JUNIPER NETWORKS

Junos® OS

RSVP Configuration Guide

Release
12.1

Published: 2012-03-13

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

Junos® OS RSVP Configuration Guide
12.1

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

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

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration Guide* • RFC 1997, *BGP Communities Attribute*

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

Convention	Description	Examples
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; interface names; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub** <**default-metric** *metric*>**;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** (***string1*** **|** ***string2*** **|** ***string3***)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

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

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to **techpubs-comments@juniper.net**, or fill out the documentation feedback form at

https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/ .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

CHAPTER 1

Introduction to RSVP

RSVP Introduction

RSVP is a resource reservation setup protocol that is used by both network hosts and routers. Hosts use RSVP to request a specific class of service (CoS) from the network for particular application flows. Routers use RSVP to deliver CoS requests to all routers along the data path. RSVP also can maintain and refresh states for a requested CoS application flow.

RSVP treats an application flow as a simplex connection. That is, the CoS request travels only in one direction—from the sender to the receiver. RSVP is a transport layer protocol that uses IP as its network layer. However, RSVP does not transport application flows. Rather, it is more of an Internet control protocol, similar to the Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP). RSVP runs as a separate software process in the Junos OS and is not in the packet forwarding path.

RSVP is not a routing protocol, but rather is designed to operate with current and future unicast and multicast routing protocols. The routing protocols are responsible for choosing the routes to use to forward packets, and RSVP consults local routing tables to obtain routes. RSVP only ensures the CoS of packets traveling along a data path.

The receiver in an application flow requests the preferred CoS from the sender. To do this, the receiver issues an RSVP CoS request on behalf of the local application. The request propagates to all routers in reverse direction of the data paths toward the sender. In this process, RSVP requests might be merged, resulting in a protocol that scales well when there are a large number of receivers.

Because the number of receivers in an application flow is likely to change and the flow of delivery paths might change during the life of an application flow, RSVP takes a soft-state approach in its design, creating and removing the protocol states in routers and hosts incrementally over time. RSVP sends periodic refresh messages to maintain its state and to recover from occasional lost messages. In the absence of refresh messages, RSVP states automatically time out and are deleted.

Junos OS RSVP Protocol Implementation

The Junos implementation of RSVP supports RSVP version 1. The software includes support for all mandatory objects and RSVP message types, and supports message integrity and node authentications through the Integrity object.

The primary purpose of the Junos RSVP software is to support dynamic signaling within MPLS label-switched paths (LSPs). Supporting resource reservations over the Internet is only a secondary purpose of the Junos OS implementation. Since supporting resource reservations is secondary, the Junos RSVP software does not support the following features:

- IP multicasting sessions.
- Traffic control. The software cannot make resource reservations for real-time video or audio sessions.

With regard to the protocol mechanism, packet processing, and RSVP objects supported, the Junos OS implementation of the software is interoperable with other RSVP implementations.

RSVP Operation Overview

RSVP creates independent sessions to handle each data flow. A session is identified by a combination of the destination address, an optional destination port, and a protocol. Within a session, there can be one or more senders. Each sender is identified by a combination of its source address and source port. An out-of-band mechanism, such as a session announcement protocol or human communication, is used to communicate the session identifier to all senders and receivers.

A typical RSVP session involves the following sequence of events:

1. A potential sender starts sending RSVP path messages to the session address.
2. A receiver, wanting to join the session, registers itself if necessary. For example, a receiver in a multicast application would register itself with IGMP.
3. The receiver receives the path messages.
4. The receiver sends appropriate Resv messages toward the sender. These messages carry a flow descriptor, which is used by routers along the path to make reservations in their link-layer media.
5. The sender receives the Resv message and then starts sending application data.

This sequence of events is not necessarily strictly synchronized. For example, receivers can register themselves before receiving path messages from the sender, and application data can flow before the sender receives Resv messages. Application data that is delivered before the actual reservation contained in the Resv message typically is treated as best-effort, non-real-time traffic with no CoS guarantee.

RSVP Authentication

The Junos OS supports both the RSVP authentication style described in RFC 2747 (allowing for multivendor compatibility) and the RSVP authentication style described in Internet draft draft-ietf-rsvp-md5-03.txt. The Junos OS uses the authentication style described in Internet draft draft-ietf-rsvp-md5-08.txt by default. If the router receives an RFC 2747-style RSVP authentication from a neighbor, it switches to this style of authentication for that neighbor. The RSVP authentication style for each neighboring router is determined separately.

RSVP and IGP Hello Packets and Timers

RSVP monitors the status of the interior gateway protocol (IGP) (IS-IS or OSPF) neighbors and relies on the IGP protocols to detect when a node fails. If an IGP protocol declares a neighbor down (because hello packets are no longer being received), RSVP also brings down that neighbor. However, the IGP protocols and RSVP still act independently when bringing a neighbor up.

In the Junos OS, RSVP typically relies on IGP hello packet detection to check for node failures. RSVP sessions are kept up even if RSVP hello packets are no longer being received, so long as the router continues to receive IGP hello packets. RSVP sessions are maintained until either the router stops receiving IGP hello packets or the RSVP Path and Resv messages time out. Configuring a short time for the IS-IS or OSPF hello timers allows these protocols to detect node failures quickly.

RSVP hellos can be relied on when the IGP does not recognize a particular neighbor (for example, if IGP is not enabled on the interface) or if the IGP is RIP (not IS-IS or OSPF). Also, the equipment of other vendors might be configured to monitor RSVP sessions based on RSVP hello packets. This equipment might also take an RSVP session down due to a loss of RSVP hello packets.

We do not recommend configuring a short RSVP hello timer. If quick discovery of a failed neighbor is needed, configure short IGP (OSPF or IS-IS) hello timers.

OSPF and IS-IS have infrastructure to manage rapid hello message sending and receiving reliably, even if the routing protocols or some other process are straining the processing capability of the router. Under the same circumstances, RSVP hellos might time out prematurely even though the neighbor is functioning normally.

RSVP Message Types

RSVP uses the following types of messages to establish and remove paths for data flows, establish and remove reservation information, confirm the establishment of reservations, and report errors:

- Path Messages on page 6
- Resv Messages on page 7
- PathTear Messages on page 7
- ResvTear Messages on page 7
- PathErr Messages on page 7
- ResvErr Messages on page 7
- ResvConfirm Messages on page 8

Path Messages

Each sender host transmits path messages downstream along the routes provided by the unicast and multicast routing protocols. Path messages follow the exact paths of application data, creating path states in the routers along the way, thus enabling routers to learn the previous-hop and next-hop node for the session. Path messages are sent periodically to refresh path states.

The refresh interval is controlled by a variable called the ***refresh-time***, which is the periodical refresh timer expressed in seconds. A path state times out if a router does not receive a specified number of consecutive path messages. This number is specified by

a variable called ***keep-multiplier***. Path states are kept for **((*keep-multiplier* + 0.5) x 1.5 x *refresh-time*)** seconds.

Resv Messages

Each receiver host sends reservation request (Resv) messages upstream toward senders and sender applications. Resv messages must follow exactly the reverse path of path messages. Resv messages create and maintain a reservation state in each router along the way.

Resv messages are sent periodically to refresh reservation states. The refresh interval is controlled by the same refresh time variable, and reservation states are kept for **((*keep-multiplier* + 0.5) x 1.5 x *refresh-time*)** seconds.

PathTear Messages

PathTear messages remove (tear down) path states as well as dependent reservation states in any routers along a path. PathTear messages follow the same path as path messages. A PathTear typically is initiated by a sender application or by a router when its path state times out.

PathTear messages are not required, but they enhance network performance because they release network resources quickly. If PathTear messages are lost or not generated, path states eventually time out when they are not refreshed, and the resources associated with the path are released.

ResvTear Messages

ResvTear messages remove reservation states along a path. These messages travel upstream toward senders of the session. In a sense, ResvTear messages are the reverse of Resv messages. ResvTear messages typically are initiated by a receiver application or by a router when its reservation state times out.

ResvTear messages are not required, but they enhance network performance because they release network resources quickly. If ResvTear messages are lost or not generated, reservation states eventually time out when they are not refreshed, and the resources associated with the reservation are released.

PathErr Messages

When path errors occur (usually because of parameter problems in a path message), the router sends a unicast PathErr message to the sender that issued the path message. PathErr messages are advisory; these messages do not alter any path state along the way.

ResvErr Messages

When a reservation request fails, a ResvErr error message is delivered to all the receivers involved. ResvErr messages are advisory; these messages do not alter any reservation state along the way.

ResvConfirm Messages

Receivers can request confirmation of a reservation request, and this confirmation is sent with a ResvConfirm message. Because of the complex RSVP flow-merging rules, a confirmation message does not necessarily provide end-to-end confirmation of the entire path. Therefore, ResvConfirm messages are an indication, not a guarantee, of potential success.

Juniper Networks routers never request confirmation using the ResvConfirm message; however, a Juniper Networks router can send a ResvConfirm message if it receives a request from another vendor's equipment.

RSVP Reservation Styles

A reservation request includes options for specifying the reservation style. The reservation styles define how reservations for different senders within the same session are treated and how senders are selected.

Two options specify how reservations for different senders within the same session are treated:

- Distinct reservation—Each receiver establishes its own reservation with each upstream sender.
- Shared reservation—All receivers make a single reservation that is shared among many senders.

Two options specify how senders are selected:

- Explicit sender—List all selected senders.
- Wildcard sender—Select all senders, which then participate in the session.

The following reservation styles, formed by a combination of these four options, currently are defined:

- Fixed filter (FF)—This reservation style consists of distinct reservations among explicit senders. Examples of applications that use fixed-filter-style reservations are video applications and unicast applications, which both require flows that have a separate reservation for each sender. The fixed filter reservation style is enabled on RSVP LSPs by default.
- Wildcard filter (WF)—This reservation style consists of shared reservations among wildcard senders. This type of reservation reserves bandwidth for any and all senders, and propagates upstream toward all senders, automatically extending to new senders as they appear. A sample application for wildcard filter reservations is an audio application in which each sender transmits a distinct data stream. Typically, only a few senders are transmitting at any one time. Such a flow does not require a separate reservation for each sender; a single reservation is sufficient.
- Shared explicit (SE)—This reservation style consists of shared reservations among explicit senders. This type of reservation reserves bandwidth for a limited group of

senders. A sample application is an audio application similar to that described for wildcard filter reservations.

RSVP Refresh Reduction

RSVP relies on soft-state to maintain the path and reservation states on each router. If the corresponding refresh messages are not sent periodically, the states eventually time out and reservations are deleted. RSVP also sends its control messages as IP datagrams with no reliability guarantee. It relies on periodic refresh messages to handle the occasional loss of Path or Resv messages.

The RSVP refresh reduction extensions, based on RFC 2961, addresses the following problems that result from relying on periodic refresh messages to handle message loss:

- Scalability—The scaling problem arises from the periodic transmission and processing overhead of refresh messages, which increases as the number of RSVP sessions increases.
- Reliability and latency—The reliability and latency problem stems from the loss of nonrefresh RSVP messages or one-time RSVP messages such as PathTear or PathErr. The time to recover from such a loss is usually tied to refresh interval and the keepalive timer.

The RSVP refresh reduction capability is advertised by enabling the refresh reduction (RR) capable bit in the RSVP common header. This bit is only significant between RSVP neighbors.

RSVP refresh reduction includes the following features:

- RSVP message bundling using the bundle message
- RSVP Message ID to reduce message processing overhead
- Reliable delivery of RSVP messages using Message ID, Message Ack, and Message Nack
- Summary refresh to reduce the amount of information transmitted every refresh interval

The RSVP refresh reduction specification (RFC 2961) allows you to enable some or all of the above capabilities on a router. It also describes various procedures that a router can use to detect the refresh reduction capabilities of its neighbor.

The Junos OS supports all of the refresh reduction extensions, some of which can be selectively enabled or disabled. The Junos OS supports Message ID and therefore can perform reliable message delivery only for Path and Resv messages.

For information about how to configure RSVP refresh reduction, see "Configuring RSVP Refresh Reduction" on page 23.

MTU Signaling in RSVP

The maximum transmission unit (MTU) is the largest size packet or frame, in bytes, that can be sent in a network. An MTU that is too large might cause retransmissions. Too

small an MTU might cause the router to send and handle relatively more header overhead and acknowledgments. There are default values for MTUs associated with various protocols. You can also explicitly configure an MTU on an interface.

When an LSP is created across a set of links with different MTU sizes, the ingress router does not know what the smallest MTU is on the LSP path. By default, the MTU for an LSP is 1,500 bytes.

If this MTU is larger than the MTU of one of the intermediate links, traffic might be dropped, because MPLS packets cannot be fragmented. Also, the ingress router is not aware of this type of traffic loss, because the control plane for the LSP would still function normally.

To prevent this type of packet loss in MPLS LSPs, you can configure MTU signaling in RSVP. This feature is described in RFC 3209. Juniper Networks supports the Integrated Services object for MTU signaling in RSVP. The Integrated Services object is described in RFCs 2210 and 2215. MTU signaling in RSVP is disabled by default.

To avoid packet loss due to MTU mismatches, the ingress router needs to do the following:

- Signal the MTU on the RSVP LSP—To prevent packet loss from an MTU mismatch, the ingress router needs to know what the smallest MTU value is along the path taken by the LSP. Once this MTU value is obtained, the ingress router can assign it to the LSP.
- Fragment packets—Using the assigned MTU value, packets that exceed the size of the MTU can be fragmented into smaller packets on the ingress router before they are encapsulated in MPLS and sent over the RSVP-signaled LSP.

Once both MTU signaling and packet fragmentation have been enabled on an ingress router, any route resolving to an RSVP LSP on this router uses the signaled MTU value. For information about how to configure this feature, see "Configuring MTU Signaling in RSVP" on page 46.

The following sections describe how MTU signaling in RSVP works:

How the Correct MTU Is Signaled in RSVP

How the correct MTU is signaled in RSVP varies depending on whether the network devices (for example, routers) explicitly support MTU signaling in RSVP or not.

