Chapter 13

Examining an RSVP Failure

The Resource Reservation Protocol (RSVP) is a signaling protocol that provides reservation setup and control. This chapter describes a real-world scenario in which RSVP fails because links in the network are incorrectly configured. It discusses some basic approaches to monitoring and examining an RSVP failure, including how, when, and why you use specific commands. This chapter also includes an examination of the RSVP log file and corrective action for the specific scenario. (See Table 22.)

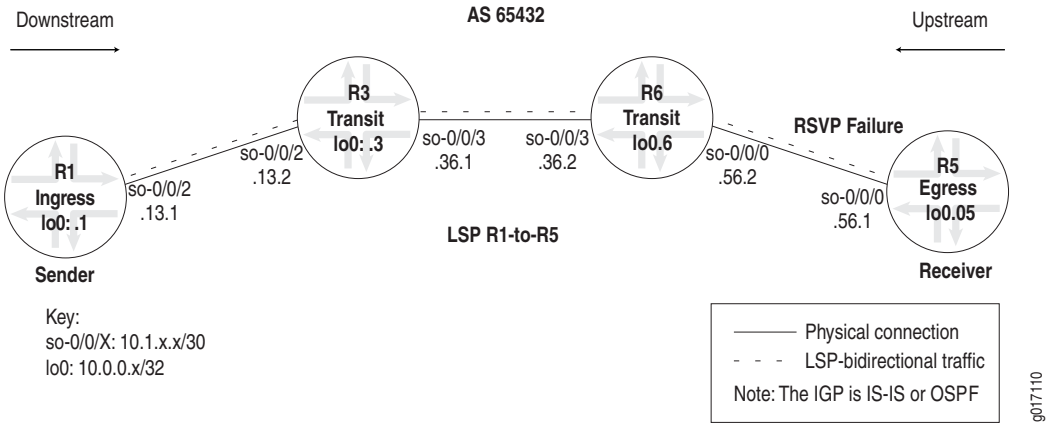
Table 22: Checklist for Examining an RSVP Failure

Examining an RSVP Failure Tasks	
Case Study for an RSVP Failure on page 154	
1. Verify the RSVP Session on page 155	show rsvp session ingress detail
2. Ping the Egress Router on page 156	ping *ip-address-interface*
3. Enable RSVP Tracing on Transit Routers on page 156	edit [edit] edit protocols rsvp [edit protocols rsvp] set traceoptions file *filename* set traceoptions flag *flag* show commit
4. View the RSVP Log File on Transit Routers on page 158	clear rsvp session (Optional) clear log *filename* (Optional) show log *filename*
5. Check the RSVP Log File on the Egress Router on page 159	show log rsvp-log
6. Determine and Correct the Problem on the Egress Router on page 160	The following sequence of commands addresses the specific problem described in this section: show configuration protocols rsvp edit [edit protocols rsvp] rename interface so-0/0/3 to interface so-0/0/0 show commit run show rsvp session ingress detail
7. Remove the Tracing Configuration on page 161	edit [edit protocols rsvp] show delete traceoptions show commit

Case Study for an RSVP Failure

Purpose This case study presents a Multiprotocol Label Switching (MPLS) network topology and RSVP failure scenario designed to demonstrate techniques and commands that are particularly useful when addressing RSVP problems in your network. The focus of the study is an unconstrained RSVP label-switched path (LSP) from R1 to R5, which uses a strict path through R3. In this case, the RSVP failure occurs when interface so-0/0/0 on R5 is configured incorrectly. (See Figure 18.)

Figure 18: RSVP Failure in an MPLS Network Topology



The MPLS network in Figure 18 is a router-only network with SONET interfaces that consists of the following components:

- A full-mesh interior Border Gateway Protocol (IBGP) topology, using AS 65432.
- MPLS and RSVP enabled on all routers.
- A send-statics policy on routers R1 and R6, that allows a new route to be advertised into the network.
- Two unidirectional LSPs between routers R1 (ingress) and R5 (egress), which allow bidirectional traffic.
- The no-cspf statement included at the [edit protocols mpls label-switched-path *path-name*] hierarchy level, indicating that the Constrained Shortest Path First (CSPF) algorithm is not used to compute the LSP path.
- A strict path configured for both unidirectional LSPs, R1-to-R5 and R5-to-R1, at the [edit protocols mpls] hierarchy level.

