensions that allow for the flooding of information regarding available link bandwidth, link coloring, and so on. Also, the traffic engineering database includes information contained in the OSPF and IS-IS databases. For example, R1 has three links configured at IS-IS Level 2, and the same three links configured in OPSF area 0.0.0.0.

For a more detailed examination of the traffic engineering database, see “Examining a CSPF Failure” on page 87.

Chapter 8

Examining a CSPF Failure

The ingress router determines the physical path for each label-switched path (LSP) by applying a Constrained Shortest Path First (CSPF) algorithm to the information in the traffic engineering database (TED). This chapter describes a real-world scenario in which the CSPF algorithm fails because of the incorrect association of links with administrative groups (also known as link coloring). It discusses some basic approaches to monitoring and examining a CSPF failure, including how, when, and why you use specific commands. This chapter also includes an examination of an example CSPF log file, traffic engineering database, and corrective action for the example scenario. (See Table 12.)

Table 12: Checklist for Examining a CSPF Failure

Examining a CSPF Failure Tasks	
Case Study for a CSPF Failure on page 88	
1. Verify That the LSP Is Established on page 89	show mpls lsp extensive
2. Check the Administrative Group Configuration on page 90	show configuration protocols mpls show mpls interface show ted database extensive *nodeID*
Examining a CSPF Failure on page 94	
1. Verify the CSPF Failure on page 94	clear mpls lsp show mpls lsp extensive
2. Examine the CSPF Log File on page 95	monitor start *filename* show log *filename* monitor stop
3. Examine the Traffic Engineering Database on page 97	show ted database extensive For output filtered for color: show ted database extensive *nodeID* | match "(NodeID | To: | Color)"
4. Check the Administrative Group Configuration on R5 on page 99	edit [edit protocols mpls] show delete interface so-0/0/1 admin-group set interface so-0/0/0 admin-group red show commit

Case Study for a CSPF Failure

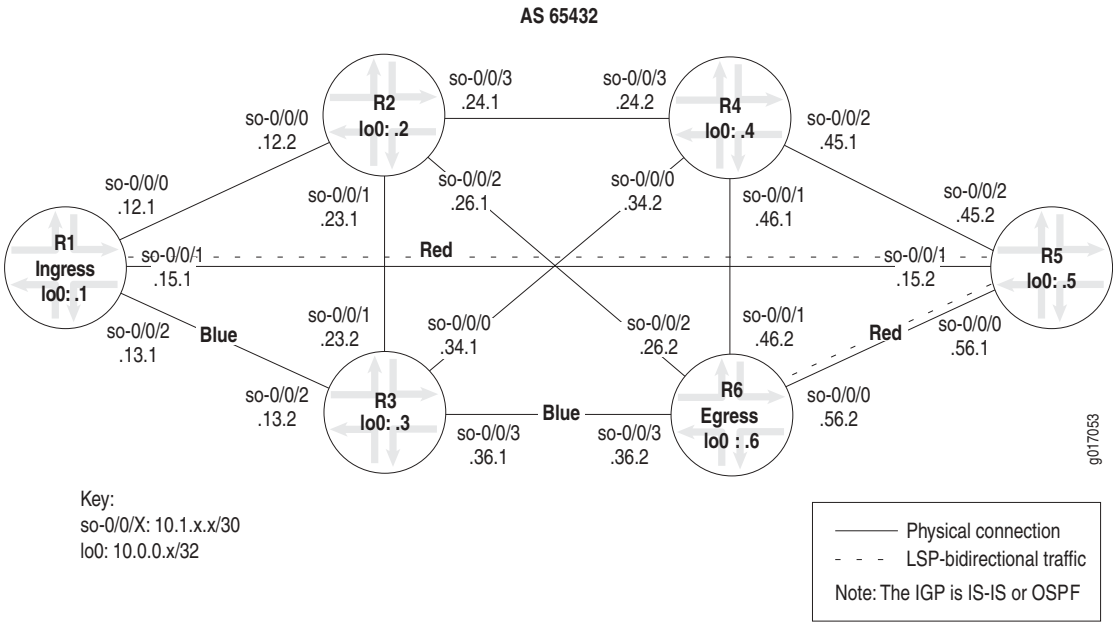
Purpose This case study presents a Multiprotocol Label Switching (MPLS) network topology and CSPF failure scenario designed to demonstrate techniques and commands that are particularly useful when addressing CSPF problems in your network. The focus of the study is the incorrect association of user-provided constraints, specifically administrative groups (also known as link coloring).

When calculating a path, the CSPF algorithm factors in user–provided constraints. The ingress router determines the physical path for each LSP by applying a CSPF algorithm to the information in the traffic engineering database. CSPF is a shortest-path-first (SPF) algorithm that has been modified to take into account constraints when calculating the shortest path across the network. Links that do not comply with the restrictions are removed from the tree and cannot be factored into the resulting SPF calculations.

CSPF integrates topology link-state information that is learned from interior gateway protocol (IGP) traffic engineering extensions and is maintained in the traffic engineering database. The information stored in the traffic engineering database includes attributes associated with the state of network resources.

The network topology shown in Figure 4 illustrates a network in which the LSP is constrained by administrative group coloring (also known as link coloring), and CSPF tracing is configured on the ingress router R1. In this example, the LSP is forced to transit R5 in accordance with the restrictions imposed.

Figure 4: CSPF Topology with Administrative Group Coloring



The network shown in Figure 4 is an MPLS router-only network with SONET interfaces. For more details about the MPLS network topology, see “Configuring CSPF Tracing” on page 73.

The MPLS network shown in Figure 4 on page 88 is configured with administrative group coloring as follows:

- The LSP R1-to-R6 is established with R1 as the ingress router and R6 as the egress router.
- The required path to R6 transits R5 on the red links. The inclusion of red coloring is not strictly necessary. To force the LSP to transit R5, you could color the links on R3 and R2 blue and then exclude the blue links.
- Both red and blue colors are used with the include and exclude statements to ensure that the LSP always transits R5. For information on configuring administrative group coloring, see the *JUNOS MPLS Applications Configuration Guide*.

Steps To Take To check that the network is configured correctly and the LSP is established, follow these steps:

1. Verify That the LSP Is Established on page 89
2. Check the Administrative Group Configuration on page 90

Step 1: Verify That the LSP Is Established

Purpose Check that the LSP shown in Figure 4 on page 88 is established and traversing the path from R1 to R6 through the red links.

Action To verify that the LSP is established, enter the following JUNOS command-line interface (CLI) operational mode command:

```
user@host> show mpls lsp extensive
user@host> show mpls lsp
```

Sample Output

```
user@R1> show mpls lsp extensive | no-more
Ingress LSP: 1 sessions

10.0.0.6
  From: 10.0.0.1, State: Up, ActiveRoute: 1, LSPname: R1-to-R6
  ActivePath:  (primary)
  LoadBalance: Random
  Metric: 100
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
 *Primary                    State: Up
          Include: red    Exclude: blue
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 20)
 10.1.15.2 S 10.1.56.2 S
    Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node
10=SoftPreempt):
          10.1.15.2 10.1.56.2
    6 May 11 19:31:42 Selected as active path
    5 May 11 19:31:42 Record Route:  10.1.15.2 10.1.56.2
    4 May 11 19:31:42 Up
    3 May 11 19:31:42 Originate Call
    2 May 11 19:31:42 CSPF: computation result accepted
    1 May 11 19:31:12 CSPF failed: no route toward 10.0.0.6[5 times]
  Created: Wed May 11 19:29:17 2005
Total 1 displayed, Up 1, Down 0
[...Output truncated...]
```

Sample Output 2

```
[edit protocols mpls]
user@R5# run show mpls lsp
Ingress LSP: 0 sessions
Total 0 displayed, Up 0, Down 0

Egress LSP: 0 sessions
Total 0 displayed, Up 0, Down 0

Transit LSP: 2 sessions
To              From            State   Rt Style Labelin Labelout LSPname
10.0.0.1        10.0.0.6        Up       1  1 FF  100352        3 R6-to-R1
10.0.0.6        10.0.0.1        Up       1  1 FF  100384        3 R1-to-R6
Total 2 displayed, Up 2, Down 0
```

What It Means Sample Output 1 from ingress router R1 shows that LSP R1-to-R6 is successfully established as indicated by the Explicit Route Object (ERO) 10.1.15.2 S 10.1.56.2 S, the log message CSPF: computation result accepted, and State: Up. Also, the LSP is routing packets correctly over the red links, avoiding the blue links or the links without any coloring. See Step 3 in "Configuring CSPF Tracing" on page 73 for information on the steps CSPF takes to select a path.

Sample Output 2 from transit router R5 shows that LSP R1-to-R6 is transiting R5 as expected.

Step 2: Check the Administrative Group Configuration

Action To check the administrative group configuration, enter the following JUNOS CLI operational mode commands, or issue the show command at the [edit protocols mpls] hierarchy level, as shown in the example below:

```
user@host> show configuration protocols mpls
user@host> show mpls interface
user@host> show ted database extensive nodeID
```

Sample Output 1

```
[edit protocols mpls]
user@R1# show
traceoptions {
    file cspf;
    flag cspf;
    flag cspf-node;
    flag cspf-link;
}
admin-groups {
    blue 4;
    red 8;
}
label-switched-path R1-to-R6 {
    to 10.0.0.6;
    metric 100;
    admin-group {
        include red;
        exclude blue;
    }
}
interface so-0/0/0.0;
interface so-0/0/1.0 {
    admin-group red;
}
```

```
interface so-0/0/2.0 {
    admin-group blue;
}
interface fxp0.0 {
    disable;
}

[edit protocols mpls]
user@R3# show
admin-groups {
    blue 4;
}
interface fxp0.0 {
    disable;
}
interface so-0/0/0.0;
interface so-0/0/1.0;
interface so-0/0/2.0 {
interface so-0/0/3.0 {
    admin-group blue;
}

[edit protocols mpls]
user@R5# show
admin-groups {
    red 8;
}
interface fxp0.0 {
    disable;
}
interface so-0/0/0.0 {
    admin-group red;
}
interface so-0/0/1.0;
interface so-0/0/2.0;

[edit protocols mpls]
user@R6# show
admin-groups {
    blue 4;
    red 8;
}
label-switched-path R6-to-R1 {
    to 10.0.0.1;
}
interface so-0/0/0.0 {
    admin-group red;
}
interface so-0/0/1.0;
interface so-0/0/2.0;
interface so-0/0/3.0 {
    admin-group blue;
}
```

Sample Output 2

```
useruser@R1> show mpls interface
Interface        State       Administrative groups
so-0/0/0.0       Up          <none>
so-0/0/1.0       Up          red
so-0/0/2.0       Up          blue
```

```
user@R1> show mpls interface
Interface        State       Administrative groups
so-0/0/0.0       Up          <none>
so-0/0/1.0       Up          red
so-0/0/2.0       Up          blue

user@R3> show mpls interface
Interface        State       Administrative groups
so-0/0/0.0       Up          <none>
so-0/0/1.0       Up          <none>
so-0/0/2.0       Up          <none>
so-0/0/3.0       Up          blue

user@R5> show mpls interface
Interface        State       Administrative groups
so-0/0/0.0       Up          red
so-0/0/1.0       Up          <none>
so-0/0/2.0       Up          <none>

user@R6> show mpls interface
Interface        State       Administrative groups
so-0/0/0.0       Up          red
so-0/0/1.0       Up          <none>
so-0/0/2.0       Up          <none>
so-0/0/3.0       Up          blue
```

Sample Output 3

```
user@R1> show ted database extensive R1
TED database: 6 ISIS nodes 6 INET nodes
NodeID: R1.00(10.0.0.1)
  Type: Rtr, Age: 665 secs, LinkIn: 3, LinkOut: 3
  Protocol: IS-IS(2)
    To: R2.00(10.0.0.2), Local: 10.1.12.1, Remote: 10.1.12.2
      Color: 0 <none>
      Metric: 10
      Static BW: 155.52Mbps
      Reservable BW: 155.52Mbps
      Available BW [priority] bps:
          [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
          [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
      Interface Switching Capability Descriptor(1):
        Switching type: Packet
        Encoding type: Packet
        Maximum LSP BW [priority] bps:
          [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
          [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
    To: R5.00(10.0.0.5), Local: 10.1.15.1, Remote: 10.1.15.2
      Color: 0x100 red
      Metric: 10
      Static BW: 155.52Mbps
      Reservable BW: 155.52Mbps
      Available BW [priority] bps:
          [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
          [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
      Interface Switching Capability Descriptor(1):
        Switching type: Packet
        Encoding type: Packet
        Maximum LSP BW [priority] bps:
          [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
          [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
    To: R3.00(10.0.0.3), Local: 10.1.13.1, Remote: 10.1.13.2
      Color: 0x10 blue
      Metric: 10
      Static BW: 155.52Mbps
```

```
Reservable BW: 155.52Mbps
Available BW [priority] bps:
    [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
    [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
Interface Switching Capability Descriptor(1):
  Switching type: Packet
  Encoding type: Packet
  Maximum LSP BW [priority] bps:
    [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
    [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
```

What It Means Sample Output 1 shows that administrative group coloring is correctly configured on all relevant routers. Administrative groups red and blue are configured at the [edit protocols mpls] hierarchy level, and relevant interfaces are associated with each administrative group correctly.

R3 is configured with blue coloring and the include and exclude statements are included in the configuration of R1 to ensure that LSP R1-to-R6 always transits R5. The inclusion of red coloring is not strictly necessary. To force the LSP to transit R5, you could color the links on R2 and R3 blue and then exclude the blue links. Red coloring is included in this example to demonstrate the fact that the CSPF algorithm excludes links that do not have a color configured, when the include statement is configured at the [edit protocols mpls] hierarchy level.

In addition, ingress router R1 has CSPF tracing configured in preparation for gathering information when the CSPF algorithm fails later in this example.

Sample Output 2 shows that the correct interfaces are associated with the red and blue administration groups on R1, R3, R5, and R6.

Sample Output 3 confirms that link coloring is correctly reported in the traffic engineering database for R1. Not shown is the traffic engineering database output for the remaining routers, which is similar to the R1 output, and correct.

Examining a CSPF Failure

Purpose When a local CSPF failure indicates that no path meets the constraints configured for the LSP, you must perform CSPF-based tracing and be familiar with the contents of the traffic engineering database to resolve the problem. See "Examine the Traffic Engineering Database" on page 97 for an analysis of the traffic engineering database.

NOTE: If an LSP does not establish immediately, wait at least a minute or so before taking diagnostic or corrective action. This is because the RSVP retry timer is set to a 30-second default, resulting in a slight delay before the correct state of the LSP is available.

Steps To Take To examine a CSPF failure, follow these steps:

1. Verify the CSPF Failure on page 94
2. Examine the CSPF Log File on page 95
3. Examine the Traffic Engineering Database on page 97
4. Check the Administrative Group Configuration on R5 on page 99

Step 1: Verify the CSPF Failure

Purpose To simulate a configuration error on the network, router R5 has the administrative group coloring removed from interface so-0/0/0. The result is a CSPF failure at R5 because there is no longer a path between R1 and R6 that includes the red color.

Action To confirm that the LSP is down and verify the configuration on routers R1 and R5, enter the following JUNOS CLI operational mode commands:

```
user@host> clear mpls lsp
user@host> show mpls lsp extensive
```

Sample Output 1

```
user@R1> clear mpls lsp

[edit protocols mpls]
user@R1# run show mpls lsp extensive
Ingress LSP: 1 sessions

10.0.0.6
  From: 0.0.0.0, State: Dn, ActiveRoute: 0, LSPname: R1-to-R6
  ActivePath: (none)
  LoadBalance: Random
  Metric: 100
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
  Primary                    State: Dn
          Include: red    Exclude: blue
    Will be enqueued for recomputation in 24 second(s).
    9 May 11 20:12:28 CSPF failed: no route toward 10.0.0.6
    8 May 11 20:12:28 Clear Call
    7 May 11 20:12:28 Deselected as active
    6 May 11 19:31:42 Selected as active path
    5 May 11 19:31:42 Record Route:  10.1.15.2 10.1.56.2
```

```
    4 May 11 19:31:42 Up
    3 May 11 19:31:42 Originate Call
    2 May 11 19:31:42 CSPF: computation result accepted
    1 May 11 19:31:12 CSPF failed: no route toward 10.0.0.6[5 times]
  Created: Wed May 11 19:29:17 2005
Total 1 displayed, Up 0, Down 1
[...Output truncated...]
```

Sample Output 2

```
[edit protocols mpls]
user@R5# run show mpls lsp
Ingress LSP: 0 sessions
Total 0 displayed, Up 0, Down 0

Egress LSP: 0 sessions
Total 0 displayed, Up 0, Down 0

Transit LSP: 1 sessions
To              From            State   Rt Style Labelin Labelout LSPname
10.0.0.1        10.0.0.6        Up       1  1 FF  100352        3 R6-to-R1
Total 1 displayed, Up 1, Down 0
```

What It Means Sample Output 1 from ingress router R1 shows that the clear mpls lsp command was issued to confirm that R1 cannot reestablish LSP R1-to-R6. The sample output from the show mpls lsp extensive command shows that LSP R1-to-R6 is down, State: Dn and ActivePath: (None); and that the CSPF has failed, CSPF failed: no route toward 10.0.0.6.

Sample Output 2 from transit router R5 shows that LSP R1-to-R6 is not included in the output, indicating that the LSP is not transiting R5.

Most network problems appear as a local CSPF failure, as shown in the sample output. The CSPF failure indicates that no path meeting the constraints for the LSP can be found in the router's traffic engineering database. To resolve these problems effectively, use CSPF tracing on the ingress router, and analyze the traffic engineering database to locate the node that should meet the constraints.

Step 2: Examine the CSPF Log File

Purpose After you have confirmed that the LSP is down, obtain more information about the possible cause of the failure.

NOTE: To obtain useful information from the CSPF log file, make sure that CSPF tracing is configured on the ingress router. For more information on configuring CSPF tracing, see "Configuring CSPF Tracing" on page 73.

Action To examine the CSPF log file, enter the following JUNOS CLI operational mode commands:

```
user@host> monitor start filename
user@host> show log filename
```

NOTE: To stop monitoring CSPF, issue the monitor stop command.

Sample Output `user@R1> monitor start cspf`

```
[edit protocols mpls]
user@R1# run show log cspf-failed3
May 27 10:22:23 trace_on: Tracing to "/var/log/cspf" started
May 27 10:22:29 CSPF adding path R1-to-R6(primary ) to CSPF queue 1
May 27 10:22:29 CSPF creating CSPF job
May 27 10:22:29
May 27 10:22:29 CSPF for path R1-to-R6(primary ), begin at R1.00 , starting
May 27 10:22:29         path include: 0x00000100    << administration group red
May 27 10:22:29         path exclude: 0x00000010    << administration group blue
May 27 10:22:29         bandwidth: CT0=0bps ; setup priority: 0; random
May 27 10:22:29 CSPF final destination 10.0.0.6
May 27 10:22:29 CSPF starting from R1.00 (10.0.0.1) to 10.0.0.6, hoplimit 254
May 27 10:22:29         constraint include 0x00000100
May 27 10:22:29         constraint exclude 0x00000010
May 27 10:22:29    Node R1.00 (10.0.0.1) metric 0, hops 0, avail 32000 32000 32000 32000
May 27 10:22:29      Link 10.1.12.1->10.1.12.2(R2.00/10.0.0.2) metric 10 color 0x00000000 bw 155.52Mbps
May 27 10:22:29         Reverse Link for 10.1.12.1->10.1.12.2 is 10.1.12.2->10.1.12.1
May 27 10:22:29         link fails include 0x00000100
May 27 10:22:29      Link 10.1.15.1->10.1.15.2(R5.00/10.0.0.5) metric 10 color 0x00000100 bw 155.52Mbps
May 27 10:22:29         Reverse Link for 10.1.15.1->10.1.15.2 is 10.1.15.2->10.1.15.1
May 27 10:22:29         link's interface switch capability descriptor #1
May 27 10:22:29           encoding: Packet, switching: Packet
May 27 10:22:29         link passes constraints
May 27 10:22:29      Link 10.1.13.1->10.1.13.2(R3.00/10.0.0.3) metric 10 color 0x00000010 bw 155.52Mbps
May 27 10:22:29         Reverse Link for 10.1.13.1->10.1.13.2 is 10.1.13.2->10.1.13.1
May 27 10:22:29         link fails include 0x00000100
May 27 10:22:29    Node R5.00 (10.0.0.5) metric 10, hops 1, avail 32000 32000 32000 32000
May 27 10:22:29      Link 10.1.15.2->10.1.15.1(R1.00/10.0.0.1) metric 10 color 0x00000100 bw 155.52Mbps
May 27 10:22:29         skipped: end point already visited
May 27 10:22:29      Link 10.1.45.2->10.1.45.1(R4.00/10.0.0.4) metric 10 color 0x00000000 bw 155.52Mbps
May 27 10:22:29         Reverse Link for 10.1.45.2->10.1.45.1 is 10.1.45.1->10.1.45.2
May 27 10:22:29         link fails include 0x00000100
May 27 10:22:29      Link 10.1.56.1->10.1.56.2(R6.00/10.0.0.6) metric 10 color 0x00000000 bw 155.52Mbps
May 27 10:22:29         Reverse Link for 10.1.56.1->10.1.56.2 is 10.1.56.2->10.1.56.1
May 27 10:22:29         link fails include 0x00000100
May 27 10:22:29 CSPF completed in 0s
May 27 10:22:29 CSPF couldn't find a route to 10.0.0.6
May 27 10:22:29 CSPF for R1-to-R6 done!
monitor stop
```

What It Means The sample output shows that the monitor start cspf command was issued to start displaying entries in the cspf log file in real time. The cspf log file is generated by the routing protocol process after the file is configured with the traceoptions statement at the [edit protocols mpls] hierarchy level. In this example, the cspf log file is configured with the cspf, cspf-node, and cspf-link flags to provide the most granular information about the steps taken by the CSPF algorithm. For information on configuring CSPF tracing, see "Configuring CSPF Tracing" on page 73.

