ERICSSON

Troubleshooting MPLS

SmartEdge OS Software

FAULT TRACING DIRECT.

7/154 51-CRA 119 1170/1-V2 Uen F

Contents

1 Overview

Specific information in this troubleshooting guide assumes a typical Multiprotocol Label Switching (MPLS) deployment using SmartEdge® routers, illustrated in Figure 1.

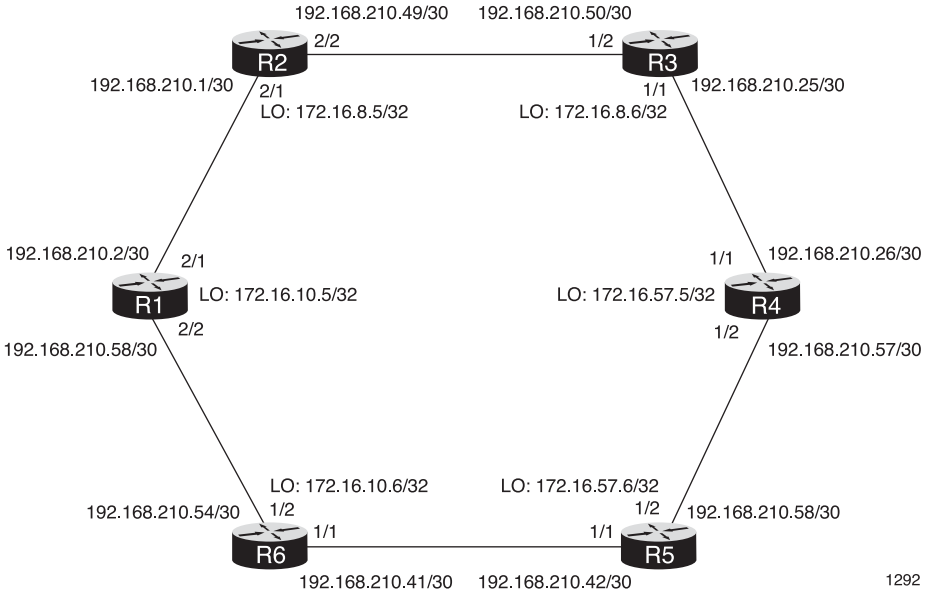

Figure 1 Typical MPLS Deployment

Label-switched routers (LSRs) forward packets through MPLS networks (such as the one in this illustration), analyzing the path only when the packet enters, and assigning a label. As the packets are forwarded along the label-switched path (LSP), each LSR makes forwarding decisions based on the label. At each hop, the LSR swaps the existing label for a new label that tells the LSR at the next hop how to forward the packet. At the egress point, an edge LSR removes the label and forwards the packet to its destination. MPLS uses Resource Reservation Protocol (RSVP) or Label Distribution Protocol (LDP) to communicate labels and their meanings among LSRs.

In the illustration, the IP addresses marked with LO are the loopback addresses for each router.

Here, we are troubleshooting a problem in traffic between R1 and R4.

To troubleshoot MPLS issues, use the following workflow:

1. Verify IP Connectivity
2. Troubleshoot MPLS Configuration, Interfaces, and Packet Flow
3. Troubleshoot MPLS Signaling with one of the following:

- Troubleshoot LDP Signaling
- Troubleshoot RSVP Signaling

2 Verify IP Connectivity

When end-user packets do not reach their destination, you can verify the connectivity of the bridge associated with the target by checking whether traffic is flowing. If traffic is not flowing, verify that the interfaces are up, that routes were learned through IGP, and that the neighbors are up. Use the steps in Table 1 to check and troubleshoot connectivity.