If the network devices support MTU signaling in RSVP, the following occur when you enable MTU signaling:

- The MTU is signaled from the ingress router to the egress router by means of the Adspec object. Before forwarding this object, the ingress router enters the MTU value associated with the interface over which the path message is sent. At each hop in the path, the MTU value in the Adspec object is updated to the minimum of the received value and the value of the outgoing interface.
- The ingress router uses the traffic specification (Tspec) object to specify the parameters for the traffic it is going to send. The MTU value signaled for the Tspec object at the ingress router is the maximum MTU value (9192 bytes). This value does not change en route to the egress router.
- When the Adspec object arrives at the egress router, the MTU value is correct for the path (meaning it is the smallest MTU value discovered). The egress router compares the MTU value in the Adspec object to the MTU value in the Tspec object. It signals the smaller MTU using the Flowspec object in the Resv message.
- When the Resv object arrives at the ingress router, the MTU value in this object is used as the MTU for the next hops that use the LSP.

In a network where there are devices that do not support MTU signaling in RSVP, you might have the following behaviors:

- If the egress router does not support MTU signaling in RSVP, the MTU is set to 1,500 bytes by default.
- A Juniper Networks transit router that does not support MTU signaling in RSVP sets an MTU value of 1,500 bytes in the Adspec object by default.

Determining an Outgoing MTU Value

The outgoing MTU value is the smaller of the values received in the Adspec object compared to the MTU value of the outgoing interface. The MTU value of the outgoing interface is determined as follows:

- If you configure an MTU value under the **[family mpls]** hierarchy level, this value is signaled.
- If you do not configure an MTU, the **inet** MTU is signaled.

MTU Signaling in RSVP Limitations

The following are limitations to MTU signaling in RSVP:

- Changes in the MTU value might cause a temporary loss of traffic in the following situations:
  - For link protection and node protection, the MTU of the bypass is only signaled at the time the bypass becomes active. During the time it takes for the new path MTU to be propagated, packet loss might occur because of an MTU mismatch.

- For fast reroute, the MTU of the path is updated only after the detour becomes active, causing a delay in an update to the MTU at the ingress router. Until the MTU is updated, packet loss might occur if there is an MTU mismatch.

  In both cases, only packets that are larger than the detour or bypass MTU are lost.

- When an MTU is updated, it triggers a change in the next hop. Any change in the next hop causes the route statistics to be lost.
- The minimum MTU supported for MTU signaling in RSVP is 1,488 bytes. This value prevents a false or incorrectly configured value from being used.
- For single-hop LSPs, the MTU value displayed by the **show** commands is the RSVP-signaled value. However, this MPLS value is ignored and the correct IP value is used.

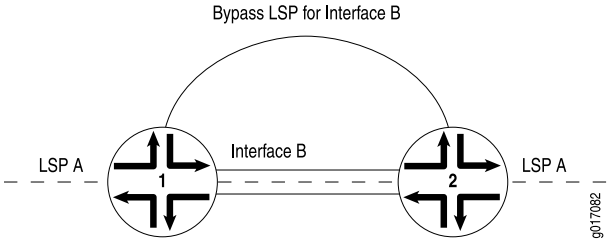
Link Protection

Link protection helps to ensure that traffic going over a specific interface to a neighboring router can continue to reach this router if that interface fails. When link protection is configured for an interface and an LSP that traverses this interface, a bypass LSP is created that will handle this traffic if the interface fails. The bypass LSP uses a different interface and path to reach the same destination. The path used can be configured explicitly, or you can rely on CSPF. The RSVP metric for the bypass LSP is set in the range of 20,000 through 29,999 (this value is not user configurable).

If a link-protected interface fails, traffic is quickly switched to the bypass LSP. Note that a bypass LSP cannot share the same egress interface with the LSPs it monitors.

In Figure 1 on page 12, link protection is enabled on Interface B between Router 1 and Router 2. It is also enabled on LSP A, an LSP that traverses the link between Router 1 and Router 2. If the link between Router 1 and Router 2 fails, traffic from LSP A is quickly switched to the bypass LSP generated by link protection.

Figure 1: Link Protection Creating a Bypass LSP for the Protected Interface



Although LSPs traversing an interface can be configured to take advantage of link protection, it is important to note that it is specifically the interface that benefits from link protection. If link protection is enabled on an interface but not on a particular LSP traversing that interface, then if the interface fails, that LSP will also fail.

NOTE: Link protection does not work on unnumbered interfaces.

To protect traffic over the entire route taken by an LSP, you should configure fast reroute. For more information, see Configuring Fast Reroute.

The following sections provide more information on link protection:

- Fast Reroute, Node Protection, and Link Protection on page 13
- Multiple Bypass LSPs on page 13

Fast Reroute, Node Protection, and Link Protection

RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*, describes two different types of traffic protection for RSVP-signaled LSPs:

- One-to-one backup—In the Junos OS this type of traffic protection is provided by fast reroute. Each LSP requires a protecting LSP to be signaled at each hop except the egress router. This protecting LSP cannot be shared.
- Facility backup—This is sometimes called many-to-one backup. In the Junos OS this type of traffic protection is provided by node and link protection. Each LSP requires a protecting LSP to be signaled at each hop except the egress router. Unlike fast reroute, this protecting LSP can be shared by other LSPs.

Table 3 on page 13 summarizes the traffic protection types.

Table 3: One-to-One Backup Compared with Facility Backup

Comparison	One-to-One Backup	Facility Backup
Name of the protecting LSP	Detour LSP	Bypass LSP
Sharing of the protecting LSP	Cannot be shared	Can be shared by multiple LSPs
Junos configuration statements	**fast-reroute**	**node-link-protection** and **link-protection**

Multiple Bypass LSPs

By default, link protection relies on a single bypass LSP to provide path protection for an interface. However, you can also specify multiple bypass LSPs to provide link protection for an interface. You can individually configure each of these bypass LSPs or create a single configuration for all of the bypass LSPs. If you do not configure the bypass LSPs individually, they all share the same path and bandwidth constraints.

The following algorithm describes how and when an additional bypass LSP is activated for an LSP:

1. If any currently active bypass can satisfy the requirements of the LSP (bandwidth, link protection, or node-link protection), the traffic is directed to that bypass.

2. If no active bypass LSP is available, scan through the manual bypass LSPs in first-in, first-out (FIFO) order, skipping those that are already active (each manual bypass can only be activated once). The first inactive manual bypass that can satisfy the requirements is activated and traffic is directed to that bypass.
3. If no manual bypass LSPs are available and if the **max-bypasses** statement activates multiple bypass LSPs for link protection, determine whether an automatically configured bypass LSP can satisfy the requirements. If an automatically configured bypass LSP is available and if the total number of active automatically configured bypass LSPs does not exceed the maximum bypass LSP limit (configured with the **max-bypasses** statement), activate another bypass LSP.

For information about how to configure multiple bypass LSPs for link protection, see "Configuring Bypass LSPs" on page 33.

Node Protection

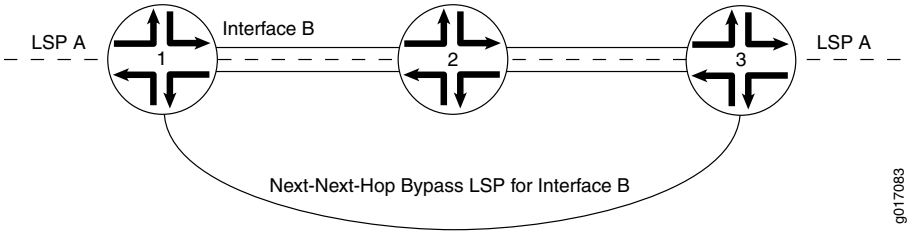
Node protection extends the capabilities of link protection. Link protection helps to ensure that traffic going over a specific interface to a neighboring router can continue to reach this router if that interface fails. Node protection ensures that traffic from an LSP traversing a neighboring router can continue to reach its destination even if the neighboring router fails.

When you enable node protection for an LSP, you must also enable link protection. Once enabled, node protection and link protection establish the following types of bypass LSPs:

- Next-hop bypass LSP—Provides an alternate route for an LSP to reach a neighboring router. This type of bypass LSP is established when you enable either node protection or link protection.
- Next-next-hop bypass LSP—Provides an alternate route for an LSP to get around a neighboring router en route to the destination router. This type of bypass LSP is established exclusively when node protection is configured. If a next-next-hop bypass LSP cannot be created, an attempt is made to signal a next-hop bypass LSP.

In Figure 2 on page 14, node protection is enabled on Interface B on Router 1. Node protection is also enabled on LSP A, an LSP that traverses the link transiting Router 1, Router 2, and Router 3. If Router 2 suffers a hardware or software failure, traffic from LSP A is switched to the next-next-hop bypass LSP generated by node protection.

Figure 2: Node Protection Creating a Next-Next-Hop Bypass LSP



The time needed by node protection to switch traffic to a next-next-hop bypass LSP can be significantly longer than the time needed by link protection to switch traffic to a next-hop bypass LSP. Link protection relies on a hardware mechanism to detect a link failure, allowing it to quickly switch traffic to a next-hop bypass LSP.

Node failures are often due to software problems on the node router. Node protection relies on the receipt of hello messages from a neighboring router to determine whether it is still functioning. The time it takes node protection to divert traffic partly depends on how often the node router sends hello messages and how long it takes the node-protected router to react to having not received a hello message. However, once the failure is detected, traffic can be quickly diverted to the next-next-hop bypass LSP.

NOTE:

Node protection provides traffic protection in the event of an error or interruption of the physical link between two routers. It does not provide protection in the event of control plane errors. The following provides an example of a control plane error:

- A transit router changes the label of a packet due to a control plane error.
- When the ingress router receives the packet, it considers the label change to be a catastrophic event and deletes both the primary LSP and the associated bypass LSP.

Related Documentation

- Configuring Node Protection or Link Protection for LSPs on page 30

RSVP Graceful Restart

RSVP graceful restart allows a router undergoing a restart to inform its adjacent neighbors of its condition. The restarting router requests a grace period from the neighbor or peer, which can then cooperate with the restarting router. The restarting router can still forward MPLS traffic during the restart period; convergence in the network is not disrupted. The restart is not visible to the rest of the network, and the restarting router is not removed from the network topology. RSVP graceful restart can be enabled on both transit routers and ingress routers. It is available for both point-to-point LSPs and point-to-multipoint LSPs.

RSVP graceful restart is described in the following sections:

- RSVP Graceful Restart Standard on page 56
- RSVP Graceful Restart Terminology on page 57
- RSVP Graceful Restart Operation on page 16
- Processing the Restart Cap Object on page 17

RSVP Graceful Restart Operation

For RSVP graceful restart to function, the feature must be enabled on the global routing instance. RSVP graceful restart can be disabled at the protocol level (for RSVP alone) or at the global level for all protocols.

RSVP graceful restart requires the following of a restarting router and the router's neighbors:

- For the restarting router, RSVP graceful restart attempts to maintain the routes installed by RSVP and the allocated labels, so that traffic continues to be forwarded without disruption. RSVP graceful restart is done quickly enough to reduce or eliminate the impact on neighboring nodes.
- The neighboring routers must have RSVP graceful restart helper mode enabled, thus allowing them to assist a router attempting to restart RSVP.

An object called Restart Cap that is sent in RSVP hello messages advertises a node's restart capability. The neighboring node sends a Recover Label object to the restarting node to recover its forwarding state. This object is essentially the old label that the restarting node advertised before the node went down.

The following lists the RSVP graceful restart behaviors, which vary depending on the configuration and on which features are enabled:

- If you disable helper mode, the Junos OS does not attempt to help a neighbor restart RSVP. Any information that arrives with a Restart Cap object from a neighbor is ignored.
- When you enable graceful restart under the routing instance configuration, the router can restart gracefully with the help of its neighbors. RSVP advertises a Restart Cap object (RSVP RESTART) in hello messages in which restart and recovery times are specified (neither value is 0).
- If you explicitly disable RSVP graceful restart under the **[protocols rsvp]** hierarchy level, the Restart Cap object is advertised with restart and recovery times specified as 0. The restart of neighboring routers is supported (unless helper mode is disabled), but the router itself does not preserve the RSVP forwarding state and cannot recover its control state.
- If after a restart RSVP realizes that no forwarding state has been preserved, the Restart Cap object is advertised with restart and recovery times specified as 0.
- If graceful restart and helper mode are disabled, RSVP graceful restart is completely disabled. The router neither recognizes nor advertises the RSVP graceful restart objects.

You cannot explicitly configure values for the restart and recovery times.

Unlike other protocols, there is no way for RSVP to determine that it has completed a restart procedure, other than a fixed timeout. All RSVP graceful restart procedures are timer-based. A **show rsvp version** command might indicate that the restart is still in progress even if all RSVP sessions are back up and the routes are restored.

Processing the Restart Cap Object

The following assumptions are made about a neighbor based on the Restart Cap object (assuming that a control channel failure can be distinguished unambiguously from a node restart):

- A neighbor that does not advertise the Restart Cap object in its hello messages cannot assist a router with state or label recovery, nor can it perform an RSVP graceful restart.
- After a restart, a neighbor advertising a Restart Cap object with a restart time equal to any value and a recovery time equal to 0 has not preserved its forwarding state. When a recovery time equals 0, the neighbor is considered dead and any states related to this neighbor are purged, regardless of the value of the restart time.
- After a restart, a neighbor advertising its recovery time with a value other than 0 can keep or has kept the forwarding state. If the local router is helping its neighbor with restart or recovery procedures, it sends a Recover Label object to this neighbor.

PART 2

Configuration

CHAPTER 2

RSVP Configuration Guidelines

Minimum RSVP Configuration

To enable RSVP on a single interface, include the **rsvp** statement and specify the interface using the **interface** statement. This is the minimum RSVP configuration. All other RSVP configuration statements are optional.

```
rsvp {
  interface interface-name;
}
```

You can include these statements at the following hierarchy levels:

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

To enable RSVP on all interfaces, substitute **all** for the ***interface-name*** variable.

If you have configured interface properties on a group of interfaces and want to disable RSVP on one of the interfaces, include the **disable** statement:

```
interface interface-name {
  disable;
}
```

You can include this statement at the following hierarchy levels:

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

Configuring RSVP and MPLS

The primary purpose of the Junos RSVP software is to support dynamic signaling within label-switched paths (LSPs). When you enable both MPLS and RSVP on a router, MPLS becomes a client of RSVP. No additional configuration is required to bind MPLS and RSVP.