The only link that passes the color constraint is between R1 and R5, 10.1.15.0/32. The CSPF algorithm is a locally run algorithm, which makes its calculations on a given router. When the CSPF algorithm runs on R5, it prunes 10.1.15.2 and selects 10.1.56.1 to send the message to R6.The link between R5 and R6 10.1.56.0/32 does not pass the color constraints, indicating a problem with R5. At this stage, it is useful to examine the traffic engineering database to determine which link on R5 should be associated with the red color.

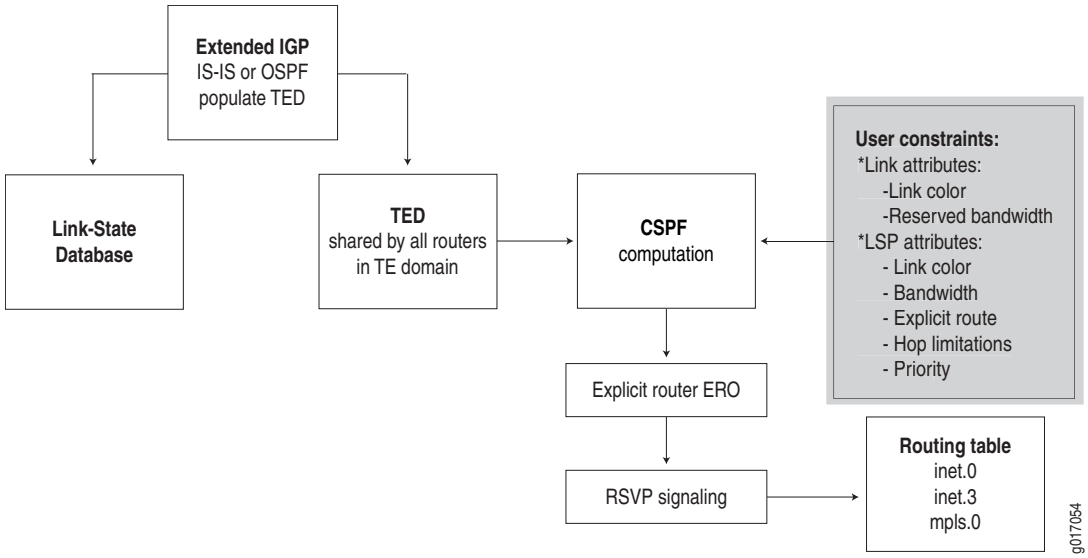
Step 3: Examine the Traffic Engineering Database

Purpose Examining the traffic engineering database is another way to locate the node that should meet the constraints but does not. Once identified, you can concentrate your troubleshooting efforts on why that node is not being represented accurately in the database.

The contents of the traffic engineering database are consistent among all routers within a given traffic engineering domain. Therefore, you can issue the show ted database command from any router in the same traffic engineering domain to obtain more granular information about the CSPF failure.

CSPF integrates topology link-state information that is learned from the IGP traffic engineering extensions and maintained in the traffic engineering database. The information stored in the traffic engineering database includes attributes associated with the state of the network resources (such as total link bandwidth, reserved link bandwidth, available link bandwidth, and link color). When calculating a path, the CSPF algorithm factors in user–provided information such as bandwidth requirements, maximum allowed hop count, and administrative groups, all of which are obtained from user configuration. (See Figure 5).

Figure 5: User–Provided Constraints



Action To examine the traffic engineering database, enter the following JUNOS CLI operational mode commands:

```
user@host> show ted database extensive
user@host> show ted database extensive NodeID | match "(NodeID|To:|Color)"
```

Sample Output 1

```
[edit protocols mpls]
user@R1# run show ted database extensive
TED database: 6 ISIS nodes 6 INET nodes
[...Output truncated...]
NodeID: R5.00(10.0.0.5)
  Type: Rtr, Age: 103 secs, LinkIn: 3, LinkOut: 3
  Protocol: IS-IS(2)
    To: R1.00(10.0.0.1), Local: 10.1.15.2, Remote: 10.1.15.1
      Color: 0x100 red
      Metric: 10
      Static BW: 155.52Mbps
      Reservable BW: 155.52Mbps
      Available BW [priority] bps:
          [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
          [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
      Interface Switching Capability Descriptor(1):
        Switching type: Packet
        Encoding type: Packet
        Maximum LSP BW [priority] bps:
          [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
          [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
    To: R4.00(10.0.0.4), Local: 10.1.45.2, Remote: 10.1.45.1
      Color: 0 <none>
      Metric: 10
      Static BW: 155.52Mbps
      Reservable BW: 155.52Mbps
      Available BW [priority] bps:
          [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
          [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
      Interface Switching Capability Descriptor(1):
        Switching type: Packet
        Encoding type: Packet
        Maximum LSP BW [priority] bps:
          [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
          [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
    To: R6.00(10.0.0.6), Local: 10.1.56.1, Remote: 10.1.56.2
      Color: 0 <none>
      Metric: 10
      Static BW: 155.52Mbps
      Reservable BW: 155.52Mbps
      Available BW [priority] bps:
          [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
          [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
      Interface Switching Capability Descriptor(1):
        Switching type: Packet
        Encoding type: Packet
        Maximum LSP BW [priority] bps:
          [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
          [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
[...Output truncated...]
```

Sample Output 2

```
[edit protocols]
user@R1# run show ted database extensive R5.00 | match "(NodeID|To:|Color)"
NodeID: R5.00(10.0.0.5)
    To: R1.00(10.0.0.1), Local: 10.1.15.2, Remote: 10.1.15.1
      Color: 0x100 red
    To: R4.00(10.0.0.4), Local: 10.1.45.2, Remote: 10.1.45.1
      Color: 0 <none>
    To: R6.00(10.0.0.6), Local: 10.1.56.1, Remote: 10.1.56.2
      Color: 0 <none>
    To: R1.00(10.0.0.1), Local: 10.1.15.2, Remote: 10.1.15.1
      Color: 0x100 red
```

```
To: R4.00(10.0.0.4), Local: 10.1.45.2, Remote: 10.1.45.1
  Color: 0 <none>
To: R6.00(10.0.0.6), Local: 10.1.56.1, Remote: 10.1.56.2
  Color: 0 <none>
```

What It Means Sample Output 1 from ingress router R1 shows a wealth of information on each node in the network, although only a portion is included in this example. The output shows the total number of IS-IS and INET nodes in the traffic engineering domain. The portion of the traffic engineering database shown represents a node (R5), and the Type field indicates Rtr (router). The Type field could also indicate Net (network) if the node were a pseudo node. The node (R5) has three input and output links that are running IS-IS Level 2, Protocol: IS-IS(2). The links lead to nodes R1, R4, and R6. The local address and remote address for each link is specified. The information on each node includes administrative groups (Color:), metrics, static bandwidth, reservable bandwidth, and available bandwidth priority level. The information contained in the traffic engineering database should be the same across all routers in the same traffic engineering domain. For a detailed description of the fields in the output of the show ted database extensive command, see the *JUNOS Routing Protocols and Policies Command Reference*.

Sample Output 2 shows filtered output that allows you to focus on exactly what is missing or incorrect.

Both outputs confirm that the link between R1 and R5, 10.1.15.0/32, is associated with the red color, while the link between R5 and R6, 10.1.56.0/32, is not associated with a color. In the network shown in Figure 4 on page 88, for the LSP to establish correctly, link 10.1.56.1 must be associated with the red color.

Step 4: Check the Administrative Group Configuration on R5

Purpose Focus on R5 to determine which interfaces are associated with the red color, and make any necessary corrections.

Action To check the administrative group configuration on R5 and make any necessary corrections, enter the following JUNOS CLI commands:

```
user@R5> edit
[edit protocols mpls]
user@R5# show
user@R5# delete interface so-0/0/1 admin-group
user@R5# set interface so-0/0/0 admin-group red
user@R5# show
user@R5# commit
```

Sample Output 1

```
user@R5> edit
Entering configuration mode

[edit protocols mpls]
user@R5# show
admin-groups {
    red 8;
}
interface fxp0.0 {
    disable;
}
interface so-0/0/0.0;
interface so-0/0/1.0 {      <<<incorrect interface configured with admin-group
    admin-group red;
}
interface so-0/0/2.0;
```

Sample Output 2

```
[edit protocols mpls]
user@R5# delete interface so-0/0/1 admin-group

[edit protocols mpls]
user@R5# set interface so-0/0/0 admin-group red

[edit protocols mpls]
user@R5# show
admin-groups {
    red 8;
    blue 4;
}
interface fxp0.0 {
    disable;
}
interface so-0/0/0.0 {      <<<correct interface configured with admin-group
    admin-group red;
}
interface so-0/0/1.0;
interface so-0/0/2.0;

[edit protocols mpls]
user@R5# commit
commit complete
```

Sample Output 3

```
user@R1> show mpls lsp
Ingress LSP: 1 sessions
To              From            State Rt ActivePath       P     LSPname
10.0.0.6        10.0.0.1        Up     1                  *     R1-to-R6
Total 1 displayed, Up 1, Down 0

Egress LSP: 1 sessions
To              From            State   Rt Style Labelin Labelout LSPname
10.0.0.1        10.0.0.6        Up       0  1 FF       3        - R6-to-R1
Total 1 displayed, Up 1, Down 0

Transit LSP: 0 sessions
Total 0 displayed, Up 0, Down 0
```

What It Means Sample Output 1 from transit router R5 shows that at the [edit protocols mpls] hierarchy level, interface so-0/0/1 is incorrectly configured with the admin-group red statement. The so-0/0/0 interface should be configured with the admin-group red statement.

Sample Output 2 shows the steps taken to correct the configuration. The administration group has been deleted from so-0/0/1 and so-0/0/0 is now associated with the red color.

Sample Output 3 shows that LSP R1-to-R6 is established.

Part 3

Examining the RSVP Log

This section describes how and when to configure Resource Reservation Protocol (RSVP) tracing on a network, and provides information about the output for the traceoptions command.

The following information is covered:

Chapter 9

Understanding the Structure of RSVP

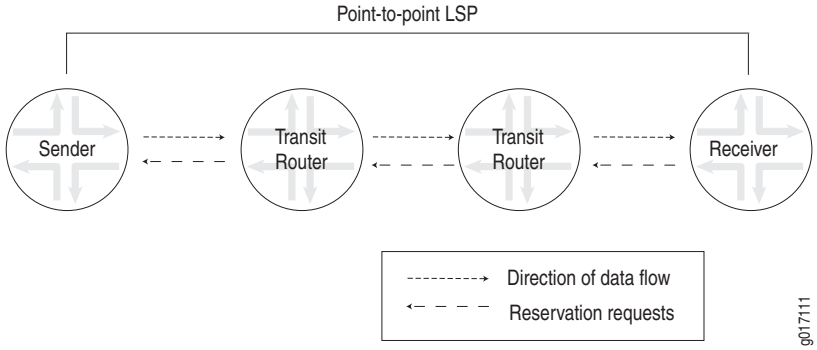
Considering that Resource Reservation Protocol (RSVP)-signaled label-switched paths (LSPs) are primarily established using RSVP Path and Resv messages, it is useful to understand the structure of RSVP when you examine a problem with an LSP. This chapter discusses the following topics:

RSVP Overview

The RSVP protocol is used by routers to deliver quality-of-service (QoS) requests to all nodes along data flow path(s) and to establish and maintain state for the requested service. RSVP requests generally result in resource reservations in each node along the data path. RSVP has the following attributes:

- Makes resource reservations for unidirectional data flows.
- Allows the receiver of a data flow to initiate and maintain the resource reservation used for that flow, as shown in Figure 6.
- Maintains a soft state in routers and hosts, providing graceful support for dynamic membership changes and automatic adaptation to routing changes.
- Depends upon present and future routing protocols, but is not a routing protocol itself.
- Provides several reservation models or styles to fit a variety of applications.
- Supports both IPv4 and IPv6. Note, you can configure the JUNOS software to tunnel IPv6 over an MPLS-based IPv4 network. For more information, see the *JUNOS MPLS Applications Configuration Guide.*

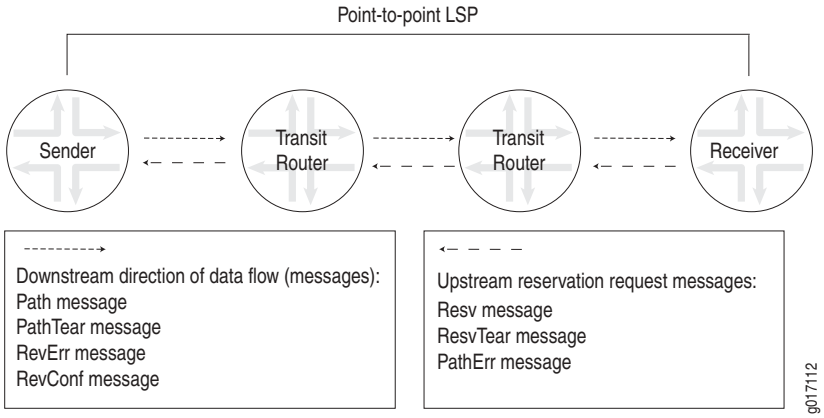
Figure 6: RSVP Reservation Request and Data Flow



RSVP Session Overview

RSVP creates independent sessions to handle each data flow. It is important to note that each session is simplex, even though bidirectional messages (Path and Resv) create the simplex session. 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. Figure 7 shows a simplified overview of an RSVP point-to-point session. For information on point-to-multipoint LSPs, see the *JUNOS MPLS Applications Configuration Guide*.

Figure 7: RSVP Session



A typical RSVP session involves the following sequence of events:

- A potential sender (ingress router) starts sending RSVP Path messages to the session address (egress router).
- The receiver receives the Path messages.
- 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.
- The sender receives the Resv message, then starts sending application data.

RSVP Message Structure

RSVP was extended by various Requests for Comments (RFCs) to function as a signaling protocol to create Multiprotocol Label Switching (MPLS) LSPs. The signaling occurs with RSVP messages which are encapsulated directly with IP datagrams using a protocol ID of 46. Each RSVP message uses a common header followed by various objects, as shown in Figure 8.

Figure 8: RSVP Common Header

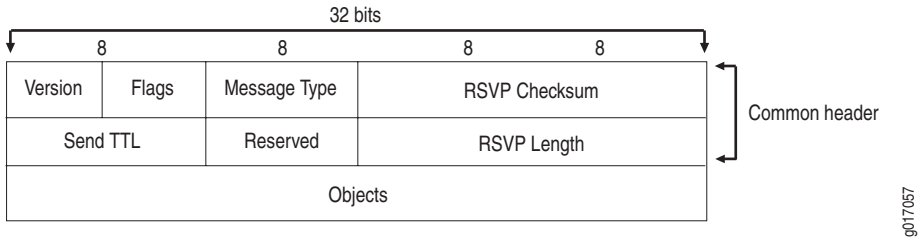


Table 13 lists and describes the fields in the RSVP common header.

Table 13: Fields in the RSVP Common Header

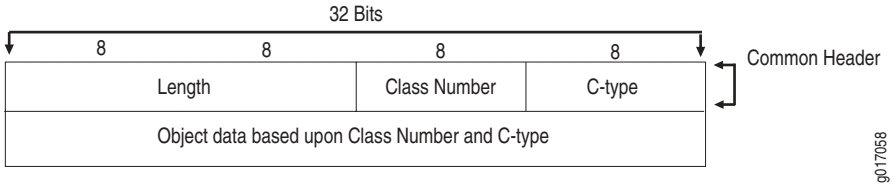
Field Name	Defined	Description
Version	4 bit	JUNOS software supports RSVP version 1.
Flags	4 bits Ox01 to 0x08 0x01: Refresh overhead reduction 0x02 to 0x08: Reserved	Used to signal support for protocol extensions to neighboring RSVP routers.
Message Type	1 Path (RFC 2205) 2 Resv (RFC 2205) 3 PathErr (RFC 2205) 4 ResvErr (RFC 2205) 5 PathTear (RFC 2205) 6 ResvTear (RFC 2205) 7 ResvConf (RFC 2205) 12 Bundle (RFC 2961) 13 Ack (RFC 2961) 15 SRefresh (RFC 2961) 20 Hello (RFC 3209) 25 Integrity Challenge (RFC 3097) 26 Integrity Response (RFC 3097)	Displays the number for the type of RSVP message encoded in the packet. For a detailed description of some message types, see “Examining RSVP Log Messages” on page 123 and “Examining RSVP Error Messages” on page 143.
RSVP Checksum	16 bits	Displays a standard IP checksum for the entire RSVP message. When the checksum is computed, the local router assumes that this field contains zeros.
Send TTL	8 bits	Derived from the IP packet time to live (TTL). If the IP TTL value does not match the value in the Send TTL field, the previous node does not support RSVP.

Field Name	Defined	Description
Reserved	8 bits	This field is no used and must be set to 0x00.
RSVP Length	16 bits	Displays the entire RSVP packet, including any optional objects that are attached to the message.
Objects	Variable	This variable-length field contains one or more RSVP objects. For a more detailed description of objects, see "RSVP Objects Structure" on page 109.

RSVP Objects Structure

RSVP objects carry the information that comprises the contents of RSVP messages. Different combinations of objects define the information necessary for RSVP to signal LSPs. Each object is represented by a fixed-length header and a variable-length data field, as shown in Figure 9.

Figure 9: RSVP Object Header



The maximum object content length is 65,528 bytes. The Class-Num and C-Type fields may be used together as a 16-bit number to define a unique type for each object. Table 14 lists and describes the fields in the RSVP object header.

Table 14: Fields in the RSVP Object Header

Field Name	Defined	Description
Length	16 bits	Contains the total object length and must always be a multiple of 4.
Class-Num	The values of this field are defined in Appendix A, RFC 2205, *Resource ReSerVation Protocol (RSVP), Version 1, Functional Specification*.	Identifies the object class; for example, Session. For more information about object classes, see Table 15

Field Name	Defined	Description
C-Type	For a breakdown of the C-Type associated with each RSVP object, see Appendix A, RFC 2205.	Coded with values that are unique to each class number (Class-Num); for example, C-Type 1.
Object Data	The Class-Num and C-Type may be used to define a unique object. C-Type is the object type and is used to accommodate different Internet address families, such as those corresponding to IPv4 and IPv6 [44]. Currently, C-Type 1 is assigned to IPv4 and C-Type 2 is used for IPv6. The structure and format of the objects may change from one family to another.	Contains the data identified by the Class-Num and C-Type fields. For more information on object data, see Table 15.

The setup and maintenance of an RSVP session requires information that is encoded in multiple objects used in the various RSVP message types. Table 15 lists and describes some RSVP objects, the messages in which they are used, and the RFC to which you can refer for further information. The objects are listed in alphabetical order.

Table 15: RSVP Objects

Object Name	RSVP Message	RFC	Description
Adspec	Path	2205	Carries a summary of available services, delay and bandwidth estimates, and operating parameters used by specific QoS control services. The summary is computed as the Adspec passes each hop. The JUNOS software uses the Adspec field for maximum transmission unit (MTU) negotiation.
Detour	Path		Used in one-to-one backup to identify detour LSPs. For more information on the Detour object, see Internet draft draft-ietf-mpls-rsvp-lsp-fastreroute-03.txt, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels.*
Error	PathErr, ResvErr, ResvConf	2205	Specifies an error in a PathErr or ResvErr message, or a confirmation in a ResvConf message.
Explicit route	Path	3209	Specifies a strict or loose path in the network topology.
FastReroute	Path		Used to control the backup for a protected LSP. The fast reroute object specifies the setup and hold priorities, the session attribute filters, and the bandwidth to be used for protection. It also allows a specific local protection technique to be requested. For more information on the fast reroute object, see Internet draft draft-ietf-mpls-rsvp-lsp-fastreroute-03.txt, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels.*
Filter	Resv ResvTear ResvErr		Defines the source of the session.

Object Name	RSVP Message	RFC	Description
FilterSpec	Resv	2205, 3209	Defines a subset of session data packets that should receive the desired QoS specified by a flow specification object.
FlowSpec	Resv	2205, 2210	Defines a desired QoS.
Hello	Hello	3209	Can be a request or a reply. Every request should generate a reply.
Hop	Path, Resv	2205	Carries the IP address of the RSVP-capable node that sent the message, and a logical outgoing interface.
Integrity	All message types	2205, 2747, 3097	Carries cryptographic data to authenticate the originating node and verify the contents of an RSVP message.
Label	Resv	3209	Contains the label value (for example, 100624) that is mapped to the LSP identified by the session value.
LabelRequest	Path	3209	Indicates, to the next downstream node, that a label assignment is requested.
Null			Has a class number of zero, and its C-Type is ignored. Its length must be at least 4, but can be any multiple of 4. A NULL object may appear anywhere in a sequence of objects, and its contents will be ignored by the receiver.
Policy data	Path, Resv, PathErr, ResvErr	2205	Carries information that allows a local policy module to decide whether an associated reservation is administratively permitted. The use of policy data objects is not fully specified at this time.
Properties		Juniper only	Specifies a Juniper Networks proprietary object used to carry information about the LSP.
RecRoute	Path, Resv	3209	Indicates the list of addresses that this Path message has transited.
RestartCap	Hello	3473	Indicates the sender node's graceful restart capability.
ResvConf	Resv, ResvConf	2205	Response to confirm a reservation request.
Scope	Resv, ResvErr, ResvTear	2205	Carries an explicit list of sender hosts towards which the information in the message is forwarded.
Sender	Path	2205, 3209	Contains a sender IP address and perhaps some additional demultiplexing information to identify a sender.
Session	All message types	2205, 3209	Contains the IP destination address (DestAddress), the IP protocol ID, and some form of generalized destination port, to define a specific session for the other objects that follow.