Although there are a number of ways to examine an RSVP failure in an MPLS network, the following sequence of steps and commands is useful in determining the origin of an RSVP failure.

Steps To Take To examine the RSVP failure, follow these steps:

1. Verify the RSVP Session on page 155
2. Ping the Egress Router on page 156
3. Enable RSVP Tracing on Transit Routers on page 156
4. View the RSVP Log File on Transit Routers on page 158
5. Check the RSVP Log File on the Egress Router on page 159
6. Determine and Correct the Problem on the Egress Router on page 160
7. Remove the Tracing Configuration on page 161

Step 1: Verify the RSVP Session

Purpose In this case study, the unconstrained RSVP LSP from router R1 to R5 uses a strict path through R3, r1-r3-r5.

Action To verify that the RSVP session is established, enter the following JUNOS command-line interface (CLI) operational mode command:

```
user@host> show rsvp session ingress detail
```

Sample Output

```
user@R1> show rsvp session ingress detail
Ingress RSVP: 1 sessions

10.0.0.5
  From: 10.0.0.1, LSPstate: Dn, ActiveRoute: 0
  LSPname: R1-to-R5, LSPpath: Primary
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: -
  Resv style: 0 -, Label in: -, Label out: -
  Time left:    -, Since: Tue Jul 19 20:42:20 2005
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 16 receiver 11956 protocol 0
  PATH rcvfrom: localclient
  Adspec: sent MTU 1500
  Path MTU: received 0
  PATH sentto: 10.1.13.2 (so-0/0/2.0) 3 pkts
  Explct route: 10.1.13.2
  Record route: <self> ...incomplete
Total 1 displayed, Up 0, Down 1
```

What It Means The sample output from ingress router R1 shows that the RSVP session has not been established (Down 1) through the explicit path (10.1.13.2). The Path message was sent to R3 (10.1.13.2) and dropped. In situations like this, you can ping the egress router (R5) to ensure operational communications in the network, and enable RSVP tracing on the router that dropped the packet (R3) to obtain valuable clues as to the nature of the problem.

Step 2: Ping the Egress Router

Purpose Ping the egress router to confirm that communication over the network is operational.

Action To ping the egress router, enter the following JUNOS CLI operational mode command:

user@host> **ping** *ip-address-interface*

Sample Output

```
[edit protocols mpls]
user@R1# run ping 10.1.56.1
PING 10.1.56.1 (10.1.56.1): 56 data bytes
64 bytes from 10.1.56.1: icmp_seq=0 ttl=255 time=0.837 ms
64 bytes from 10.1.56.1: icmp_seq=1 ttl=255 time=0.792 ms
64 bytes from 10.1.56.1: icmp_seq=2 ttl=255 time=0.856 ms
^C
--- 10.1.56.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.792/0.828/0.856/0.027 ms
```

What It Means The sample output confirms that communication between router R1 and the IP address of the relevant interface on router R5 (10.1.56.1) is operational.

Step 3: Enable RSVP Tracing on Transit Routers

Purpose RSVP tracing on transit routers (R3 and R6) can provide useful information about the problem.

Action To enable RSVP tracing on transit routers, follow these steps:

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

   user@host> **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 all or one of the following RSVP-specific tracing flags:

   [edit protocols rsvp]
   user@host# **set traceoptions flag error detail**
   user@host# **set traceoptions flag path detail**
   user@host# **set traceoptions flag pathtear detail**

4. Verify and commit the configuration:

   user@host# **show**
   user@host# **commit**

5. Complete the above steps on any other transit routers that might provide useful information towards resolution of the problem.