Table 1 Verify IP Connectivity

Task	Root Command	Notes	Checked?
Step 1: Verify IP Connectivity From Local Router to Remote Router	**ping** ***target-ip-addr*** **source** ***ip-addr*** **traceroute**		
Step 2: Verify that the Interfaces Are Up	**show ip interface brief**		
Step 3: Verify Routes Were Learned Correctly	**show ip route**		
Step 4: Verify Neighbors are Known to Each Other	**show ospf neighbor**		
Step 5: Verify Ports are Bound to the Correct Interfaces	**show bindings**		

2.1 Step 1: Verify IP Connectivity From Local Router to Remote Router

On the local router, enter the **ping** ***target-ip-addr*** **source** ***ip-addr*** command, targeting the remote router:

```
[local]R1#ping 172.16.8.6 source 172.16.10.5
PING 172.16.8.6 (172.16.8.6): source 172.16.10.5, 36 data bytes,
timeout is 1 second !!!!!

----172.16.8.6 PING Statistics----
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.882/2.119/2.740/0.359 ms
```

You can also use the **traceroute** command (targeting the loopback address for the egress PE router) to identify the problem or the path:

```
[local]R1#traceroute 172.16.8.6
se_traceroute to 172.16.8.6 (172.16.8.6), 30 hops max, 40 byte packets
 1  172.16.10.5(172.16.10.5)    4.439 ms  3.763 ms  2.838 ms ----> R1 router
 2  172.16.8.5(172.16.8.5)    2.320 ms  2.802 ms  2.256 ms ----> R2 router
 3  172.16.8.6 (172.16.8.6)    4.034 ms  2.921 ms  2.885 ms --> Egress router
```

If the **ping** and **traceroute** commands were not successful, then continue with the following steps.

2.2 Step 2: Verify that the Interfaces Are Up

If the ping does not return a response, or the **traceroute** command does not work, verify that the interfaces are Up on this router and its neighboring routers with the **show ip interface brief** command:

```
[local]R1#show ip interface brief
Mon Feb  8 16:41:05 2010
Name               Address              MTU   State    Bindings
PE-loop            172.16.10.5/32       1500  Up       (Loopback)
. . .
backbone1          192.168.210.2/30     1500  Up       ethernet 2/1
mgmt               10.21.1.131/24       1500  Up       ethernet 1/12
```

The example displays the relevant interfaces and indicates that they are up.

2.3 Step 3: Verify that Routes Were Learned Correctly

To verify that the routes for all the routers was learned correctly, use the **show ip route** command, which displays output similar to the following:

```
[local]R1#show ip route
Codes: C - connected, S - static, S dv - dvsr, R - RIP, e B - EBGP,
I B - IBGP, O   - OSPF, O3  - OSPFv3, IA - OSPF(v3) inter-area,
N1  - OSPF(v3) NSSA external type 1, N2  - OSPF(v3) NSSA external type 2
E1  - OSPF(v3) external type 1, E2  - OSPF(v3) external type 2
I   - IS-IS, L1 - IS-IS level-1,  L2  - IS-IS level-2, N - NAT
IPH - IP Host, SUB A - Subscriber address, SUB S - Subscriber static
MIP F - Mobile-IP Foreign Agent, MIP H - Mobile-IP Home Agent
A - Derived Default, MH - Media Nexthop
>   - Active Route, * - LSP

Type  Network         Next Hop       Dist   Metric  UpTime   Interface
> O   10.16.50.1/32                  200     2       00:45:11  backbone1
> O   172.16.8.5      172.16.8.6      200     3       00:45:11  backbone1
> C   10.21.1.0/24                   0       0       15w6d      mgmt
> C   172.16.8.5/32   192.168.210.50  0       0       3d21h     PE-loop
> O   172.16.8.6/32   192.168.210.26  110     2       00:45:11  backbone1
> O   172.16.57.5/32  192.168.210.26  110     3       00:45:11  backbone1
> O   172.16.57.6/32  192.168.210.58  110     4       00:45:11  backbone1
> S   155.53.0.0/16   10.21.1.254     1       0       15w6d     mgmt
> C   192.168.210.41/30               0       0       1w4d      ge-2/2
```

2.4 Step 4: Verify that Neighbors Are Known to Each Other

If the expected routes are not in the **show ip route** output, enter the **show ospf neighbor** command, which displays output similar to the following, Verify that neighbors are known to each other:

```
[local]R1#show ospf neighbor

  --- OSPF Neighbors for Instance 1/Router ID 172.16.10.5 ---
NeighborID   NeighborAddress Pri State    DR-State IntfAddress    TimeLeft
172.16.8.2    172.16.8.5      1   Full     BDR      172.16.8.0        30
```

