Chapter 11

Examining RSVP Log Messages

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

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

Table 18: Checklist for Examining RSVP Log Messages

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

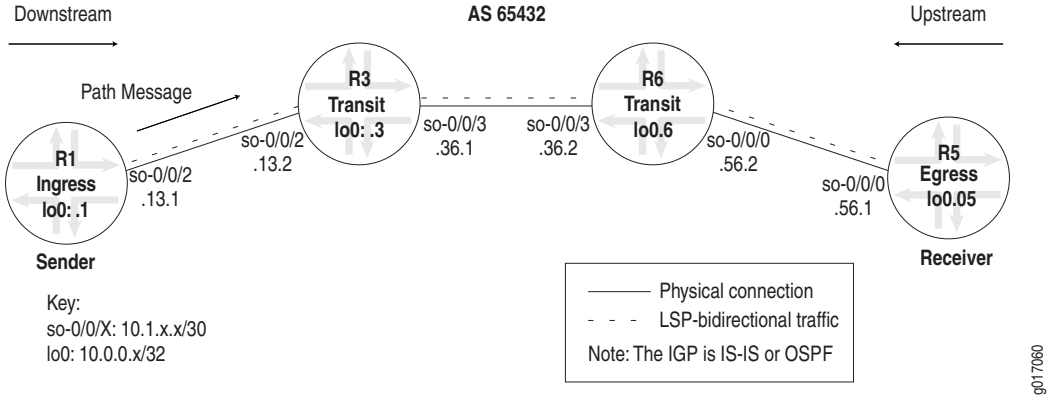
NOTE: To display tracing output, make sure that RSVP trace options are enabled. See "Working with RSVP Tracing" on page 113, for information on configuring RSVP trace options.

Examining the Path Message

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

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

Figure 11: RSVP Path Message



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

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

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

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

Sample Output 1

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

Sample Output 2

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

user@R1> monitor start rsvp-log

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

What It Means

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

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

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

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

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

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

- Hop Len 12 10.1.13.1/0x08678198

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

- Time Len 8 30000 ms

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

- SrcRoute Len 28 10.1.13.2 S 10.1.36.2 S 10.1.56.1 S

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

- LabelRequest Len 8 EtherType 0x800

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

- Properties Len 12 Primary path

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

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

  The SessionAttribute object indicates a variety of parameters:

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

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

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

    Table 19 shows the SessionAttribute object flags.

Table 19: Session Attribute Object Flags

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

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

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

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

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

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

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

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

- ADspec Len 48 MTU 1500

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

- RecRoute Len 12 10.1.13.1

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

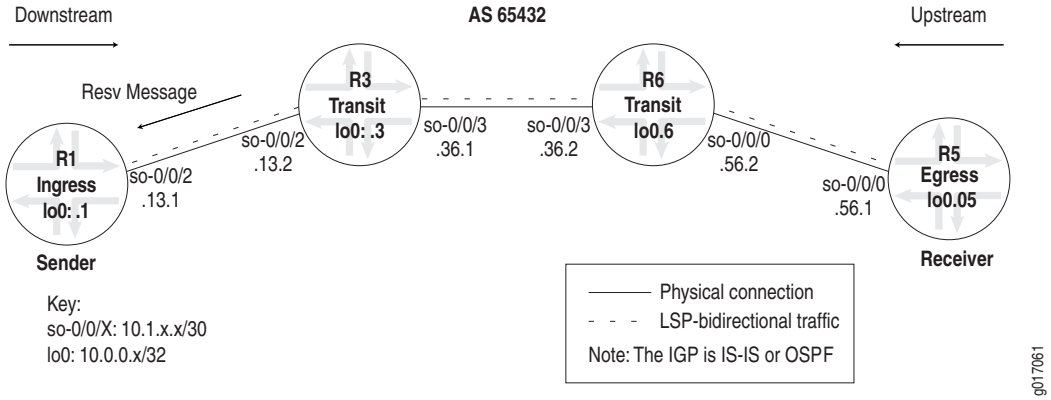
For information on objects that can appear in the Path message but do not appear in the sample output, such as **Detour**, **Explicit route**, **FastReroute**, and **Integrity**, see Table 15 on page 110.