Object Name	RSVP Message	RFC	Description
SessionAttribute	Path	3209	Indicates a variety of parameters including setup priority, hold priority, flags, name length, and session name.
SrcRoute	Path		Contains the list of addresses in the Explicit Route Object (ERO).
Style	Resv	2205, 3209	Defines the reservation style, plus style-specific information that is not in flow specification or filter specification objects.
Time	Path, Resv	2205	Contains the value for the refresh period used by the creator of the message.
Tspec	Path	2205	Defines the traffic characteristics of a sender's data flow.

Chapter 10

Working with RSVP Tracing

This chapter describes how and when to configure tracing for a Resource Reservation Protocol (RSVP) signaled label-switched path (LSP) in a Multiprotocol Label Switched (MPLS) network. With each flag that you configure, different kinds of information about RSVP are provided by the RSVP log file output. (See Table 16.)

Table 16: Checklist for Working with RSVP Tracing

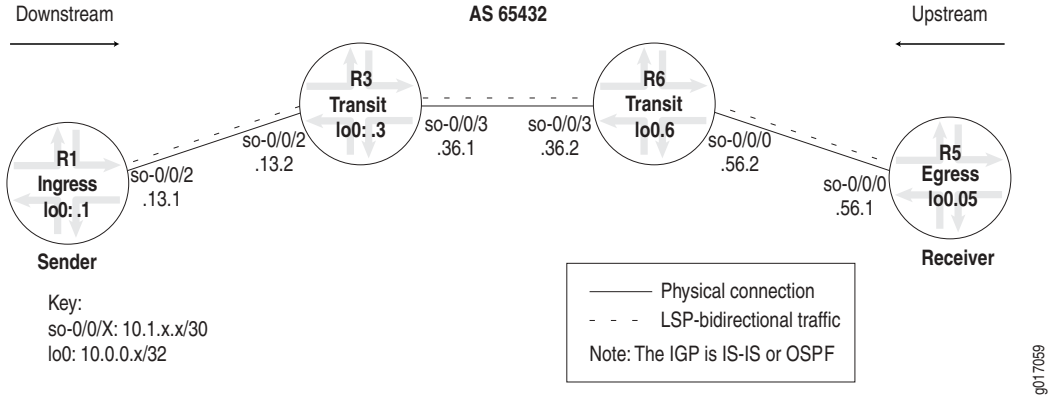
Working with RSVP Tracing Tasks	Possible Action or Command
Enabling RSVP Tracing on page 114	
1. Configure RSVP Tracing on page 115	[edit] edit protocols rsvp [edit protocols rsvp] set traceoptions file *filename* set traceoptions flag *flag* show commit
2. Display the RSVP Log File on page 117	
a. (Optional) Clear the RSVP Session and Log File on page 117	clear rsvp session clear log *filename*
b. Display Real-Time RSVP Log Entries on page 118	monitor start *filename* monitor stop
c. View the RSVP Log File on page 119	show log *filename*
d. Deactivate and Reactivate RSVP Tracing on page 120	[edit protocols rsvp] deactivate traceoptions activate traceoptions

Enabling RSVP Tracing

Purpose When the output of the show mpls lsp extensive command indicates that there is a problem with the LSP, you can enable RSVP tracing on the routers included in the LSP, especially the ingress and egress routers, and examine the RSVP log file to obtain more detailed information and solve the problem faster.

Figure 10 illustrates the example network topology used throughout the RSVP section. The example MPLS network uses Intermediate System-to-Intermediate System (IS-IS) Level 2 and a policy to create traffic. However, IS-IS Level 1 or an Open Shortest Path First (OSPF) area can be used and the policy omitted if the network has existing Border Gateway Protocol (BGP) traffic.

Figure 10: MPLS Network Topology



The MPLS network shown in Figure 10 is a router-only network with SONET interfaces that consist of the following components:

- A full-mesh interior BGP (IBGP) topology, using AS 65432.
- MPLS and RSVP enabled on all routers.
- A send-statics policy on router R1 that allows a new route to be advertised into the network.
- Two unidirectional LSPs between R1 and R5, allowing bidirectional traffic.

See the *JUNOS MPLS Network Operations Guide* for information on configuring an MPLS network.

Steps To Take To enable RSVP tracing, follow these steps:

1. Configure RSVP Tracing on page 115
2. Display the RSVP Log File on page 117

Step 1: Configure RSVP Tracing

Action To configure a log file and specify RSVP tracing flags, follow these steps:

1. In configuration mode, go to the following hierarchy level:

   ```
   [edit]
   user@host# edit protocols rsvp
   ```

2. Configure a log file:

   ```
   [edit protocols rsvp]
   user@host# set traceoptions file filename
   ```

3. Depending on your situation, specify the appropriate RSVP-specific tracing flag from Table 17 on page 116. For example:

   ```
   [edit protocols mpls]
   user@host# set traceoptions flag path detail
   ```

4. Verify and commit the configuration:

   ```
   user@host# show
   user@host# commit
   ```

Sample Output

```
user@R1> edit
Entering configuration mode

[edit]
user@R1# edit protocols rsvp

[edit protocols rsvp]
user@R1# set traceoptions file rsvp-log

[edit protocols rsvp]
user@R1# set traceoptions flag error detail

[edit protocols rsvp]
user@R1# set traceoptions flag path detail

[edit protocols rsvp]
user@R1# set traceoptions flag pathtear detail

[edit protocols rsvp]
user@R1# show
traceoptions {
    file rsvp-log;
    flag error detail;
    flag path detail;
    flag pathtear detail;
}
interface so-0/0/2.0;
interface fxp0.0 {
    disable;
}

[edit protocols rsvp]
user@R1# commit
commit complete
```

What It Means The sample output shows the configuration of RSVP tracing on ingress router R1. The log file rsvp-log contains all the information gathered for the configured flags. In the sample output, three flags are configured: error, path, and pathtear. All flags are configured with the detail option. Each flag that you configure provides slightly different information about RSVP traffic. The error flag traces all detected error conditions, the path flag traces all Path messages, and the pathtear flag traces PathTear messages. The detail option shows granular details about the flag included in the configuration. .

NOTE: Use the tracing flags detail and all with caution. These flags may cause the central processing unit (CPU) to become very busy.

Table 17 shows the tracing flags you can configure at the [edit protocols rsvp traceoptions] hierarchy level.

Table 17: RSVP Tracing Flags

Flag	Description
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

For information about examining an RSVP log file, see “Examining RSVP Log Messages” on page 123 and “Examining RSVP Error Messages” on page 143.

Step 2: Display the RSVP Log File

Purpose There are at least two ways to display the RSVP log file. After you configure and commit the tracing configuration, information is immediately sent to the log file. The log information can be displayed in real time on your computer screen with the monitor start command, or you can issue the show log *filename* command to display the entries already gathered in the log file.

Also, you may need to issue clear commands to ensure that your records are current. However, if your network is large with many LSPs and RSVP sessions, this may not be advisable. For more information about the clear rsvp session command, see the *JUNOS Routing Protocols and Policies Command Reference.*

Steps To Take To display the RSVP log file, follow these steps:

1. (Optional) Clear the RSVP Session and Log File on page 117
2. Display Real-Time RSVP Log Entries on page 118
3. View the RSVP Log File on page 119
4. Deactivate and Reactivate RSVP Tracing on page 120

1. (Optional) Clear the RSVP Session and Log File

Action To clear the RSVP session and log file, enter the following JUNOS command-line interface (CLI) operational mode commands:

```
user@host> clear rsvp session
user@host> clear log filename
```

Sample Output

```
user@R1> clear rsvp session

user@R1> clear log rsvp-log
```

What It Means The sample output shows that the clear commands were issued correctly, with the following results:

- The RSVP sessions were reset and restarted. For more information about options for the clear rsvp session command that can limit the impact to your network, see the *JUNOS Routing Protocols and Policies Command Reference.*
- The contents of the log file were removed. For more information about the clear log command, see *JUNOS System Basics and Services Command Reference.*

2. Display Real-Time RSVP Log Entries

Action To display real-time log entries on your computer screen, enter the following JUNOS CLI operational mode command:

user@host> **monitor start** *filename*

NOTE: To stop displaying real-time RSVP log entries on your computer screen, issue the monitor stop command. The monitor stop command does not stop tracing information from going into the RSVP log file.

Sample Output

```
user@R1> monitor start rsvp-log

user@R1>
*** rsvp-log ***
Jun 16 17:12:23 R1 clear-log[9511]: logfile cleared
Jun 16 18:34:51 trace_on: Tracing to "/var/log/rsvp-log" started
Jun 16 18:35:09 RSVP send Path 10.0.0.1->10.0.0.5 Len=216 so-0/0/2.0
Jun 16 18:35:09   Session7 Len 16 10.0.0.5(port/tunnel ID 26619) Proto 0
Jun 16 18:35:09   Hop      Len 12 10.1.13.1/0x08678198
Jun 16 18:35:09   Time     Len  8 30000 ms
Jun 16 18:35:09   SrcRoute Len 28  10.1.13.2 S 10.1.36.2 S 10.1.56.1 S
Jun 16 18:35:09   LabelRequest Len  8 EtherType 0x800
Jun 16 18:35:09   Properties Len 12 Primary path
Jun 16 18:35:09   SessionAttribute Len 16 Prio (7,0) flag 0x0 "R1-to-R5"
Jun 16 18:35:09   Sender7  Len 12 10.0.0.1(port/lsp ID  3)
Jun 16 18:35:09   Tspec    Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500
Jun 16 18:35:09   ADspec   Len 48 MTU 1500
Jun 16 18:35:09   RecRoute Len 12  10.1.13.1
Jun 16 18:35:27 RSVP recv Path 10.0.0.5->10.0.0.1 Len=216 so-0/0/2.0
Jun 16 18:35:27   Session7 Len 16 10.0.0.1(port/tunnel ID 23942) Proto 0
Jun 16 18:35:27   Hop      Len 12 10.1.13.2/0x08680198
Jun 16 18:35:27   Time     Len  8 30000 ms
Jun 16 18:35:27   SrcRoute Len 12  10.1.13.1 S
Jun 16 18:35:27   LabelRequest Len  8 EtherType 0x800
Jun 16 18:35:27   Properties Len 12 Primary path
Jun 16 18:35:27   SessionAttribute Len 16 Prio (7,0) flag 0x0 "R5-to-R1"
Jun 16 18:35:27   Sender7  Len 12 10.0.0.5(port/lsp ID  2)
Jun 16 18:35:27   Tspec    Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500
Jun 16 18:35:27   ADspec   Len 48 MTU 1500
Jun 16 18:35:27   RecRoute Len 28  10.1.13.2 10.1.36.2 10.1.56.1
monitor stop
```

Sample Output The sample output shows real-time tracing information displayed on your computer screen (*** rsvp-log ***), and that display to the computer screen was started (monitor start) and then stopped (monitor stop). Even though you have stopped displaying log file entries on your screen, the tracing is still occurring on the router configured with trace options. The log file displays a Path message that was sent from R1 to R5, and another that R1 received from R5, indicating that the two unidirectional LSPs between R1 and R5 are established. For more information about Path messages, see “Examining RSVP Log Messages” on page 123.

If you stop monitoring to your screen and want to view the contents of the log file, use the show log *filename* command. For steps to view the log file, see “View the RSVP Log File” on page 119.

3. View the RSVP Log File

Action To view the contents of the RSVP log file, enter the following JUNOS CLI operational mode command:

user@host> **show log** *filename*

Sample Output

```
user@R1> show log rsvp-log
Jun 16 17:12:23 R1 clear-log[9511]: logfile cleared
Jun 16 18:34:51 trace_on: Tracing to "/var/log/rsvp-log" started
Jun 16 18:35:09 RSVP send Path 10.0.0.1->10.0.0.5 Len=216 so-0/0/2.0
Jun 16 18:35:09   Session7 Len 16 10.0.0.5(port/tunnel ID 26619) Proto 0
Jun 16 18:35:09   Hop      Len 12 10.1.13.1/0x08678198
Jun 16 18:35:09   Time     Len  8 30000 ms
Jun 16 18:35:09   SrcRoute Len 28  10.1.13.2 S 10.1.36.2 S 10.1.56.1 S
Jun 16 18:35:09   LabelRequest Len  8 EtherType 0x800
Jun 16 18:35:09   Properties Len 12 Primary path
Jun 16 18:35:09   SessionAttribute Len 16 Prio (7,0) flag 0x0 "R1-to-R5"
Jun 16 18:35:09   Sender7  Len 12 10.0.0.1(port/lsp ID  3)
Jun 16 18:35:09   Tspec    Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500
Jun 16 18:35:09   ADspec   Len 48 MTU 1500
Jun 16 18:35:09   RecRoute Len 12  10.1.13.1
Jun 16 18:35:27 RSVP recv Path 10.0.0.5->10.0.0.1 Len=216 so-0/0/2.0
Jun 16 18:35:27   Session7 Len 16 10.0.0.1(port/tunnel ID 23942) Proto 0
Jun 16 18:35:27   Hop      Len 12 10.1.13.2/0x08680198
Jun 16 18:35:27   Time     Len  8 30000 ms
Jun 16 18:35:27   SrcRoute Len 12  10.1.13.1 S
Jun 16 18:35:27   LabelRequest Len  8 EtherType 0x800
Jun 16 18:35:27   Properties Len 12 Primary path
Jun 16 18:35:27   SessionAttribute Len 16 Prio (7,0) flag 0x0 "R5-to-R1"
Jun 16 18:35:27   Sender7  Len 12 10.0.0.5(port/lsp ID  2)
Jun 16 18:35:27   Tspec    Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500
Jun 16 18:35:27   ADspec   Len 48 MTU 1500
Jun 16 18:35:27   RecRoute Len 28  10.1.13.2 10.1.36.2 10.1.56.1
```

What It Means The sample output shows the tracing information in the rsvp-log file. The first entry shows that the log file was cleared, and the second entry shows that tracing is going to the rsvp-log file in the /var/log/ directory.

The log file displays a Path message that was sent from R1 to R5, and another that R1 received from R5, indicating that the two unidirectional LSPs between R1 and R5 are established. For more information about Path messages, see “Examining RSVP Log Messages” on page 123.

4. Deactivate and Reactivate RSVP Tracing

Purpose When you configure and commit a tracing configuration, tracing information is immediately sent to the configured log file. The tracing activity goes on in the background and can create additional activity on the CPU. In this case, it is good practice to deactivate trace options, and then reactivate it when you need more tracing information.

NOTE: Implementing trace options consumes CPU resources and affects the packet processing performance.

Action To deactivate and then reactivate tracing, enter the following JUNOS CLI operational mode command:

```
[edit protocols rsvp]
user@host# deactivate traceoptions
user@host# activate traceoptions
```

Sample Output

```
[edit protocols rsvp]
user@R1# deactivate traceoptions

[edit protocols rsvp]
user@R1# show
inactive: traceoptions {
    file rsvp-log;
    flag error detail;
    flag path detail;
    flag pathtear detail;
}
interface so-0/0/0.0;
interface so-0/0/1.0;
interface so-0/0/2.0;
interface fxp0.0 {
    disable;
}

[edit protocols rsvp]
user@R1# commit
commit complete

[edit protocols rsvp]
user@R1# activate traceoptions

[edit protocols rsvp]
user@R1# show
traceoptions {
    file rsvp-log;
    flag error detail;
    flag path detail;
    flag pathtear detail;
}
```

```
interface so-0/0/0.0;
interface so-0/0/1.0;
interface so-0/0/2.0;
interface fxp0.0 {
    disable;
}

[edit protocols rsvp]
user@R1# commit
commit complete
```

What It Means The sample output shows that trace options was deactivated and then reactivated.

In a configuration, you can deactivate statements and identifiers so that they do not take effect when you issue the commit command. Any deactivated statements and identifiers are marked with the inactive: tag. They remain in the configuration, but are not activated when you issue a commit command.

Chapter 11

Examining RSVP Log Messages

The Resource Reservation Protocol (RSVP) uses the messages listed in Table 18 to establish and remove paths for data flows, establish and remove reservation information, and confirm the establishment of reservations. The RSVP tracing log file provides useful information about RSVP traffic in the network. This chapter describes the purpose of each RSVP message (except the PathErr and ResvErr messages) that can appear in the output of the rsvp-log file configured at the [edit protocols rsvp traceoptions] hierarchy level.

For information on RSVP PathErr and ResvErr messages, see "Examining RSVP Error Messages" on page 143.

Table 18: Checklist for Examining RSVP Log Messages

Examining RSVP Log Messages Tasks	Possible Action or Command
Examining the Path Message on page 124	monitor start *filename* monitor stop
Examining the Resv Message on page 129	monitor start *filename* monitor stop
Examining the PathTear Message on page 132	monitor start *filename* monitor stop
Examining the ResvTear Message on page 135	monitor start *filename* monitor stop
Examining the Hello Message on page 138	monitor start *filename* monitor stop
About ResvConfirm Messages on page 141	Not applicable.

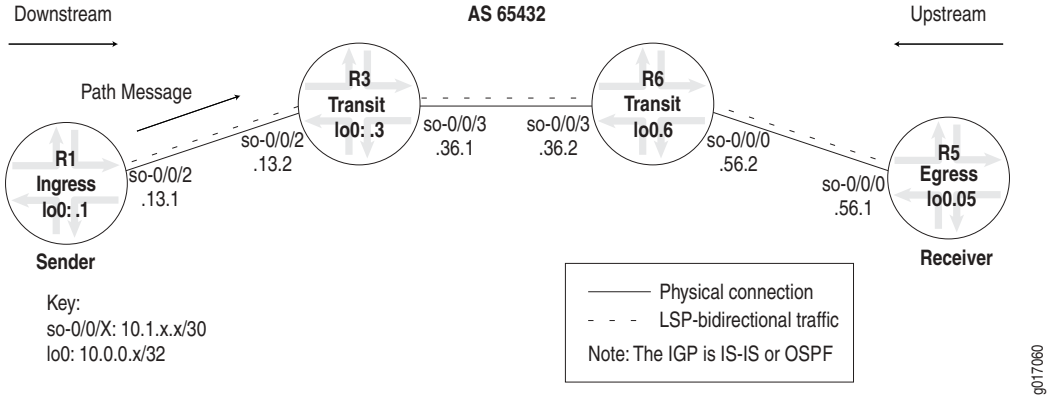
NOTE: To display tracing output, make sure that RSVP trace options are enabled. See "Working with RSVP Tracing" on page 113, for information on configuring RSVP trace options.

Examining the Path Message

Purpose 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, and enabling routers to learn the previous-hop and next-hop node for the session. Path messages are sent periodically to refresh path states.

Figure 11 shows an RSVP Path message that flows downstream from ingress router R1 to egress router R5, and transits routers R3 and R6. The originating router (R1) sets the IP router-alert option so that intermediate routers look at the contents of the Path message.

Figure 11: RSVP Path Message



A Path message can contain the following objects: Adspec, Detour, Explicit route, FastReroute, Hop, Integrity, LabelRequest, Policy data, Properties, record route (RecRoute), Sender, Session, SessionAttribute, source route (SrcRoute), Time, and Tspec. For more information on RSVP message objects, see "RSVP Objects" on page 110.

To ensure that Path messages are displayed in the output, include the path flag at the [edit protocols rsvp traceoptions] hierarchy level.

Action To examine the Path message, enter the following JUNOS command-line interface (CLI) command:

```
user@R1> monitor start filename
```

Sample Output 1

```
[edit protocols rsvp]
user@R1# show
traceoptions {
    file rsvp-log;
    flag packets detail;
    flag path detail;
}
interface so-0/0/2.0;
interface fxp0.0 {
    disable;
}
```

Sample Output 2

```
user@R1> clear log rsvp-log

user@R1> monitor start rsvp-log

user@R1>
*** rsvp-log ***
Jun 16 18:36:48 RSVP send Path 10.0.0.1->10.0.0.5 Len=216 so-0/0/2.0
Jun 16 18:36:48   Session7 Len 16 10.0.0.5(port/tunnel ID 26619) Proto 0
Jun 16 18:36:48   Hop      Len 12 10.1.13.1/0x08678198
Jun 16 18:36:48   Time     Len  8 30000 ms
Jun 16 18:36:48   SrcRoute Len 28  10.1.13.2 S 10.1.36.2 S 10.1.56.1 S
Jun 16 18:36:48   LabelRequest Len  8 EtherType 0x800
Jun 16 18:36:48   Properties Len 12 Primary path
Jun 16 18:36:48   SessionAttribute Len 16 Prio (7,0) flag 0x0 "R1-to-R5"
Jun 16 18:36:48   Sender7  Len 12 10.0.0.1(port/lsp ID  4)
Jun 16 18:36:48   Tspec    Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500
Jun 16 18:36:48   ADspec   Len 48 MTU 1500
Jun 16 18:36:48   RecRoute Len 12  10.1.13.1
monitor stop
```

What It Means

Sample Output 1 shows the configuration of RSVP tracing on ingress router R1. The packets and path flags are included at the [edit protocols rsvp traceoptions] hierarchy level to provide slightly different information about RSVP traffic. For more information about RSVP tracing flags, see Table 17 on page 116. The detail option is included to show granular details about the configured flags.

Sample Output 2 shows clear commands, the output for the rsvp-log file, and that monitoring was started and then stopped.

The first line of the rsvp-log output indicates that this is a Path message. The source address of the IP packet is 10.0.0.1 (R1). The IP destination address is 10.0.0.5 (R5). The outgoing interface on this router is so-0/0/2.0.

All subsequent lines of sample output indicate object values for this Path message and are indented in the output. To facilitate this discussion, each line of output for each object is displayed before the corresponding explanation.

- Session7 Len 16 10.0.0.5(port/tunnel ID 26619) Proto 0

  The Session object (Session7) indicates that this is C-Type 7 for LSP tunnel IPv4, defined in RFC 3209. The RSVP session is defined by three values: the destination IP address (10.0.0.5), a 16-bit field that indicates the tunnel ID (26619) and is unique for the length of the RSVP session, and the protocol number (Proto 0).