2.5 Step 5: Verify that Ports Are Bound to the Correct Interfaces

Before continuing, verify that the ports are bound to the correct interfaces in the context. Use the **show bindings** command to verify the bindings.

```
[local]R1#show bindings
Circuit          State Encaps         Bind Type  Bind Name

1/1:1 vpi-vci 1 1000    Down  bridge1483     interface  atm-br@br
1/2:1 vpi-vci 1 1000    Down  atm pppoe
2/1                     Up    ethernet       interface  ge-2/1@local
2/2                     Up    ethernet       interface  ge-2/2@local
2/3                     Up    ethernet
2/4                     Down  ethernet       interface  ge2/4@local
3/1                     Up    ethernet
3/1 clips 138453        Up    eth clips      authen     00:12:17:b4+
3/2                     Down  ethernet       interface  fa-3/2@SIGTR+
3/3                     Down  ethernet       interface  fa-3/3@CN-1
3/4                     Down  pppoe          chap pap
3/5                     Down  ethernet
3/6                     Down  ethernet       interface  subscr+@PPPoE
3/8                     Up    ethernet       interface  dhcp@local
3/10                    Down  ethernet       interface  eth-br@br
3/11                    Down  ethernet
3/12                    Down  ethernet
6/1                     Up    ethernet       interface  mgmt@local
MPLS LSP 1              Up    mpls
MPLS LSP 2              Up    mpls
MPLS LSP 3              Up    mpls
MPLS LSP 9              Up    mpls
MPLS LSP 15             Up    mpls
MPLS LSP 16             Up    mpls
MPLS LSP 17             Up    mpls
MPLS LSP 18             Up    mpls
MPLS LSP 19             Up    mpls

Summary:
   total: 27
      up: 16            down: 11
   bound: 10         unbound: 17
    auth: 2        interface: 10      subscriber: 0           bypass: 0
    no-bind: 15          atm: 1           chdlc: 0            dot1q: 0
      ether: 14           fr: 0             gre: 0
       mpls: 9              ppp: 0         pppoe: 2
      clips: 1             vpls: 0          ipip: 0
      ipsec: 0       ipv6v4-man: 0      ipv6v4-auto: 0
```

3 Troubleshoot MPLS Configuration, Interfaces, and Packet Flow

Use the following table as a guide to troubleshoot common MPLS issues on the SmartEdge® router.

Table 2 Tasks to Troubleshoot MPLS Functionality

Task	Command	Notes	Checked ?
Step 1: Check MPLS Configuration	**show configuration mpls**		
Step 2: Verify MPLS Interfaces	**ping** **show port** **show mpls interface**	• Can you ping the loopback? • Are interfaces bound to the local context reachable? • Are the MPLS loop back and two interfaces enabled and have the state of Up?	
Step 3: Verify that Packets Are Sent Over the LSP	**ping mpls ldp *address*** **ping mpls rsvp *lsp-name*** **traceroute mpls**		
Step 4: Verify That MPLS and LDP Are Enabled	**show mpls interface** **show ldp interface** **show ldp binding**		
Step 5: View LSP Information	**show mpls lsp**		

Table 2 Tasks to Troubleshoot MPLS Functionality

Task	Command	Notes	Checked ?
Step 6: Verify Incoming and Outgoing MPLS Labels	**show mpls label-mapping**		
Step 7: Troubleshoot Static MPLS	**show log active fac mpls-static** **show mpls-static lsp** [**detail**] **show configuration mpls-static** **show mpls-static lm** **show ip route lsp** **debug circuit mpls-static** with the optional **all lsp**, or **event** keyword		

3.1 Step 1: Check MPLS Configuration

To verify that MPLS has been enabled, enter the **show configuration mpls** command, as in the following example:

```
[local]R1#show configuration mpls

context local
!
router-id 172.16.10.5
!
router mpls
interface backbone1
interface backbone2
interface lb1
```

The **router mpls** command enables MPLS.