Sample Output

```
user@R3> edit
Entering configuration mode

[edit]
user@R3# edit protocols rsvp

[edit protocols rsvp]
user@R3# set traceoptions file rsvp-log

[edit protocols rsvp]
user@R3# set traceoptions flag error detail

[edit protocols rsvp]
user@R3# set traceoptions flag path detail

[edit protocols rsvp]
user@R3# 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 fxp0.0 {
    disable;
}
interface all;

[edit protocols rsvp]
user@R3# commit
commit complete
```

What It Means

The sample output shows a configuration of RSVP tracing on transit router R3. The same tracing configuration is placed on R6 (not shown). Various 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 "RSVP Tracing Flags" on page 116. With all configured flags, the detail option is included to show granular details about errors and paths.

NOTE: Use the trace options detail flag with caution because it may cause the CPU to become very busy. For information on removing a tracing configuration, see "Remove the Tracing Configuration" on page 161.

After you have configured tracing and issued the commit command, the routing protocol process (rpd) immediately starts monitoring RSVP. Any RSVP activity that relates to the configured flags is placed in the log file.

Step 4: View the RSVP Log File on Transit Routers

Purpose Transit router messages that appear in the RSVP log file can help you analyze the problem with an RSVP session. You may need to issue the clear rsvp session and clear log *filename* commands to ensure that your records are current. However, if your network is large with many RSVP sessions, this may not be advisable because it may take a while for all sessions to reestablish. However, the clear rsvp session command has various options you can include to minimize the effect on your network. For more information about the clear rsvp session command, see the *JUNOS Routing Protocols and Policies Command Reference.*

Action To view the RSVP log file, enter the following JUNOS CLI operational mode commands:

```
user@host> clear rsvp session (Optional)
user@host> clear log filename (Optional)
user@host> show log filename
```

Sample Output 1

```
user@R3> clear rsvp session

user@R3> clear log rsvp-log

user@R3> show log rsvp-log
Jul 21 16:51:23 R3 clear-log[30656]: logfile cleared
Jul 21 16:51:24 RSVP recv Path 10.0.0.1->10.0.0.5 Len=208 so-0/0/2.0
Jul 21 16:51:24   Session7 Len 16 10.0.0.5(port/tunnel ID 11956) Proto 0
Jul 21 16:51:24   Hop      Len 12 10.1.13.1/0x086cd198
Jul 21 16:51:24   Time     Len  8 30000 ms
Jul 21 16:51:24   SrcRoute Len 20  10.1.13.2 S 10.1.36.2 S
Jul 21 16:51:24   LabelRequest Len  8 EtherType 0x800
Jul 21 16:51:24   Properties Len 12 Primary path
Jul 21 16:51:24   SessionAttribute Len 16 Prio (7,0) flag 0x0 "R1-to-R5"
Jul 21 16:51:24   Sender7  Len 12 10.0.0.1(port/lsp ID  32)
Jul 21 16:51:24   Tspec    Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500
Jul 21 16:51:24   ADspec   Len 48 MTU 1500
Jul 21 16:51:24   RecRoute Len 12  10.1.13.1
Jul 21 16:51:24 RSVP send Path 10.0.0.1->10.0.0.5 Len=208 so-0/0/3.0
Jul 21 16:51:24   Session7 Len 16 10.0.0.5(port/tunnel ID 11956) Proto 0
Jul 21 16:51:24   Hop      Len 12 10.1.36.1/0x08680264
Jul 21 16:51:24   Time     Len  8 30000 ms
Jul 21 16:51:24   SrcRoute Len 12  10.1.36.2 S
Jul 21 16:51:24   LabelRequest Len  8 EtherType 0x800
Jul 21 16:51:24   Properties Len 12 Primary path
Jul 21 16:51:24   SessionAttribute Len 16 Prio (7,0) flag 0x0 "R1-to-R5"
Jul 21 16:51:24   Sender7  Len 12 10.0.0.1(port/lsp ID  32)
Jul 21 16:51:24   Tspec    Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500
Jul 21 16:51:24   ADspec   Len 48 MTU 1500
Jul 21 16:51:24   RecRoute Len 20  10.1.36.1 10.1.13.1
```