- Hop Len 12 10.1.13.1/0x08678198

  The Hop object indicates the IP address of the interface (10.1.13.1) on the router (R1) sending the Path message. At the next node, the Hop object contains the previous hop IP address.

- Time Len 8 30000 ms

  The Time object indicates how long before RSVP must refresh the session state (30000 ms). By default, the value is recorded in milliseconds. RFC 3209 states that a router can refresh the state within plus or minus 50 percent of the time. In this case, RFC 3209 allows a router to refresh the state between 15 and 45 seconds.

- SrcRoute Len 28 10.1.13.2 S 10.1.36.2 S 10.1.56.1 S

  The source route (SrcRoute) object is the list of addresses in the Explicit Route Object (ERO). The S indicates a strict next hop, as shown in the example. An L indicates a loose next hop.

- LabelRequest Len 8 EtherType 0x800

  The LabelRequest object indicates, to the next downstream node, that a label assignment is requested. Ethertype 0x800 indicates that a label for an IP packet is required.

- Properties Len 12 Primary path

  The Properties object is a Juniper Networks proprietary object used to carry information about the label-switched path (LSP). In this case, the object indicates that the Path message is signaling a primary physical path.

- SessionAttribute Len 16 Prio (7,0) flag 0x0 "R1-to-R5"

  The SessionAttribute object indicates a variety of parameters:

  - The setup priority of the RSVP session is 7 [Prio (7,0)]. The setup priority determines the resources used by this session, and can be in the range from 0 through 7. The value 0 is the highest priority. The setup priority is used to decide whether this session can preempt another session.

  - The hold priority is 0 [Prio (7,0)]. The hold priority of a session determines resources held by other sessions, and can be in the range from 0 through 7. The value 0 is the highest priority. The hold priority is used to decide whether this session can be preempted by another session.

  - The 8-bit flag field (flag 0x0) has no bits turned on (correlating to the hexadecimal value 0).

    Table 19 shows the SessionAttribute object flags.

Table 19: Session Attribute Object Flags

Flag	Description
Bit 0 (value 0x1)	Local protection requested—Permits transit routers to use a local repair mechanism which may result in violation of the ERO. When a fault is detected on an adjacent downstream link or node, a transit router can reroute traffic for fast service restoration.
Bit 1 (value 0x2)	Label recording requested—Indicates that label information is included with a route record.
Bit 2 (value 0x4)	Shared explicit (SE) style requested—Indicates that the ingress node may reroute this tunnel without tearing it down. A tunnel egress node should use the SE style when responding with an Resv message.

Flag	Description
Bit 3 (value 0x08)	Bandwidth protection requested—Indicates to the point of local repair (PLR) along the protected LSP path that a backup path with a bandwidth guarantee is requested. If no fast reroute object is included in the Path message, the bandwidth guaranteed is that of the protected LSP. If a fast reroute object is in the Path message, then the bandwidth specified must be guaranteed.
Bit 4 (value 0x10)	Node protection requested—Indicates to the PLRs along a protected LSP path that a backup path is requested. The backup path must bypass at least the next node of the protected LSP.
Bit 5 (value 0x20)	ERO expansion—Indicates that a new ERO expansion is requested.
Bit 6 (value 0x40)	Soft preemption requested—Indicates that soft preemption is used if the LSP is preempted.
Bit 7 (value 0x80)	Undefined.

- Sender7 Len 12 10.0.0.1(port/lsp ID 4)

  The Sender object defines the source of session 10.0.0.1 (R1). The number (7) after sender indicates that this is C-Type 7 for IPv4, defined in RFC 3209. The sender is defined by the source IP address (10.0.0.1) and the LSP ID (4). The LSP ID changes, depending on the signaling path.

- Tspec Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500

  The traffic specification (Tspec) object indicates the allocated bandwidth. This RSVP session uses the default of 0, no bandwidth is reserved. The Tspec object includes two different types of RSVP bandwidth allocations: controlled load and guaranteed delivery.

  - Controlled load specifies a maximum transmission rate and a maximum burst size. The peak value is always set to infinity (Inf), unless guaranteed delivery is specified. RFC 3209 recommends support only for null service and controlled load bandwidth services. Guaranteed delivery is not currently recommended, so there should never be a value for Inf in the Tspec object.

  - Guaranteed delivery specifies a peak transmission rate. The JUNOS software does not support guaranteed delivery. Instead you can specify a maximum transmission rate; for example, 45 Mbps. Because it is possible to burst at the maximum rate, the size parameter indicates a maximum burst size of 45 Mbps. The lowercase m (m20) and uppercase M (M 1500) indicate the minimum and maximum sizes for the RSVP maximum transmission unit (MTU) rate. RSVP treats any packet smaller than m20 as 20 bytes, and any packet larger than M1500 as 1500 bytes.

- ADspec Len 48 MTU 1500

  The ADspec object carries a summary of available services, delay and bandwidth estimates, and operating parameters (MTU 1500) used by specific quality-of-service (QoS) control services.

- RecRoute Len 12 10.1.13.1

  The record route object (RecRoute) indicates the list of addresses that this Path message has transited, in this case, 10.1.13.1.

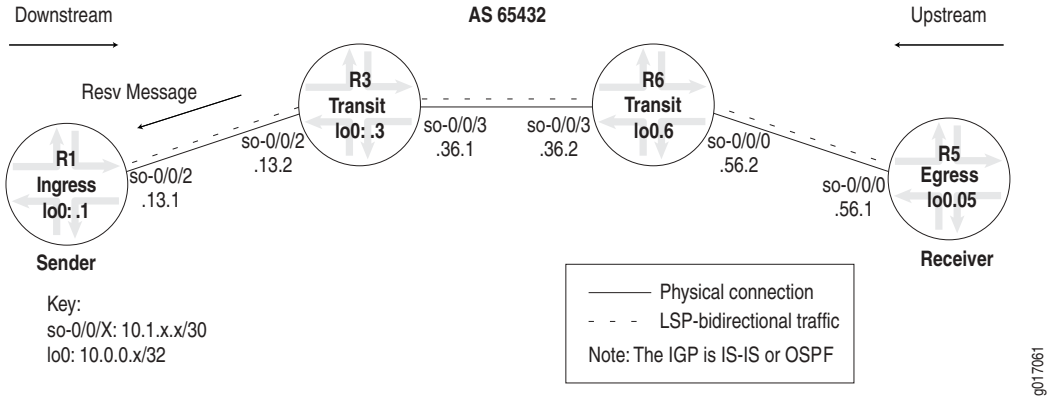
For information on objects that can appear in the Path message but do not appear in the sample output, such as Detour, Explicit route, FastReroute, and Integrity, see Table 15 on page 110.

Examining the Resv Message

Purpose 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.

Figure 12 shows an RSVP Resv message that flows upstream from R3 toward the destination interface address (10.1.13.1) on ingress router R1, ensuring that the network allocates resources along the reverse path that the downstream messages followed.

Figure 12: RSVP Resv Message



To ensure that Resv messages are displayed in the output, include the resv flag at the [edit protocols rsvp traceoptions] hierarchy level.

Action To examine the Resv message, enter the following JUNOS CLI command:

user@R1> **monitor start** *filename*

Sample Output 1

```
[edit protocols rsvp]
user@R1# show
traceoptions {
    file rsvp-log;
    flag packets detail;
    flag resv detail;
}
interface so-0/0/2.0;
interface fxp0.0 {
    disable;
}
```

Sample Output 2

```
user@R1> clear log rsvp-log

user@R1> monitor start rsvp-log

user@R1>
*** rsvp-log ***
Jun 29 15:57:19 RSVP recv Resv 10.1.13.2->10.1.13.1 Len=136 so-0/0/2.0
Jun 29 15:57:19   Session7 Len 16 10.0.0.5(port/tunnel ID 26619) Proto 0
Jun 29 15:57:19   Hop      Len 12 10.1.13.2/0x08678198
Jun 29 15:57:19   Time     Len  8 30000 ms
Jun 29 15:57:19   Style    Len  8 FF
Jun 29 15:57:19   Flow     Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500
Jun 29 15:57:19   Filter7  Len 12 10.0.0.1(port/lsp ID  5)
Jun 29 15:57:19   Label    Len  8  100624
Jun 29 15:57:19   RecRoute Len 28  10.1.13.2 10.1.36.2 10.1.56.1
monitor stop
```

What It Means

Sample Output 1 shows the configuration of RSVP tracing on ingress router R1. The packets and resv flags are included at the [edit protocols rsvp traceoptions] hierarchy level to provide slightly different information about RSVP traffic. For more information about RSVP tracing flags, see Table 17 on page 116. The detail option is included to show granular details about the configured flags.

Sample Output 2 shows clear commands, the output for the rsvp-log file, and that monitoring was started and then stopped.

The first line of the rsvp-log output indicates that this is an Resv message. The source address of the IP packet is 10.1.13.2 (R3). The destination address of the IP packet is 10.1.13.1 (R1). The incoming interface on R1 is interface so-0/0/2.

All subsequent lines of sample output indicate object values for this Resv message and are indented in the output. To facilitate this discussion, each line of output for each object is displayed before the corresponding explanation.

- Session7 Len 16 10.0.0.5(port/tunnel ID 26619) Proto 0

  The Session object (Session7) indicates that this is C-Type 7 for LSP tunnel IPv4, defined in RFC 3209. The RSVP session is defined by three values: the destination IP address (10.0.0.5), a 16-bit field that indicates the tunnel ID (26619) and is unique for the length of the RSVP session, and the protocol number (Proto 0). Note that the Session object in the Path message on page 125 is the same as in the Resv message.

- Hop Len 12 10.1.13.2/0x08678198

  The Hop object indicates the IP address of the interface (10.1.13.2) on the router (R3) sending the Resv message.

- Time Len 8 30000 ms

  The Time object indicates how long before RSVP must refresh the session state (30000 ms). By default the value is recorded in milliseconds. RFC 3209 dictates that a router can refresh the state within plus or minus 50 percent of the time. In this case, RFC 3209 allows a router to refresh the state between 15 and 45 seconds.

- Style Len 8 FF

  The Style object indicates the reservation style. The reservation style for this ResvTear message is fixed filter (FF), indicating that the bandwidth allocation in a Resv message cannot be shared with any other session or sender/filter combination. Each different physical path is identified by an LSP ID, listed in the filter object. A reservation message that indicates a fixed filter style consists of distinct reservations among explicit senders. For this session, the router cannot share the bandwidth with any other RSVP LSP signaling messages that share the same session ID and have different LSP IDs.

  Other available reservation styles are shared explicit (SE) and wildcard filter (WF). For more information on reservation styles, see the *JUNOS MPLS Applications Configuration Guide*.

- Flow Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500

  The Flow object indicates the allocated bandwidth and is the same information contained in the Tspec object in the Path message. This RSVP session uses the default of 0, no bandwidth is reserved. The Flow object includes two different types of RSVP bandwidth allocations: controlled load and guaranteed delivery.

  - Controlled load specifies a maximum transmission rate and a maximum burst size. The peak value is always set to infinity (Inf), unless guaranteed delivery is specified. RFC 3209 recommends support only for null service and controlled load bandwidth services. Guaranteed delivery is not currently recommended, so there should never be a value for Inf in the Flow object.

  - Guaranteed delivery specifies a peak transmission rate; for example, 45 Mbps. The JUNOS software does not support guaranteed delivery. Instead you can specify a maximum transmission rate; for example, 45 Mbps. Because it is possible to burst at the maximum rate, the size parameter indicates a maximum burst size of 45 Mbps. The lowercase m (m20) and uppercase M (M 1500) indicate the minimum and maximum sizes for the RSVP MTU rate. RSVP treats any packet smaller than m20 as 20 bytes, and any packet larger than M1500 as 1500 bytes.

- Filter7 Len 12 10.0.0.1(port/lsp ID 5)

  The Filter object defines the source of the session 10.0.0.1 (R1). The number (7) after Filter indicates that this is C-Type 7 for IPv4, defined in RFC 3209. The Filter object contains the source address of the LSP and the LSP ID. The LSP ID changes, depending on the signaling path. The Filter object contains the same information as the Sender object of the Path message.

- Label Len 8 100624

  The Label object contains the label value (100624) that is mapped to the LSP identified by the session value.

- RecRoute Len 28 10.1.13.2 10.1.36.2 10.1.56.1

  The record route object (RecRoute) contains the list of IP addresses through which this Resv message passed.

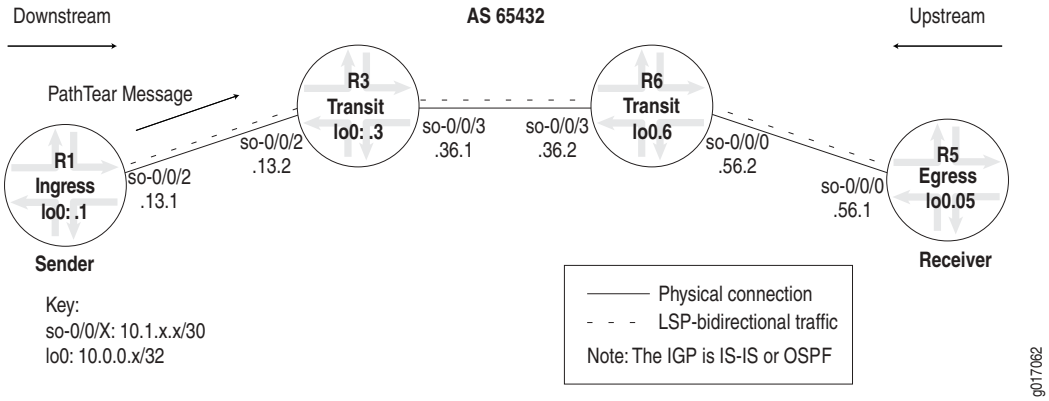
Examining the PathTear Message

Purpose 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 message typically is initiated by a sender application or 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.

Figure 13 show an RSVP PathTear message that flows downstream from ingress router R1 (10.0.0.1) towards egress router R5 (10.0.0.5). PathTear messages set the IP router-alert option so that intermediate routers check the contents of the PathTear message, ensuring that the network removes the allocation of resources along the path that the downstream Path message followed.

Figure 13: RSVP PathTear Message



To ensure that PathTear messages are displayed in the output, include the pathtear flag at the [edit protocols rsvp traceoptions] hierarchy level.

Action To examine the PathTear message, enter the following JUNOS CLI command:

user@R1> **monitor start** *filename*

Sample Output 1

```
[edit protocols rsvp]
user@R1# show
traceoptions {
    file rsvp-log;
    flag packets detail;
    flag pathtear detail;
}
interface so-0/0/2.0;
interface fxp0.0 {
    disable;
}
```

Sample Output 2

```
user@R1> clear log rsvp-log

user@R1> monitor start rsvp-log

user@R1>
*** rsvp-log ***
[...Output truncated...]
Jun 30 10:05:25 RSVP send PathTear 10.0.0.1->10.0.0.5 Len=84 so-0/0/2.0
Jun 30 10:05:25   Session7 Len 16 10.0.0.5(port/tunnel ID 26619) Proto 0
Jun 30 10:05:25   Hop      Len 12 10.1.13.1/0x08678198
Jun 30 10:05:25   Sender7  Len 12 10.0.0.1(port/lsp ID  10)
Jun 30 10:05:25   Tspec    Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500
monitor stop
```

What It Means

Sample Output 1 shows the configuration of RSVP tracing on ingress router R1. The packets and pathtear flags are included at the [edit protocols rsvp traceoptions] hierarchy level to provide slightly different information about RSVP traffic. For more information about RSVP tracing flags, see Table 17 on page 116. The detail option is included to show granular details about the configured flags.

Sample Output 2 shows clear commands, the output for the rsvp-log file, and that monitoring was started and then stopped.

The first line of the rsvp-log output indicates that this is a PathTear message originating from address 10.0.0.1 and destined for 10.0.0.5. The outgoing interface is so-0/0/2.0 on R1. When a Path message containing an route record object (RRO) is received by an intermediate router, the router stores a copy of it in the path state block. The PathTear message deletes state information for the specified RSVP session from the path state blocks for all routers with knowledge of this MPLS tunnel.

All subsequent lines of sample output indicate object values for this PathTear message and are indented in the output. To facilitate this discussion, each line of output for each object is displayed before the corresponding explanation.

- Session7 Len 16 10.0.0.5(port/tunnel ID 26619) Proto 0

  The Session object (Session7) indicates that this is C-Type 7 for LSP tunnel IPv4, defined in RFC 3209. The RSVP session is defined by three values: the destination IP address (10.0.0.5), a 16-bit field that indicates the tunnel ID (26619) and is unique for the length of the RSVP session, and the protocol number (Proto 0).

- Hop Len 12 10.1.13.1/0x08678198

  The Hop object indicates the IP address of the last interface (10.1.13.1) that this RSVP PathTear message visited.

- Sender7 Len 12 10.0.0.1(port/lsp ID 10)

  The Sender object defines the source of the session 10.0.0.1 (R1). The number (7) after sender indicates that this is C-Type 7 for IPv4, defined in RFC 3209. The Sender is defined by the source IP address and the LSP ID. The LSP ID changes, depending on the signaling path.

- Tspec Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500

  The traffic specification (Tspec) object indicates the allocated bandwidth. This RSVP session uses the default of 0, no bandwidth is reserved. The Tspec object includes two different types of RSVP bandwidth allocations: controlled load and guaranteed delivery.

  - Controlled load specifies a maximum transmission rate and a maximum burst size. The peak value is always set to infinity (Inf), unless guaranteed delivery is specified. RFC 3209 recommends support only for null service and controlled load bandwidth services. Guaranteed delivery is not currently recommended, so there should never be a value for Inf in the Tspec object.

  - Guaranteed delivery specifies a peak transmission rate. The JUNOS software does not support guaranteed delivery. Instead you can specify a maximum transmission rate; for example, 45 Mbps. Because it is possible to burst at the maximum rate, the size parameter indicates a maximum burst size of 45 Mbps. The lowercase m (m20) and uppercase M (M 1500) indicate the minimum and maximum sizes for the RSVP MTU rate. RSVP treats any packet smaller than m20 as 20 bytes, and any packet larger than M1500 as 1500 bytes.

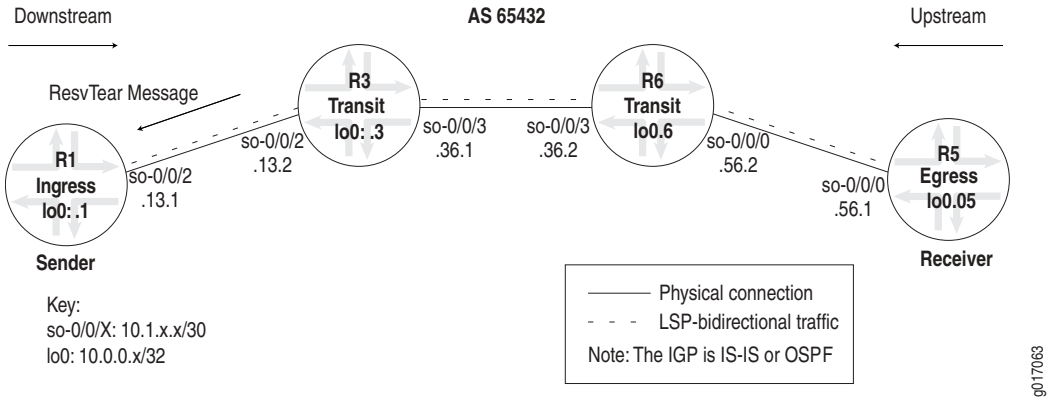
Examining the ResvTear Message

Purpose ResvTear messages remove reservation states along a path, travelling upstream toward senders of the session. In a sense, ResvTear messages do the opposite of Resv messages. ResvTear messages typically are initiated by a receiver application or 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.

Figure 14 shows an RSVP ResvTear message that flows upstream from router R3 to R1, ensuring that the network removes resources allocated along the reverse path that the downstream messages followed.

Figure 14: RSVP ResvTear Message



To ensure that ResvTear messages are displayed in the output, include the resvtear flag at the [edit protocols rsvp traceoptions] hierarchy level.

Action To examine the ResvTear message, enter the following JUNOS CLI command:

user@R1> **monitor start** *filename*

Sample Output 1

```
[edit protocols rsvp]
user@R1# show
traceoptions {
    file rsvp-log;
    flag packets detail;
    flag resvtear detail;
}
interface so-0/0/2.0;
interface fxp0.0 {
    disable;
}
```

Sample Output 2

```
user@R1> clear log rsvp-log

user@R1> monitor start rsvp-log

user@R1>
*** rsvp-log ***
[...Output truncated...]
Jun 30 09:27:43 RSVP recv ResvTear 10.1.13.2->10.1.13.1 Len=56 so-0/0/2.0
Jun 30 09:27:43   Session7 Len 16 10.0.0.5(port/tunnel ID 26619) Proto 0
Jun 30 09:27:43   Hop      Len 12 10.1.13.2/0x08678198
Jun 30 09:27:43   Style    Len  8 FF
Jun 30 09:27:43   Filter7  Len 12 10.0.0.1(port/lsp ID  7)
monitor stop
```

What It Means

Sample Output 1 shows the configuration of RSVP tracing on ingress router R1. The packets and resvtear flags are included at the [edit protocols rsvp traceoptions] hierarchy level to provide slightly different information about RSVP traffic. For more information about RSVP tracing flags, see Table 17 on page 116. The detail option is included to show granular details about the configured flags.

Sample Output 2 shows clear commands, the output for the rsvp-log file, and that monitoring was started and then stopped.