3.2 Step 2: Verify MPLS Interfaces

Before you begin verifying MPLS and LSP interfaces, test them with simple pings. Check the following:

Are the loopback addresses of the other routers reachable? Ping router R3 from R1:

```
[local]R1#ping 172.16.8.6
PING 172.16.8.6 (172.16.8.6): source 192.168.210.2, 36 data bytes,
timeout is 1 second
!!!!!
```

Are the interfaces bound to the local context reachable? Ping the interfaces on the R3 router; for example targeting the interface on `slot 1, port 2` (`192.168.210.50`):

```
[local]R1#ping 192.168.210.50
PING 192.168.210.50 (192.168.210.50): source 192.168.210.2, 36 data bytes,
timeout is 1 second
!!!!!

----192.168.210.50 PING Statistics----
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.727/2.440/2.876/0.460 ms
```

If the ping fails, check the status of the interfaces with the **show port** command and determine if the interfaces in the MPLS configuration are up.

If the port is down, check the cable and verify that **no shutdown** is configured on the port. If everything is working correctly, perform the same checks on the device that the router is connected to so that you can bring this port up to determine a Layer 1 issue exists.

Use the **show mpls interface** command to verify that the interfaces are configured correctly on a router in the MPLS backbone. Verify that the MPLS loopback and the two backbone interfaces are enabled and have a state of `Up`. The following example shows that the MPLS interfaces are working correctly:

```
[local]R1#show mpls interface
  --- All MPLS Interfaces ---

Inst Address/Mask       Name           Enabled  State  Bound to
1    192.168.210.2/30   backbone1      Yes      Up     2/2
1    192.168.210.58/30  backbone2      Yes      Up     2/1
1    172.16.10.5/32     lb1            Yes      Up     Loopback
```

3.3 Step 3: Verify That Packets Are Sent Over the LSP

Note: This section assumes that the label switched path is built using LDP.

To verify that packets are flowing over the LSP, use the **ping** command:

```
[local]R1#ping mpls ldp 172.16.8.6/32
Sending 5 100-byte MPLS echos to LDP 172.16.8.6/32,
source 172.16.8.6/32,
    timeout is 1 second, send interval is 0 msec:
!!!!!
```

3.4 Step 4: Verify that MPLS and LDP Are Enabled

If there are no LSPs, verify that MPLS and LDP are enabled for their respective interfaces with the **show mpls interface**, **show ldp interface**, and **show ldp binding** commands. For more information on testing LDP LSPs, see Section 4 on page 14.

```
[local]R1#show mpls interface

  --- All MPLS Interfaces ---

Inst Address/Mask       Name      Enabled  State  Bound to
1    172.16.10.5/32      loop      Yes      Up     Loopback
1    192.168.210.2/30    backbone1       Yes      Up     9/19
1    192.168.210.58/30   backbone2       Yes      Up     2/12

[local]R1#show ldp interface
Flag:
B - Bound, U - Up, D - Deleted, S - Stale, E - Hold expired
T - Bind Stale L - Loopback
Interface     Local Addr            Flag RemoteLSRId      HoldExpr
loop          172.16.10.5/32        BUL
backbone1     192.168.210.2/30      BU   192.168.210.2:0   14
backbone2     192.168.210.58/30     BU   192.168.210.58:0  12
```

You can see in this output that the LDP interfaces are enabled and up (see the BU flags).

When LSPs are missing—for example, if `100.1.1.1` were missing—you check the FECs that the LDP has learned by entering the **show ldp binding** command.

```
[local]R1#show ldp binding
 > active binding, Local/In - local/input label binding
 From - source of remote label, Remote/Out - remote/output
label binding
  Prefix/FEC         Learned-From    Local/In   Remote/Out Interface
> 10.21.1.0/24       local           3
                     100.1.1.2:0                3
                     100.1.1.4:0                3
                     100.1.1.3:0                3
> 100.1.1.1/32       local           3
                     100.1.1.2:0                524291
                     100.1.1.4:0                524291
                     100.1.1.3:0                524292
> 100.1.1.2/32       100.1.1.2:0     524291     3          backbone1
                     100.1.1.4:0                524292
                     100.1.1.3:0                524293
> 100.1.1.3/32       100.1.1.2:0     524295     524295     backbone1
>                    100.1.1.4:0                524295     backbone2
                     100.1.1.3:0                3
  100.1.1.4/32       100.1.1.2:0     524296     524296
>                    100.1.1.4:0                3          backbone2
                     100.1.1.3:0                524294
> 192.168.1.0/30     local           3
                     100.1.1.2:0                3
                     100.1.1.4:0                524294
                     100.1.1.3:0                524295
> 192.168.1.4/30     local           3
                     100.1.1.2:0                524297
                     100.1.1.4:0                3
                     100.1.1.3:0                524296
> 192.168.1.8/30     100.1.1.2:0     524293     3          backbone1
                     100.1.1.4:0                524293
                     100.1.1.3:0                3
> 192.168.1.12/30    100.1.1.4:0     524294     3          backbone2
                     100.1.1.2:0                524294
                     100.1.1.3:0                3
> 192.168.16.24/30   local           3
```

