

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

| | |
|---------------------------------|--|
| Syntax | (aggregate no-aggregate); |
| Hierarchy Level | [edit protocols rsvp interface <i>interface-name</i>], [edit protocols rsvp peer-interface <i>peer-interface-name</i>] |
| Description | Control the use of RSVP aggregate messages on an interface or peer interface: aggregate—Use RSVP aggregate messages. no-aggregate—Do not use RSVP aggregate messages. Aggregate messages can pack multiple RSVP messages into a single transmission, thereby reducing network overhead and enhancing efficiency. The number of supportable sessions and processing overhead are significantly improved when aggregation is enabled. Not all routers connected to a subnet need to support aggregation simultaneously. Each RSVP router negotiates its intention to use aggregate messages on a per-neighbor basis. Only when both routers agree are aggregate messages sent. |
| Default | Aggregation is disabled. |
| Usage Guidelines | See “Configure RSVP Aggregation” on page 163. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |

authentication-key

| | |
|---------------------------------|---|
| Syntax | authentication-key <i>key</i> ; |
| Hierarchy Level | [edit protocols rsvp interface <i>interface-name</i>], [edit protocols rsvp peer-interface <i>peer-interface-name</i>] |
| Description | <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> |
| Options | <i>key</i> —Authentication password. It can be 1 to 16 contiguous digits or letters. Separate decimal digits with periods. Separate hexadecimal digits with periods and precede the string with 0x. If you include spaces in the password, enclose the entire password in quotation marks (" "). |
| Usage Guidelines | See “Configure RSVP Authentication” on page 167. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |

bandwidth

| | |
|---------------------------------|---|
| Syntax | bandwidth <i>bps</i> ; |
| Hierarchy Level | [edit protocols rsvp interface <i>interface-name</i>], [edit protocols rsvp interface <i>interface-name</i> link-protection] |
| Description | <p>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.</p> <p>This statement also allows you to specify the bandwidth for a bypass LSP.</p> |
| Default | The hardware raw bandwidth is used. |
| Options | <p><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])).</p> <p>Range: Any positive integer</p> <p>Default: 0 (no bandwidth is reserved)</p> |
| Usage Guidelines | See “Reserve Bandwidth on an Interface” on page 167 and “Configure Node Protection or Link Protection” on page 164. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |

class-of-service

| | |
|---------------------------------|---|
| Syntax | class-of-service <i>class-of-service-value</i> ; |
| Hierarchy Level | [edit protocols rsvp interface <i>interface-name</i> link-protection] |
| Description | 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. |
| Options | <i>cos-value</i> —CoS value. A higher value typically corresponds to a higher level of service. Range —0 through 7 Default —If you do not specify a CoS value, the IP precedence bits from the packet's IP header are used as the packet's CoS value. |
| Usage Guidelines | See "Configure Node Protection or Link Protection" on page 164. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |

disable

| | |
|---------------------------------|---|
| Syntax | disable; |
| Hierarchy Level | [edit 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>] |
| Description | Explicitly disable RSVP or RSVP graceful restart. Explicitly disable link protection on the specified interface. |
| Default | RSVP is enabled on interfaces and peer interfaces configured with the RSVP interface statement. RSVP graceful restart is enabled on the router. Link protection is disabled. |
| Usage Guidelines | See "Enable RSVP" on page 163, "Configure RSVP Graceful Restart" on page 165, and "Configure Node Protection or Link Protection" on page 164. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |

graceful-restart

| | |
|---------------------------------|--|
| Syntax | graceful-restart { disable; helper-disable; } |
| Hierarchy Level | [edit protocols rsvp] [edit protocols rsvp peer-interface <i>peer-interface-name</i>] |
| Description | Disable RSVP graceful restart or RSVP graceful restart helper mode on the router. The optional statements are explained separately. |
| Usage Guidelines | See “Configure RSVP Graceful Restart” on page 165. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |

hello-interval

| | |
|---------------------------------|--|
| Syntax | hello-interval <i>seconds</i> ; |
| Hierarchy Level | [edit protocols rsvp interface <i>interface-name</i>] [edit protocols rsvp peer-interface <i>peer-interface-name</i>] |
| Description | Enable the sending of hello packets on the interface. If you configure a nonzero hello interval and $(2 * \text{keep-multiplier} + 1)$ consecutive hello exchanges with a neighbor are lost, the neighbor and all sessions to and from that neighbor are declared down. |
| Options | <i>seconds</i> —Length of time between hello packets. A value of 0 disables the sending of hello packets on the interface. Range: 1 through 60 seconds Default: 9 seconds |
| Usage Guidelines | See “Configure the RSVP Hello Interval” on page 166. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |

helper-disable

| | |
|---------------------------------|---|
| Syntax | helper-disable; |
| Hierarchy Level | [edit protocols rsvp graceful-restart] |
| Description | Disable RSVP graceful restart helper mode on the router. |
| Default | Helper mode is enabled by default. |
| Usage Guidelines | See “Configure RSVP Graceful Restart” on page 165. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |

interface

| | |
|---------------------------------|---|
| Syntax | interface <i>interface-name</i> { disable; authentication-key <i>key</i> ; subscription <i>percentage</i> ; } |
| Hierarchy Level | [edit protocols rsvp] |
| Description | Enable RSVP on one or more router interfaces. |
| Default | RSVP is disabled on all interfaces. |
| Options | <i>interface-name</i> —Name of an interface. To configure all interfaces, you can specify all. For details about specifying interfaces, see the <i>JUNOS Internet Software Configuration Guide: Network Interfaces and Class of Service</i> . The remaining statements are explained separately. |
| Usage Guidelines | See “Enable RSVP” on page 163. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |

keep-multiplier

| | |
|---------------------------------|---|
| Syntax | keep-multiplier <i>number</i> ; |
| Hierarchy Level | [edit protocols rsvp] |
| Description | Set the keep multiplier value. |
| Options | <i>number</i> —Multiplier value. Range: 1 through 255 Default: 3 |
| Usage Guidelines | See “Configure RSVP Timers” on page 169. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |

link-protection

link-protection (MPLS)

| | |
|---------------------------------|--|
| Syntax | link-protection; |
| Hierarchy Level | [edit protocols mpls label-switched-path <i>lsp-name</i>] |
| Description | Enables 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. |
| Default | Link protection is disabled. |
| Usage Guidelines | See “Configure Node Protection or Link Protection” on page 164. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |

link-protection (RSVP)

| | |
|---------------------------------|---|
| Syntax | link-protection { disable; bandwidth <i>bandwidth</i> ; class-of-service <i>class-of-service-value</i> ; path <i>address</i> <strict loose>; } |
| Hierarchy Level | [edit protocols rsvp interface <i>interface-name</i>] |
| Description | Enables 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 <i>lsp-name</i>] hierarchy level. The remaining statements are explained separately. |
| Default | Link protection is disabled. |
| Usage Guidelines | See “Configure Node Protection or Link Protection” on page 164. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |

no-aggregate

See aggregate on page 175.

node-link-protection

| | |
|---------------------------------|--|
| Syntax | node-link-protection; |
| Hierarchy Level | [edit protocols mpls label-switched-path <i>lsp-name</i>] |
| Description | Enables 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. |
| Default | Node and link protection is disabled. |
| Usage Guidelines | See “Configure Node Protection or Link Protection” on page 164. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |

path

| | |
|---------------------------------|---|
| Syntax | path <i>address</i> <strict loose>; |
| Hierarchy Level | [edit protocols rsvp interface <i>interface-name</i> link-protection] |
| Description | Configure an explicit path (a sequence of strict or loose routes) to control where and how a bypass LSP is established. |
| Default | No path is configured. CSPF automatically calculates the path the bypass LSP takes. |
| Options | <p><i>address</i>—IP address of each transit router in the LSP. You must specify the address or host name 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>Default: If you do not specify any routers explicitly, no routing limitations are imposed on the bypass LSP.</p> <p>loose—The next address in the path statement is loose. The LSP can traverse other routers before reaching this router. Default: strict</p> <p>strict—The LSP must go to the next address specified in the path statement without traversing other nodes. This is the default.</p> |
| Usage Guidelines | See “Configure Node Protection or Link Protection” on page 164. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |

peer-interface

| | |
|---------------------------------|---|
| Syntax | peer-interface <i>peer-name</i> ; |
| Hierarchy Level | [edit protocols rsvp] |
| Description | Configure the name of the LMP peer device. |
| Usage Guidelines | See “Configure Peer Interfaces on OSPF and RSVP” on page 268. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |

preemption

| | |
|---------------------------------|---|
| Syntax | preemption (aggressive disabled normal); |
| Hierarchy Level | [edit protocols rsvp] |
| Description | Control RSVP session preemption. |
| 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. |
| Default | normal |
| Usage Guidelines | See “Preempt RSVP Sessions” on page 170. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |

refresh-time

| | |
|---------------------------------|---|
| Syntax | refresh-time <i>seconds</i> ; |
| Hierarchy Level | [edit protocols rsvp] |
| Description | Set the refresh time. |
| Options | <i>seconds</i> —Refresh time. Range: 1 through 65,535 Default: 30 seconds |
| Usage Guidelines | See “Configure RSVP Timers” on page 169. |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |

rsvp

| | |
|---------------------------------|--|
| Syntax | rsvp { ... } |
| Hierarchy Level | [edit protocols] |
| Description | <p>Enable RSVP routing on the router.</p> <p>You must include the <code>rsvp</code> statement in the configuration to enable RSVP on the router. See “Minimum RSVP Configuration” on page 162.</p> |
| Default | RSVP is disabled on the router. |
| Usage Guidelines | See “Enable RSVP” on page 163. |
| Required Privilege Level | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p> |

subscription

| | |
|---------------------------------|--|
| Syntax | subscription <i>percentage</i> ; |
| Hierarchy Level | [edit protocols rsvp interface <i>interface-name</i>] |
| Description | <p>Configure the subscription factor on the interface, which is the percentage of the link bandwidth that can be used for the RSVP reservation process.</p> <p>You can use the subscription factor to shut down new RSVP sessions on a per-interface basis. If you set the percentage to 0, no new sessions (including those with zero bandwidth requirements) are permitted on the interface. Existing RSVP sessions are not affected by changing the subscription factor. To clear an existing session, issue the <code>clear rsvp session</code> command.</p> |
| Options | <p><i>percentage</i>—Percentage of the interface’s bandwidth that RSVP allows to be used for reservations. If you specify a value greater than 100, you are oversubscribing the interface.</p> <p>Range: 0 through 65,000</p> <p>Default: 100 percent</p> |
| Usage Guidelines | See “Reserve Bandwidth on an Interface” on page 167. |
| Required Privilege Level | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p> |

traceoptions

Syntax traceoptions {
 file *filename* <replace> <size *size*> <files *number*> <no-stamp>
 <(world-readable | no-world-readable)>;
 flag *flag* <*flag-modifier*> <disable>;
 }

Hierarchy Level [edit protocols rsvp]

Description RSVP protocol-level trace options.

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

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

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

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

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

Range: 2 through 1000

Default: 2 files

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

lmp—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 “Trace RSVP Protocol Traffic” on page 170.

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 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 “Configure the RSVP Update Threshold on an Interface” on page 168.

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