Sample Output 2

```
user@R6> clear rsvp session

user@R6> clear log rsvp-log

user@R6> show log rsvp-log
Jul 21 17:01:21 R6 clear-log[41496]: logfile cleared
Jul 21 17:01:23 RSVP recv Path 10.0.0.1->10.0.0.5 Len=208 so-0/0/3.0
Jul 21 17:01:23   Session7 Len 16 10.0.0.5(port/tunnel ID 11956) Proto 0
Jul 21 17:01:23   Hop      Len 12 10.1.36.1/0x08680264
Jul 21 17:01:23   Time     Len  8 30000 ms
Jul 21 17:01:23   SrcRoute Len 12  10.1.36.2 S
```

```
Jul 21 17:01:23   LabelRequest Len  8 EtherType 0x800
Jul 21 17:01:23   Properties Len 12 Primary path
Jul 21 17:01:23   SessionAttribute Len 16 Prio (7,0) flag 0x0 "R1-to-R5"
Jul 21 17:01:23   Sender7  Len 12 10.0.0.1(port/lsp ID  32)
Jul 21 17:01:23   Tspec    Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500
Jul 21 17:01:23   ADspec   Len 48 MTU 1500
Jul 21 17:01:23   RecRoute Len 20  10.1.36.1 10.1.13.1
Jul 21 17:01:23 RSVP send Path 10.0.0.1->10.0.0.5 Len=204 so-0/0/0.0
Jul 21 17:01:23   Session7 Len 16 10.0.0.5(port/tunnel ID 11956) Proto 0
Jul 21 17:01:23   Hop      Len 12 10.1.56.2/0x086f9000
Jul 21 17:01:23   Time     Len  8 30000 ms
Jul 21 17:01:23   LabelRequest Len  8 EtherType 0x800
Jul 21 17:01:23   Properties Len 12 Primary path
Jul 21 17:01:23   SessionAttribute Len 16 Prio (7,0) flag 0x0 "R1-to-R5"
Jul 21 17:01:23   Sender7  Len 12 10.0.0.1(port/lsp ID  32)
Jul 21 17:01:23   Tspec    Len 36 rate 0bps size 0bps peak Infbps m 20 M 1500
Jul 21 17:01:23   ADspec   Len 48 MTU 1500
Jul 21 17:01:23   RecRoute Len 28  10.1.56.2 10.1.36.1 10.1.13.1
```

What It Means Sample Output 1 from transit router R3 shows that R3 (so-0/0/2.0) correctly received a Path request message (recv Path) from R1, and correctly sent the Path message (send Path) through interface so-0/0/3.0 to R6. The route record object (RecRoute) indicates the list of addresses this Path message transited, in this case, 10 1.36.1 and 10.1.13.1.

Sample Output 2 from transit router R6 shows that R6 (so-0/0/3.0) correctly received a Path request message (recv Path) from R3, and correctly sent the Path message (send Path) through interface so-0/0/0 to R5. The route record object (RecRoute) indicates the list of addresses this Path message transited, in this case, 10.1.56.2, 10 1.36.1, and 10.1.13.1.

With the information above, the focus shifts to egress router R5 as the source of the problem, with indications that R5 ignored the RSVP message.

Step 5: Check the RSVP Log File on the Egress Router

Purpose After placing an RSVP tracing configuration on router R5 similar to that on routers R3 and R6, display the RSVP log file for useful information about the problem on router R5. For steps to configure RSVP tracing, see “Enable RSVP Tracing on Transit Routers” on page 156.

Action To check the RSVP log file, enter the following JUNOS CLI operational mode command:

user@host> **show log rsvp-log**

Sample Output

```
user@R5> show log rsvp-log
Jul 21 10:53:16 R5 clear-log[40071]: logfile cleared
Jul 21 11:02:37 trace_on: Tracing to "/var/log/rsvp-log" started
Jul 21 11:03:07 RSVP error, send to DISABLED interface? Hello New
10.1.56.1->10.1.56.2 Len=8 so-0/0/0.0
```

What It Means The sample output shows that R5 did not receive the Path message because of a disabled interface, so-0/0/0.0.