3.5 Step 5: View LSP Information

To view the LSPs, use the **show mpls lsp** command. Use the **detail** keyword to view detailed information.

In the output, the left column displays whether an LSP is signaled by LDP or RSVP. In this example, the LSP type is RSVP. Minimally, the loopback addresses of all PE routers should be displayed in the output.

If the **show mpls interface**, **show mpls label-mapping**, and **show mpls lsp** commands successfully display results, the MPLS backbone is up and running and VPNs, media, and signaling can connect across the backbone.

```
[local]R1#show mpls lsp
Codes : S - MPLS-Static, R - RSVP, L - LDP, B - BGP

Type Endpoint            Direct Next-hop  Out Label      Adjacency Id
L    172.16.8.5/32       192.168.210.1    0              0x1300070
L    172.16.8.5/32       192.168.210.54   458761         0x1300010
L    172.16.8.6/32       192.168.210.1    458753         0x130004d
L    172.16.8.6/32       192.168.210.54   458757         0x1300071
L    172.16.57.5/32      192.168.210.1    458754         0x1300050
L    172.16.57.5/32      192.168.210.54   458758         0x1300025
L    172.16.57.6/32      192.168.210.54   458764         0x1300012
L    172.16.57.6/32      192.168.210.1    458769         0x1300066


[local]R1#show mpls lsp detail
------------------------------------------------------------
Type                : LDP             LSP Circuit         : N/A
Egress              : 172.16.57.6     Client ID           : 3
Traffic-Eng         : default         RIB Table ID        : 0x0
Direct Next Hop     : 192.168.210.49  Direct Next Hop Cct : 2/2:1023:63/1/1/20
Adjacency ID        : 0x1300023       Out Label Count     : 1
Tunnel ID           : 0x0             Flags               : 0x10
Out Label Stack     : 524302
Special Procedures  :
Tx Packets          : 0               Tx Bytes            : 0

------------------------------------------------------------
Type                : RSVP            LSP Circuit         : 255/3:1023:63/0/1/6
Egress              : 172.16.8.5/32   Client ID           : 2
Traffic-Eng         : default         RIB Table ID        : 0x0
Direct Next Hop     : 192.168.210.1   Direct Next Hop Cct : 2/1:1023:63/1/1/18
Adjacency ID        : 0x130003b       Out Label Count     : 1
Tunnel ID           : 0x8             Flags               : 0x44010
Alt label           : 0x70015         Alt action          : PUSH
Alt Egress          : 192.168.210.54  Alt LSP Cct         : 255/3:1023:63/0/1/1
2
Out Label Stack     : 0
```

3.6 Step 6: Verify MPLS Labels

To display how incoming and outgoing labels are mapped and how the operation is performed on the incoming labels, use the **show mpls label-mapping** command.

```
[local]R1#show mpls label-mapping
Codes : S - MPLS-Static, R - RSVP, L - LDP, B - BGP

Type    In Label  Action  Direct Next hop    Out Label   Adjacency Id
        0         pop                         0           0x0
        131072    php     0.0.0.0             3           0x0
L       458752    swap    192.168.210.1       458757      0x1300026
L       458753    swap    192.168.210.54      0           0x1300027
L       458754    swap    192.168.210.1       458759      0x1300028
L       458755    swap    192.168.210.54      0           0x1300029
L       458756    swap    192.168.210.1       0           0x130002a
L       458757    swap    192.168.210.54      0           0x130002b
L       458758    swap    192.168.210.1       0           0x130002c
```

