

## Chapter 12

# Summary of RSVP Configuration Statements

This chapter provides a reference for each of the Resource Reservation Protocol (RSVP) configuration statements. The statements are organized alphabetically.

## aggregate

---

<b>Syntax</b>	(aggregate   no-aggregate);
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols rsvp interface <i>interface-name</i> ], [edit logical-routers <i>logical-router-name</i> protocols rsvp peer-interface <i>peer-interface-name</i> ], [edit protocols rsvp interface <i>interface-name</i> ], [edit protocols rsvp peer-interface <i>peer-interface-name</i> ]
<b>Description</b>	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.
<b>Default</b>	Aggregation is disabled.
<b>Usage Guidelines</b>	See “Configuring RSVP Refresh Reduction” on page 259.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

## authentication-key

---

<b>Syntax</b>	authentication-key <i>key</i> ;
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols rsvp interface <i>interface-name</i> ], [edit logical-routers <i>logical-router-name</i> protocols rsvp peer-interface <i>peer-interface-name</i> ], [edit protocols rsvp interface <i>interface-name</i> ], [edit protocols rsvp peer-interface <i>peer-interface-name</i> ]
<b>Description</b>	<p>Authentication key (password). Neighboring routers use the password to verify the authenticity of packets sent from this interface or peer interface.</p> <p>RSVP uses HMAC-MD5 authentication, which is defined in RFC 2104, <i>HMAC: Keyed-Hashing for Message Authentication</i>.</p> <p>All routers that are connected to the same IP subnet must use the same authentication scheme and password.</p>
<b>Options</b>	<p><i>key</i>—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 (" ").</p>
<b>Usage Guidelines</b>	See “Configuring RSVP Authentication” on page 263.
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>

## bandwidth

---

<b>Syntax</b>	bandwidth <i>bps</i> ;
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols rsvp interface <i>interface-name</i> ], [edit logical-routers <i>logical-router-name</i> protocols rsvp interface <i>interface-name</i> link-protection], [edit logical-routers <i>logical-router-name</i> protocols rsvp interface <i>interface-name</i> link-protection bypass <i>bypass-name</i> ], [edit protocols rsvp interface <i>interface-name</i> ], [edit protocols rsvp interface <i>interface-name</i> link-protection], [edit protocols rsvp interface <i>interface-name</i> link-protection bypass <i>bypass-name</i> ]
<b>Description</b>	For certain logical interfaces (such as ATM, PVC, or Frame Relay), you cannot determine the correct bandwidth from the hardware. This statement allows you to specify the actual available bandwidth.  This statement also allows you to specify the bandwidth for a bypass LSP. If you have configured multiple bypasses, this statement is mandatory and is applied to all of the bypass LSPs.
<b>Default</b>	The hardware raw bandwidth is used.
<b>Options</b>	<i>bps</i> —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]). <b>Range:</b> Any positive integer <b>Default:</b> 0 (no bandwidth is reserved)
<b>Usage Guidelines</b>	See “Configuring the Bandwidth for Bypass LSPs” on page 267, “Configuring Node Protection or Link Protection” on page 265, and “Configuring Bypass LSPs” on page 267.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

## bypass

```

bypass bypass-name {
    bandwidth bps;
    hop-limit number;
    path address <strict | loose>;
    to address;
}

```

**Hierarchy Level** [edit logical-routers *logical-router-name* protocols rsvp interface *interface-name* link-protection],  
[edit protocols rsvp interface *interface-name* link-protection]

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

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

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

The remaining statements are explained separately.

**Usage Guidelines** See “Configuring Bypass LSPs” on page 267.

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

## class-of-service

---

<b>Syntax</b>	class-of-service <i>class-of-service-value</i> ;
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols rsvp interface <i>interface-name</i> link-protection], [edit protocols rsvp interface <i>interface-name</i> link-protection]
<b>Description</b>	CoS value given to all packets in the bypass LSP.  The CoS value might affect the scheduling or queuing algorithm of traffic traveling along an LSP.
<b>Options</b>	<i>cos-value</i> —CoS value. A higher value typically corresponds to a higher level of service. <b>Range</b> —0 through 7 <b>Default</b> —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.
<b>Usage Guidelines</b>	See “Configuring the Class of Service for Bypass LSPs” on page 268.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