The first line of the rsvp-log output indicates that this is an ResvTear message from R3 (10.1.13.2) to R1 (10.0.0.1). The outgoing interface is so-0/0/2.0 on R3. When a Path message containing an RRO is received by an intermediate router, the router stores a copy of it in the path state block. The ResvTear message deletes state information for the specified RSVP session from the reservation state blocks of routers with knowledge of this MPLS tunnel.

All subsequent lines of sample output indicate object values for this ResvTear message and are indented in the output. To facilitate this discussion, each line of output for each object is displayed before the corresponding explanation.

- Session7 Len 16 10.0.0.5(port/tunnel ID 26619) Proto 0

  The Session object (Session7) indicates that this is C-Type 7 for LSP tunnel IPv4, defined in RFC 3209. The RSVP session is defined by three values: the destination IP address (10.0.0.5), a 16-bit field that indicates the tunnel ID (26619) and is unique for the length of the RSVP session, and the protocol number (Proto 0).

- Hop Len 12 10.1.13.1/0x08678198

  The Hop object indicates the last IP address (10.1.13.1) that this RSVP ResvTear message visited.

- Style Len 8 FF

  The Style object indicates the reservation style. The reservation style for this ResvTear message is fixed filter (FF), indicating that the bandwidth allocation in a Resv message cannot be shared with any other session, or sender/filter combination. Each different physical path is identified by an LSP ID, listed in the Filter object. A reservation message that indicates a fixed filter style consists of distinct reservations among explicit senders. For this session, the router cannot share the bandwidth with any other RSVP LSP signaling messages that share the same session ID and have different LSP IDs.

  Other available reservation styles are shared explicit (SE) and wildcard filter (WF). For more information on reservation styles, see the *JUNOS MPLS Applications Configuration Guide*.

- Filter7 Len 12 10.0.0.1(port/lsp ID 7)

  The Filter object defines the source of the session 10.0.0.1 (R1). The number after Filter (Filter7) indicates that this is C-Type 7 for IPv4, defined in RFC 3209. It contains the source address of the LSP and the LSP ID. The LSP ID changes, depending on the signaling path. The Filter object contains the same information as the Sender object of the Path message.

Examining the Hello Message

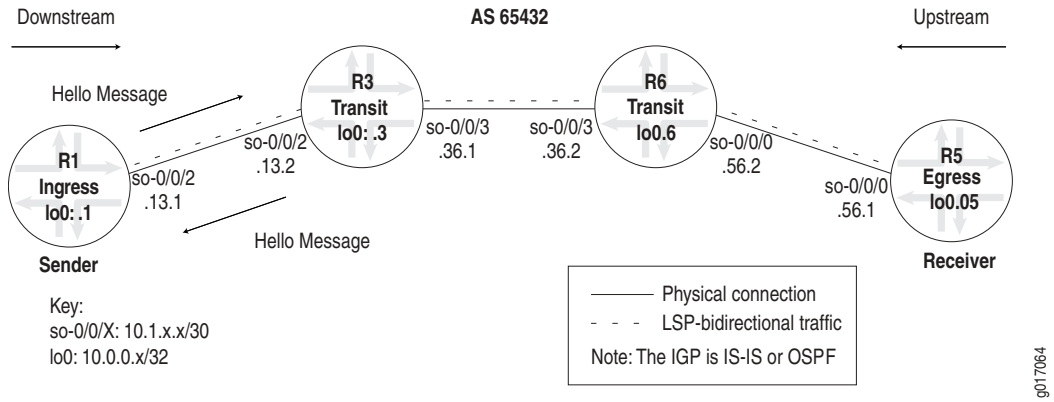
Purpose RSVP monitors the status of the interior gateway protocol (IGP) (Intermediate System-to-Intermediate System [ISIS] or Open Shortest Path First [OSPF]) neighbors and relies on the IGP protocols to detect when a node fails. If an IGP protocol declares a neighbor down (because Hello messages are no longer being received), RSVP also brings down that neighbor. However, the IGP protocols and RSVP still act independently when bringing a neighbor up.

RSVP Hello messages are exchanged between neighbors. The destination address is the neighbor node. RSVP Hello messages are used to determine loss of interface more quickly than determined by the RSVP state timeout.

NOTE: RSVP Hello messages are required to establish the protocol or to maintain adjacency information. RSVP Hello messages do not establish state.

Figure 15 shows two RSVP Hello messages exchanged between routers R1 and R3.

Figure 15: RSVP Hello Message



To ensure that Hello messages are displayed in the output, include the packets flag at the [edit protocols rsvp traceoptions] hierarchy level.

Action To examine the Hello message, enter the following JUNOS CLI command:

user@R1> **monitor start** *filename*

Sample Output 1

```
[edit protocols rsvp]
user@R1# show
traceoptions {
    file rsvp-log;
    flag packets detail;
}
interface so-0/0/2.0;
interface fxp0.0 {
    disable;
}
```

Sample Output 2

```
user@R1> clear log rsvp-log

user@R1> monitor start rsvp-log

user@R1>
*** rsvp-log ***
[...Output truncated...]
Jun 29 15:48:59 RSVP send Hello New 10.1.13.1->10.1.13.2 Len=32 so-0/0/2.0
Jun 29 15:48:59   HelloReq Len 12
Jun 29 15:48:59   RestartCap Len 12 restart time 0, recovery time 0
Jun 29 15:48:59 RSVP recv Hello New 10.1.13.2->10.1.13.1 Len=32 so-0/0/2.0
Jun 29 15:48:59   HelloRply Len 12
Jun 29 15:48:59   RestartCap Len 12 restart time 0, recovery time 0
monitor stop
```

What It Means

Sample Output 1 shows the configuration of RSVP tracing on ingress router R1. The packets flag is included at the [edit protocols rsvp traceoptions] hierarchy level to provide information about RSVP traffic. For more information about RSVP tracing flags, see Table 17 on page 116. The detail option is included to show granular details about the configured flag.

Sample Output 2 shows clear commands, the output for the rsvp-log file, and that monitoring was started and then stopped. The rsvp-log output shows two RSVP Hello messages exchanged between R1 and R3.

The first Hello message in the rsvp-log output is a request sent from R1 (10.1.13.1) to R3 (10.1.13.2). The outgoing interface is so-0/0/2.0 on R1. The second Hello message was a reply sent from R3 to R1, also through the outgoing interface so-0/0/2.0 on R3.

The next two lines of output indicate object values for the two Hello messages, and are indented in the output. To facilitate this discussion, each line of output for each object is displayed before the corresponding explanation.

- HelloReq Len 12

  The Hello request (HelloReq) object indicates that this is a Hello request. RFC 3209 defines the RSVP Hello message. An RSVP Hello message can either be a request or a reply. Every request should generate a reply.

- RestartCap Len 12 restart time 0, recovery time 0

  The restart object (RestartCap) indicates the graceful restart capability of the sender node. The restart time of 0 milliseconds is the length of time that this node takes to restart its RSVP traffic engineering functionality. At the end of this time, the node can send and receive RSVP messages again. The recovery time of 0 milliseconds indicates the length of time the LSR retains MPLS forwarding information. A recovery time of 0 in this case indicates that no forwarding state was preserved across a restart. Because both values are set to 0, graceful restart was not enabled for this RSVP session.

- HelloRply Len 12

  The Hello reply (HelloRply) object indicates that this is an RSVP Hello message sent from R3 to R1 out of interface so-0/0/2.0.

In standard RSVP, node failure detection occurs as a consequence of the RSVP soft-state timeout model. However, detection typically requires several minutes to time out the soft state. Hello packets allow the detection of the neighboring node state changes more quickly.

In JUNOS software, RSVP Hello messages are optional and are backward-compatible with RSVP implementations that do not support Hello messages. For neighboring routers that do not support Hello messages or on which RSVP Hello is disabled, RSVP uses the soft-state timeout for loss detection and cannot benefit from fast IGP Hello detection.

Configuring a short time for the IS-IS or OSPF Hello timers allows these protocols to detect node failures more quickly. RSVP also benefits from early detection by the IGP protocols. It is not necessary to explicitly configure a short RSVP Hello timer. If you do configure the RSVP Hello timer, you can configure a longer value and can still expect the failure of a neighboring router to be quickly detected by IGP.

Between Hello-capable neighbors, Hello messages are sent unicast toward each other. A loss of (2 x keep-multiplier + 1) consecutive Hello messages causes the neighbor's state to go down, and all RSVP sessions to and from that neighbor are declared to be down.

By default, RSVP sends Hello messages every 9 seconds. For information on how to configure the RSVP Hello message timer, see the *JUNOS MPLS Applications Configuration Guide*.

About ResvConfirm Messages

Purpose 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.

Chapter 12

Examining RSVP Error Messages

The Resource Reservation Protocol (RSVP) uses the messages listed in Table 20 to report errors in a Multiprotocol Label Switching (MPLS) network. The RSVP tracing log file provides useful information about RSVP traffic in the network. This chapter describes the purpose of each RSVP error message that can appear in the output of the rsvp-log file configured at the [edit protocols rsvp traceoptions] hierarchy level.

For information on RSVP log messages, see "Examining RSVP Log Messages" on page 123.

Table 20: Checklist for Examining RSVP Error Messages

Examining RSVP Error Messages Tasks	Possible Action or Command
Examining the PathErr Message on page 144	monitor start *filename* monitor stop
Examining the ResvErr Message on page 147	monitor start *filename* monitor stop
Understanding RSVP Error Message Codes on page 150	

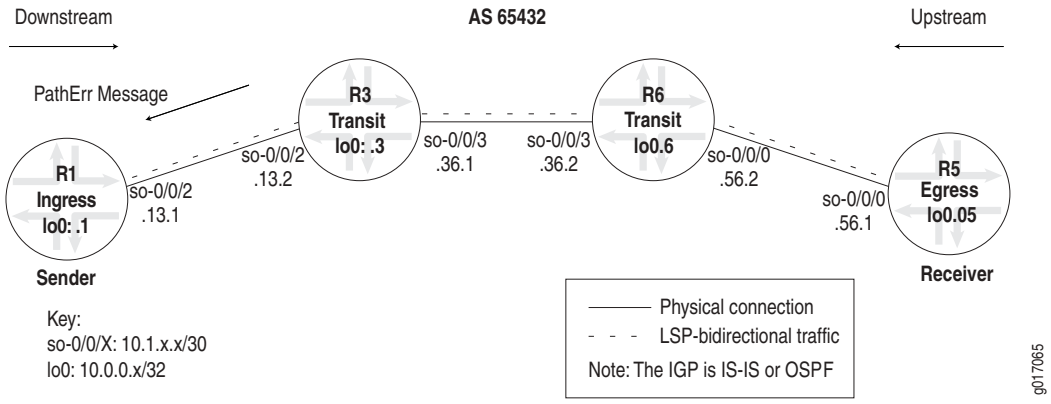
NOTE: To display tracing output, make sure that RSVP trace options are enabled. See "Working with RSVP Tracing" on page 113, for information on configuring RSVP tracing.

Examining the PathErr Message

Purpose 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.

Figure 16 shows an RSVP PathErr message that flows upstream toward the destination address (10.1.13.1) on ingress router (R1). From the perspective of the upstream flow, the destination address is the next-hop interface (so-0/0/2 on R1). This message notifies the sending node (R1) that an error occurred during label-switched path (LSP) signaling. This RSVP PathErr message originates at R3 (even though R1 had the problem), and is destined for R1.

Figure 16: RSVP PathErr Message



The RSVP PathErr message contains the session and sender information, the error code, and the requested bandwidth information. For more information on RSVP PathErr messages, see the *JUNOS MPLS Applications Configuration Guide.*

To ensure that PathErr messages are displayed in the output, include the error flag at the [edit protocols rsvp traceoptions] hierarchy level.

Action To examine PathErr messages, enter the following JUNOS command-line interface (CLI) command:

user@R1> **monitor start** *filename*

Sample Output 1

```
[edit protocols rsvp]
user@R1# show
traceoptions {
    file rsvp-log;
    flag packets detail;
    flag error detail;
}
interface so-0/0/2.0;
interface fxp0.0 {
    disable;
}
```

Sample Output 2

```
user@R1> clear log rsvp-log

user@R1> monitor start rsvp-log

user@R1>
*** rsvp-log ***
[...Output truncated...]
Jun 30 13:52:30 RSVP recv PathErr 10.1.13.2->10.1.13.1 Len=160 so-0/0/2.0
Jun 30 13:52:30   Session7 Len 16 10.0.0.5(port/tunnel ID 26679) Proto 0
Jun 30 13:52:30   Error    Len 12 code 24 value 7 flag 0 by 10.1.36.1
Jun 30 13:52:30   Sender7  Len 12 10.0.0.1(port/lsp ID  2)
Jun 30 13:52:30   Tspec    Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500
Jun 30 13:52:30   ADspec   Len 48 MTU 1500
Jun 30 13:52:30   RecRoute Len 28  10.1.36.2 10.1.36.1 10.1.13.1
```

What It Means

Sample Output 1 shows the configuration of RSVP tracing on ingress router R1. The packets and error flags are included at the [edit protocols rsvp traceoptions] hierarchy level to provide slightly different information about RSVP traffic. For more information about RSVP tracing flags, see Table 17 on page 116. The detail option is included to show granular details about the configured flags.

Sample Output 2 shows clear commands, the output for the rsvp-log file, and that monitoring was started and then stopped.

The first line of the output from the rsvp-log file indicates that this is a PathErr message. The source address of the IP packet is 10.1.13.2 (R3). The destination address of the IP packet is 10.1.13.1 (R1). The incoming interface on R1 is so-0/0/2.0.

All subsequent lines of sample output indicate object values for this PathErr message and are indented in the output. To facilitate this discussion, each line of output for each object is displayed before the corresponding explanation.

- Session7 Len 16 10.0.0.5(port/tunnel ID 26679) Proto 0

  The Session object indicates the session ID for the LSP that experienced the error condition (R1-to-R5). The session ID consists of the destination IP address (10.0.0.5) of the LSP, a protocol value (Proto 0), and a 16-bit tunnel ID (26679).

- Error Len 12 code 24 value 7 flag 0 by 10.1.36.1

  The Error object indicates the error (code 24 value 7) and the source IP address (10.1.36.1) of the interface with the error. In this case, R3 has a routing problem (24) in which the record route object (RRO), in the output of the show mpls lsp extensive command, indicates a routing loop (07). For more information on error codes, see Table 21 on page 150.

  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*.

- Sender7 Len 12 10.0.0.1(port/lsp ID 2)

  The Sender object indicates the sender of the message. The number 7 indicates the C-Type defined in RFC 3209. This object contains the source address of the LSP (10.0.0.1) and the LSP ID (2). The LSP ID can change, depending upon the signaling path.

- Tspec Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500

  The Tspec object indicates the allocated bandwidth and is the same information contained in the Tspec object in the Path message. This RSVP session uses the default of 0, no bandwidth is reserved. The Tspec object includes two different types of RSVP bandwidth allocations: controlled load and guaranteed delivery.

  - Controlled load specifies a maximum transmission rate and a maximum burst size. The peak value is always set to infinity (Inf), unless guaranteed delivery is specified. RFC 3209 recommends support only for null service and controlled load bandwidth services. Guaranteed delivery is not currently recommended, so there should never be a value for Inf in the Tspec object.

  - Guaranteed delivery specifies a peak transmission rate. The JUNOS software does not support guaranteed delivery. Instead you can specify a maximum transmission rate; for example, 45 Mbps. Because it is possible to burst at the maximum rate, the size parameter indicates a maximum burst size of 45 Mbps. The lowercase m (m20) and uppercase M (M 1500) indicate the minimum and maximum sizes for the RSVP maximum transmission unit (MTU) rate. RSVP treats any packet smaller than m20 as 20 bytes, and any packet larger than M1500 as 1500 bytes.

- ADspec Len 48 MTU 1500

  The Adspec object carries a summary of available services, delay and bandwidth estimates, and operating parameters (MTU 1500) used by specific quality-of-service (QoS) control services.

- RecRoute Len 28 10.1.36.2 10.1.36.1 10.1.13.1

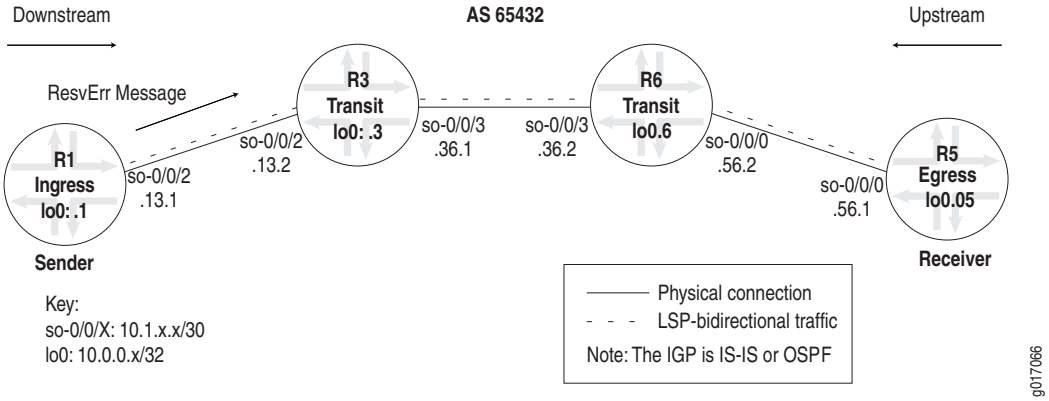
  The record route object (RecRoute) indicates the list of addresses this Path message has transited, in this case, 10.1.36.1 (R6), to 10.1.36.1 (R3), to 10.1.13.1 (R1).

Examining the ResvErr Message

Purpose 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.

Figure 17 shows an RSVP ResvErr message that flows downstream to the destination address of the LSP 10.0.0.5 (R5), indicating that an error with the reservation allocation occurred while sending Resv messages back to the ingress node. The destination address of the ResvErr message is the interface from R1 to R3 (so-0/0/2.0), which the Resv message just left.

Figure 17: RSVP ResvErr Message



To ensure that ResvErr messages are displayed in the output, include the error flag at the [edit protocols rsvp traceoptions] hierarchy level.

Action To examine the ResvErr message, enter the following JUNOS CLI command:

```
user@R1> monitor start filename
```

Sample Output 1

```
[edit protocols rsvp]
user@R1# show
traceoptions {
    file rsvp-log;
    flag packets detail;
    flag error detail;
}
interface so-0/0/2.0;
interface fxp0.0 {
    disable;
}
```

Sample Output 2

```
user@R1> clear log rsvp-log

user@R1> monitor start rsvp-log
```

```
user@R1>
*** rsvp-log ***
[...Output truncated...]
Jan 15 15:44:57 RSVP send ResvErr 10.1.13.1->10.0.13.2 Len=104 so-0/0/2.0
Jan 15 15:44:57  Session7 Len 16 10.0.0.5(port/tunnel ID 13527) Proto 0
Jan 15 15:44:57  Hop Len 12 10.0.13.1/0x08554198
Jan 15 15:44:57  Error Len 12 code 4 value 0 flag 0 by 10.0.16.1
Jan 15 15:44:57  Style   Len  8 FF
Jan 15 15:44:57  Flow Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500
Jan 15 15:44:57  Filter7 Len 12 10.0.0.1(port/lsp ID  2)
monitor stop
```

What It Means Sample Output 1 shows the configuration of RSVP tracing on ingress router R1. The packets and error flags are included at the [edit protocols rsvp traceoptions] hierarchy level to provide slightly different information about RSVP traffic. For more information about RSVP tracing flags, see Table 17 on page 116. The detail option is included to show granular details about the configured flags.

Sample Output 2 shows clear commands, the output for the rsvp-log file, and that monitoring was started and then stopped.

The first line of sample output from the rsvp-log file indicates that this is a ResvErr message. The source address of the IP packet is 10.1.13.1 (R1) and the destination address is 10.1.13.2 (R3). The outgoing interface on R1 is interface so-0/0/2.0. The ResvErr message is in response to a Resv message indicating an error with the reserved LSP allocation.

All subsequent lines of sample output indicate object values for this ResvErr message and are indented in the output. To facilitate this discussion, each line of output for each object is displayed before the corresponding explanation.

- Session7 Len 16 10.0.0.5(port/tunnel ID 13527) Proto 0

  The Session object indicates the session ID for the LSP (R1-to-R5) that experienced the error condition (R5). The session ID consists of the destination IP address (10.0.0.5) of the LSP, a protocol value (Proto 0), and a 16-bit tunnel ID (13527).

- Hop Len 12 10.0.13.1/0x08554198

  The Hop object indicates the last IP address (10.1.13.1) visited by this ResvErr message.

- Error Len 12 code 4 value 0 flag 0 by 10.0.16.1

  The Error object indicates the error code for the message. In this case, error code 4 value 0 flag 0 is defined by RFC 2205, *Resource ReSerVation Protocol (RSVP), Version 1, Functional Specification*. The definition specifies that there is no sender information for this Resv message. Although there is path state for this session, it does not include the sender matching some flow descriptor contained in the Resv message. Therefore, the Resv message cannot be forwarded.

- Style Len 8 FF

  The Style object indicates the reservation style. The reservation style for this ResvErr message is fixed filter (FF), indicating that the bandwidth allocation in an Resv message cannot be shared with any other session, or sender/filter combination. Each different physical path is identified by an LSP ID, listed in the Filter object. A reservation message that indicates a fixed filter style consists of distinct reservations among explicit senders. For this session, the router cannot share the bandwidth with any other RSVP LSP signaling messages that share the same session ID and have different LSP IDs.

  Other available reservation styles are shared explicit (SE) and wildcard filter (WF). For more information on reservation styles, see the *MPLS Applications Configuration Guide*.

- Flow Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500

  The Flow object indicates the allocated bandwidth and is the same information contained in the Tspec object in the Path message. In the upstream direction (the direction in which the Resv message flowed), the flow object indicates the bandwidth requested and the minimum and maximum packet sizes. In this case, this RSVP session uses the default of 0, no bandwidth is reserved. The flow object includes two different types of RSVP bandwidth allocations: controlled load and guaranteed delivery.