You can configure MPLS to set up signaled paths by using the **label-switched-path** statement at the **[edit protocols mpls]** hierarchy level. Each LSP translates into a request for RSVP to initiate an RSVP session. This request is passed through the internal interface between label switching and RSVP. After examining the request information, checking RSVP states, and checking the local routing tables, RSVP initiates one session for each LSP. The session is sourced from the local router and is destined for the target of the LSP.

When an RSVP session is successfully created, the LSP is set up along the paths created by the RSVP session. If the RSVP session is unsuccessful, RSVP notifies MPLS of its status. It is up to MPLS to initiate backup paths or continue retrying the initial path.

To pass label-switching signaling information, RSVP supports four additional objects: Label Request object, Label object, Explicit Route object, and Record Route object. For an LSP to be set up successfully, all routers along the path must support MPLS, RSVP, and the four objects. Of the four objects, the Record Route object is not mandatory.

To configure MPLS and make it a client of RSVP, do the following:

- Enable MPLS on all routers that will participate in the label switching (this is, on all routers that might be part of a label-switching path).
- Enable RSVP on all routers and on all router interfaces that form the LSP.
- Configure the routers at the beginning of the LSP.

Example: Configuring RSVP and MPLS

The following shows a sample configuration for a router at the beginning of an LSP:

```
[edit]
protocols {
   mpls {
      label-switched-path sf-to-london {
         to 192.168.1.4;
      }
   }
   rsvp {
      interface so-0/0/0;
   }
}
```

The following shows a sample configuration for all the other routers that form the LSP:

```
[edit]
protocols {
   mpls {
      interface so-0/0/0;
   }
   rsvp {
      interface so-0/0/0;
   }
}
```

Configuring RSVP Interfaces

The following sections describe how to configure RSVP interfaces:

Configuring RSVP Refresh Reduction

You can configure RSVP refresh reduction on each interface by including the following statements in the interface configuration:

- **aggregate**—Enable all RSVP refresh reduction features: RSVP message bundling, RSVP message ID, reliable message delivery, and summary refresh.
- **no-aggregate**—Disable RSVP message bundling and summary refresh.
- **reliable**—Enable RSVP message ID and reliable message delivery.
- **no-reliable**—Disable RSVP message ID, reliable message delivery, and summary refresh.

For more information on RSVP refresh reduction, see "RSVP Refresh Reduction" on page 9.

Table 4 on page 24 lists various combinations of the RSVP refresh reduction configuration statements and how they alter the behavior of the Junos OS. The table describes only the expected behavior based on the configuration on the router. The actual behavior is dictated not only by the local configuration on this router, but also on the refresh reduction capabilities of its RSVP neighbors. Note that by configuring the **aggregate** statement, you enable all RSVP refresh reduction features, including reliable message delivery.

Table 4: RSVP Refresh Reduction Behavior

Configuration Statement	Send Capability	Receive Capability
aggregate or **aggregate** and **reliable**	RR bit = 1BundleMessage ID (Path/Resv messages)Ack/Nack (all messages)Summary Refresh	BundleAck/Nack (all messages)Summary Refresh
aggregate and **no-reliable**	RR bit = 1BundleAck/Nack (all messages)	BundleMessage ID (all messages)
reliable or **reliable** and **no-aggregate**	RR bit = 0Message ID (Path/Resv messages)Ack/Nack (all messages)	BundleMessage ID (all messages)Ack/Nack

The send capability shown in Table 4 on page 24 lists the RSVP messages and objects related to RSVP refresh reduction that the router is capable of sending. This does not mean that all these messages are exchanged between this router and a neighbor. For example, if the router is configured with the **aggregate** statement, but RSVP refresh reduction is not enabled on its neighbor, then no Summary Refresh message is sent to this neighbor even though the router is capable of sending it.

The receive capability shown in Table 4 on page 24 lists the messages and objects related to RSVP refresh reduction that the router is capable of receiving and processing without generating any errors or resulting in error conditions.

If the **no-reliable** statement is configured on the router (reliable message delivery is disabled), the router accepts RSVP messages that include the Message ID object but ignore the Message ID object and continue performing standard message processing. No error is generated in this case, and RSVP operates normally.

However, not all combinations between two neighbors with different refresh reduction capabilities function correctly. For example, a router is configured with either the **aggregate** statement and **no-reliable** statement or with the **reliable** and **no-aggregate** statements. If an RSVP neighbor sends a Summary Refresh object to this router, no error is generated, but the Summary Refresh object cannot be processed. Consequently, RSVP states can time out on this router if the neighbor is relying only on Summary Refresh to refresh those RSVP states.

We recommend, unless there are specific requirements, that you configure RSVP refresh reduction in a similar manner on each RSVP neighbor.

To enable all RSVP refresh reduction features on an interface, include the **aggregate** statement:

```
aggregate;
```

You can include this statement at the following hierarchy levels:

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

To disable RSVP message bundling and summary refresh, include the **no-aggregate** statement:

```
no-aggregate;
```

You can include this statement at the following hierarchy levels:

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

To enable RSVP message ID and reliable message delivery on an interface, include the **reliable** statement:

```
reliable;
```

You can include this statement at the following hierarchy levels:

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

To disable RSVP message ID, reliable message delivery, and summary refresh, include the **no-reliable** statement:

```
no-reliable;
```

You can include this statement at the following hierarchy levels:

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

Determining the Refresh Reduction Capability of RSVP Neighbors

To determine the RSVP refresh reduction capability of an RSVP neighbor, you need the following information:

- The RR bit advertised by the neighbor
- The local configuration of RSVP refresh reduction
- The actual RSVP messages received from the neighbor

To obtain this information, you can issue a **show rsvp neighbor detail** command. Sample output follows:

```
user@host> show rsvp neighbor detail
```

```
RSVP neighbor: 6 learned
    Address: 192.168.224.178 via: fxp1.0 status: Up
      Last changed time: 10:06, Idle: 5 sec, Up cnt: 1, Down cnt: 0
      Message received: 36
      Hello: sent 69, received: 69, interval: 9 sec
      Remote instance: 0x60b8feba, Local instance: 0x74bc7a8d
      Refresh reduction:  not operational

    Address: 192.168.224.186 via: fxp2.0 status: Down
      Last changed time: 10:17, Idle: 40 sec, Up cnt: 0, Down cnt: 0
      Message received: 6
      Hello: sent 20, received: 0, interval: 9 sec
      Remote instance: 0x0, Local instance: 0x2ae1b339
      Refresh reduction:  incomplete
        Remote end: disabled, Ack-extension: enabled

    Address: 192.168.224.188 via: fxp2.0 status: Up
      Last changed time: 4:15, Idle: 0 sec, Up cnt: 1, Down cnt: 0
      Message received: 55
      Hello: sent 47, received: 31, interval: 9 sec
      Remote instance: 0x6436a35b, Local instance: 0x663849f0
      Refresh reduction:  operational
        Remote end: enabled, Ack-extension: enabled
```

For more information on the **show rsvp neighbor detail** command, see the *Junos OS Routing Protocols and Policies Command Reference*.

Configuring the RSVP Hello Interval

RSVP monitors the status of the interior gateway protocol (IGP) (IS-IS or OSPF) neighbors and relies on the IGP protocols to detect when a node fails. If an IGP protocol declares a neighbor down (because hello packets are no longer being received), RSVP also brings down that neighbor. However, the IGP protocols and RSVP still act independently when bringing a neighbor up.

For Juniper Networks routers, configuring a shorter or longer RSVP hello interval has no impact on whether or not an RSVP session is brought down. RSVP sessions are kept up even if RSVP hello packets are no longer being received. RSVP sessions are maintained until either the router stops receiving IGP hello packets or the RSVP Path and Resv messages time out.

However, the RSVP hello interval might impact when another vendor's equipment brings down an RSVP session. For example, a neighboring non-Juniper Networks router might be configured to monitor RSVP hello packets.

To modify how often RSVP sends hello packets, include the **hello-interval** statement:

```
hello-interval seconds;
```

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

Configuring RSVP Authentication

All RSVP protocol exchanges can be authenticated to guarantee that only trusted neighbors participate in setting up reservations. By default, RSVP authentication is disabled.

RSVP authentication uses a Hashed Message Authentication Code (HMAC)-MD5 message-based digest. This scheme produces a message digest based on a secret authentication key and the message contents. (The message contents also include a sequence number.) The computed digest is transmitted with RSVP messages. Once you have configured authentication, all received and transmitted RSVP messages with all neighbors are authenticated on this interface.

MD5 authentication provides protection against forgery and message modification. It also can prevent replay attacks. However, it does not provide confidentiality, because all messages are sent in clear text.

By default, authentication is disabled. To enable authentication, configure a key on each interface by including the **authentication-key** statement:

authentication-key *key*;

You can include this statement at the following hierarchy levels:

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

Configuring the Bandwidth Subscription for Class Types

By default, RSVP allows 100 percent of the bandwidth for a class type to be used for RSVP reservations. When you oversubscribe a class type for a multiclass LSP, the aggregate demand of all RSVP sessions is allowed to exceed the actual capacity of the class type.

For detailed instructions on how to configure the bandwidth subscription for class types, see Configuring the Bandwidth Subscription Percentage for LSPs.

Configuring the RSVP Update Threshold on an Interface

The interior gateway protocols (IGPs) maintain the traffic engineering database, but the current available bandwidth on the traffic engineering database links originates from RSVP. When a link's bandwidth changes, RSVP informs the IGPs, which can then update the traffic engineering database and forward the new bandwidth information to all network nodes. The network nodes then know how much bandwidth is available on the traffic engineering database link (local or remote), and CSPF can correctly compute the paths.

However, IGP updates can consume excessive system resources. Depending on the number of nodes in a network, it might not be desirable to perform an IGP update for small changes in bandwidth. By configuring the **update-threshold** statement at the **[edit protocols rsvp]** hierarchy level, you can adjust the threshold at which a change in the reserved bandwidth triggers an IGP update.

You can configure a value of from 1 percent through 20 percent (the default is 10 percent) for when to trigger an IGP update. If the change in the reserved bandwidth is greater than or equal to the configured threshold percentage of the static bandwidth on that interface, then an IGP update occurs. For example, if you have configured the **update-threshold** statement to be 15 percent and the router discovers that the reserved bandwidth on a

link has changed by 10 percent of the link bandwidth, RSVP does not trigger an IGP update. However, if the reserved bandwidth on a link changes by 20 percent of the link bandwidth, RSVP triggers an IGP update.

To adjust the threshold at which a change in the reserved bandwidth triggers an IGP update, include the **update-threshold** statement:

```
update-threshold percentage;
```

You can include this statement at the following hierarchy levels:

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

Because of the update threshold, it is possible for Constrained Shortest Path First (CSPF) to compute a path using outdated traffic engineering database bandwidth information on a link. If RSVP attempts to establish an LSP over that path, it might find that there is insufficient bandwidth on that link. When this happens, RSVP triggers an IGP traffic engineering database update, flooding the updated bandwidth information on the network. CSPF can then recompute the path by using the updated bandwidth information, and attempt to find a different path, avoiding the congested link. Note that this functionality is the default and does not need any additional configuration.

You can configure the **rsvp-error-hold-time** statement at the **[edit protocols mpls]** hierarchy level or the **[edit logical-systems** ***logical-system-name*** **protocols mpls]** hierarchy level to improve the accuracy of the traffic engineering database (including the accuracy of bandwidth estimates for LSPs) using information provided by PathErr messages. See Improving Traffic Engineering Database Accuracy with RSVP PathErr Messages.

Configuring RSVP for Unnumbered Interfaces

The Junos OS supports RSVP traffic engineering over unnumbered interfaces. Traffic engineering information about unnumbered links is carried in the IGP traffic engineering extensions for OSPF and IS-IS as described in RFC 4203, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*, and RFC 4205, *Intermediate System to Intermediate System (IS-IS) Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*. Unnumbered links can also be specified in the MPLS traffic engineering signaling as described in RFC 3477, *Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)*. This feature allows you avoid having to configure IP addresses for each interface participating in the RSVP-signaled network.

To configure RSVP for unnumbered interfaces, you must configure the router with a router ID using the **router-id** statement specified at the **[edit routing-options]** hierarchy level. The router ID must be available for routing (you can typically use the loopback address). The RSVP control messages for the unnumbered links are sent using the router ID address (rather than a randomly selected address).

To configure link protection and fast reroute on a router with unnumbered interfaces enabled, you must configure at least two addresses. We recommend that you configure a secondary interface on the loopback in addition to configuring the router ID.

Configuring RSVP Node ID Hellos

You can configure node-ID based RSVP hellos to ensure that Juniper Networks routers can interoperate with the equipment of other vendors. By default, the Junos OS uses interface-based RSVP hellos. Node-ID based RSVP hellos are specified in RFC 4558, *Node-ID Based Resource Reservation Protocol (RSVP) Hello: A Clarification Statement*. RSVP node-ID hellos are useful if you have configured BFD to detect problems over RSVP interfaces, allowing you to disable interface-hellos for these interfaces. You can also use node-ID hellos for graceful-restart procedures.

Node-ID hellos can be enabled globally for all RSVP neighbors. By default, node-ID hello support is disabled. If you have not enabled RSVP node IDs on the router, the Junos OS does not accept any node-ID hello packets.

To enable RSVP node-ID hellos globally on the router, include the **node-hello** statement:

```
node-hello;
```

You can include this statement at the following hierarchy levels:

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

You can also explicitly disable RSVP interface hellos globally. This type of configuration might be necessary in networks where the Juniper Networks router has numerous RSVP connections with equipment from other vendors. However, if you disable RSVP interface hellos globally, you can also configure a hello interval on an RSVP interface using the hello-interval statement. This configuration disables RSVP interface hellos globally, but enables RSVP interface hellos on the specified interface (the RSVP interface you configure the **hello-interval** statement on). This configuration might be necessary in a heterogeneous network in which some devices support RSVP node ID hellos and other devices support RSVP interface hellos.

To disable RSVP interface hellos globally on the router, include the **no-interface-hello** statement:

```
no-interface-hello;
```

You can include this statement at the following hierarchy levels:

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

Configuring Hello Acknowledgments for Nonsession RSVP Neighbors

The **hello-acknowledgements** statement controls the hello acknowledgment behavior between RSVP neighbors regardless of whether or not they are in the same session.