## disable

---

<b>Syntax</b>	disable;
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols rsvp], [edit logical-routers <i>logical-router-name</i> protocols rsvp graceful-restart], [edit logical-routers <i>logical-router-name</i> protocols rsvp interface <i>interface-name</i> ], [edit logical-routers <i>logical-router-name</i> protocols rsvp interface <i>interface-name</i> link-protection], [edit logical-routers <i>logical-router-name</i> protocols rsvp peer-interface <i>peer-interface-name</i> ], [edit protocols rsvp], [edit protocols rsvp graceful-restart], [edit protocols rsvp interface <i>interface-name</i> ], [edit protocols rsvp interface <i>interface-name</i> link-protection], [edit protocols rsvp peer-interface <i>peer-interface-name</i> ]
<b>Description</b>	Explicitly disable RSVP or RSVP graceful restart. Explicitly disable link protection on the specified interface.
<b>Default</b>	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.
<b>Usage Guidelines</b>	See “Minimum RSVP Configuration” on page 257, “Configuring RSVP Graceful Restart” on page 271, and “Configuring Node Protection or Link Protection” on page 265.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

## graceful-deletion-timeout

---

<b>Syntax</b>	graceful-deletion-timeout <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit protocols rsvp]
<b>Description</b>	Specify the time, in seconds, before completing graceful deletion of signaling.
<b>Options</b>	<i>seconds</i> —Time before completing graceful deletion of signaling. <b>Range:</b> 1 through 300 seconds <b>Default:</b> 30 second
<b>Usage Guidelines</b>	See “Configuring the Graceful Deletion Timeout Interval” on page 415.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

## graceful-restart

---

<b>Syntax</b>	<pre> graceful-restart {   disable;   helper-disable;   maximum-helper-recovery-time <i>seconds</i>;   maximum-helper-restart-time <i>seconds</i>; } </pre>
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> routing-options], [edit protocols rsvp], [edit routing-options]
<b>Description</b>	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.
<b>Options</b>	<p><b>disable</b>—Disable graceful restart on the router or for RSVP.</p> <p><b>helper-disable</b>—Disable RSVP graceful restart helper mode (this option is only available at the [edit protocols rsvp] hierarchy level). <b>Default:</b> Helper mode is enabled by default.</p> <p><b>maximum-helper-recovery-time</b>—The maximum amount 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. <b>Default:</b> 180 seconds <b>Range:</b> 1 through 3600 seconds</p> <p><b>maximum-helper-restart-time</b>—The maximum amount 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. <b>Default:</b> 20 seconds <b>Range:</b> 1 through 1800 seconds</p>
<b>Usage Guidelines</b>	See “Configuring RSVP Graceful Restart” on page 271.
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>

## hello-interval

---

<b>Syntax</b>	hello-interval <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols rsvp interface <i>interface-name</i> ], [edit logical-routers <i>logical-router-name</i> protocols rsvp peer-interface <i>peer-interface-name</i> ], [edit protocols rsvp interface <i>interface-name</i> ], [edit protocols rsvp peer-interface <i>peer-interface-name</i> ]
<b>Description</b>	Enable the sending of hello packets on the interface.  If you configure a nonzero hello interval and (2 x keep-multiplier + 1) consecutive hello exchanges with a neighbor are lost, the neighbor and all sessions to and from that neighbor are declared down.
<b>Options</b>	<i>seconds</i> —Length of time between hello packets. A value of 0 disables the sending of hello packets on the interface. <b>Range:</b> 1 through 60 seconds <b>Default:</b> 9 seconds
<b>Usage Guidelines</b>	See “Configuring the RSVP Hello Interval” on page 262.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

## hop-limit

---

	hop-limit <i>number</i> ;
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols rsvp interface <i>interface-name</i> link-protection], [edit logical-routers <i>logical-router-name</i> protocols rsvp interface <i>interface-name</i> link-protection bypass <i>bypass-name</i> ], [edit protocols rsvp interface <i>interface-name</i> link-protection], [edit protocols rsvp interface <i>interface-name</i> link-protection bypass <i>bypass-name</i> ]
<b>Description</b>	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.
<b>Option</b>	<i>number</i> —Maximum number of hops a bypass can traverse. <b>Range:</b> 2 through 255 hops <b>Default:</b> 255 hops
<b>Usage Guidelines</b>	See “Configuring the Hop Limit for Bypass LSPs” on page 268.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