  - Controlled load specifies a maximum transmission rate and a maximum burst size. The peak value is always set to infinity (Inf), unless guaranteed delivery is specified. RFC 3209 recommends support only for null service and controlled load bandwidth services. Guaranteed delivery is not currently recommended, so there should never be a value for Inf in the Flow object.

  - Guaranteed delivery specifies a peak transmission rate. The JUNOS software does not support guaranteed delivery. Instead you can specify a maximum transmission rate; for example, 45 Mbps. Because it is possible to burst at the maximum rate, the size parameter indicates a maximum burst size of 45 Mbps. The lowercase m (m20) and uppercase M (M 1500) indicate the minimum and maximum sizes for the RSVP MTU rate. RSVP treats any packet smaller than m20 as 20 bytes, and any packet larger than M1500 as 1500 bytes.

- Filter7 Len 12 10.0.0.1(port/lsp ID 2)

  The Filter object defines the source (ingress) of the session 10.0.0.1 (R1). The number 7 after Filter indicates that this is C-Type 7 for IPv4, defined in RFC 3209. It contains the source address of the LSP and the LSP ID. The LSP ID changes, depending on the signaling path. The Filter object contains the same information as the Sender object of the Path message.

Understanding RSVP Error Message Codes

Table 21 lists and describes the RSVP error message codes from RFC 2205, *Resource ReSerVation Protocol (RSVP), Version 1, Functional Specification* and RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels*. The following error codes appear predominantly in the error object of the ResvErr message. A few of these error codes appear in the PathErr message.

Table 21: RSVP Error Codes

Error Code	Name	Meaning/Value	RSVP Message
00	Confirmation	Value = 00	ResvConf
01	Admission Control Failure Subcode: ■ 1 Delay bound cannot be met ■ 2 Requested bandwidth unavailable ■ 3 MTU in flowspec larger than interface MTU	Reservation request was rejected by admission control due to unavailable resources. The 16 bits of the Error Value field are: ssur cccc cccc cccc. If ssur = 0, the low order bits contain a subcode.	ResvErr
02	Policy Control Failure	Path or Resv message rejected for administrative reason; for example, preemption.	PathErr, ResvErr
03	No Path Information	No Path state exists for this session; Resv message cannot be forwarded.	ResvErr
04	No Sender Information	Path state does not include sender information that matches the flow descriptor; Resv message cannot be forwarded.	ResvErr
05	Conflicting	Reservation style conflicts with existing reservation style; Resv message cannot be forwarded.	ResvErr
06	Unknown Reservation Style	Reservation style unknown; Resv message cannot be forwarded.	ResvErr
07	Conflicting Destination Port	RSVP sessions with identical destination address and protocol values have zero and non-zero destination port values.	PathErr, ResvErr
08	Conflicting Sender Ports	RSVP sessions with identical destination address and protocol values have zero and non-zero sender ports.	PathErr
09 to 11	Reserved		
12	Service Preempted Subcode: Reserved for future definition	The service request defined by the style object and the flow descriptor has been administratively preempted. Value=ssur cccc cccc cccc. If ssur=0, low order bits contain subcode.	ResvErr

Error Code	Name	Meaning/Value	RSVP Message
13	Unknown Object Class	Contains a 16-bit value composed of Class-Num and C-Type of the unknown object. This error is sent only if RSVP will reject the message, as determined by the high-order bits of the Class-Num.	PathErr, ResvErr
14	Unknown Object C-Type	Comprised of Class_Num, C-Type of object.	ResvErr
15-19	Reserved		
20	Reserved for API	Contains an API error code that was detected asynchronously and must be reported by upcall.	ResvErr
21	Traffic Control Error Subcode: ■ 01 Service Conflict—Trying to merge two incompatible service requests. ■ 02 Service Unsupported—Traffic control can't provide requested service or acceptable replacement. ■ 03 Bad Flowspec—Malformed or unreasonable request. ■ 04 Bad Tspec— Malformed or unreasonable request. ■ 05 Bad Adspec—Malformed or unreasonable request.	Traffic control failed due to format or parameters. Path or Resv message cannot be forwarded. Value=ss00 cccc cccc cccc; ss bits=00.	ResvErr
22	Traffic Control System Error	System error detected; RSVP is not expected to interpret this value.	ResvErr
23	RSVP System Error	Implementation-dependent value; RSVP is not expected to interpret this value.	ResvErr

Error Code	Name	Meaning/Value	RSVP Message
24	Routing Problem Subcode: ■ 01 Bad Explicit Route Object ■ 02 Bad Strict node ■ 03 Bad loose node ■ 04 Bad initial sub-object ■ 05 No route available toward destination ■ 06 Unacceptable label value ■ 07 RRO indicated routing loops ■ 08 MPLS being negotiated, but non-RSVP capable router stands in the path ■ 09 MPLS label allocation failure ■ 10 Unsupported L3PID	For information on this error code, see RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels.*	PathErr ResvErr
25	Notify Error subcode: ■ 01 RRO too large for MTU ■ 02 RRO notification ■ 03 Tunnel locally required	For information on this error code, see RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels.*	ResvErr

Chapter 13

Examining an RSVP Failure

The Resource Reservation Protocol (RSVP) is a signaling protocol that provides reservation setup and control. This chapter describes a real-world scenario in which RSVP fails because links in the network are incorrectly configured. It discusses some basic approaches to monitoring and examining an RSVP failure, including how, when, and why you use specific commands. This chapter also includes an examination of the RSVP log file and corrective action for the specific scenario. (See Table 22.)

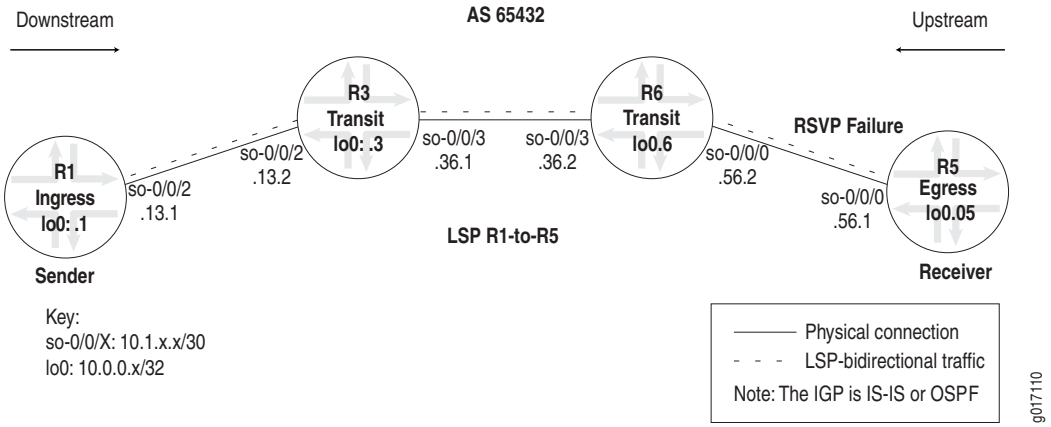
Table 22: Checklist for Examining an RSVP Failure

Examining an RSVP Failure Tasks	
Case Study for an RSVP Failure on page 154	
1. Verify the RSVP Session on page 155	show rsvp session ingress detail
2. Ping the Egress Router on page 156	ping *ip-address-interface*
3. Enable RSVP Tracing on Transit Routers on page 156	edit [edit] edit protocols rsvp [edit protocols rsvp] set traceoptions file *filename* set traceoptions flag *flag* show commit
4. View the RSVP Log File on Transit Routers on page 158	clear rsvp session (Optional) clear log *filename* (Optional) show log *filename*
5. Check the RSVP Log File on the Egress Router on page 159	show log rsvp-log
6. Determine and Correct the Problem on the Egress Router on page 160	The following sequence of commands addresses the specific problem described in this section: show configuration protocols rsvp edit [edit protocols rsvp] rename interface so-0/0/3 to interface so-0/0/0 show commit run show rsvp session ingress detail
7. Remove the Tracing Configuration on page 161	edit [edit protocols rsvp] show delete traceoptions show commit

Case Study for an RSVP Failure

Purpose This case study presents a Multiprotocol Label Switching (MPLS) network topology and RSVP failure scenario designed to demonstrate techniques and commands that are particularly useful when addressing RSVP problems in your network. The focus of the study is an unconstrained RSVP label-switched path (LSP) from R1 to R5, which uses a strict path through R3. In this case, the RSVP failure occurs when interface so-0/0/0 on R5 is configured incorrectly. (See Figure 18.)

Figure 18: RSVP Failure in an MPLS Network Topology



The MPLS network in Figure 18 is a router-only network with SONET interfaces that consists of the following components:

- A full-mesh interior Border Gateway Protocol (IBGP) topology, using AS 65432.
- MPLS and RSVP enabled on all routers.
- A send-statics policy on routers R1 and R6, that allows a new route to be advertised into the network.
- Two unidirectional LSPs between routers R1 (ingress) and R5 (egress), which allow bidirectional traffic.
- The no-cspf statement included at the [edit protocols mpls label-switched-path *path-name*] hierarchy level, indicating that the Constrained Shortest Path First (CSPF) algorithm is not used to compute the LSP path.
- A strict path configured for both unidirectional LSPs, R1-to-R5 and R5-to-R1, at the [edit protocols mpls] hierarchy level.

Although there are a number of ways to examine an RSVP failure in an MPLS network, the following sequence of steps and commands is useful in determining the origin of an RSVP failure.

Steps To Take To examine the RSVP failure, follow these steps:

1. Verify the RSVP Session on page 155
2. Ping the Egress Router on page 156
3. Enable RSVP Tracing on Transit Routers on page 156
4. View the RSVP Log File on Transit Routers on page 158
5. Check the RSVP Log File on the Egress Router on page 159
6. Determine and Correct the Problem on the Egress Router on page 160
7. Remove the Tracing Configuration on page 161

Step 1: Verify the RSVP Session

Purpose In this case study, the unconstrained RSVP LSP from router R1 to R5 uses a strict path through R3, r1-r3-r5.

Action To verify that the RSVP session is established, enter the following JUNOS command-line interface (CLI) operational mode command:

```
user@host> show rsvp session ingress detail
```

Sample Output

```
user@R1> show rsvp session ingress detail
Ingress RSVP: 1 sessions

10.0.0.5
  From: 10.0.0.1, LSPstate: Dn, ActiveRoute: 0
  LSPname: R1-to-R5, LSPpath: Primary
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: -
  Resv style: 0 -, Label in: -, Label out: -
  Time left:    -, Since: Tue Jul 19 20:42:20 2005
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 16 receiver 11956 protocol 0
  PATH rcvfrom: localclient
  Adspec: sent MTU 1500
  Path MTU: received 0
  PATH sentto: 10.1.13.2 (so-0/0/2.0) 3 pkts
  Explct route: 10.1.13.2
  Record route: <self> ...incomplete
Total 1 displayed, Up 0, Down 1
```

What It Means The sample output from ingress router R1 shows that the RSVP session has not been established (Down 1) through the explicit path (10.1.13.2). The Path message was sent to R3 (10.1.13.2) and dropped. In situations like this, you can ping the egress router (R5) to ensure operational communications in the network, and enable RSVP tracing on the router that dropped the packet (R3) to obtain valuable clues as to the nature of the problem.

Step 2: Ping the Egress Router

Purpose Ping the egress router to confirm that communication over the network is operational.

Action To ping the egress router, enter the following JUNOS CLI operational mode command:

user@host> **ping** *ip-address-interface*

Sample Output

```
[edit protocols mpls]
user@R1# run ping 10.1.56.1
PING 10.1.56.1 (10.1.56.1): 56 data bytes
64 bytes from 10.1.56.1: icmp_seq=0 ttl=255 time=0.837 ms
64 bytes from 10.1.56.1: icmp_seq=1 ttl=255 time=0.792 ms
64 bytes from 10.1.56.1: icmp_seq=2 ttl=255 time=0.856 ms
^C
--- 10.1.56.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.792/0.828/0.856/0.027 ms
```

What It Means The sample output confirms that communication between router R1 and the IP address of the relevant interface on router R5 (10.1.56.1) is operational.

Step 3: Enable RSVP Tracing on Transit Routers

Purpose RSVP tracing on transit routers (R3 and R6) can provide useful information about the problem.

Action To enable RSVP tracing on transit routers, follow these steps:

1. In configuration mode, go to the following hierarchy level:

   user@host> **edit**
   user@host# **edit protocols rsvp**

2. Configure a log file:

   [edit protocols rsvp]
   user@host# **set traceoptions file** *filename*

3. Depending on your situation, specify all or one of the following RSVP-specific tracing flags:

   [edit protocols rsvp]
   user@host# **set traceoptions flag error detail**
   user@host# **set traceoptions flag path detail**
   user@host# **set traceoptions flag pathtear detail**

4. Verify and commit the configuration:

   user@host# **show**
   user@host# **commit**

5. Complete the above steps on any other transit routers that might provide useful information towards resolution of the problem.

Sample Output

```
user@R3> edit
Entering configuration mode

[edit]
user@R3# edit protocols rsvp

[edit protocols rsvp]
user@R3# set traceoptions file rsvp-log

[edit protocols rsvp]
user@R3# set traceoptions flag error detail

[edit protocols rsvp]
user@R3# set traceoptions flag path detail

[edit protocols rsvp]
user@R3# set traceoptions flag pathtear detail

[edit protocols rsvp]
user@R1# show
traceoptions {
    file rsvp-log;
    flag error detail;
    flag path detail;
    flag pathtear detail;
}
interface fxp0.0 {
    disable;
}
interface all;

[edit protocols rsvp]
user@R3# commit
commit complete
```

What It Means

The sample output shows a configuration of RSVP tracing on transit router R3. The same tracing configuration is placed on R6 (not shown). Various flags are included at the [edit protocols rsvp traceoptions] hierarchy level to provide slightly different information about RSVP traffic. For more information about RSVP tracing flags, see "RSVP Tracing Flags" on page 116. With all configured flags, the detail option is included to show granular details about errors and paths.

NOTE: Use the trace options detail flag with caution because it may cause the CPU to become very busy. For information on removing a tracing configuration, see "Remove the Tracing Configuration" on page 161.

After you have configured tracing and issued the commit command, the routing protocol process (rpd) immediately starts monitoring RSVP. Any RSVP activity that relates to the configured flags is placed in the log file.

Step 4: View the RSVP Log File on Transit Routers

Purpose Transit router messages that appear in the RSVP log file can help you analyze the problem with an RSVP session. You may need to issue the clear rsvp session and clear log *filename* commands to ensure that your records are current. However, if your network is large with many RSVP sessions, this may not be advisable because it may take a while for all sessions to reestablish. However, the clear rsvp session command has various options you can include to minimize the effect on your network. For more information about the clear rsvp session command, see the *JUNOS Routing Protocols and Policies Command Reference.*

Action To view the RSVP log file, enter the following JUNOS CLI operational mode commands:

```
user@host> clear rsvp session (Optional)
user@host> clear log filename (Optional)
user@host> show log filename
```

Sample Output 1

```
user@R3> clear rsvp session

user@R3> clear log rsvp-log

user@R3> show log rsvp-log
Jul 21 16:51:23 R3 clear-log[30656]: logfile cleared
Jul 21 16:51:24 RSVP recv Path 10.0.0.1->10.0.0.5 Len=208 so-0/0/2.0
Jul 21 16:51:24   Session7 Len 16 10.0.0.5(port/tunnel ID 11956) Proto 0
Jul 21 16:51:24   Hop      Len 12 10.1.13.1/0x086cd198
Jul 21 16:51:24   Time     Len  8 30000 ms
Jul 21 16:51:24   SrcRoute Len 20  10.1.13.2 S 10.1.36.2 S
Jul 21 16:51:24   LabelRequest Len  8 EtherType 0x800
Jul 21 16:51:24   Properties Len 12 Primary path
Jul 21 16:51:24   SessionAttribute Len 16 Prio (7,0) flag 0x0 "R1-to-R5"
Jul 21 16:51:24   Sender7  Len 12 10.0.0.1(port/lsp ID  32)
Jul 21 16:51:24   Tspec    Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500
Jul 21 16:51:24   ADspec   Len 48 MTU 1500
Jul 21 16:51:24   RecRoute Len 12  10.1.13.1
Jul 21 16:51:24 RSVP send Path 10.0.0.1->10.0.0.5 Len=208 so-0/0/3.0
Jul 21 16:51:24   Session7 Len 16 10.0.0.5(port/tunnel ID 11956) Proto 0
Jul 21 16:51:24   Hop      Len 12 10.1.36.1/0x08680264
Jul 21 16:51:24   Time     Len  8 30000 ms
Jul 21 16:51:24   SrcRoute Len 12  10.1.36.2 S
Jul 21 16:51:24   LabelRequest Len  8 EtherType 0x800
Jul 21 16:51:24   Properties Len 12 Primary path
Jul 21 16:51:24   SessionAttribute Len 16 Prio (7,0) flag 0x0 "R1-to-R5"
Jul 21 16:51:24   Sender7  Len 12 10.0.0.1(port/lsp ID  32)
Jul 21 16:51:24   Tspec    Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500
Jul 21 16:51:24   ADspec   Len 48 MTU 1500
Jul 21 16:51:24   RecRoute Len 20  10.1.36.1 10.1.13.1
```

Sample Output 2

```
user@R6> clear rsvp session

user@R6> clear log rsvp-log

user@R6> show log rsvp-log
Jul 21 17:01:21 R6 clear-log[41496]: logfile cleared
Jul 21 17:01:23 RSVP recv Path 10.0.0.1->10.0.0.5 Len=208 so-0/0/3.0
Jul 21 17:01:23   Session7 Len 16 10.0.0.5(port/tunnel ID 11956) Proto 0
Jul 21 17:01:23   Hop      Len 12 10.1.36.1/0x08680264
Jul 21 17:01:23   Time     Len  8 30000 ms
Jul 21 17:01:23   SrcRoute Len 12  10.1.36.2 S
```

```
Jul 21 17:01:23   LabelRequest Len  8 EtherType 0x800
Jul 21 17:01:23   Properties Len 12 Primary path
Jul 21 17:01:23   SessionAttribute Len 16 Prio (7,0) flag 0x0 "R1-to-R5"
Jul 21 17:01:23   Sender7  Len 12 10.0.0.1(port/lsp ID  32)
Jul 21 17:01:23   Tspec    Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500
Jul 21 17:01:23   ADspec   Len 48 MTU 1500
Jul 21 17:01:23   RecRoute Len 20  10.1.36.1 10.1.13.1
Jul 21 17:01:23 RSVP send Path 10.0.0.1->10.0.0.5 Len=204 so-0/0/0.0
Jul 21 17:01:23   Session7 Len 16 10.0.0.5(port/tunnel ID 11956) Proto 0
Jul 21 17:01:23   Hop      Len 12 10.1.56.2/0x086f9000
Jul 21 17:01:23   Time     Len  8 30000 ms
Jul 21 17:01:23   LabelRequest Len  8 EtherType 0x800
Jul 21 17:01:23   Properties Len 12 Primary path
Jul 21 17:01:23   SessionAttribute Len 16 Prio (7,0) flag 0x0 "R1-to-R5"
Jul 21 17:01:23   Sender7  Len 12 10.0.0.1(port/lsp ID  32)
Jul 21 17:01:23   Tspec    Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500
Jul 21 17:01:23   ADspec   Len 48 MTU 1500
Jul 21 17:01:23   RecRoute Len 28  10.1.56.2 10.1.36.1 10.1.13.1
```

What It Means Sample Output 1 from transit router R3 shows that R3 (so-0/0/2.0) correctly received a Path request message (recv Path) from R1, and correctly sent the Path message (send Path) through interface so-0/0/3.0 to R6. The route record object (RecRoute) indicates the list of addresses this Path message transited, in this case, 10 1.36.1 and 10.1.13.1.

Sample Output 2 from transit router R6 shows that R6 (so-0/0/3.0) correctly received a Path request message (recv Path) from R3, and correctly sent the Path message (send Path) through interface so-0/0/0 to R5. The route record object (RecRoute) indicates the list of addresses this Path message transited, in this case, 10.1.56.2, 10 1.36.1, and 10.1.13.1.

With the information above, the focus shifts to egress router R5 as the source of the problem, with indications that R5 ignored the RSVP message.

Step 5: Check the RSVP Log File on the Egress Router

Purpose After placing an RSVP tracing configuration on router R5 similar to that on routers R3 and R6, display the RSVP log file for useful information about the problem on router R5. For steps to configure RSVP tracing, see “Enable RSVP Tracing on Transit Routers” on page 156.

Action To check the RSVP log file, enter the following JUNOS CLI operational mode command:

user@host> **show log rsvp-log**

Sample Output

```
user@R5> show log rsvp-log
Jul 21 10:53:16 R5 clear-log[40071]: logfile cleared
Jul 21 11:02:37 trace_on: Tracing to "/var/log/rsvp-log" started
Jul 21 11:03:07 RSVP error, send to DISABLED interface? Hello New
10.1.56.1->10.1.56.2 Len=8 so-0/0/0.0
```

What It Means The sample output shows that R5 did not receive the Path message because of a disabled interface, so-0/0/0.0.

Step 6: Determine and Correct the Problem on the Egress Router

Purpose Check the configuration of interface so-0/0/0.0 on egress router R5 to determine the reason it was disabled.