Hello messages received from RSVP neighbors that are not part of a common RSVP session are discarded. If you configure the **hello-acknowledgements** statement at the **[edit protocols rsvp]** hierarchy level, hello messages from nonsession neighbors are

acknowledged with a hello acknowledgment message. When hellos are received from nonsession neighbors, an RSVP neighbor relationship is created and periodic hello messages can now be received from the nonsession neighbor. The **hello-acknowledgements** statement is disabled by default. Configuring this statement allows RSVP-capable routers to be discovered using hello packets and verifies that the interface is able to receive RSVP packets before sending any MPLS LSP setup messages.

Once you enable hello acknowledgments for nonsession RSVP neighbors, the router continues to acknowledge hello messages from any nonsession RSVP neighbors unless the interface itself goes down or you change the configuration. Interface-based neighbors are not automatically aged out.

```
hello-acknowledgements;
```

You can include this statement at the following hierarchy levels:

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

Configuring Node Protection or Link Protection for LSPs

When you configure node protection or link protection on a router, bypass LSPs are created to the next-hop or next-next-hop routers for the LSPs traversing the router. You must configure node protection or link protection for each LSP that you want protected. To extend protection along the entire path used by an LSP, you must configure protection on each router that the LSP traverses.

You can configure node protection or link protection for both static and dynamic LSPs.

To configure node protection on a router for a specified LSP, include the **node-link-protection** statement:

```
node-link-protection;
```

You can include this statement at the following hierarchy levels:

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

To configure link protection on a router for a specified LSP, include the link-protection statement:

```
link-protection;
```

You can include this statement at the following hierarchy levels:

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

NOTE: To complete the configuration of node or link protection, you must also configure link protection on all unidirectional RSVP interfaces that the LSPs traverse, as described in "Configuring Link Protection on Interfaces Used by LSPs" on page 32.

Switching LSPs Away from a Network Node

You can configure the router to switch active LSPs away from a network node using a bypass LSP enabled for an interface. This feature might be used to maintain active networks when a device needs to be replaced without interrupting traffic transiting the network. The LSPs can be either static or dynamic.

1. You first need to configure either link or node protection for the traffic that needs to pass around the network device you intend to disable. To function properly, the bypass LSP must use a different logical interface than the protected LSP.
2. To prepare the router to begin switching traffic away from a network node, configure the **always-mark-connection-protection-tlv** statement:

   always-mark-connection-protection-tlv;

   The router then marks all OAM traffic transiting this interface in preparation for switching the traffic to an alternate path based on the OAM functionality.

   You can configure this statement at the following hierarchy levels:

   - **[edit protocols mpls interface *interface-name*]**
   - **[edit logical-systems *logical-system-name* protocols mpls interface *interface-name*]**
3. You then need to configure the **switch-away-lsps** statement to switch the traffic from the protected LSP to the bypass LSP, effectively bypassing the default downstream network device. The actual link itself is not brought down by this configuration.

   To configure the router to switch traffic away from a network node, configure the **switch-away-lsps** statement:

   switch-away-lsps;

   You can configure this statement at the following hierarchy levels:

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

Note the following limitations related to switching active LSPs away from a network node:

- The switch-away feature is supported on MX Series routers only.
- The switch-away feature is not supported for switching traffic from primary point-to-multipoint LSPs to bypass point-to-multipoint LSPs. If you configure the **switch-away-lsps** statement for a point-to-multipoint LSP, traffic is not switched to the bypass point-to-multipoint LSP.

- If you configure the switch-away feature on an interface along the path of a dynamic LSP, new dynamic LSPs cannot be established over that path. The switch-away feature prevents the make-before-break behavior of RSVP-signaled LSPs. The make-before-break behavior normally causes the router to first attempt to re-signal a dynamic LSP before tearing down the original.

Related Documentation

- Configuring Node Protection or Link Protection for LSPs on page 30

Configuring Inter-AS Node and Link Protection

To interoperate with other vendors' equipment, the Junos OS supports the record route object (RRO) node ID subobject for use in inter-AS link and node protection configurations. The RRO node ID subobject is defined in RFC 4561, *Definition of a Record Route Object (RRO) Node-Id Sub-Object*. This functionality is enabled by default in Junos OS Release 9.4 and later.

If you have Juniper Networks routers running Junos OS Release 9.4 and later releases in the same MPLS-TE network as routers running Junos OS Release 8.4 and earlier releases, you might need to disable the RRO node ID subobject by configuring the **no-node-id-subobject** statement:

```
no-node-id-subobject;
```

You can include this statement at the following hierarchy levels:

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

Configuring Link Protection on Interfaces Used by LSPs

When you configure node protection or link protection on a router for LSPs as described in "Configuring Node Protection or Link Protection for LSPs" on page 30, you also must configure the **link-protection** statement on the RSVP interfaces used by the LSPs.

To configure link protection on the interfaces used by the LSPs, include the link-protection statement:

```
link-protection {
    disable;
    admin-group
        exclude group-names;
        include-all group-names;
        include-any group-names;
    }
    bandwidth bps;
    bypass bypass-name {
        bandwidth bps;
        description text;
        hop-limit number;
        no-cspf;
        path address <strict | loose>;
        priority setup-priority reservation-priority;
```

```
        to address;
    }
    class-of-service cos-value;
    hop-limit number;
    max-bypasses number;
    no-cspf;
    no-node-protection;
    optimize-timer seconds;
    path address <strict | loose>;
    priority setup-priority reservation-priority;
    subscription percent {
        ct0 percent;
        ct1 percent;
        ct2 percent;
        ct3 percent;
    }
}
```

You can include this statement at the following hierarchy levels:

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

All the statements under **link-protection** are optional.

The following sections describe how to configure link protection:

- Configuring Bypass LSPs on page 33
- Configuring Administrative Groups for Bypass LSPs on page 34
- Configuring the Bandwidth for Bypass LSPs on page 35
- Configuring Class of Service for Bypass LSPs on page 35
- Configuring the Hop Limit for Bypass LSPs on page 36
- Configuring the Maximum Number of Bypass LSPs on page 36
- Disabling CSPF for Bypass LSPs on page 37
- Disabling Node Protection for Bypass LSPs on page 37
- Configuring the Optimization Interval for Bypass LSPs on page 37
- Configuring an Explicit Path for Bypass LSPs on page 38
- Configuring the Amount of Bandwidth Subscribed for Bypass LSPs on page 39
- Configuring Priority and Preemption for Bypass LSPs on page 39

Configuring Bypass LSPs

You can configure specific bandwidth and path constraints for a bypass LSP. You can also individually configure each bypass LSP generated when you enable multiple bypass LSPs. If you do not configure the bypass LSPs individually, they all share the same path and bandwidth constraints (if any).

If you specify the **bandwidth**, **hop-limit**, and **path** statements for the bypass LSP, these values take precedence over the values configured at the **[edit protocols rsvp interface**

interface-name **link-protection]** hierarchy level. The other attributes (**subscription**, **no-node-protection**, and **optimize-timer**) are inherited from the general constraints.

To configure a bypass LSP, specify a name for the bypass LSP using the **bypass** statement. The name can be up to 64 characters in length.

```
bypass bypass-name {
  bandwidth bps;
  description text;
  class-of-service cos-value;
  hop-limit number;
  no-cspf;
  path address <strict | loose>;
  priority setup-priority reservation-priority;
  to address;
}
```

You can include this statement at the following hierarchy levels:

- **[edit protocols rsvp** interface *interface-name* **link-protection]**
- **[edit logical-systems** *logical-system-name* **protocols rsvp** interface *interface-name* **link-protection]**

Configuring the Next-Hop or Next-Next-Hop Node Address for Bypass LSPs

If you configure a bypass LSP, you must also configure the **to** statement. The **to** statement specifies the address for the interface of the immediate next-hop node (for link protection) or the next-next-hop node (for node-link protection). The address specified determines whether this is a link protection bypass or a node-link protection bypass. On multiaccess networks (for example, a LAN), this address is also used to specify which next-hop node is being protected.

Configuring Administrative Groups for Bypass LSPs

Administrative groups, also known as link coloring or resource class, are manually assigned attributes that describe the “color” of links, such that links with the same color conceptually belong to the same class. You can use administrative groups to implement a variety of policy-based LSP setups. You can configure administrative groups for bypass LSPs. For more information about configuring administrative groups, see Configuring Administrative Groups.

To configure administrative groups for bypass LSPs, include the **admin-group** statement:

```
admin-group {
  exclude group-names;
  include-all group-names;
  include-any group-names;
}
```

To configure an administrative group for all of the bypass LSPs, include the **admin-group** statement at the following hierarchy levels:

- **[edit protocols rsvp** interface *interface-name* **link-protection]**

- **[edit logical-systems *logical-system-name* protocols rsvp** interface ***interface-name*** **link-protection]**

To configure an administrative groups for a specific bypass LSP, include the **admin-group** statement at the following hierarchy levels:

- **[edit protocols rsvp** interface ***interface-name*** **link-protection** bypass ***bypass-name*****]**
- **[edit logical-systems *logical-system-name* protocols rsvp** interface ***interface-name*** **link-protection** bypass ***bypass-name*****]**

Configuring the Bandwidth for Bypass LSPs

You can specify the amount of bandwidth allocated for automatically generated bypass LSPs or you can individually specify the amount of bandwidth allocated for each LSP.

If you have enabled multiple bypass LSPs, this statement is required.

To specify the bandwidth allocation, include the **bandwidth** statement:

bandwidth *bps*;

For automatically generated bypass LSPs, include the **bandwidth** statement at the following hierarchy levels:

- **[edit protocols rsvp** interface ***interface-name*** **link-protection]**
- **[edit logical-systems *logical-system-name* protocols rsvp** interface ***interface-name*** **link-protection]**

For individually configured bypass LSPs, include the **bandwidth** statement at the following hierarchy levels:

- **[edit protocols rsvp** interface ***interface-name*** **link-protection** bypass ***bypass-name*****]**
- **[edit logical-systems *logical-system-name* protocols rsvp** interface ***interface-name*** **link-protection** bypass ***bypass-name*****]**

Configuring Class of Service for Bypass LSPs

You can specify the class-of-service value for bypass LSPs by including the **class-of-service** statement:

class-of-service *cos-value*;

To apply a class-of-service value to all the automatically generated bypass LSPs, include the **class-of-service** statement at the following hierarchy levels:

- **[edit protocols rsvp** interface ***interface-name*** **link-protection]**
- **[edit logical-systems *logical-system-name* protocols rsvp** interface ***interface-name*** **link-protection]**

To configure a class-of-service value for a specific bypass LSPs, include the **class-of-service** statement at the following hierarchy levels:

- **[edit protocols rsvp** interface *interface-name* **link-protection** bypass *bypass-name***]**
- **[edit logical-systems** *logical-system-name* **protocols rsvp** interface *interface-name* **link-protection** bypass *bypass-name***]**

Configuring the Hop Limit for Bypass LSPs

You can specify the maximum number of hops a bypass can traverse. By default, each bypass can traverse a maximum of 255 hops (the ingress and egress routers count as one hop each, so the minimum hop limit is two).

To configure the hop limit for bypass LSPs, include the **hop-limit** statement:

hop-limit *number*;

For automatically generated bypass LSPs, include the **hop-limit** statement at the following hierarchy levels:

- **[edit protocols rsvp** interface *interface-name* **link-protection]**
- **[edit logical-systems** *logical-system-name* **protocols rsvp** interface *interface-name* **link-protection]**

For individually configured bypass LSPs, include the **hop-limit** statement at the following hierarchy levels:

- **[edit protocols rsvp** interface *interface-name* **link-protection** bypass *bypass-name***]**
- **[edit logical-systems** *logical-system-name* **protocols rsvp** interface *interface-name* **link-protection** bypass *bypass-name***]**

Configuring the Maximum Number of Bypass LSPs

You can specify the maximum number of dynamic bypass LSPs permitted for protecting an interface using the **max-bypasses** statement at the **[edit protocols rsvp interface** *interface-name* **link-protection]** hierarchy level. When this statement is configured, multiple bypasses for link protection are enabled. Call admission control (CAC) is also enabled.

By default, this option is disabled and only one bypass is enabled for each interface. You can configure a value of between **0** through **99** for the **max-bypasses** statement. Configuring a value of **0** prevents the creation of any dynamic bypass LSPs for the interface. If you configure a value of **0** for the **max-bypasses** statement, you need to configure one or more static bypass LSPs to enable link protection on the interface.

If you configure the **max-bypasses** statement, you must also configure the **bandwidth** statement (discussed in "Configuring the Bandwidth for Bypass LSPs" on page 35).

To configure the maximum number of bypass LSPs for a protected interface, include the **max-bypasses** statement:

max-bypasses *number*;

You can include this statement at the following hierarchy levels:

- **[edit protocols rsvp** interface ***interface-name*** **link-protection]**
- **[edit logical-systems** ***logical-system-name*** **protocols rsvp** interface ***interface-name*** **link-protection]**

Disabling CSPF for Bypass LSPs

Under certain circumstances, you might need to disable CSPF computation for bypass LSPs and use the configured Explicit Route Object (ERO) if available. For example, a bypass LSP might need to traverse multiple OSPF areas or IS-IS levels, preventing the CSPF computation from working. To ensure that link and node protection function properly in this case, you have to disable CSPF computation for the bypass LSP.

You can disable CSPF computation for all bypass LSPs or for specific bypass LSPs.

To disable CSPF computation for bypass LSPs, include the **no-cspf** statement:

```
no-cspf;
```

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

Disabling Node Protection for Bypass LSPs

You can disable node protection on the RSVP interface. Link protection remains active. When this option is configured, the router can only initiate a next-hop bypass, not a next-next-hop bypass.

To disable node protection for bypass LSPs, include the **no-node-protection** statement:

```
no-node-protection;
```

You can include this statement at the following hierarchy levels:

- **[edit protocols rsvp** interface ***interface-name*** **link-protection]**
- **[edit logical-systems** ***logical-system-name*** **protocols rsvp** interface ***interface-name*** **link-protection]**

Configuring the Optimization Interval for Bypass LSPs

You can configure an optimization interval for bypass LSPs using the **optimize-timer** statement. At the end of this interval, an optimization process is initiated that attempts to either minimize the number of bypasses currently in use, minimize the total amount of bandwidth reserved for all of the bypasses, or both. You can configure an optimization interval from 1 through 65,535 seconds. A default value of 0 disables bypass LSP optimization.