Examining the Resv Message

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

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

Figure 12: RSVP Resv Message



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

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

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

Sample Output 1

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

Sample Output 2

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

user@R1> monitor start rsvp-log

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

What It Means

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

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

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

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

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

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

- Hop Len 12 10.1.13.2/0x08678198

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

- Time Len 8 30000 ms

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

- Style Len 8 FF

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

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

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

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

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

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

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

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

- Label Len 8 100624

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

- RecRoute Len 28 10.1.13.2 10.1.36.2 10.1.56.1

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

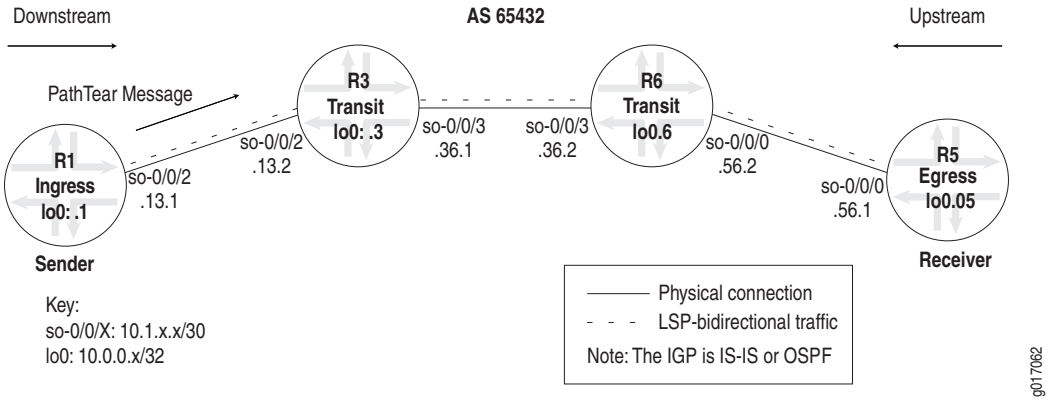
Examining the PathTear Message

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

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

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

Figure 13: RSVP PathTear Message



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

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

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

Sample Output 1

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

Sample Output 2

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

user@R1> monitor start rsvp-log

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

What It Means

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

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

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

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

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

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

- Hop Len 12 10.1.13.1/0x08678198

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

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

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

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

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

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

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

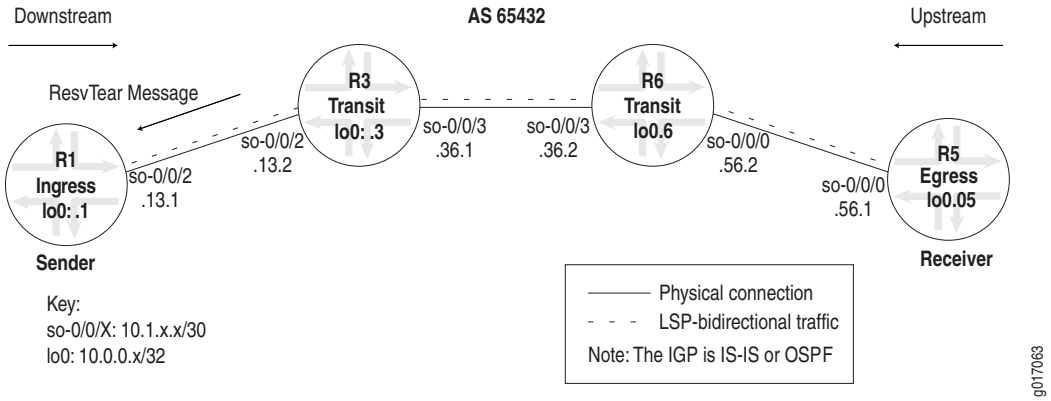
Examining the ResvTear Message

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

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

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

Figure 14: RSVP ResvTear Message



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

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

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

Sample Output 1

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

Sample Output 2

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

user@R1> monitor start rsvp-log

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

What It Means

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

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

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

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

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

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

- Hop Len 12 10.1.13.1/0x08678198

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

- Style Len 8 FF

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

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

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

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

Examining the Hello Message

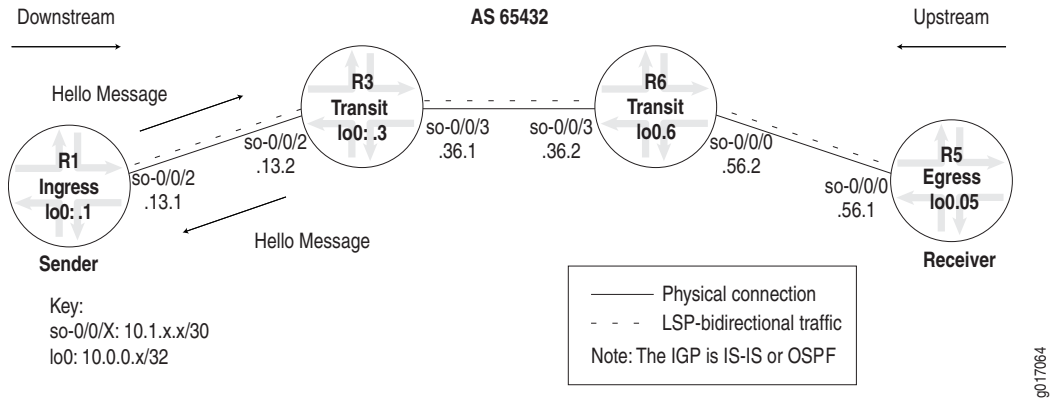
Purpose RSVP monitors the status of the interior gateway protocol (IGP) (Intermediate System-to-Intermediate System [ISIS] or Open Shortest Path First [OSPF]) neighbors and relies on the IGP protocols to detect when a node fails. If an IGP protocol declares a neighbor down (because Hello messages are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

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

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

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

Figure 15: RSVP Hello Message



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

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

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

Sample Output 1

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

Sample Output 2

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

user@R1> monitor start rsvp-log

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

What It Means

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

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

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

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

- HelloReq Len 12

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

- RestartCap Len 12 restart time 0, recovery time 0

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

- HelloRply Len 12

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

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

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

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

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

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

About ResvConfirm Messages

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

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