## interface

---

<b>Syntax</b>	<pre> interface <i>interface-name</i> {   disable;   aggregate;   authentication-key <i>key</i>;   bandwidth <i>bps</i>;   hello-interval <i>seconds</i>;   link-protection {     bandwidth <i>bps</i>;     bypass <i>bypass-name</i> {       to <i>address</i>;       bandwidth <i>bps</i>;       hop-limit <i>number</i>;       path <i>address</i> &lt;strict   loose&gt;;     }     class-of-service <i>class-of-service-value</i>;     hop-limit <i>number</i>;     max-bypasses <i>number</i>;     no-node-protection;     optimize-timer <i>number</i>;     path <i>address</i> &lt;strict   loose&gt;;     subscription <i>percentage</i>;   }   no-aggregate;   no-reliable;   reliable;   subscription <i>percentage</i>; } </pre>
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols rsvp], [edit protocols rsvp]
<b>Description</b>	Enable RSVP on one or more router interfaces.
<b>Default</b>	RSVP is disabled on all interfaces.
<b>Options</b>	<i>interface-name</i> —Name of an interface. To configure all interfaces, specify all. For details about specifying interfaces, see the <i>JUNOS Network Interfaces and Class of Service Configuration Guide</i> .
	The remaining statements are explained separately.
<b>Usage Guidelines</b>	See “Minimum RSVP Configuration” on page 257.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

## keep-multiplier

---

<b>Syntax</b>	keep-multiplier <i>number</i> ;
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols rsvp], [edit protocols rsvp]
<b>Description</b>	Set the keep multiplier value.
<b>Options</b>	<i>number</i> —Multiplier value. <b>Range:</b> 1 through 255 <b>Default:</b> 3
<b>Usage Guidelines</b>	See “Configuring RSVP Timers” on page 272.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

## link-protection

---

See the following sections:

link-protection (MPLS) on page 288

link-protection (RSVP) on page 289

### ***link-protection (MPLS)***

<b>Syntax</b>	link-protection;
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols mpls label-switched-path <i>lsp-name</i> ], [edit protocols mpls label-switched-path <i>lsp-name</i> ]
<b>Description</b>	Enable link protection on the specified LSP. To fully enable link protection, you also need to configure the link-protection statement at the [edit protocols rsvp interface <i>interface-name</i> ] hierarchy level.
<b>Default</b>	Link protection is disabled.
<b>Usage Guidelines</b>	See “Configuring Node Protection or Link Protection” on page 265.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

**link-protection (RSVP)**

**Syntax** link-protection {  
 disable;  
 bandwidth *bps*;  
 bypass *bypass-name* {  
 to *address*;  
 bandwidth *bps*;  
 hop-limit *number*;  
 path *address* <strict | loose>;  
 }  
 class-of-service *class-of-service-value*;  
 hop-limit *number*;  
 max-bypasses *number*;  
 no-node-protection;  
 optimize-timer *seconds*;  
 path *address* <strict | loose>;  
 subscription *percent*;  
 }

**Hierarchy Level** [edit logical-routers *logical-router-name* protocols rsvp interface *interface-name*],  
 [edit protocols rsvp interface *interface-name*]

**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.

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

The remaining statements are explained separately.

**Default** Link protection is disabled.

**Usage Guidelines** See “Configuring Node Protection or Link Protection” on page 265.

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

## max-bypasses

---

<b>Syntax</b>	max-bypasses <i>number</i> ;
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols rsvp interface <i>interface-name</i> ], [edit protocols rsvp interface <i>interface-name</i> ]
<b>Description</b>	Specify the maximum number of bypasses 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 to both automatically and manually configured bypasses. By default, this option is disabled and only one bypass is enabled for each interface. If you configure max-bypasses, you must also configure the bandwidth option.
<b>Usage Guidelines</b>	See “Configuring the Maximum Number of Bypass LSPs” on page 269.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

## no-aggregate

---

**See** aggregate on page 279.

## no-reliable

---

**See** reliable on page 294.

## node-link-protection

---

<b>Syntax</b>	node-link-protection;
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols mpls label-switched-path <i>lsp-name</i> ], [edit protocols mpls label-switched-path <i>lsp-name</i> ]
<b>Description</b>	Enable node and link protection on the specified LSP. To fully enable node and link protection, you also need to configure the link-protection statement at the [edit protocols rsvp interface <i>interface-name</i> ] hierarchy level.
<b>Default</b>	Node and link protection is disabled.
<b>Usage Guidelines</b>	See “Configuring Node Protection or Link Protection” on page 265.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