When you configure the **optimize-timer** statement, bypass LSPs are reoptimized automatically when you configure or change the configuration of any of the following:

- Administrative group for a bypass LSP—The configuration for an administrative group has been changed on a link along the path used by the bypass LSP. Configure an administrative group using the **admin-group** statement at the **[edit protocols rsvp interface *interface-name* link-protection]** hierarchy level.
- Fate sharing group—The configuration for a fate sharing group has been changed. Configure a fate sharing group using the **group** statement at the **[edit routing-options fate-sharing]** hierarchy level.
- IS-IS overload—The configuration for IS-IS overload has been changed on a router along the path used by the bypass LSP. Configure IS-IS overload using the **overload** statement at the **[edit protocols isis]** hierarchy level.
- IGP metric—The IGP metric has been changed on a link along the path used by the bypass LSP.

To configure the optimization interval for bypass LSPs, include the **optimize-timer** statement:

optimize-timer *seconds*;

You can include this statement at the following hierarchy levels:

- **[edit protocols rsvp** interface *interface-name* **link-protection]**
- **[edit logical-systems *logical-system-name* protocols rsvp** interface *interface-name* **link-protection]**

Configuring an Explicit Path for Bypass LSPs

By default, when you establish a bypass LSP to an adjacent neighbor, CSPF is used to discover the least-cost path. The **path** statement allows you to configure an explicit path (a sequence of strict or loose routes), giving you control over where and how the bypass LSP is established. To configure an explicit path, include the **path** statement:

path *address* <strict | loose>;

For automatically generated bypass LSPs, include the **path** statement at the following hierarchy levels:

- **[edit protocols rsvp** interface *interface-name* **link-protection]**
- **[edit logical-systems *logical-system-name* protocols rsvp** interface *interface-name* **link-protection]**

For individually configured bypass LSPs, include the **path** statement at the following hierarchy levels:

- **[edit protocols rsvp** interface *interface-name* **link-protection** bypass *bypass-name***]**
- **[edit logical-systems *logical-system-name* protocols rsvp** interface *interface-name* **link-protection** bypass *bypass-name***]**

Configuring the Amount of Bandwidth Subscribed for Bypass LSPs

You can configure the amount of bandwidth subscribed to bypass LSPs. You can configure the bandwidth subscription for the whole bypass LSP or for each class type that might traverse the bypass LSP. You can configure any value between 1 percent and 65,535 percent. By configuring a value less than 100 percent, you are undersubscribing the bypass LSPs. By configuring a value greater than 100 percent, you are oversubscribing the bypass LSPs.

The ability to oversubscribe the bandwidth for the bypass LSPs makes it possible to more efficiently use network resources. You can configure the bandwidth for the bypass LSPs based on the average network load as opposed to the peak load.

To configure the amount of bandwidth subscribed for bypass LSPs, include the **subscription** statement:

```
subscription percentage {
    ct0 percentage;
    ct1 percentage;
    ct2 percentage;
    ct3 percentage;
}
```

You can include this statement at the following hierarchy levels:

- **[edit protocols rsvp** interface *interface-name* **link-protection]**
- **[edit logical-systems** *logical-system-name* **protocols rsvp** interface *interface-name* **link-protection]**

Configuring Priority and Preemption for Bypass LSPs

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

For more detailed information on configuring setup priority and reservation priority for LSPs, see Configuring Priority and Preemption for LSPs.

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

```
priority setup-priority reservation-priority;
```

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

Configuring RSVP Setup Protection

You can configure the facility-backup fast reroute mechanism to provide setup protection for LSPs which are in the process of being signaled. Both point-to-point LSPs and point-to-multipoint LSPs are supported. This feature is applicable in the following scenario:

1. A failed link or node is present on the strict explicit path of an LSP before the LSP is signaled.
2. There is also a bypass LSP protecting the link or node.
3. RSVP signals the LSP through the bypass LSP. The LSP appears as if it was originally set up along its primary path and then failed over to the bypass LSP because of the link or node failure.
4. When the link or node has recovered, the LSP can be automatically reverted to the primary path.

You should configure the **setup-protection** statement at the **[edit protocols rsvp]** on each of the routers along the LSP path on which you want to enable LSP setup protection. You should also configure IGP traffic engineering on all of the routers on the LSP path. You can issue a **show rsvp session** command to determine whether or not the LSP has setup protection enabled on a router acting as a point of local repair (PLR) or a merge point.

To enable RSVP setup protection, include the **setup-protection** statement

```
setup-protection;
```

You can include this statement at the following hierarchy levels:

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

Configuring RSVP Graceful Restart

The following RSVP graceful restart configurations are possible:

- Graceful restart and helper mode are both enabled (the default).
- Graceful restart is enabled but helper mode is disabled. A router configured in this way can restart gracefully, but cannot help a neighbor with its restart and recovery procedures.
- Graceful restart is disabled but helper mode is enabled. A router configured in this way cannot restart gracefully, but can help a restarting neighbor.
- Graceful restart and helper mode both are disabled. This configuration completely disables RSVP graceful restart (including restart and recovery procedures and helper mode). The router behaves like a router that does not support RSVP graceful restart.

NOTE: In order to turn on RSVP graceful restart, you must set the global graceful restart timer to at least 180 seconds.

The following sections describe how to configure RSVP graceful restart:

Enabling Graceful Restart for All Routing Protocols

To enable graceful restart for RSVP, you need to enable graceful restart for all the protocols that support graceful restart on the router. For more information about graceful restart, see the *Junos OS Routing Protocols Configuration Guide*.

To enable graceful restart on the router, include the **graceful-restart** statement:

```
graceful-restart;
```

You can include this statement at the following hierarchy levels:

- **[edit routing-options]**
- **[edit logical-systems *logical-system-name* routing-options]**

Disabling Graceful Restart for RSVP

By default, RSVP graceful restart and RSVP helper mode are enabled when you enable graceful restart. However, you can disable one or both of these capabilities.

To disable RSVP graceful restart and recovery, include the **disable** statement at the **[edit protocols rsvp graceful-restart]** hierarchy level:

```
disable;
```

Disabling RSVP Helper Mode

To disable RSVP helper mode, include the **helper-disable** statement at the **[edit protocols rsvp graceful-restart]** hierarchy level:

```
helper-disable;
```

Configuring the Maximum Helper Recovery Time

To configure the amount of time the router retains the state of its RSVP neighbors while they undergo a graceful restart, include the **maximum-helper-recovery-time** statement at the **[edit protocols rsvp graceful-restart]** hierarchy level. This value is applied to all neighboring routers, so it should be based on the time required by the slowest RSVP neighbor to recover.

```
maximum-helper-recovery-time seconds;
```

Configuring the Maximum Helper Restart Time

To configure the delay between when the router discovers that a neighboring router has gone down and when it declares the neighbor down, include the **maximum-helper-restart-time** statement at the **[edit protocols rsvp graceful-restart]** hierarchy level. This value is applied to all neighboring routers, so it should be based on the time required by the slowest RSVP neighbor to restart.

```
maximum-helper-restart-time seconds;
```

Configuring Load Balancing Across RSVP LSPs

By default, when you have configured several RSVP LSPs to the same egress router, the LSP with the lowest metric is selected and carries all traffic. If all of the LSPs have the same metric, one of the LSPs is selected at random and all traffic is forwarded over it.

Alternatively, you can load-balance traffic across all of the LSPs by enabling per-packet load balancing.

To enable per-packet load balancing on an ingress LSP, configure the **policy-statement** statement as follows:

```
[edit policy-options]
policy-statement policy-name {
  then {
    load-balance per-packet;
  }
  accept;
}
```

You then need to apply this statement as an export policy to the forwarding table. For more information on how to configure the **policy-statement** statement, see the *Junos OS Policy Framework Configuration Guide*.

Once per-packet load balancing is applied, traffic is distributed equally between the LSPs (by default).

You need to configure per-packet load balancing if you want to enable PFE fast reroute. To enable PFE fast reroute, include the **policy-statement** statement for per-packet load balancing shown in this section in the configuration of each of the routers where a reroute might take place. See also Configuring Fast Reroute.

You can also load-balance the traffic between the LSPs in proportion to the amount of bandwidth configured for each LSP. This capability can better distribute traffic in networks with asymmetric bandwidth capabilities across external links, since the configured bandwidth of an LSP typically reflects the traffic capacity of that LSP.

To configure RSVP LSP load balancing, include the **load-balance** statement with the **bandwidth** option:

```
load-balance {
  bandwidth;
}
```

You can configure this statement at the following hierarchy levels:

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

Keep the following information in mind when you use the **load-balance** statement:

- If you configure the **load-balance** statement, the behavior of currently running LSPs is not altered. To force currently running LSPs to use the new behavior, you can issue a **clear mpls lsp** command.
- The **load-balance** statement only applies to ingress LSPs that have per-packet load balancing enabled.
- For Differentiated Services–aware traffic engineered LSPs, the bandwidth of an LSP is calculated by summing the bandwidth of all of the class types.

Configuring RSVP Automatic Mesh

BGP and MPLS VPNs are based on a peer model. To add a new site to an existing VPN, you need to configure the CE router at the new site and the PE router connected to the CE router. You do not have to modify the configuration of all of the other PE routers participating in the VPN. The PE routers automatically learn about the routes associated with the new site (a process called automatic discovery).

The requirements are a bit different if you need to add a new PE router (as opposed to a CE router) to the network. A BGP and MPLS VPN requires that the BGP session be fully meshed and that there also be a full mesh of PE router-to-PE router MPLS LSPs between all of the PE routers in the network. When you add a new PE router to the network, all of the existing PE routers must be reconfigured to peer with the new PE router. Much of the configuration effort can be reduced if you configure BGP route reflectors (mitigating the full mesh requirement for BGP) and if you configure LDP as the signaling protocol for MPLS.

However, if you need to add a new PE router to a network configured with a full mesh of RSVP-signaled LSPs, you need to reconfigure each of the PE routers to have a peer relationship with the new PE router. You can configure RSVP automatic mesh to address this particular operational scenario. When you enable RSVP automatic mesh, RSVP LSPs are dynamically created between a new PE router and the existing PE routers, eliminating the need to reconfigure all of the PE routers manually. For dynamic tunnel creation to function properly, BGP must be configured to exchange routes between all of the participating PE routers. If two BGP peers did not exchange routes, it would not be possible to configure a dynamic tunnel between them.

RSVP includes numerous capabilities that are not available in LDP, including fast reroute. RSVP automatic mesh helps to reduce the operation and maintenance requirements for RSVP, making it possible to deploy RSVP in larger and more complicated networks.

Every PE router can reach every other PE router in the network because this information is distributed by the IGP. A PE router can set up an RSVP LSP to any other PE router in the network so long as it knows that such an LSP is required. To build a full mesh of LSPs

between the PE routers requires that each PE router know which of the other PE routers make up the full mesh.

You can configure RSVP to establish LSPs automatically for any new PE router added to a full mesh of LSPs. To enable this feature, you must configure the **rsvp-te** statement on all of the PE routers in the full mesh.

NOTE: You cannot configure RSVP automatic mesh in conjunction with CCC. CCC cannot use the dynamically generated tunnels.

To configure RSVP automatic mesh, include the **rsvp-te** statement:

```
rsvp-te {
   destination-networks network-prefix;
   label-switched-path-template {
      default-template;
      template-name;
   }
}
```

You can configure these statements at the following hierarchy levels:

- **[edit routing-options dynamic-tunnels *tunnel-name*]**
- **[edit logical-systems *logical-system-name* routing-options dynamic-tunnels *tunnel-name*]**

You can configure the following optional statements for RSVP automatic mesh:

- **destination-networks**—Specify the IP version 4 (IPv4) prefix range for the destination network. Dynamic tunnels within the specified IPv4 prefix range are allowed to be initiated.
- **label-switched-path-template**—You can configure either the default template explicitly using the **default-template** option or you can configure an LSP template of your own using the ***template-name*** option. The LSP template acts as a model configuration for all of the dynamically generated LSPs.

Configuring Timers for RSVP Refresh Messages

RSVP uses two related timing parameters:

- **refresh-time**—The refresh time controls the interval between the generation of successive refresh messages. The default value for the refresh time is 45 seconds. This number is derived from the **refresh-time** statement's default value of 30, multiplied by a fixed value of 1.5. This computation differs from RFC 2205, which states that the refresh time should be multiplied by a random value in the range from 0.5 through 1.5.

  Refresh messages include path and Resv messages. Refresh messages are sent periodically so that reservation states in neighboring nodes do not time out. Each path and Resv message carries the refresh timer value, and the receiving node extracts this value from the messages.

- **keep-multiplier**—The keep multiplier is a small, locally configured integer from 1 through 255. The default value is 3. It indicates the number of messages that can be lost before a particular state is declared stale and must be deleted. The keep multiplier directly affects the lifetime of an RSVP state.

To determine the lifetime of a reservation state, use the following formula:

lifetime = (*keep-multiplier* + 0.5) x (1.5 x *refresh-time*)

In the worst case, **(*keep-multiplier* – 1)** successive refresh messages must be lost before a reservation state is deleted.

We do not recommend configuring a short RSVP hello timer. If quick discovery of a failed neighbor is needed, configure short IGP (OSPF or IS-IS) hello timers.

By default, the refresh timer value is 30 seconds. To modify this value, include the **refresh-time** statement:

```
refresh-time seconds;
```

You can include this statement at the following hierarchy levels:

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

The default value of the keep multiplier is 3. To modify this value, include the **keep-multiplier** statement:

```
keep-multiplier number;
```

You can include this statement at the following hierarchy levels:

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

Preempting RSVP Sessions

Whenever bandwidth is insufficient to handle all RSVP sessions, you can control the preemption of RSVP sessions. By default, an RSVP session is preempted only by a new higher-priority session.

To always preempt a session when the bandwidth is insufficient, include the **preemption** statement with the **aggressive** option:

```
preemption aggressive;
```

You can include this statement at the following hierarchy levels:

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

To disable RSVP session preemption, include the **preemption** statement with the **disabled** option:

```
preemption disabled;
```

To return to the default (that is, preempt a session only for a new higher-priority session), include the **preemption** statement with the **normal** option:

```
preemption normal;
```

You can include this statement at the following hierarchy levels:

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

Configuring MTU Signaling in RSVP

To configure maximum transmission unit (MTU) signaling in RSVP, you need to configure MPLS to allow IP packets to be fragmented before they are encapsulated in MPLS. You also need to configure MTU signaling in RSVP. For troubleshooting purposes, you can configure MTU signaling alone without enabling packet fragmentation.