3.7 Step 7: Troubleshoot Static MPLS

To troubleshoot static MPLS, perform the following steps:

1. Examine static MPLS events in the log using the **`show log active fac`** command, filtering it by the **`mpls-static`** facility.

```
[local]Redback#show log active fac mpls-static
Jul 12 16:55:30.975: [0001]: %MPLS-STATIC-3-ERR: RIB query for lsp lsp1 next-hop address
25.0.101.2 returned error 8
Jul 12 16:55:30.984: %MPLS-STATIC-6-INFO: Registration with LM was successful
```

2. Verify static MPLS LSP status (State) and display the LSP name, LSP ID, direct next-hop, endpoint, and out label for a static MPLS circuit, using the following command:

```
[local]Redback#show mpls-static lsp
                Static LSPs

LSP                 ID     Next-hop        Out-Label   Endpoint        State
lsp1                1      25.0.101.2      3           52.0.0.101      Up
```

3. Check the static MPLS configuration by entering the **`show configuration mpls-static`** command.

```
[local]Redback#show configuration mpls-static
Building configuration...

Current configuration:

context local
!
 router mpls-static
  interface core-101
  interface loopback0
  lsp lsp1
   egress 52.0.0.101
   next-hop 25.0.101.2
   out-label 3
!
! ** End Context **
!
End
```

Verify that static MPLS has been enabled on an interface, with label-action mapping for intermediate and egress LSRs.

Also verify that **`router mpls-static`** is configured in a context, with the LSP, next hop, out-label, and egress identified.

For more information about the requirements for static MPLS, see *Configuring MPLS*.

4. Examine the label-mapping with the **`show mpls-static lsp detail`** command.

```
[local]Redback#show mpls-static lsp detail
                  Static LSPs

LSP                  ID     Next-hop        Out-Label    Endpoint        State

                --- Static label-switched-path lsp1 ---

Tunnel id           : 1
Endpoint            : 52.0.0.101      Next Hop            : 25.0.101.2
State               : Up              Out Label           : 3
LSP Circuit         : Cct invalid
Outgoing Circuit    : 3/10:1023:63/1/1/6
Outgoing Intf grid  : 0x10000001
```

You can also enable label mapping debug messages with the **debug mpls-static lm** command.

5. Examine static MPLS LSPs in the forwarding table with the **show ip route lsp** command.

```
 [local]Redback#show ip route lsp
Codes: S - static, RSVP - RSVP, LDP - LDP, BGP - BGP
Type    Network             UpTime Interface       Label    LSP Circuit
> S     52.0.0.101/32      03:36:35 core-101        3
```

6. You can enable debug messages for a static MPLS circuit by using the **debug circuit mpls-static** command with the **all**, **lsp**, or **event** keywords.

4 Troubleshoot LDP Signaling

To troubleshoot LDP signaling issues, perform the tasks in Table 3.

Table 3 Tasks to Troubleshoot LDP Issues

Task	Command	Checked?
Step 1: Check the Forwarding Plane (LDP)	**ping mpls ldp** ***endpoint-ip-addr /prefix-length num-pings***	
Step 2: Verify that LDP LSPs Exist	**show mpls lsp**	
Step 3: Verify that MPLS and LDP Were Enabled on Their Interfaces	**show mpls interface** **show ldp interface**	
Step 4: Verify that LDP Neighbors are Functioning	**show ldp neighbor**	
Step 5: Check FEC to LDP binding	**show ldp binding**	

Table 3 Tasks to Troubleshoot LDP Issues

Task	Command	Checked?
Step 6: Troubleshoot Inactive LDP Binding	`show ip route` `show ip route registered prefix`	

Step 7: Collect LDP Debug Information	`debug ldp all`
	`debug ip routing all`
	`debug ldp filter`
	`debug ldp message`	

Caution!

Run the **`debug`** commands for a only short time to minimize performance impact.

4.1 Step 1: Check the Forwarding Plane (LDP)

To verify that an LDP LSP is forwarding correctly, run the **`ping mpls ldp`** ***`endpoint-ip-addr/prefix-length num-pings`*** command.