## optimize-timer

---

<b>Syntax</b>	optimize-timer <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols mpls label-switched-path <i>lsp-name</i> ], [edit protocols mpls label-switched-path <i>lsp-name</i> ]
<b>Description</b>	Configure the optimize timer, a periodic optimization process that reshuffles data LSPs among bypasses 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.
<b>Options</b>	<i>seconds</i> —Specify the number of seconds between bypass optimizations. <b>Range:</b> 0 through 65,535 seconds <b>Default:</b> 0 (disabled)
<b>Usage Guidelines</b>	See “Configuring the Optimization Interval for Bypass LSPs” on page 269.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

## path

---

<b>Syntax</b>	<code>path address &lt;strict   loose&gt;;</code>
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols rsvp interface <i>interface-name</i> link-protection], [edit logical-routers <i>logical-router-name</i> protocols rsvp interface <i>interface-name</i> link-protection bypass <i>bypass-name</i> ], [edit protocols rsvp interface <i>interface-name</i> link-protection], [edit protocols rsvp interface <i>interface-name</i> link-protection bypass <i>bypass-name</i> ]
<b>Description</b>	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.
<b>Default</b>	No path is configured. CSPF automatically calculates the path the bypass LSP takes.
<b>Options</b>	<p><i>address</i>—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.</p> <p><b>Default:</b> If you do not specify any routers explicitly, no routing limitations are imposed on the bypass LSP.</p> <p><i>loose</i>—The next address in the path statement is loose. The LSP can traverse other routers before reaching this router. <b>Default:</b> strict</p> <p><i>strict</i>—The LSP must go to the next address specified in the path statement without traversing other nodes. This is the default.</p>
<b>Usage Guidelines</b>	See “Configuring an Explicit Path for Bypass LSPs” on page 270.
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>

## peer-interface

---

<b>Syntax</b>	<code>peer-interface peer-name;</code>
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols rsvp], [edit protocols rsvp]
<b>Description</b>	Configure the name of the LMP peer device.
<b>Usage Guidelines</b>	See “Configuring Peer Interfaces in RSVP and OSPF” on page 410.
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>

preemption

---

<b>Syntax</b>	preemption (aggressive   disabled   normal   soft-preemption);
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols rsvp], [edit protocols rsvp]
<b>Description</b>	Control RSVP session preemption.
<b>Options</b>	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 soft-preemption statement is explained separately.
<b>Default</b>	normal
<b>Usage Guidelines</b>	See “Preempting RSVP Sessions” on page 274.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

refresh-time

---

<b>Syntax</b>	refresh-time <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols rsvp], [edit protocols rsvp]
<b>Description</b>	Set the refresh time.
<b>Options</b>	<i>seconds</i> —Refresh time. <b>Range:</b> 1 through 65,535 <b>Default:</b> 30 seconds
<b>Usage Guidelines</b>	See “Configuring RSVP Timers” on page 272.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

## reliable

---

<b>Syntax</b>	(reliable   no-reliable);
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols rsvp interface <i>interface-name</i> ], [edit protocols rsvp interface <i>interface-name</i> ]
<b>Description</b>	Enable reliable message delivery on the interface.
<b>Usage Guidelines</b>	See “Configuring RSVP Refresh Reduction” on page 259.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

## rsvp

---

<b>Syntax</b>	rsvp { ... }
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols], [edit protocols]
<b>Description</b>	Enable RSVP routing on the router.  You must include the rsvp statement in the configuration to enable RSVP on the router. See “Minimum RSVP Configuration” on page 257.
<b>Default</b>	RSVP is disabled on the router.
<b>Usage Guidelines</b>	See “Minimum RSVP Configuration” on page 257.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

## soft-preemption

---

<b>Syntax</b>	soft-preemption { cleanup-timer; }
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols rsvp preemption], [edit protocols rsvp preemption]
<b>Description</b>	Soft preemption attempts to establish a new path for a preempted LSP before tearing it down.
<b>Options</b>	cleanup-timer—A value of 0 disables soft preemption. <b>Range:</b> 0 through 180 seconds <b>Default:</b> 30 seconds
<b>Usage Guidelines</b>	See “Configuring MPLS Soft Preemption” on page 87.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