To configure MTU signaling in RSVP, include the **path-mtu** statement:

```
path-mtu {
  allow-fragmentation;
  rsvp {
    mtu-signaling;
  }
}
```

You can include this statement at the following hierarchy levels:

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

The following sections describe how to enable packet fragmentation and MTU signaling in RSVP:

- Enabling MTU Signaling in RSVP on page 46
- Enabling Packet Fragmentation on page 47

Enabling MTU Signaling in RSVP

To enable MTU signaling in RSVP, include the **rsvp mtu-signaling** statement:

```
rsvp mtu-signaling;
```

You can include this statement at the following hierarchy levels:

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

Once you have committed the configuration, changes in the MTU signaling behavior for RSVP take effect the next time the path is refreshed.

You can configure the **mtu-signaling** statement by itself at the **[edit protocols mpls path-mtu rsvp]** hierarchy level. This can be useful for troubleshooting. If you configure just the **mtu-signaling** statement, you can use the **show rsvp session detail** command to determine what the smallest MTU is on an LSP. The **show rsvp session detail** command displays the MTU value received and sent in the Adspec object.

Enabling Packet Fragmentation

To allow IP packets to be fragmented before they are encapsulated in MPLS, include the **allow-fragmentation** statement:

```
allow-fragmentation;
```

You can include this statement at the following hierarchy levels:

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

NOTE: Do not configure the **allow-fragmentation** statement alone. Always configure it in conjunction with the **mtu-signaling** statement.

Configuring RSVP to Pop the Label on the Ultimate-Hop Router

You can control the label value advertised on the egress router of an LSP. The default advertised label is label 3 (Implicit Null label). If label 3 is advertised, the penultimate-hop router removes the label and sends the packet to the egress router. When ultimate-hop popping is enabled, label 0 (IP version 4 [IPv4] Explicit Null label) is advertised. Ultimate-hop popping ensures that any packets traversing an MPLS network include a label.

To configure ultimate-hop popping for RSVP, include the **explicit-null** statement:

```
explicit-null;
```

You can include this statement at the following hierarchy levels:

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

NOTE: Juniper Networks routers queue packets based on the incoming label. Routers from other vendors might queue packets differently. Keep this in mind when working with networks containing routers from multiple vendors.

For more information about labels, see Label Description and Label Allocation.

Disabling Adjacency Down and Neighbor Down Notification in IS-IS and OSPF

Whenever IS-IS is deactivated, the IS-IS adjacencies are brought down. IS-IS signals to RSVP to bring down any RSVP neighbors associated with the IS-IS adjacencies, and this further causes the associated LSPs signaled by RSVP to go down as well.

A similar process occurs whenever OSPF is deactivated. The OSPF neighbors are brought down. OSPF signals to RSVP to bring down any of the RSVP neighbors associated with the OSPF neighbors, and this further causes the associated LSPs signaled by RSVP to go down as well.

If you need to migrate from IS-IS to OSPF or from OSPF to IS-IS, the IGP notification to RSVP for an adjacency or neighbor down event needs to be ignored. Using the **no-adjacency-down-notification** or **no-neighbor-down-notification** statements, you can disable IS-IS adjacency down notification or OSPF neighbor down notification, respectively, until the migration is complete. The network administrator is responsible for configuring the statements before the migration, and then removing them from the configuration afterward, so that IGP notification can function normally.

To disable adjacency down notification in IS-IS, include the **no-adjacency-down-notification** statement:

```
no-adjacency-down-notification;
```

You can include this statement at the following hierarchy levels:

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

To disable neighbor down notification in OSPF, include the **no-neighbor-down-notification** statement:

```
no-neighbor-down-notification;
```

You can include this statement at the following hierarchy levels:

- **[edit protocols ospf area *area-id* interface *interface-name*]**
- **[edit logical-systems *logical-system-name* protocols ospf area *area-id* interface *interface-name*]**

Enabling Ultimate-Hop Popping on Point-to-Multipoint LSPs

By default, for both point-to-point and point-to-multipoint LSPs, penultimate-hop popping is used for MPLS traffic. MPLS labels are removed from packets on the router just before the egress router of the LSP. The plain IP packets are then forwarded to the egress router. For ultimate-hop popping, the egress router is responsible for both removing the MPLS label and processing the plain IP packet.

It can be beneficial to enable ultimate-hop popping on point-to-multipoint LSPs, particularly when transit traffic is traversing the same egress device. If you enable

ultimate-hop popping, a single copy of traffic can be sent over the incoming link, saving significant bandwidth. By default, ultimate-hop popping is disabled.

You enable ultimate-hop popping for point-to-multipoint LSPs by configuring the **tunnel-services** statement. When you enable ultimate-hop popping, the Junos OS selects one of the available virtual loopback tunnel (VT) interfaces to loop back the packets to the PFE for IP forwarding. By default, the VT interface selection process is performed automatically. Bandwidth admission control is used to limit the number of LSPs that can be used on one VT interface. Once all the bandwidth is consumed on one interface, the Junos OS selects another VT interface with sufficient bandwidth for admission control.

If an LSP requires more bandwidth than is available from any of the VT interfaces, ultimate-hop popping cannot be enabled and penultimate-hop popping is enabled instead.

You can explicitly configure which VT interfaces handle the RSVP traffic by including the **devices** option for the **tunnel-services** statement. The **devices** option allows you to specify which VT interfaces are to be used by RSVP. If you do not configure this option, all of the VT interfaces available to the router can be used.

For ultimate-hop popping on point-to-multipoint LSPs to function properly, the egress router must have a PIC that provides tunnel services, such as the tunnel services PIC or the adaptive services PIC. Tunnel services are needed for popping the final MPLS label and for returning packets for IP address lookups.

If you configure the **tunnel-services** statement on an operating router, only the behavior of newly signaled LSPs changes. Existing LSPs are not affected. To force all existing LSPs to use ultimate-hop popping, issue a **clear mpls lsp** command. Note that this causes all of the MPLS LSPs on the router to be signaled again.

To enable ultimate-hop popping for the egress point-to-multipoint LSPs on a router, configure the **tunnel-services** statement:

```
tunnel-services {
  devices device-names;
}
```

You can configure this statement at the **[edit protocols rsvp]** hierarchy level.

To enable ultimate-hop popping for egress point-to-multipoint LSPs, you must also configure the **interface** statement with the **all** option:

```
interface all;
```

You must configure this statement at the **[edit protocols rsvp]** hierarchy level.

Tracing RSVP Protocol Traffic

To trace RSVP protocol traffic, include the **traceoptions** statement:

```
traceoptions {
  file filename <files number> <size size> <world-readable | no-world-readable>;
  flag flag <flag-modifier> <disable>;
}
```

You can include this statement at the following hierarchy levels:

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

You can specify the following RSVP-specific flags in the RSVP **traceoptions** statement:

Use the **file** statement to specify the name of the file that receives the output of the tracing operation. All files are placed in the directory **/var/log**. We recommend that you place RSVP tracing output in the file **rsvp-log**.

- **all**—All tracing operations.
- **error**—All detected error conditions
- **event**—RSVP-related events (helps to trace events related to RSVP graceful restart)
- **lmp**—RSVP-Link Management Protocol (LMP) interactions
- **packets**—All RSVP packets
- **path**—All path messages
- **pathtear**—PathTear messages
- **resv**—Resv messages
- **resvtear**—ResvTear messages
- **route**—Routing information
- **state**—Session state transitions

For general information about tracing and global tracing options, see the *Junos OS Routing Protocols Configuration Guide*.

Examples: Tracing RSVP Protocol Traffic

Trace RSVP path messages in detail:

```
[edit]
protocols {
   rsvp {
      traceoptions {
         file rsvp size 10m files 5;
         flag path;
      }
   }
}
```

Trace all RSVP messages:

```
[edit]
protocols {
   rsvp {
      traceoptions {
         file rsvp size 10m files 5;
         flag packets;
```

```
    }
  }
}
```

Trace all RSVP error conditions:

```
[edit]
protocols {
  rsvp {
    traceoptions {
      file rsvp size 10m files 5;
      flag error;
    }
  }
}
```

PART 3

Administration

CHAPTER 3

RSVP Standards and Terminology

Supported RSVP Standards

The Junos OS substantially supports the following RFCs and Internet drafts, which define standards for RSVP.

- RFC 2205, *Resource ReSerVation* [sic] *Protocol (RSVP)—Version 1 Functional Specification*
- RFC 2210, *The Use of RSVP with IETF Integrated Services*
- RFC 2211, *Specification of the Controlled-Load Network Element Service*
- RFC 2212, *Specification of Guaranteed Quality of Service*
- RFC 2215, *General Characterization Parameters for Integrated Service Network Elements*
- RFC 2745, *RSVP Diagnostic Messages*
- RFC 2747, *RSVP Cryptographic Authentication* (updated by RFC 3097)
- RFC 2961, *RSVP Refresh Overhead Reduction Extensions*
- RFC 3097, *RSVP Cryptographic Authentication—Updated Message Type Value*
- RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels*

  The Null Service Object for maximum transmission unit (MTU) signaling in RSVP is not supported.
- RFC 3473, *Generalized Multi-Protocol* [sic] *Label Switching (GMPLS) Signaling Resource ReserVation* [sic] *Protocol-Traffic Engineering (RSVP-TE) Extensions*

  Only Section 9, “Fault Handling,” is supported.
- RFC 3477, *Signalling Unnumbered Links in Resource ReSerVation* [sic] *Protocol - Traffic Engineering (RSVP-TE)*
- RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*

  Node protection in facility backup is not supported.

- RFC 4203, *OSPF Extensions in Support of Generalized Multi-Protocol* [sic] *Label Switching (GMPLS)*

  (OSPF extensions can carry traffic engineering information over unnumbered links.)

- RFC 4558, *Node-ID Based Resource Reservation Protocol (RSVP) Hello: A Clarification Statement*
- RFC 4561, *Definition of a Record Route Object (RRO) Node-Id Sub-Object*

  The RRO node ID subobject is for use in inter-AS link and node protection configurations.

- Internet draft draft-ietf-mpls-rsvp-te-p2mp-01.txt, *Extensions to RSVP-TE for Point to Multipoint TE LSPs* (expires June 2005)

The following RFCs do not define standards, but provide information about RSVP and related technologies. The IETF classifies them variously as "Experimental" or "Informational."

- RFC 2209, *Resource ReSerVation* [sic] *Protocol (RSVP)—Version 1 Message Processing Rules*
- RFC 2216, *Network Element Service Specification Template*
- RFC 4125, *Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*
- RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*

Related Documentation

- Supported GMPLS Standards
- Supported LDP Standards
- Supported MPLS Standards
- Accessing Standards Documents on the Internet

RSVP Graceful Restart Standard

RSVP graceful restart is described in RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions* (only Section 9, "Fault Handling").

RSVP Graceful Restart Terminology

R

Recovery time (in milliseconds)

Applies only when the control channel is up (the hello exchange is complete) before the restart time. Applies only to nodal faults.

When a graceful restart is in progress, the time left to complete a recovery is advertised. At other times, this value is zero. The maximum advertised recovery time is 2 minutes (120,000 milliseconds).

During the recovery time, a restarting node attempts to recover its lost states with assistance from its neighbors. The neighbor of the restarting node must send the path messages with the recovery labels to the restarting node within a period of one-half the recovery time. The restarting node considers its graceful restart complete after its advertised recovery time.

Restart time (in milliseconds)

The default value is 60,000 milliseconds (1 minute). The restart time is advertised in the hello message. The time indicates how long a neighbor should wait to receive a hello message from a restarting router before declaring that router dead and purging states.

The Junos OS can override a neighbor's advertised restart time if the time is greater than one-third the local restart time. For example, given the default restart time of 60 seconds, a router would wait 20 seconds or less to receive a hello message from a restarting neighbor. If the restart time is zero, the restarting neighbor can immediately be declared dead.

CHAPTER 4

Summary of RSVP Configuration Statements

admin-group

Syntax

```
admin-group {
  exclude [ group-names ];
  include-all [ group-names ];
  include-any [ group-names ];
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection bypass *bypass-name*],
[edit protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]

Release Information

Statement introduced in Junos OS Release 9.2.

Description

Enable you to configure administrative groups for bypass label-switched paths (LSPs). You can configure administrative groups either globally for all bypass LSPs traversing an interface or for just a specific bypass LSP.

Options

exclude *group-names*—Specify the administrative groups to exclude for a bypass LSP.

include-all *group-names*—Specify the administrative groups whose links the bypass LSP must traverse.

include-any *group-names*—Specify the administrative groups whose links the bypass LSP can traverse.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Administrative Groups for Bypass LSPs on page 34

aggregate

Syntax (aggregate | no-aggregate);

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*],
[edit logical-systems *logical-system-name* protocols rsvp peer-interface *peer-interface-name*],
[edit protocols rsvp interface *interface-name*],
[edit protocols rsvp peer-interface *peer-interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Control the use of RSVP aggregate messages on an interface or peer interface:

- **aggregate**—Use RSVP aggregate messages.
- **no-aggregate**—Do not use RSVP aggregate messages.

  Aggregate messages can pack multiple RSVP messages into a single transmission, thereby reducing network overhead and enhancing efficiency. The number of supportable sessions and processing overhead are significantly improved when aggregation is enabled.

  Not all routers connected to a subnet need to support aggregation simultaneously. Each RSVP router negotiates its intention to use aggregate messages on a per-neighbor basis. Only when both routers agree are aggregate messages sent.

Default Aggregation is disabled.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring RSVP Refresh Reduction on page 23

authentication-key

Syntax authentication-key *key*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*],
[edit logical-systems *logical-system-name* protocols rsvp peer-interface *peer-interface-name*],
[edit protocols rsvp interface *interface-name*],
[edit protocols rsvp peer-interface *peer-interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Authentication key (password). Neighboring routers use the password to verify the authenticity of packets sent from this interface or peer interface.

RSVP uses HMAC-MD5 authentication, which is defined in RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*.

All routers that are connected to the same IP subnet must use the same authentication scheme and password.

Options ***key***—Authentication password. It can be 1 through 16 contiguous digits or letters. Separate decimal digits with periods. Separate hexadecimal digits with periods and precede the string with 0x. If you include spaces in the password, enclose the entire password in quotation marks (" ").

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring RSVP Authentication on page 26

bandwidth

Syntax bandwidth *bps*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection bypass *bypass-name*],
[edit protocols rsvp interface *interface-name*],
[edit protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description For certain logical interfaces (such as Asynchronous Transfer Mode [ATM], Permanent Virtual Circuit [PVC], or Frame Relay), you cannot determine the correct bandwidth from the hardware. This statement enables you to specify the actual available bandwidth.

This statement also enables you to specify the bandwidth for a bypass label switched path (LSP). If you have configured multiple bypasses, this statement is mandatory and is applied to all of the bypass LSPs.

Default The hardware raw bandwidth is used.

Options *bps*—Bandwidth in bits per second. You can specify this as an integer value. If you do so, count your zeros carefully, or you can use the abbreviations **k** (for a thousand), **m** (for a million), or **g** (for a billion [also called a thousand million]).

Range: Any positive integer

Default: 0 (no bandwidth is reserved)

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring the Bandwidth for Bypass LSPs on page 35
- Configuring Link Protection on Interfaces Used by LSPs on page 32
- Configuring Bypass LSPs on page 33

bypass (Signaled LSP)

Syntax

```
bypass bypass-name {
  bandwidth bps;
  description text;
  hop-limit number;
  no-cspf;
  path address <strict | loose>;
  priority setup-priority reservation-priority;
  to address;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp interface *interface-name* link-protection]

Release Information

Statement introduced before Junos OS Release 7.4.
The **description** option was added in Junos OS Release 10.4.