Action To determine the problem on R5, enter the following JUNOS CLI commands:

```
user@R5> show configuration protocols rsvp
user@R5> edit
[edit protocols rsvp]
user@R5# rename interface so-0/0/3 to interface so-0/0/0
user@R5# show
user@R5# commit
user@R5# run show rsvp session ingress detail
```

Sample Output 1

```
user@R5> show configuration protocols rsvp
traceoptions {
    file rsvp-log;
    flag error detail;
    flag path detail;
    flag pathtear detail;
}
interface so-0/0/3.0;   <<< so-0/0/3 incorrectly included
interface so-0/0/1.0;
interface so-0/0/2.0;
interface fxp0.0 {
    disable;
}
```

Sample Output 2

```
[edit protocols rsvp]
user@R5# rename interface so-0/0/3 to interface so-0/0/0

[edit protocols rsvp]
user@R5# show
traceoptions {
    file rsvp-log;
    flag packets detail;
    flag error detail;
}
interface so-0/0/0.0;
interface so-0/0/1.0;
interface so-0/0/2.0;
interface fxp0.0 {
    disable;
}

[edit protocols rsvp]
user@R5# commit
commit complete
```

Sample Output 3

```
[edit protocols mpls]
user@R5# run show rsvp session ingress detail
Ingress RSVP: 1 sessions
To              From            State   Rt Style Labelin Labelout LSPname
10.0.0.1        10.0.0.5        Up       1  1 FF       -   103104 R5-to-R1
Total 1 displayed, Up 1, Down 0

Egress RSVP: 1 sessions
To              From            State   Rt Style Labelin Labelout LSPname
10.0.0.5        10.0.0.1        Up       0  1 FF       3        - R1-to-R5
Total 1 displayed, Up 1, Down 0

Transit RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0
```

What It Means Sample Output 1 from egress router R5 shows three interfaces configured at the [edit protocols rsvp] hierarchy level, non of which is so-0/0/0.0. On examination of the network topology, it is apparent that the so-0/0/0.0 interface was configured incorrectly as so-0/0/3.0.

Sample Output 2 shows the correct configuration of interfaces at the [edit protocols rsvp] hierarchy level, and the rename command issued to correct the configuration error.

Sample Output 3 shows that the RSVP-signaled LSP (R1-to-R5) is correctly established after the changes to the RSVP configuration are committed.

Step 7: Remove the Tracing Configuration

Purpose It is considered best practice to remove any configuration elements that are no longer required, such as tracing configurations.

Action To remove the tracing configuration, enter the following JUNOS CLI commands:

```
user@R5> edit
[edit protocols rsvp]
user@R5# show
user@R5# delete traceoptions
user@R5# show
user@R5# commit
```

Sample Output 1

```
user@R5> edit
Entering configuration mode

[edit]
user@R5# edit protocols rsvp

[edit protocols rsvp]
user@R5# show
traceoptions {
    file rsvp-log;
    flag error detail;
    flag path detail;
    flag pathtear detail;
}
interface so-0/0/3.0;
interface so-0/0/1.0;
interface so-0/0/2.0;
interface fxp0.0 {
```

```
    disable;
}

[edit protocols rsvp]
user@R5# delete traceoptions

[edit protocols rsvp]
user@R5# show
interface so-0/0/3.0;
interface so-0/0/1.0;
interface so-0/0/2.0;
interface fxp0.0 {
    disable;
}

[edit protocols rsvp]
user@R5# commit
commit complete
```

What It Means The sample output from egress router R5 shows that tracing is deleted from the R5 configuration. In addition, the tracing configuration was removed from all routers (not shown).

NOTE: Use the trace options detail flag with caution because it may cause the CPU to become very busy.

Part 4
Appendix

Appendix A

Command-Line Interface Overview

This appendix provides an overview of the JUNOS software command-line interface (CLI). For more detailed information about using the JUNOS software CLI, see the *JUNOS Interfaces Command Reference, JUNOS Routing Protocols Command Reference,* and the *System Basics and Services Command Reference*.

The CLI is the interface to the software that you use whenever you access the router—whether from the console or through a remote network connection. The CLI, which automatically starts after the router finishes booting, provides commands that you use to perform various tasks, including configuring the JUNOS software, and monitoring and troubleshooting the software, network connectivity, and the router hardware.

The CLI has two modes:

CLI Operational Mode

In operational mode you enter commands to monitor and troubleshoot the software, network connectivity, and router by entering commands.

When you log in to the router and the CLI starts, you are at the top level of the CLI operational mode. At this level, there are several broad groups of CLI commands (see Table 23).

Table 23: CLI Operational Mode Top-Level Commands

Command	Description
clear	Clear statistics and protocol database information. Syntax: clear <arp | bfd | bgp | firewall | helper | igmp | ike | ilmi | interfaces | ipv6 | isis | ldp | log | mld | mpls | msdp | multicast | ospf | pim | rip | ripng | route | rsvp | services | snmp | system | vrrp>
configure	Enter CLI configuration mode. Alternative commands: configure <exclusive | private>
file	Perform file manipulation operations, such as copy, delete, list, rename, and show. Syntax: file <archive source destination | compare | compress source destination | copy | delete | list | rename | show>
help	Provide help information. Syntax: help <reference | syslog | topic>
monitor	Monitor a log file or interface traffic in real time. Syntax: monitor <interface> <start | stop | list> <traffic>
mtrace	Display trace information about a multicast path from a source to a receiver. Syntax: mtrace <source-name> <from-source | monitor | to-gateway>
ping	Verify IP connectivity to another IP host or Asynchronous Transfer Mode (ATM) connectivity (ping ATM) using Operation Administration and Maintenance (OAM) cells to an ATM endstation. Syntax: ping *host-name* <interface *source-interface*> <bypass-routing> <count requests> <detail> <do-not-fragment> <inet | inet6> <interval seconds> <logical-router *logical-router-name*> <loose-source value> <pattern string> <rapid> <record-route> <routing-instance *routing-instance-name*> <size bytes> <strict strict-source value> <tos type-of-service> <ttl value> <verbose> <via route> <wait seconds> Syntax: ping atm interface *interface* <count *count*> <end-to-end | segment> <interval *interval*> <sequence-number *sequence-number*> <vci *vci*> <brief> Syntax: ping vpn-interface *vpn-interface host* <local *echo-address*>
pipe	Filter the output of an operational mode or configuration mode command. Syntax: | <compare <filename | rollback n> | count | display <detail | inheritance | xml> | except pattern | find pattern | hold | last | match pattern | no-more | resolve <full-names> | save filename | trim columns>
quit	Log out from the CLI process. Syntax: quit

Command	Description
request	■ Stop or reboot router components, switch between primary and backup components, display messages, and display system information. Syntax: request <chassis | ipsec switch | message | routing-engine | security | services flow-collector | support information> ■ Stop or reboot the router, load software packages, and back up the router's file systems. Syntax: request <chassis | ipsec switch | message | routing-engine | security | services
restart	Restart the router hardware or software processes. Syntax: restart <adaptive-services | chassis-control | class-of-service | disk-monitoring | ecc-error-logging | firewall | interface-control | kernel-replication | l2tp-service | mib-process | network-access-service | pgm | pic-services-logging | remote-operations routing | sampling | snmp> <gracefully | immediately | soft>
set	Set CLI properties, the router's date and time, and the craft interface display text. Syntax: set <chassis | cli | date | date ntp>
show	Show information about all aspects of the software, including interfaces and routing protocols. Syntax: show <accounting | aps | arp | as-path | bgp | chassis | class-of-service | cli | configuration | connections | dvmrp | firewall | helper | host | igmp | ike | ilmi | interfaces | ipsec | ipv6 | isis | l2circuit | l2vpn | ldp | link-management | log | mpls | msdp | multicast | ntp | ospf | ospf3 | passive monitoring | pfe | pim | policer | policy | rip | ripng | route | rsvp | sap | services | snmp | system | task | ted | version | vrrp>
ssh	Open a secure shell to another host. Syntax: ssh *host-name* <bypass-routing> <interface *interface-name*> <inet | inet6> <routing instance *routing-instance-name*> <source *source-name*> <v1 | v2> <vpn-interface *vpn-interface-name*>
start	Start a software process. Syntax: start shell
telnet	Start a telnet session to another host. Syntax: telnet *host-name* <8bit> <bypass-routing> < inet | inet6> <interface *interface-name*> <logical-router *logical-router-name*> <noresolve> <port *port-number*> <routing-instance *routing-instance-name*> <source *source-address*>
test	Run various diagnostic debugging commands. Syntax: test configuration (filename | terminal)
traceroute	Trace the route to a remote host. Syntax: traceroute *host-name* <as-number-lookup> <bypass-routing> <gateway address> <inet><inet6> <logical-router *logical-router-name*> <noresolve> <routing-instance *routing-instance-name*> <source address> <tos value> <ttl value> <interface *interface-name*> <wait *seconds*>

Using the CLI Operational Mode

This section describes how to use the CLI operational mode. You can do the following:

Entering the CLI Operational Mode

To enter the JUNOS software CLI, use the following command:

```
user@host> cli
```

You are in the CLI when you see the > prompt, preceded by a string that defaults to the name of the user and the name of the router. For example:

```
user@host>
```

Getting Help on Commands at a Hierarchy Level

The CLI provides context-sensitive help at every level of the command hierarchy. The help information tells you which commands are available at the current level in the hierarchy and provides a brief description of each.

To get help while in the CLI, type ?. You do not need to press Enter after typing the question mark. You have the following options:

- If you type the question mark at the command-line prompt, the CLI lists the available commands and options.
- If you type the question mark after entering the complete name of a command or command option, the CLI lists the available commands and options, then redisplays the command names and options that you typed.
- If you type the question mark in the middle of a command name, the CLI lists possible command completions that match the letters you have entered so far, then redisplays the letters that you typed.

Getting Help About Commands

To get help about operational mode CLI commands, you can do the following:

- Listing Top-Level Operational Mode CLI Commands on page 169
- Listing CLI Commands That Start with a Particular Letter on page 169
- Listing All Available Commands of a Particular Type on page 169

Listing Top-Level Operational Mode CLI Commands

To list all available commands at the top level of the CLI operational mode, use the following command (see Table 23 on page 166):

```
user@host> ?

Possible completions:
  clear               Clear information in the system
  configure           Manipulate software configuration information
  file                Perform file operations
  help                Provide help information
  monitor             Show real-time debugging information
  mtrace              Trace multicast path from source to receiver
  ping                Ping remote target
  quit                Exit the management session
  request             Make system-level requests
  restart             Restart software process
  set                 Set CLI properties, date/time, craft interface message
  show                Show system information
  ssh                 Start secure shell on another host
  start               Start shell
  telnet              Telnet to another host
  test                Perform diagnostic debugging
  traceroute          Trace route to remote host
```

Listing CLI Commands That Start with a Particular Letter

To list all commands that start with the letter **c**, use the following CLI command:

```
user@host> c?

Possible completions:
  clear                    Clear information in the system
  configure                Manipulate software configuration information
user@host> c
```

Listing All Available Commands of a Particular Type

To list all available **clear** commands, use the following CLI command:

```
user@host> clear ?

Possible completions:
  arp                 Clear address resolution information
  bfd                 Clear Bidirectional Forwarding Detection information
  bgp                 Clear Border Gateway Protocol information
  cli                 Clear command-line interface settings
  esis                Clear end system-to-intermediate system information
  firewall            Clear firewall counters
```

```
  helper              Clear port-forwarding helper information
  igmp                Clear Internet Group Management Protocol information
  ike                 Clear IKE information
  ilmi                Clear interim local management interface statistics
  interfaces          Clear interface information
  ipsec               Clear IP Security information
  ipv6                Clear IP version 6 information
  isis               Clear Intermediate System-to-Intermediate System
                     information
  ldp                 Clear Label Distribution Protocol information
  log                 Clear contents of log file
  mld                 Clear multicast listener discovery information
  mpls                Clear Multiprotocol Label Switching information
  msdp                Clear Multicast Source Discovery Protocol information
  multicast           Clear multicast information
  ospf                Clear Open Shortest Path First information
  ospf3               Clear Open Shortest Path First version 3 information
  pgm                 Clear Pragmatic Generalized Multicast information
  pim                 Clear Protocol Independent Multicast information
  rip                 Clear Routing Information Protocol information
  ripng               Clear Routing Information Protocol for IPv6 information
  rsvp               Clear Resource Reservation Protocol information
                     services
  snmp                Clear Simple Network Management Protocol information
  system              Clear system information
  vpls                Clear VPLS information
  vrrp                Clear Virtual Router Redundancy Protocol statistics
```

Having the CLI Complete Commands

You do not always have to remember or type the full command or option name for the CLI to recognize it. To display all possible command or option completions, type the partial command followed by a question mark.

To complete a command or option that you have partially typed, press the Tab key or the spacebar. If the partially typed letters begin a string that uniquely identifies a command, the complete command name appears. Otherwise, a beep indicates that you have entered an ambiguous command, and the possible completions are displayed.

Command completion also applies to other strings, such as filenames and usernames. To display all possible values, type a partial string followed by a question mark. However, to complete these strings, press the Tab key; pressing the space bar does not work.

Using CLI Command Completion

To complete the show interfaces command, do the following:

user@host> **show in<Spacebar>**terfaces **<Enter>**

```
Physical interface: at-0/1/0, Enabled, Physical link is Up
  Interface index: 11, SNMP ifIndex: 65
  Link-level type: ATM-PVC, MTU: 4482, Clocking: Internal, SONET mode
  Speed: OC12, Loopback: None, Payload scrambler: Enabled
  Device flags   : Present Running
  Link flags     : 0x01
[...Output truncated...]
```

To display a list of all log files whose names start with the string "messages," and then display the contents of one of the files, do the following:

user@host> **show log mes?**

```
Possible completions:
  <filename>                     Log file to display
  messages                       Size: 1417052, Last changed: Mar  3 00:33
  messages.0.gz                  Size: 145575, Last changed: Mar  3 00:00
  messages.1.gz                  Size: 134253, Last changed: Mar  2 23:00
  messages.10.gz                 Size: 137022, Last changed: Mar  2 14:00
  messages.2.gr                  Size: 137112, Last changed: Mar  2 22:00
  messages.3.gz                  Size: 121633, Last changed: Mar  2 21:00
  messages.4.gz                  Size: 135715, Last changed: Mar  2 20:00
  messages.5.gz                  Size: 137504, Last changed: Mar  2 19:00
  messages.6.gz                  Size: 134591, Last changed: Mar  2 18:00
  messages.7.gz                  Size: 132670, Last changed: Mar  2 17:00
  messages.8.gz                  Size: 136596, Last changed: Mar  2 16:00
  messages.9.gz                  Size: 136210, Last changed: Mar  2 15:00
```

```
user@host> show log mes<Tab>sages.4<Tab>.gz<Enter>
Jan 15 21:00:00 myhost newsyslog[1381]: logfile turned over
[...Output truncated...]
```

Displaying CLI Command History

You can display a list of recent commands that you issued. To display the command history, use the show cli history command:

user@host> **show cli history**

```
03-03 01:00:50 -- show cli history
03-03 01:01:12 -- show interfaces terse
03-03 01:01:22 -- show interfaces lo0
03-03 01:01:44 -- show bgp next-hop-database
03-03 01:01:51 -- show cli history
```

By default, this command displays the last 100 commands issued in the CLI. Specify a number with the command to display that number of recent commands. For example:

user@host> **show cli history 3**

```
01:01:44 – show bgp next-hop-database
01:01:51 -- show cli history
01:02:51 -- show cli history 3
```

CLI Configuration Mode

In configuration mode, you configure the JUNOS software by creating a hierarchy of configuration statements. You can do this by using the CLI or by creating a text (ASCII) file that contains the statement hierarchy. (The statement hierarchy is identical in both the CLI and text configuration file.) You can configure all properties of the JUNOS software, including interfaces, general routing information, routing protocols, and user access, as well as several system hardware properties. When you have finished entering the configuration statements, you commit them, which activates the configuration on the router.

Table 24 explains each CLI configuration mode command. The commands are organized alphabetically.

Table 24: CLI Configuration Mode Commands

Command	Description
activate	Remove the **inactive:** tag from a statement, effectively reading the statement or identifier to the configuration. Statements or identifiers that have been activated take effect when you next issue the **commit** command. Syntax: **activate** (*statement-path* | *identifier*)
annotate	Add comments to a configuration. Syntax: **annotate** *statement-path* "*comment-string*"
commit	Commit the set of changes to the database and cause the changes to take operational effect. Syntax: **commit** <<at <*string*>> <and-quit> <check> <confirmed <*minutes*>> <synchronize>
copy	Make a copy of an existing statement in the configuration. Syntax: **copy** *existing-statement-path* **to** *new-statement-path*
deactivate	Add the **inactive:** tag to a statement, effectively commenting out the statement or identifier from the configuration. Statements or identifiers marked as inactive do not take effect when you issue the **commit** command. Syntax: **deactivate** (*statement-path* | *identifier*)
delete	Delete a statement or identifier. All subordinate statements and identifiers contained within the specified statement path are deleted with it. Syntax: **delete** (*statement-path* | i*dentifier*)
edit	Move inside the specified statement hierarchy. If the statement does not exist, it is created. Syntax: **edit** *statement-path*
exit	Exit the current level of the statement hierarchy, returning to the level prior to the last edit command, or exit from configuration mode. The **quit** and **exit** commands are synonyms. Syntax: **exit** (configuration-mode)
help	Display help about available configuration statements. Syntax: **help** (apropos | topic | reference) <*string*>
insert	Insert an identifier into an existing hierarchy. Syntax: **insert** (*statement-path*) *identifier1* (before | after) *identifier2*

Command	Description
load	Load a configuration from an ASCII configuration file or from terminal input. Your current location in the configuration hierarchy is ignored when the load operation occurs. Syntax: load (merge | override | patch | replace) (*filename* | terminal)
quit	Exit the current level of the statement hierarchy, returning to the level prior to the last edit command, or exit from configuration mode. The quit and exit commands are synonyms. Syntax: quit configuration-mode
rename	Rename an existing configuration statement or identifier. Syntax: rename <*statement-path*> *identifier1* to *identifier2*
rollback	Return to a previously committed configuration. The software saves the last 50 committed configurations, including the rollback number, date, time, and name of the user who issued the commit configuration command. rollback 0 erases any configuration changes made to the current candidate configuration. The currently operational JUNOS software configuration is stored in the file juniper.conf, and the last three committed configurations are stored in the files juniper.conf.1.gz, juniper.conf.2.gz, and juniper.conf.3.gz. These four files are located in the directory /config/, which is on the router's flash drive. The remaining 46 previous committed configurations, the files juniper.conf.4.gz through juniper.conf.49.gz, are stored in the directory /var/db/config/, which is on the router's hard disk. Syntax: rollback <*number*>
run	Run a CLI command without exiting from configuration mode. Syntax: run *command*
save	Save the configuration to an ASCII file, by default in the users home directory. The contents of the current level of the statement hierarchy (and below) are saved, along with the statement hierarchy containing it. This allows a section of the configuration to be saved, while fully specifying the statement hierarchy. Syntax: save *filename*
set	Create a statement hierarchy and set identifier values. This is similar to edit except that your current level in the hierarchy does not change, and you can set identifier values whereas edit only allows access to a statement-path. Syntax: set (*statement-path* | *identifier)*
show	Display the current configuration. Syntax: show (*statement-path* | *identifier)*
status	Display the users currently editing the configuration.
top	Return to the top level of configuration command mode, which is indicated by the [edit] banner, or execute a command from the top level of the configuration. Syntax: top <*configuration-command*>
up	Move up one level in the statement hierarchy. Syntax: up <*number*>
update	Update a private database.

Configuration Statements and Identifiers

You configure all router properties by including statements in the configuration. A statement consists of a keyword, which is fixed text, and, optionally, an identifier. An identifier is an identifying name that you define, such as the name of an interface, or a username, which allows you and the CLI to discriminate among a collection of statements.

The following list shows the statements available at the top level of the configuration mode (that is, the trunk of the hierarchy tree). Table 25 on page 175 describes each statement.

```
[edit]
user@host# set ?
Possible completions:
> access                Network access configuration
> accounting-options    Accounting data configuration
> applications          Define applications by protocol characteristics
+ apply-groups          Groups from which to inherit configuration data
> chassis               Chassis configuration
> class-of-service      Class-of-service configuration
> firewall              Define a firewall configuration
> forwarding-options    Configure options to control packet sampling
> groups                Configuration groups
> interfaces            Interface configuration
> isdn                  ISDN process configuration
> logical-routers       Logical routers
> policy-options        Routing policy option configuration
> protocols             Routing protocol configuration
> routing-instances     Routing instance configuration
> routing-options       Protocol-independent routing option configuration
> security              Security configuration
> services              Service PIC applications settings
> snmp                  Simple Network Management Protocol configuration
> system                System parameters
```

An angle bracket (>) before the statement name indicates that it is a container statement and you can define other statements at levels below it.

If there is no angle bracket (>) before the statement name, the statement is a leaf statement; you cannot define other statements at hierarchy levels below it.

A plus sign (+) before the statement name indicates that it can contain a set of values. To specify a set, include the values in brackets. For example:

```
[edit]
user@host# set policy-options community my-as1-transit members [65535:10
65535:11]
```

In some statements, you can include an identifier. For some identifiers, such as interface names, you must specify the identifier in a precise format. For example, the interface name so-0/0/0 refers to a SONET/SDH interface that is on the Flexible PIC Concentrator (FPC) in slot 0, in the first Physical Interface Card (PIC) location, and in the first port on the PIC. For other identifiers, such as interface descriptive text, policy, and firewall term names, you can specify any name, including special characters, spaces, and tabs.

You must enclose in quotation marks (double quotes) identifiers and any strings that include the following characters: space tab ( ) [ ] { } ! @ # $ % ^ & | ' = ?

Table 25 describes each top-level CLI configuration mode statement.