## subscription

---

<b>Syntax</b>	subscription <i>percentage</i> ;
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols rsvp interface <i>interface-name</i> ], [edit logical-routers <i>logical-router-name</i> protocols rsvp interface <i>interface-name</i> link-protection], [edit protocols rsvp interface <i>interface-name</i> ], [edit protocols rsvp interface <i>interface-name</i> link-protection]
<b>Description</b>	Configures the amount of bandwidth subscribed to a bypass LSP. The subscription is the percentage of the link bandwidth that can be used for the RSVP reservation process.
<b>Options</b>	<i>percentage</i> —Percentage of the bypass LSP bandwidth that RSVP allows to be used for reservations. If you specify a value greater than 100, you are oversubscribing the bypass LSP. <b>Range:</b> 0 through 65,000 <b>Default:</b> 100 percent
<b>Usage Guidelines</b>	See “Configuring the Amount of Bandwidth Subscribed for Bypass LSPs” on page 270.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

## traceoptions

---

<b>Syntax</b>	<pre> traceoptions {   file <i>filename</i> &lt;replace&gt; &lt;size <i>size</i>&gt; &lt;files <i>number</i>&gt; &lt;no-stamp&gt;     &lt;(world-readable   no-world-readable)&gt;;   flag <i>flag</i> &lt;<i>flag-modifier</i>&gt; &lt;disable&gt;; } </pre>
<b>Hierarchy Level</b>	[edit logical-routers <i>logical-router-name</i> protocols rsvp], [edit protocols rsvp]
<b>Description</b>	RSVP protocol-level trace options.
<b>Default</b>	The default RSVP protocol-level trace options are those inherited from the routing protocols traceoptions statement included at the [edit routing-options] hierarchy level.
<b>Options</b>	<p><b>disable</b>—(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.</p> <p><i>filename</i>—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.</p> <p><i>files number</i>—(Optional) Maximum number of trace files. When a trace file named <i>trace-file</i> reaches its maximum size, it is renamed <i>trace-file.0</i>, then <i>trace-file.1</i>, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p><b>Range:</b> 2 through 1000 <b>Default:</b> 2 files</p>

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

#### **RSVP Tracing Flags**

all—All tracing operations

error—All detected error conditions

event—RSVP-related events

Imp—RSVP-LMP interactions

packets—All RSVP packets

path—All path messages

pathtear—PathTear messages

resv—Resv messages

resvtear—ResvTear messages

state—Session state transitions

#### **Global Tracing Flags**

all—All tracing operations

general—A combination of the normal and route trace operations

normal—All normal operations  
**Default:** If you do not specify this option, only unusual or abnormal operations are traced.

policy—Policy operations and actions

route—Routing table changes

state—State transitions

task—Interface transactions and processing

timer—Timer usage

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

detail—Provide detailed trace information

receive—Packets being received

send—Packets being transmitted

no-stamp—(Optional) Do not place timestamp information at the beginning of each line in the trace file.

**Default:** If you omit this option, timestamp information is placed at the beginning of each line of the tracing output.

no-world-readable—(Optional) Disallow any user to read the log file.

replace—(Optional) Replace an existing trace file if there is one.

**Default:** If you do not include this option, tracing output is appended to an existing trace file.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file.0*. When the *trace-file* again reaches its maximum 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.

If you specify a maximum file size, you also must specify a maximum number of trace files with the *files* option.

**Syntax:** *xk* to specify KB, *xm* to specify MB, or *xg* to specify GB

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

**Default:** 1 MB

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

**Usage Guidelines** See “Tracing RSVP Protocol Traffic” on page 277.

**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.

## update-threshold

---

**Syntax** update-threshold *threshold*;

**Hierarchy Level** [edit logical-routers *logical-router-name* protocols rsvp interface *interface-name*],  
 [edit protocols rsvp interface *interface-name*]

**Description** Adjust the threshold at which a change in bandwidth triggers an IGP update.

**Range:** 1 through 20 percent

**Default:** 10 percent

**Usage Guidelines** See “Configuring the RSVP Update Threshold on an Interface” on page 264.

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