Description

Enables you to configure specific bandwidth and path constraints for a bypass LSP. It is possible to individually configure multiple bypass LSPs. If you do not configure the bypass LSPs individually, they all share the same path and bandwidth constraints.

If you specify the **bandwidth**, **hop-limit**, and **path** statements for the bypass LSP, these values take precedence over the values configured at the **[edit protocols rsvp interface *interface-name* link-protection]** hierarchy level. The other attributes (**subscription**, **no-node-protection**, and **optimize-timer**) are inherited from the general constraints.

Options

bypass-name—(Required) Specify a name for the bypass LSP. The name can be up to 64 characters.

description—Provides a textual description of the bypass LSP. Enclose any descriptive text that includes spaces in quotation marks (" "). Any descriptive text you include is displayed in the output of the **show mpls lsp bypass detail** command and has no effect on the operation of the bypass LSP. The description text can be no more than 80 characters in length.

to *address*—(Required) Specify the address for the interface of the immediate next-hop node (for link protection) or the next-next-hop node (for node-link protection). The address specified determines whether this is a link protection bypass or a node-link protection bypass. On multiaccess networks (for example, a LAN), this address is also used to specify which next-hop node is being protected.

The remaining statements are explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Bypass LSPs on page 33

bypass (Static LSP)

Syntax

```
bypass bypass-name {
  bandwidth bps;
  description string;
  next-hop (address | interface-name | address/interface-name);
  push out-label;
  to address;
}
```

Hierarchy Level

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

Release Information

Statement introduced before Junos OS Release 10.1.

Description

Configure specific bandwidth and path constraints for a bypass ingress LSP. It is possible to configure multiple bypass LSPs individually. If you do not, they all share the same path and bandwidth constraints.

The remaining statements are explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Static LSPs

class-of-service

Syntax class-of-service *cos-value*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection bypass *bypass-name*],
[edit protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Class-of-service (CoS) value given to all packets in the bypass LSP. You can specify a single CoS value for all the bypass LSPs traversing an interface. You can also configure CoS values for specific bypass LSPs traversing an interface.

The CoS value might affect the scheduling or queuing algorithm of traffic traveling along an LSP.

Options ***cos-value***—CoS value. A higher value typically corresponds to a higher level of service.

Range: 0 through 7

Default: If you do not specify a CoS value, the IP precedence bits from the packet's IP header are used as the packet's CoS value.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring Class of Service for Bypass LSPs on page 35

disable

Syntax disable;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols rsvp],
[edit logical-systems *logical-system-name* protocols rsvp graceful-restart],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit logical-systems *logical-system-name* protocols rsvp peer-interface *peer-interface-name*],
[edit protocols rsvp],
[edit protocols rsvp graceful-restart],
[edit protocols rsvp interface *interface-name*],
[edit protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp peer-interface *peer-interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Explicitly disable RSVP or RSVP graceful restart. Explicitly disable link protection on the specified interface.

Default RSVP is enabled on interfaces and peer interfaces configured with the RSVP **interface** statement. RSVP graceful restart is enabled on the router. Link protection is disabled.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Minimum RSVP Configuration on page 21
- Configuring RSVP Graceful Restart on page 40
- Configuring Link Protection on Interfaces Used by LSPs on page 32

fast-reroute

Syntax fast-reroute optimize-timer *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement added in Junos OS Release 7.5.

Description Configure the optimize timer for fast reroute. The optimize timer triggers a periodic optimization process that recomputes the fast reroute detour LSPs to use network resources more efficiently.

Options ***seconds***—Specify the number of seconds between fast reroute detour LSP optimizations.

Range: 0 through 65,535 seconds

Default: 0 (disabled)

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring the Optimization Interval for Fast Reroute Paths

graceful-deletion-timeout

Syntax graceful-deletion-timeout *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the time, in seconds, before completing graceful deletion of signaling.

Options ***seconds***—Time before completing graceful deletion of signaling.

Range: 1 through 300 seconds

Default: 30 seconds

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Gracefully Tearing Down GMPLS LSPs

graceful-restart

Syntax

```
graceful-restart {
  disable;
  helper-disable;
  maximum-helper-recovery-time seconds;
  maximum-helper-restart-time seconds;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* routing-options],
[edit protocols rsvp],
[edit routing-options]

Release Information Statement introduced before Junos OS Release 7.4.

Description Enable graceful restart on the router. You must configure the **graceful-restart** statement at the **[edit routing-options]** hierarchy level to enable graceful restart on the router.

Options

disable—Disable graceful restart on the router or for RSVP.

helper-disable—Disable RSVP graceful restart helper mode (this option is only available at the **[edit protocols rsvp]** hierarchy level).

Default: Helper mode is enabled by default.

maximum-helper-recovery-time *seconds*—The maximum length of time the router stores the state of neighboring routers when they undergo a graceful restart. The value applies to all neighboring routers, so it should be based on the time that the slowest RSVP neighbor requires for restart.

Default: 180 seconds

Range: 1 through 3600 seconds

maximum-helper-restart-time *seconds*—The maximum length of time the router waits between when it discovers that a neighboring router has gone down and when it declares the neighbor down. This value is applied to all neighboring routers, so it should be based on the time that the slowest RSVP neighbor requires for restart.

Default: 20 seconds

Range: 1 through 1800 seconds

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring RSVP Graceful Restart on page 40

hello-acknowledgements

Syntax hello-acknowledgements;

Hierarchy Level [edit logical-systems *logical-systems-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement introduced in Junos OS Release 10.2.

Description Enable hello messages from nonsession neighbors to be acknowledged with a hello acknowledgment message. Once hello acknowledgments are enabled, the router continues to acknowledge hello messages from any nonsession RSVP neighbors unless the interface itself goes down or the configuration is changed by an administrator.

Default Hello acknowledgments are disabled.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring Hello Acknowledgments for Nonsession RSVP Neighbors on page 29

hello-interval

Syntax hello-interval *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*],
[edit logical-systems *logical-system-name* protocols rsvp peer-interface *peer-interface-name*],
[edit protocols rsvp interface *interface-name*],
[edit protocols rsvp peer-interface *peer-interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Enable the sending of hello packets on the interface.

Options ***seconds***—Length of time between hello packets. A value of 0 disables the sending of hello packets on the interface.

Range: 1 through 60 seconds

Default: 9 seconds

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring the RSVP Hello Interval on page 26

hop-limit

Syntax hop-limit *number*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection bypass *bypass-name*],
[edit protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the maximum number of hops a bypass can traverse. By default, each bypass can traverse a maximum of 255 hops, including the ingress and egress routers.

Options *number*—Maximum number of hops a bypass can traverse.

Range: 2 through 255 hops

Default: 255 hops

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring the Hop Limit for Bypass LSPs on page 36

interface

Syntax

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

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement introduced before Junos OS Release 7.4.

Description Enable RSVP on one or more router interfaces.

Default RSVP is disabled on all interfaces.

Options ***interface-name***—Name of an interface. To configure all interfaces, specify **all**. For details about specifying interfaces, see the *Junos OS Network Interfaces Configuration Guide*.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Minimum RSVP Configuration on page 21

keep-multiplier

Syntax keep-multiplier *number*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement introduced before Junos OS Release 7.4.

Description Set the keep multiplier value.

Options ***number***—Multiplier value.

Range: 1 through 255

Default: 3

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring Timers for RSVP Refresh Messages on page 44

link-protection (RSVP)

Syntax

```
link-protection {
  disable;
  admin-group {
    exclude [ group-names ];
    include-all [ group-names ];
    include-any [ group-names ];
  }
  bandwidth bps;
  bypass bypass-name {
    bandwidth bps {
      ct0 bps;
      ct1 bps;
      ct2 bps;
      ct3 bps;
    }
    description text;
    class-of-service cos-value;
    hop-limit number;
    no-cspf;
    path address <strict | loose>;
    priority setup-priority reservation-priority;
    to address;
  }
  class-of-service cos-value;
  hop-limit number;
  max-bypasses number;
  no-cspf;
  no-node-protection;
  optimize-timer seconds;
  path address <strict | loose>;
  priority setup-priority reservation-priority;
  subscription percentage;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*], [edit protocols rsvp interface *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Enable link protection on the specified interface. Using link protection, you can configure a network to reroute traffic quickly around broken links. To fully enable link protection, you also need to configure the **link-protection** statement at the **[edit protocols mpls label-switched-path *lsp-name*]** hierarchy level. You can configure single or multiple bypasses for protected interface.

Default Link protection is disabled.

Options **no-node-protection**—Disable node-link protection on the RSVP interface. Link protection remains active. When this option is configured, the router can only initiate a next-hop bypass, not a next-next-hop bypass.

The remaining statements are explained separately.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring Link Protection on Interfaces Used by LSPs on page 32
- link-protection (Dynamic LSPs)

load-balance

Syntax
```
load-balance {
  bandwidth;
}
```

Hierarchy Level
[edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Load-balance traffic between RSVP LSPs.

Options
bandwidth—Load-balance traffic between RSVP LSPs based on the bandwidth configured for each LSP.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring Load Balancing Across RSVP LSPs on page 42

max-bypasses

Syntax max-bypasses *number*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*], [edit protocols rsvp interface *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Range modified in Junos OS Release 9.3.

Description Specify the maximum number of dynamic bypass LSPs permitted for protecting this interface. When this option is configured, multiple bypasses for link protection are enabled. Call admission control (CAC) is also enabled. The limit on bypasses configured applies only to dynamically generated bypass LSPs. By default, this option is disabled and only one dynamic bypass LSP is enabled for each interface. If you configure **max-bypasses**, you must also configure the **bandwidth** statement.

Options *number*—Configure the maximum number of bypass LSPs. If you configure a value of 0, no dynamic bypass LSPs are allowed to be established for the interface. Only static bypass LSPs can be configured.

Range: 0 through 99

Default: 1

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring the Maximum Number of Bypass LSPs on page 36

no-local-reversion

Syntax no-local-reversion;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement introduced in Junos OS Release 10.4.

Description Disables RSVP local revertive mode as specified in RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*. RSVP local revertive mode is supported on all Juniper Networks routers running the Junos OS. It is the default behavior. If you include this statement, the Juniper Networks router uses global revertive mode instead. You might need to disable RSVP local revertive mode on Juniper Networks routers if your network includes equipment that does not support this mode.

The following information can also be found in RFC 4090. Refer to the full RFC for additional information. When an LSP fails, the connection can be repaired locally using a traffic protection mechanism such as fast reroute. To restore the LSP to a full working path, RFC 4090 specifies the following strategies:

- Local revertive mode—Upon detecting that the path is restored, the point of local repair (PLR) resignals each of the LSPs that were formerly routed over the restored path. Every LSP successfully resignaled along the restored path is switched back.
- Global revertive mode—The ingress router of each tunnel is responsible for reoptimizing the LSPs that used the failed path. There are several potential reoptimization triggers: RSVP error messages, inspection of OSPF LSAs or IS-IS LSPs, and timers. This re-optimization process can proceed as soon as the failure is detected. It is not tied to the restoration of the failed path.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

node-hello

Syntax node-hello;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement introduced in JUNOS Release 10.0.

Description Enables node-ID based RSVP hellos globally on all of the RSVP interfaces on the router to allow Juniper Networks routers to interoperate with the equipment of other vendors. By default, the JUNOS Software uses interface-based RSVP hellos and node-ID based RSVP hellos are disabled. If you have not enabled RSVP node IDs on the router, the JUNOS software does not accept any node-ID hello packets.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring RSVP Node ID Hellos on page 29

no-adjacency-down-notification

Syntax no-adjacency-down-notification;

Hierarchy Level [edit logical-systems *logical-system-name* protocols isis interface *interface-name*],
[edit protocols isis interface *interface-name*]

Release Information Statement introduced in Junos OS Release 8.0.

Description Disable adjacency down notification for IS-IS to allow for migration from IS-IS to OSPF without disruption of the RSVP neighbors and associated RSVP-signaled LSPs.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Disabling Adjacency Down and Neighbor Down Notification in IS-IS and OSPF on page 48

no-cspf

Syntax no-cspf;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection bypass *bypass-name*],
[edit protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]

Release Information Statement introduced in Junos OS Release 7.5.

Description Disable CSPF computation on all bypass LSPs or on a specific bypass LSP. You need to disable CSPF for link protection to function properly on interarea paths.

Default CSPF is enabled.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Disabling CSPF for Bypass LSPs on page 37

no-interface-hello

Syntax no-interface-hello;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement introduced in JUNOS Release 10.0.

