Chapter 10

Working with RSVP Tracing

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

Table 16: Checklist for Working with RSVP Tracing

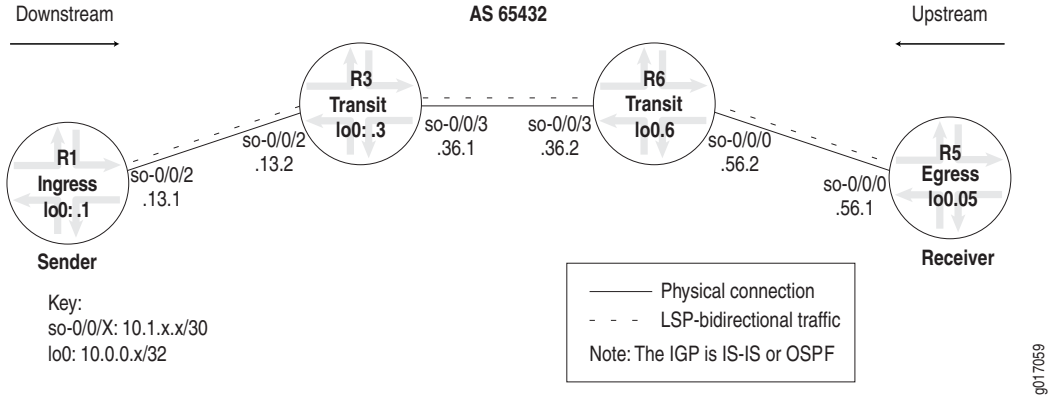
Working with RSVP Tracing Tasks	Possible Action or Command
Enabling RSVP Tracing on page 114	
1. Configure RSVP Tracing on page 115	[edit] edit protocols rsvp [edit protocols rsvp] set traceoptions file *filename* set traceoptions flag *flag* show commit
2. Display the RSVP Log File on page 117	
a. (Optional)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

Enabling RSVP Tracing

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

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

Figure 10: MPLS Network Topology



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

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

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

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

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

Step 1: Configure RSVP Tracing

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

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

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

2. Configure a log file:

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

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

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

4. Verify and commit the configuration:

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

Sample Output

```
user@R1> edit
Entering configuration mode

[edit]
user@R1# edit protocols rsvp

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

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

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

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

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

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

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

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

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

Table 17: RSVP Tracing Flags

Flag	Description
all	All tracing operations
error	All detected error conditions
event	RSVP-related events
lmp	RSVP-LMP interactions
packets	All RSVP packets
path	All Path messages
pathtear	PathTear messages
resv	Resv messages
resvtear	ResvTear messages
route	Routing information
state	Session state transitions

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

Step 2: Display the RSVP Log File

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

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

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

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

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

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

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

Sample Output

```
user@R1> clear rsvp session

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

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

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

2. Display Real-Time RSVP Log Entries

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

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

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

Sample Output

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

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

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

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

3. View the RSVP Log File

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

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

Sample Output

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

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

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

4. Deactivate and Reactivate RSVP Tracing

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

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

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

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

Sample Output

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

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

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

[edit protocols rsvp]
user@R1# activate traceoptions

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

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

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

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

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