Step 6: Determine and Correct the Problem on the Egress Router

Purpose Check the configuration of interface so-0/0/0.0 on egress router R5 to determine the reason it was disabled.

Action To determine the problem on R5, enter the following JUNOS CLI commands:

```
user@R5> show configuration protocols rsvp
user@R5> edit
[edit protocols rsvp]
user@R5# rename interface so-0/0/3 to interface so-0/0/0
user@R5# show
user@R5# commit
user@R5# run show rsvp session ingress detail
```

Sample Output 1

```
user@R5> show configuration protocols rsvp
traceoptions {
    file rsvp-log;
    flag error detail;
    flag path detail;
    flag pathtear detail;
}
interface so-0/0/3.0;   <<< so-0/0/3 incorrectly included
interface so-0/0/1.0;
interface so-0/0/2.0;
interface fxp0.0 {
    disable;
}
```

Sample Output 2

```
[edit protocols rsvp]
user@R5# rename interface so-0/0/3 to interface so-0/0/0

[edit protocols rsvp]
user@R5# show
traceoptions {
    file rsvp-log;
    flag packets detail;
    flag error 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@R5# commit
commit complete
```

Sample Output 3

```
[edit protocols mpls]
user@R5# run show rsvp session ingress detail
Ingress RSVP: 1 sessions
To              From            State   Rt Style Labelin Labelout LSPname
10.0.0.1        10.0.0.5        Up       1  1 FF       -   103104 R5-to-R1
Total 1 displayed, Up 1, Down 0

Egress RSVP: 1 sessions
To              From            State   Rt Style Labelin Labelout LSPname
10.0.0.5        10.0.0.1        Up       0  1 FF       3        - R1-to-R5
Total 1 displayed, Up 1, Down 0

Transit RSVP: 0 sessions
Total 0 displayed, Up 0, Down 0
```

What It Means Sample Output 1 from egress router R5 shows three interfaces configured at the [edit protocols rsvp] hierarchy level, non of which is so-0/0/0.0. On examination of the network topology, it is apparent that the so-0/0/0.0 interface was configured incorrectly as so-0/0/3.0.

Sample Output 2 shows the correct configuration of interfaces at the [edit protocols rsvp] hierarchy level, and the rename command issued to correct the configuration error.

Sample Output 3 shows that the RSVP-signaled LSP (R1-to-R5) is correctly established after the changes to the RSVP configuration are committed.

Step 7: Remove the Tracing Configuration

Purpose It is considered best practice to remove any configuration elements that are no longer required, such as tracing configurations.

Action To remove the tracing configuration, enter the following JUNOS CLI commands:

```
user@R5> edit
[edit protocols rsvp]
user@R5# show
user@R5# delete traceoptions
user@R5# show
user@R5# commit
```

Sample Output 1

```
user@R5> edit
Entering configuration mode

[edit]
user@R5# edit protocols rsvp

[edit protocols rsvp]
user@R5# show
traceoptions {
    file rsvp-log;
    flag error detail;
    flag path detail;
    flag pathtear detail;
}
interface so-0/0/3.0;
interface so-0/0/1.0;
interface so-0/0/2.0;
interface fxp0.0 {
```

```
    disable;
}

[edit protocols rsvp]
user@R5# delete traceoptions

[edit protocols rsvp]
user@R5# show
interface so-0/0/3.0;
interface so-0/0/1.0;
interface so-0/0/2.0;
interface fxp0.0 {
    disable;
}

[edit protocols rsvp]
user@R5# commit
commit complete
```

What It Means The sample output from egress router R5 shows that tracing is deleted from the R5 configuration. In addition, the tracing configuration was removed from all routers (not shown).

NOTE: Use the trace options detail flag with caution because it may cause the CPU to become very busy.