Description Allows you to explicitly disable RSVP interface hellos globally on the router. This type of configuration might be necessary in networks where the Juniper Networks router has numerous RSVP connections with equipment from other vendors. However, if you disable RSVP interface hellos globally, you can also configure a hello interval on an RSVP interface using the **hello-interval** statement. This configuration disables RSVP interface hellos globally but enables RSVP interface hellos on the specified interface. This configuration might be necessary in a heterogeneous network where some devices support RSVP node ID hellos and other devices support RSVP interface hellos.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring RSVP Node ID Hellos on page 29
- **hello-interval on page 69**

no-neighbor-down-notification

Syntax no-neighbor-down-notification;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-id* interface *interface-name*],
[edit protocols ospf area *area-id* interface *interface-name*]

Release Information Statement introduced in Junos OS Release 8.0.

Description Disable neighbor down notification for OSPF to allow for migration from OSPF to IS-IS without disruption of the RSVP neighbors and associated RSVP-signaled LSPs.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Disabling Adjacency Down and Neighbor Down Notification in IS-IS and OSPF on page 48

no-node-id-subobject

Syntax no-node-id-subobject;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement introduced in Junos OS Release 9.4.

Description Disable the record route object (RRO) node ID subobject for compatibility with earlier versions of the Junos OS. To interoperate with other vendors' equipment, the Junos OS supports the RRO node ID subobject for use in inter-AS link and node protection configurations.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring Inter-AS Node and Link Protection on page 32

no-p2mp-sublsp

Syntax no-p2mp-sublsp;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement introduced in Junos OS Release 9.2.

Description Reject Resv messages that include the S2L_SUB_LSP object. By default, Resv messages that include the S2L_SUB_LSP object are accepted. However, in a network which includes Juniper Networks devices running both Junos OS Release 9.2 and later and Junos OS Release 9.1 and earlier, it is necessary to configure the **no-p2mp-sublsp** statement on devices running Junos OS Release 9.2 and later to ensure that point-to-multipoint LSPs function properly.

Default Resv messages that include the S2L_SUB_LSP object are accepted.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Preserving Point-to-Multipoint LSP Functioning with Different Junos OS Releases

node-link-protection

Syntax node-link-protection;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Enable node and link protection on the specified LSP. To fully enable node and link protection, you also need to include the **link-protection** statement at the **[edit protocols rsvp interface *interface-name*]** hierarchy level.

Default Node and link protection is disabled.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring Node Protection or Link Protection for LSPs on page 30

optimize-timer

Syntax optimize-timer *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp interface *interface-name* link-protection]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure an optimize timer for a bypass LSP. The optimize timer initiates a periodic optimization process that reshuffles data LSPs among bypass LSPs to achieve the most efficient use of network resources. The optimization process attempts to either minimize the number of bypasses currently in use, minimize the total amount of bandwidth reserved for all bypasses, or both.

Options ***seconds***—Specify the number of seconds between optimizations.

Range: 0 through 65,535 seconds

Default: 0 (disabled)

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring the Optimization Interval for Bypass LSPs on page 37

path

Syntax path *address* <strict | loose>;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection bypass *bypass-name*],
[edit protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure an explicit path (a sequence of strict or loose routes) to control where and how a bypass LSP is established. If multiple bypasses are configured, they all will use the same explicit path.

Default No path is configured. CSPF automatically calculates the path the bypass LSP takes.

Options ***address***—IP address of each transit router in the LSP. You must specify the address or hostname of each transit router, although you do not need to list each transit router if its type is **loose**. As an option, you can include the ingress and egress routers in the path. Specify the addresses in order, starting with the ingress router (optional) or the first transit router, and continuing sequentially along the path until reaching the egress router (optional) or the router immediately before the egress router.

Default: If you do not specify any routers explicitly, no routing limitations are imposed on the bypass LSP.

loose—(Optional) The next address in the **path** statement is loose. The LSP can traverse other routers before reaching this router.

Default: **strict**

strict—(Optional) The LSP must go to the next address specified in the **path** statement without traversing other nodes. This is the default.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring an Explicit Path for Bypass LSPs on page 38

peer-interface

Syntax

```
peer-interface peer-interface-name {
  disable;
  (aggregate | no-aggregate);
  authentication-key key;
  hello-interval seconds;
  (reliable | no-reliable);
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp], [edit protocols rsvp]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the name of the LMP peer device.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring RSVP and OSPF for LMP Peer Interfaces

preemption

Syntax

```
preemption {
  (aggressive | disabled | normal);
  soft-preemption {
    cleanup-timer seconds;
  }
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement introduced before Junos OS Release 7.4.

Description Control RSVP session preemption.

Default normal

Options

aggressive—Preempt RSVP sessions whenever bandwidth is insufficient to handle all sessions. A session is preempted whenever bandwidth is lowered or a new higher-priority session is established.

disabled—Do not preempt RSVP sessions.

normal—Preempt RSVP sessions to accommodate new higher-priority sessions when bandwidth is insufficient to handle all sessions.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Preempting RSVP Sessions on page 45

priority

Syntax priority *setup-priority reservation-priority*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection bypass *bypass-name*],
[edit protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*],

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the setup priority and reservation priority for a bypass LSP. If insufficient link bandwidth is available during session establishment, the setup priority is compared with other setup priorities for established sessions on the link to determine whether some of them should be preempted to accommodate the new session. The session with the lower-hold priority is preempted.

Options

reservation-priority—Reservation priority, used to keep a reservation after it has been set up. A smaller number has a higher priority. The priority must be greater than or equal to the setup priority to prevent preemption loops.

Range: 0 through 7, where 0 is the highest and 7 is the lowest priority.

Default: 0 (Once the session is set up, no other session can preempt it.)

setup-priority—Setup priority.

Range: 0 through 7, where 0 is the highest and 7 is the lowest priority.

Default: 7 (The session cannot preempt any existing sessions.)

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Priority and Preemption for Bypass LSPs on page 39
- Configuring Priority and Preemption for LSPs

refresh-time

Syntax refresh-time *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement introduced before Junos OS Release 7.4.

Description Set the refresh time.

Options ***seconds***—Refresh time.
Range: 1 through 65,535
Default: 30 seconds

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring Timers for RSVP Refresh Messages on page 44

reliable

Syntax (reliable | no-reliable);

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*],
[edit logical-systems *logical-system-name* protocols rsvp peer-interface *peer-interface-name*],
[edit protocols rsvp interface *interface-name*],
[edit protocols rsvp peer-interface *peer-interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Enable reliable message delivery on the interface.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring RSVP Refresh Reduction on page 23

rsvp

Syntax rsvp { ... }

Hierarchy Level [edit logical-systems *logical-system-name* protocols],
[edit protocols]

Release Information Statement introduced before Junos OS Release 7.4.

Description Enable RSVP routing on the router.

You must include the **rsvp** statement in the configuration to enable RSVP on the router.

Default RSVP is disabled on the router.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Minimum RSVP Configuration on page 21

rsvp-te

Syntax

```
rsvp-te entry-name {
  destination-networks network-prefix;
  label-switched-path-template {
    default-template;
    template-name;
  }
}
```

Hierarchy Level [edit logical-systems *logical-system-name* routing-options dynamic-tunnels *tunnel-name*], [edit routing-options dynamic-tunnels *tunnel-name*]

Release Information Statement introduced in Junos OS Release 10.1.

Description Enable RSVP to automatically establish LSPs for any new PE router added to a full mesh of LSPs. To enable this feature, you must configure the **rsvp-te** statement on all of the PE routers in the full mesh.

Options

destination-networks *network-prefix*—Specify the IP version 4 (IPv4) prefix range for the destination network. Dynamic tunnels within the specified IPv4 prefix range are allowed to be initiated.

entry-name—Specify the entry for the RSVP tunnel.

label-switched-path-template—Configure the default template using the **default-template** option, or configure your own template using the ***template-name*** option.

Usage Guidelines See "Configuring RSVP Automatic Mesh" on page 43.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

setup-protection

Syntax setup-protection;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Description The facility-backup fast reroute mechanism can provide setup protection for LSPs which are in the process of being signaled. Both point-to-point LSPs and point-to-multipoint LSPs are supported. You should configure the **setup-protection** statement on each of the routers along the LSP path on which you want to enable LSP setup protection. You should also configure IGP traffic engineering on all of the routers on the LSP path.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring RSVP Setup Protection on page 40

soft-preemption

Syntax
```
soft-preemption {
  cleanup-timer seconds;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp preemption],
[edit protocols rsvp preemption]

Release Information Statement introduced before Junos OS Release 7.4.

Description Enable soft preemption to attempt to establish a new path for a preempted LSP before tearing it down.

Options **cleanup-timer**—A value of 0 disables soft preemption.

Range: 0 through 180 seconds

Default: 30 seconds

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring MPLS Soft Preemption

static-label-switched-path

Syntax

```
static-label-switched-path lsp-name {
  bypass bypass-name {
    bandwidth bps;
    description string;
    next-hop (address | interface-name | address/interface-name);
    push out-label;
    to address;
  }
  ingress {
    bandwidth bps;
    class-of-service cos-value;
    description string;
    install {
      destination-prefix <active>;
    }
    link-protection bypass-name name;
    metric metric;
    next-hop (address | interface-name | address/interface-name);
    node-protection bypass-name name next-next-label label;
    no-install-to-address;
    policing {
      filter filter-name;
      no-auto-policing;
    }
    preference preference;
    push out-label;
    to address;
  }
  transit incoming-label {
    bandwidth bps;
    description string;
    link-protection bypass-name name;
    next-hop (address | interface-name | address/interface-name);
    node-protection bypass-name name next-next-label label;
    pop;
    swap out-label;
  }
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols mpls],
[edit protocols mpls]

Release Information Statement introduced in Junos OS Release 10.1.

Description Configure a static LSP.

Options *lsp-name*—Name of the path.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring Static LSPs

subscription

Syntax

```
subscription percentage {
  ct0 percentage;
  ct1 percentage;
  ct2 percentage;
  ct3 percentage;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*],
[edit logical-systems *logical-system-name* protocols rsvp interface *interface-name* link-protection],
[edit protocols rsvp interface *interface-name*],
[edit protocols rsvp interface *interface-name* link-protection]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure the amount of bandwidth subscribed to a class type (when you have enabled Differentiated Services) or bypass LSP (when you have enabled link protection). **subscription** is the percentage of the link bandwidth that can be used for the RSVP reservation process.

Options

ct*number percentage*—Percentage of the class-type bandwidth allowed for reservations. If you specify a value greater than 100, you are oversubscribing the class type. You can specify bandwidth subscriptions for class types 0 through 3. This option is not available for bypass LSPs.

Range: 0 through 65,000

Default: 100 percent

percentage—Percentage of the class-type or bypass LSP bandwidth allowed for reservations. If you specify a value greater than 100, you are oversubscribing the class type or bypass LSP.

Range: 0 through 65,000

Default: 100 percent

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring the Bandwidth Subscription Percentage for LSPs
- Configuring the Amount of Bandwidth Subscribed for Bypass LSPs on page 39

traceoptions

Syntax

```
traceoptions {
  file filename <files number> <size size> <world-readable | no-world-readable>;
  flag flag <flag-modifier> <disable>;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp],
[edit protocols rsvp]

Release Information Statement introduced before Junos OS Release 7.4.

Description Enable RSVP-level trace options.

Default The default RSVP-level trace options are those inherited from the routing protocols **traceoptions** statement included at the **[edit routing-options]** hierarchy level.

Options

disable—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as **all**.

filename—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**. We recommend that you place RSVP tracing output in the file **rsvp-log**.

files *number*—(Optional) Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

Range: 2 through 1000

Default: 2 files

If you specify a maximum number of files, you must also include the **size** statement to specify the maximum file size.

flag—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements.

- **all**—All tracing operations
- **error**—All detected error conditions
- **event**—RSVP-related events
- **lmp**—RSVP-LMP interactions
- **packets**—All RSVP packets
- **path**—All path messages
- **pathtear**—PathTear messages
- **resv**—Resv messages

- **resvtear**—ResvTear messages
- **route**—Routing information
- **state**—Session state transitions

flag-modifier—(Optional) Modifier for the tracing flag. You can specify one or more of these modifiers:

- **detail**—Provide detailed trace information
- **receive**—Packets being received
- **send**—Packets being transmitted

no-world-readable—(Optional) Enable only certain users to read the log file.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the ***trace-file*** again reaches this size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

Syntax: ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify GB

Range: 10 KB through the maximum file size supported on your system

Default: 1 MB

If you specify a maximum file size, you must also include the **files** statement to specify the maximum number of files.

world-readable—(Optional) Enable any user to read the log file.

Required Privilege Level

routing and trace—To view this statement in the configuration.
routing-control and trace-control—To add this statement to the configuration.

Related Documentation

- Tracing RSVP Protocol Traffic on page 49

transit

Syntax

```
transit incoming-label {
  bandwidth bps;
  description string;
  link-protection bypass-name name;
  next-hop (address | interface-name | address/interface-name);
  node-protection bypass-name name next-next-label label;
  pop;
  swap out-label;
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 10.1.

Description

Configure a transit static LSP.

The remaining statements are explained separately.

Options

incoming-label—Incoming label value.

Range: 1000000 through 1048575

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Static LSPs

tunnel-services

Syntax
```
tunnel-services {
  devices device-names;
}
```

Hierarchy Level [edit protocols rsvp]

Release Information Statement introduced in Junos OS Release 8.1.

Description Enable ultimate-hop popping on point-to-multipoint LSPs. The Junos OS selects one of the available virtual tunnel (VT) interfaces to de-encapsulate the egress traffic. By default, the selection process is performed automatically.

Default Ultimate-hop popping is disabled.

Options **devices *device-names***—Specify which VT interfaces are used to handle the RSVP traffic.

Range: 0 to 8 devices

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Enabling Ultimate-Hop Popping on Point-to-Multipoint LSPs on page 48

update-threshold

Syntax update-threshold *threshold*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rsvp interface *interface-name*],
[edit protocols rsvp interface *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Adjust the threshold at which a change in bandwidth triggers an interior gateway protocol (IGP) update.

Options ***threshold***—Specify the percentage change in bandwidth to trigger an IGP update.

Range: 1 through 20 percent

Default: 10 percent

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring the RSVP Update Threshold on an Interface on page 27

PART 4

Index

Index

Symbols

A

B

C

D

N

O

P

R

U

W