Table 25: Configuration Mode Top-Level Statements

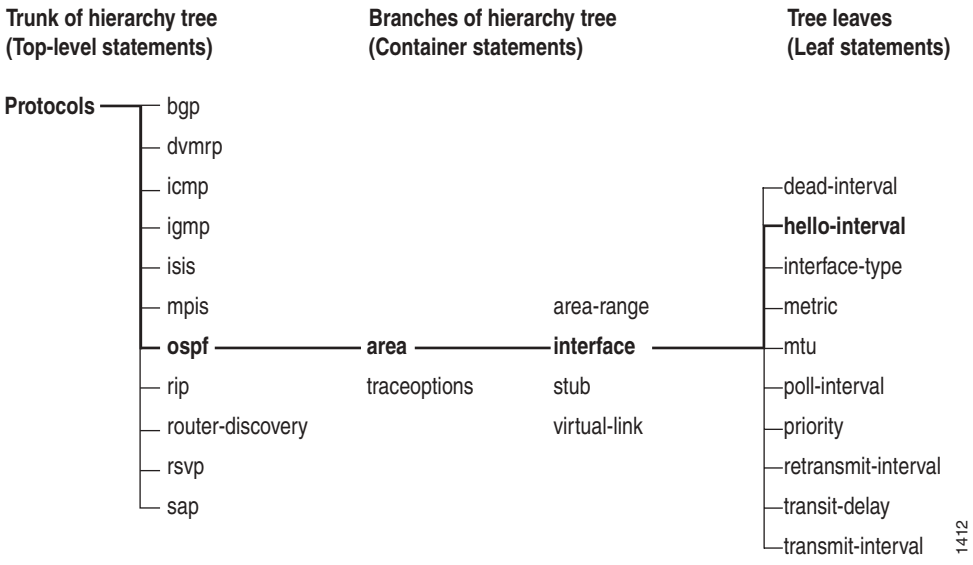
Statement	Description
accounting-options	Configure accounting statistics data collection for interfaces and firewall filters. For information about the statements in this hierarchy, see the *JUNOS Network Management Configuration Guide*.
chassis	Configure properties of the router chassis, including the clock source, conditions that activate alarms, and SONET/SDH framing and concatenation properties. For information about the statements in this hierarchy, see the *JUNOS Network Interfaces Configuration Guide* and the *JUNOS Class of Service Configuration Guide*.
class-of-service	Configure class-of-service parameters. For information about the statements in this hierarchy, see the *JUNOS Network Interfaces Configuration Guide* and the *JUNOS Class of Service Configuration Guide*.
firewall	Define filters that select packets based on their contents. For information about the statements in this hierarchy, see the *JUNOS Policy Framework Configuration Guide*.
forwarding-options	Define forwarding options, including traffic sampling options. For information about the statements in this hierarchy, see the *JUNOS Network Interfaces Configuration Guide* and the *JUNOS Class of Service Configuration Guide*.
groups	Configure configuration groups.
interfaces	Configure interface information, such as encapsulation, interfaces, virtual channel identifiers (VCIs), and data-link channel identifiers (DLCIs). For information about the statements in this hierarchy, see the *JUNOS Network Interfaces Configuration Guide* and the *JUNOS Class of Service Configuration Guide*.
policy-options	Define routing policies, which allow you to filter and set properties in incoming and outgoing routes. For information about the statements in this hierarchy, see the *JUNOS Routing Protocols Configuration Guide*.
protocols	Configure routing protocols, including Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP), and Resource Reservation Protocol (RSVP). For information about the statements in this hierarchy, see the chapters that discuss how to configure the individual routing protocols in the *JUNOS Routing Protocols Configuration Guide* and the *JUNOS MPLS Applications Configuration Guide*.
routing-instances	Configure multiple routing instances. For information about the statements in this hierarchy, see the *JUNOS Routing Protocols Configuration Guide*.

Statement	Description
routing-options	Configure protocol-independent routing options, such as static routes, autonomous system (AS) numbers, confederation members, and global tracing (debugging) operations to log. For information about the statements in this hierarchy, see the *JUNOS Routing Protocols Configuration Guide*.
snmp	Configure Simple Network Management Protocol (SNMP) community strings, interfaces, traps, and notifications. For information about the statements in this hierarchy, see the *JUNOS Network Management Configuration Guide*.
system	Configure systemwide properties, including the hostname, domain name, Domain Name System (DNS) server, user logins and permissions, mappings between hostnames and addresses, and software processes.

Configuration Statement Hierarchy

The JUNOS software configuration consists of a hierarchy of *statements*. There are two types of statements: *container statements*, which are statements that contain other statements, and *leaf statements*, which do not contain other statements (see Figure 19). All of the container and leaf statements together form the *configuration hierarchy*.

Figure 19: Configuration Mode Hierarchy of Statements



Each statement at the top level of the configuration hierarchy resides at the trunk (or root level) of a hierarchy tree. The top-level statements are container statements, containing other statements that form the tree branches. The leaf statements are the leaves of the hierarchy tree. An individual hierarchy of statements, which starts at the trunk of the hierarchy tree, is called a *statement path*. Figure 19 illustrates the hierarchy tree, showing a statement path for the portion of the protocol configuration hierarchy that configures the hello interval on an interface in an OSPF area.

The protocols statement is a top-level statement at the trunk of the configuration tree. The ospf, area, and interface statements are all subordinate container statements of a higher statement (they are branches of the hierarchy tree), and the hello-interval statement is a leaf on the tree, which, in this case, contains a data value: the length of the hello interval, in seconds.

The CLI represents the statement path shown in Figure 19 as [protocols ospf area *area-number* interface *interface-name*], and displays the configuration as follows:

```
protocols {
    ospf {
        area 0.0.0.0 {
            interface so-0/0/0 {
                hello-interval 5;
            }
            interface so-0/0/1 {
                hello-interval 5;
            }
        }
    }
}
```

The CLI indents each level in the hierarchy to indicate each statement's relative position in the hierarchy and generally sets off each level with braces, using an open brace at the beginning of each hierarchy level and a closing brace at the end. If the statement at a hierarchy level is empty, the braces are not printed. Each leaf statement ends with a semicolon. If the hierarchy does not extend as far as a leaf statement, the last statement in the hierarchy ends with a semicolon.

The CLI uses this indented representation when it displays the current system configuration, and you use this format when creating ASCII files that contain the software configuration. However, the format of ASCII configuration files is not as strict as the CLI output of the configuration. Although the braces and semicolons are required, the indentation and use of new lines, as shown above, are not required in ASCII configuration files.

Using the CLI Configuration Mode

This section describes how to use the CLI configuration mode. You can do the following tasks:

Entering Configuration Mode

If many users enter configuration mode at the same time, everyone can make configuration changes and commit all changes. If one user enters configuration mode when another user is also in configuration mode, a message indicates who the user is and what portion of the configuration that user is viewing or editing. To enter configuration mode, use the following CLI command:

user@host> **configure**

```
Entering configuration mode
Current configuration users:
    root terminal p3 (pid 1088) on since 1999-05-13 01:03:27 EDT
        [edit interfaces so-3/0/0 unit 0 family inet]
The configuration has been changed but not committed
```

- If, when you enter configuration mode, the configuration contains changes that have not been committed, a message appears:

  user@host> **configure**

  ```
  Entering configuration mode
  The configuration has been changed but not committed
  ```

- If, while in configuration mode, you try to make a change while the configuration is locked by another user, a message indicates that the configuration database is locked, who the user is, and what portion of the configuration the user is viewing or editing:

  [edit]
  user@host# **set system host-name ipswitch**

  ```
  error: configuration database locked by:
      user2 terminal d0 (pid 1828) on since 19:47:58 EDT, idle 00:02:11
          exclusive [edit protocols]
  ```

- If you enter configuration mode with the configure exclusive command, you lock the candidate configuration for as long as you remain in configuration mode, allowing you to make changes without interference from other users. If another user is also in configuration mode and has the configuration locked, a message indicates who the user is and what portion of the configuration the user is viewing or editing:

  user@host> **configure exclusive**

  ```
  Entering configuration mode
  Users currently editing the configuration:
  ```

```
    root terminal p3 (pid 1088) on since 2000-10-30 19:47:58 EDT, idle
00:00:44
    exclusive [edit interfaces so-3/0/0 unit 0 family inet]
```

Exiting Configuration Mode

To exit configuration mode, use the exit configuration-mode configuration mode command from any level or use the exit command from the top level. If you try to exit from configuration mode using the exit command and the configuration contains changes that have not been committed, you see a message and prompt:

```
[edit]
user@host# exit

The configuration has been changed but not committed
Exit with uncommitted changes? [yes,no] (yes) <Enter>
Exiting configuration mode
user@host>
```

To exit with uncommitted changes without having to respond to a prompt, use the exit configuration-mode command.

Moving Among Levels of the Hierarchy

The CLI commands in Table 26 help you navigate the levels of the configuration statement hierarchy.

Table 26: CLI Configuration Mode Navigation Commands

Command	Description
edit	To move down through an existing configuration command hierarchy, or to create a hierarchy and move down to that level, use the edit configuration mode command, specifying the hierarchy level at which you want to be.
exit	To move up the hierarchy, use the exit configuration mode command. This command is, in effect, the opposite of the edit command.
up	To move up the hierarchy one level at a time, use the up configuration mode command.
top	To move directly to the top level, use the top configuration mode command.

Displaying the Current Configuration

You can display the following information about the current configuration:

- Displaying the Configuration at the Current Hierarchy Level on page 180
- Displaying the Last Committed Current Configuration on page 180
- Displaying Users Currently Editing the Configuration on page 180

Displaying the Configuration at the Current Hierarchy Level

To display the configuration at the current hierarchy level or at the specified level, use the show configuration mode command.

```
user@host> show <statement-path>
```

The configuration statements appear in a fixed order. The CLI indents each level in the hierarchy to indicate each statement's relative position in the hierarchy and generally sets off each level with braces, using an open brace at the beginning of each hierarchy level and a closing brace at the end. If the statement at a hierarchy level is empty, the braces are not printed. Each leaf statement ends with a semicolon. If the hierarchy does not extend as far as a leaf statement, the last statement in the hierarchy ends with a semicolon. Interfaces appear alphabetically by type, and then in numerical order by slot number, PIC number, and port number.

Displaying the Last Committed Current Configuration

You also can use the CLI operational mode show configuration command to display the last committed current configuration, which is the configuration currently running on the router:

```
user@host> show configuration
```

Displaying Users Currently Editing the Configuration

To display the users currently editing the configuration, use the status configuration mode command:

```
[edit]
user@host# status

Current configuration users:
  user terminal p0 (pid 518) on since 2002-03-12 18:24:27 PST
      [edit protocols]
```

The system displays who is editing the configuration (user), how the user is logged in (terminal p0), the date and time the user logged in (2002-03-12 18:24:27 PST), and what level of the hierarchy the user is editing ([edit protocols]).

Modifying the Configuration

To configure the router or to modify an existing router configuration, you add statements to the configuration. For each statement hierarchy, you create the hierarchy starting with a statement at the top level and continuing with statements that move progressively lower in the hierarchy.

To modify the hierarchy, you use two configuration mode commands:

- set—Creates a statement hierarchy and sets identifier values. After you issue a set command, you remain at the same level in the hierarchy. The set command has the following syntax:

  set <*statement-path*> *statement* <*identifier*>

  statement-path is the hierarchy to the configuration statement and the statement itself. If you have already moved to the statement's hierarchy level, you omit this. *statement* is the configuration statement itself. *identifier* is a string that identifies an instance of a statement.

- edit—Moves to a particular hierarchy level. If that hierarchy level does not exist, the edit command creates it and then moves to it. The edit command has the following syntax:

  edit <*statement-path*> *statement* <*identifier*>

Removing a Statement

To delete a statement or identifier, use the delete configuration mode command. Deleting a statement or an identifier effectively "unconfigures" the functionality associated with that statement or identifier, returning that functionality to its default condition. When you delete a statement, the statement and all its subordinate statements and identifiers are removed from the configuration.

delete <*statement-path*> <*identifier*>

To delete the entire hierarchy starting at the current hierarchy level, do not specify a statement or an identifier in the delete command:

```
[edit]
user@host# delete

Delete everything under this level? [yes, no] (no) ?
    Possible completions:
        no          Don't delete everything under this level
        yes         Delete everything under this level
Delete everything under this level? [yes, no] (no)
```

Running Operational Mode CLI Commands from Configuration Mode

To display the output of an operational mode show or other command while configuring the software, you can execute a single operational mode command by issuing the run configuration mode command and specifying the operational mode command:

```
[edit]
user@host# run operational-mode-command
```

Displaying Configuration Mode Command History

To display a list of the recent commands you issued while in configuration mode, use the run show cli history command. By default, this command displays the last 100 commands issued in the CLI.

```
[edit]
user@host# run show cli history

12:40:08 -- show
12:40:17 -- edit protocols
12:40:27 -- set isis
12:40:29 -- edit isis
12:40:40 -- run show cli history
```

Committing a Configuration

To commit a configuration, you can do the following:

- Saving Configuration Changes and Activating the Configuration on page 182
- Saving Configuration Changes, Activating the Configuration, and Exiting Configuration Mode on page 182

Saving Configuration Changes and Activating the Configuration

To save software configuration changes to the configuration database and activate the configuration on the router, use the commit configuration mode command:

```
[edit]
user@host# commit

commit complete
```

The configuration is checked for syntax errors. If the syntax is correct, the configuration is activated and becomes the current, operational router configuration. If the configuration contains syntax errors, a message indicates the location of the error and the configuration is not activated. You must correct the error before recommitting the configuration.

Saving Configuration Changes, Activating the Configuration, and Exiting Configuration Mode

To save software configuration changes, activate the configuration on the router, and exit configuration mode, use the commit and-quit configuration mode command. This command succeeds only if the configuration contains no errors.

```
[edit]
user@host# commit and-quit

commit complete
exiting configuration mode
user@host>
```

Saving a Configuration to a File

To save the configuration to a text (ASCII) file so that you can edit it with a text editor of your choice, use the save configuration mode command. By default, the configuration is saved to that file in your home directory, which is on the flash disk.

```
[edit]
user@host# save filename

Wrote 475 lines of configuration to 'filename'
```

Returning to a Previously Committed Configuration

To return to a previously committed configuration, you can do the following:

- Returning to the Most Recently Committed Configuration on page 183
- Activating the Configuration You Loaded on page 183
- Returning to a Configuration Prior to the Most Recently Committed One on page 183
- Displaying Previous Configurations on page 184

Returning to the Most Recently Committed Configuration

To return to the most recently committed configuration and load it into configuration mode without activating it, use the rollback configuration mode command:

```
[edit]
user@host# rollback

load complete
```

Activating the Configuration You Loaded

To activate the configuration that you loaded, use the commit command:

```
[edit]
user@host# rollback
load complete
[edit]
user@host# commit
```

Returning to a Configuration Prior to the Most Recently Committed One

To return to a configuration prior to the most recently committed one, include the number in the rollback command. *number* can be a number in the range 0 through 9. The most recently saved configuration is number 0 (which is the default configuration to which the system returns), and the oldest saved configuration is number 9.

```
[edit]
user@host# rollback number

load complete
```

Displaying Previous Configurations

To display previous configurations, including the rollback number, date, time, the name of the user who committed changes, and the method of commit, use the rollback ? command.

```
[edit]
user@host# rollback ?

Possible completions:
<[Enter]> Execute this command
<number> Numeric argument
  0                    2005-02-27 12:52:10 PST by abc via cli
  1                    2005-02-26 14:47:42 PST by def via cli
  2                    2005-02-14 21:55:45 PST by ghi via cli
  3                    2005-02-10 16:11:30 PST by jkl via cli
  4                    2005-02-10 16:02:35 PST by mno via cli
  5                    2005-03-16 15:10:41 PST by pqr via cli
  6                    2005-03-16 14:54:21 PST by stu via cli
  7                    2005-03-16 14:51:38 PST by vwx via cli
  8                    2005-03-16 14:43:29 PST by yzz via cli
  9                    2005-03-16 14:15:37 PST by abc via cli
  10                   2005-03-16 14:13:57 PST by def via cli
  11                   2005-03-16 12:57:19 PST by root via other
  12                   2005-03-16 10:45:23 PST by root via other
  13                   2005-03-16 10:08:13 PST by root via other
  14                   2005-03-16 01:20:56 PST by root via other
  15                   2005-03-16 00:40:37 PST by ghi via cli
  16                   2005-03-16 00:39:29 PST by jkl via cli
  17                   2005-03-16 00:32:36 PST by mno via cli
  18                   2005-03-16 00:31:17 PST by pqr via cli
  19                   2005-03-15 19:59:00 PST by stu via cli
  20                   2005-03-15 19:53:39 PST by vwx via cli
  21                   2005-03-15 18:07:19 PST by yzz via cli
  22                   2005-03-15 17:59:03 PST by abc via cli
  23                   2005-03-15 15:05:14 PST by def via cli
  24                   2005-03-15 15:04:51 PST by ghi via cli
  25                   2005-03-15 15:03:42 PST by jkl via cli
  26                   2005-03-15 15:01:52 PST by mno via cli
  27                   2005-03-15 14:58:34 PST by pqr via cli
  28                   2005-03-15 13:09:37 PST by root via other
  29                   2005-03-12 11:01:20 PST by stu via cli
  30                   2005-03-12 10:57:35 PST by vwx via cli
  31                   2005-03-11 10:25:07 PST by yzz via cli
  32                   2005-03-10 23:40:58 PST by abc via cli
  33                   2005-03-10 23:40:38 PST by def via cli
  34                   2005-03-10 23:14:27 PST by ghi via cli
  35                   2005-03-10 23:10:16 PST by jkl via cli
  36                   2005-03-10 23:01:51 PST by mno via cli
  37                   2005-03-10 22:49:57 PST by pqr via cli
  38                   2005-03-10 22:24:07 PST by stu via cli
  39                   2005-03-10 22:20:14 PST by vwx via cli
  40                   2005-03-10 22:16:56 PST by yzz via cli
  41                   2005-03-10 22:16:41 PST by abc via cli
  42                   2005-03-10 20:44:00 PST by def via cli
  43                   2005-03-10 20:43:29 PST by ghi via cli
  44                   2005-03-10 20:39:14 PST by jkl via cli
  45                   2005-03-10 20:31:30 PST by root via other
```

```
  46                   2005-03-10 18:57:01 PST by mno via cli
  47                   2005-03-10 18:56:18 PST by pqr via cli
  48                   2005-03-10 18:47:49 PST by stu via cli
  49                   2005-03-10 18:47:34 PST by vw via cli
|   Pipe through a command
[edit]
```

Getting Help About Statements

In configuration mode, you can use the help command to display help based on a text string contained in a statement name. This command displays help for statements at the current hierarchy level and below.

user@host# **help** *string*

You can also display help based on a text string contained in a statement name using the help topic and help reference commands. The help topic command displays usage guidelines for the statement, whereas the help reference command displays summary information about the statement.

```
user@host# help topic ?
  access                Network access control
  accounting-options    Accounting data collection
  applications          Application protocols
  bgp                   Border Gateway Protocol
  chassis               Platform
  class-of-service      Class of service (CoS)
  connections           Circuit cross-connect (CCC)
  dvmrp                 Distance Vector Multicast Routing Protocol
  firewall              Firewalls and filters
  forwarding-options    Packet sampling
  groups                Configuration groups
  igmp                  Internet Group Management Protocol
  interfaces            Interfaces
  isis                  Intermediate System-to-Intermediate System
  l2circuit             Layer 2 virtual circuits
  layer2-vpns           Layer 2 VPNs
  layer3-vpns           Layer 3 VPNs
  ldp                   Label Distribution Protocol
  link-management       Link Management Protocol
  logical-routers       Logical routers
  mld                   Multicast Listener Discovery protocol
  mpls                  Multiprotocol Label Switching
  msdp                  Multicast Source Discovery Protocol
  ospf                  Open Shortest Path First protocol
  pgm                   Pragmatic Generalized Multicast
  pim                   Protocol-Independent Multicast and data MDT
  policy-options        Routing policy
  rip                   Routing Information Protocol
  ripng                 Routing Information Protocol Next Generation
  rmon                  Remote Monitoring
  router-advertisement  Neighbor discovery
  router-discovery      Internet Control Message Protocol router discovery
  routing-instances     Routing instances
  routing-options       Protocol-independent routing options
  rsvp                  Resource Reservation Protocol
  sap                   Session Advertisement Protocol
```

```
  security                Internet Protocol security (IPSec)
  services                Service sets for Adaptive Services PIC
  snmp                    Simple Network Management Protocol
  system                  System parameters
  vpls                    Virtual private LAN service
  vpns                    Virtual private networks
```

```
[edit]
user@help# help topic access ?
Possible completions:
  examples
  l2tp                    Overview of Layer 2 Tunneling Protocol configuration
  point-to-point          Overview of Point-to-Point Protocol configuration
  radius-disconnect-port  Port number for RADIUS disconnect server
  radius-server           RADIUS server configuration
  traceoptions            Trace options for access processes
  tunnel-profile          Join multilink bundles based on endpoint discriminator
```

```
[edit]
user@host# help topic access point-to-point
Configuring the Point-to-Point Protocol

   To configure the Point-to-Point Protocol (PPP), do the following:
     * Configuring the Challenge Handshake Authentication Protocol

     * Configuring the Authentication Order

user@host# help reference string
```

If you do not type an option for a statement that requires one, a message indicates the type of information expected. In this example, you need to type an area number to complete the command:

```
[edit]
user@host# set protocols ospf area<Enter>

syntax error, expecting <identifier>.
```

In this example, you need to type a value for the hello interval to complete the command:

```
[edit]
user@host# set protocols ospf area 45 interface so-0/0/0
                hello-interval<Enter>

syntax error, expecting <data>
```

If you have omitted a required statement at a particular hierarchy level, when you attempt to move from that hierarchy level or when you issue the **show** command in configuration mode, a message indicates which statement is missing. For example:

```
[edit protocols pim interface so-0/0/0]
user@host# top
Warning: missing mandatory statement: 'mode'
[edit]
user@host# show
protocols {
    pim {
        interface so-0/0/0 {
            priority 4;
            version 2;
            # Warning: missing mandatory statement(s): 'mode'
        }
    }
}
```

Part 5
Index

Index

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V