Enter the command on the ingress LSR for the LSP being tested, with the egress LSR as the target. (The endpoint IP address is typically the loopback address where the LSP terminates).

```
[local]R1#ping mpls ldp 172.16.57.5/32
Sending 5 100-byte MPLS echos to LDP 172.16.57.5/32, source 172.16.10.5,
    timeout is 1 second, send interval is 0 msec:
!!!!!
```

4.2 Step 2: Verify that LDP LSPs Exist

If pinging the egress LSR produces no response, you can run the **show mpls lsp** command to see whether LSPs have been created. You can also run this command to identify a specific LSP to ping or investigate further.

The following example shows details about the LDP LSPs:

```
[local]R1#show mpls lsp
Codes : S - MPLS-Static, R - RSVP, L - LDP, B - BGP
Type Endpoint      Direct Next-hop  Out Label  Adjacency Id
L    172.16.8.5/32    192.168.210.1    0          0x1300070
L    172.16.8.5/32    192.168.210.54   524295     0x8300070
L    172.16.8.6/32    192.168.210.1    524295     0x130001d
L    172.16.57.5/32   192.168.210.54   3          0x1300013
L    172.16.57.6/32   192.168.210.54   3          0x830006e
L    172.16.57.6/32   192.168.210.1    3          0x130001b
```

Add the optional **detail** keyword for additional detail.

Using the Adjacency ID, `0x8300070`, and top label, `0x80007`, from Section 4.1 on page 16, you can see that the Out Label `524295` in this output corresponds to the top label `0x80007` because they are both associated with the Adjacency ID `0x8300070`. Therefore, for this LSP, there are two possible direct next hops. However, the path is through `192.168.1.2` (it has both Out Label `524295` and Adjacency ID `0x8300070`).

If the output does not show an LSP for the loopback address of the endpoint router, verify that MPLS and LDP are enabled on the appropriate interfaces; see Section 4.3 on page 17.

4.3 Step 3: Verify that MPLS and LDP Are Enabled on Their Interfaces

If there are no LSPs, verify that MPLS and LDP were enabled on their interfaces by using the **show mpls interface** and **show ldp interface** commands. Command output should be similar to the following:

```
[local]R1#show mpls interface
  -- All MPLS Interfaces --
Inst Address/Mask       Name       Enabled  State  Bound to
1    172.16.10.5/32       loop       Yes      Up     Loopback
1    192.168.210.2/30     backbone1        Yes      Up     9/19
1    192.168.210.58/30    backbone2        Yes      Up     2/12

[local]R1#show ldp interface
Flag:  B - Bound, U - Up, D - Deleted, S - Stale, E - Hold expired
T - Bind Stale L - Loopback
Interface  Local Addr            Flag RemoteLSRId        HoldExpr
loop       172.16.20.5/32        BUL
backbone1  192.168.210.2/30      BU   100.1.1.2:0        14
backbone2  192.168.210.58/30     BU   100.1.1.4:0        12
```

The interfaces should be enabled and their states should be Up.

4.4 Step 4: Check the State of LDP Neighbors

If there are no LSPs, but the LDP interfaces are enabled and up, check the LDP neighbors with the **`show ldp neighbor`** command. Look for a state of `Oper` (operational) for the expected neighbors. The output should be similar to the following:

```
[local]R1#show ldp neighbor
PeerFlags:
A - LocalActiveOpen, D - Deleted, R - Reseting, E - OpenExtraDelay

N - OpenNoDelay, P - SetMD5Passwd, T - RetainRoute, F - FlushState

X - ExplicitNullEnabled, C - ExplicitNullStatusChanging

G - Graceful Restart Supported, L - Session Life Extended

V - Reachable Via RSVP-TE LSP
SHld - Session Holdtime Left, HHld - Hello Holdtime Left
NeighborAddr    LDP Identifier    State   Flag SHld HHld Interface
172.16.8.5      172.16.8.5:0       Oper    G    84   14   backbone1
172.16.8.6      172.16.8.6:0       Oper    G    69   31   none - remote
172.16.10.6     172.16.10.6:0      Oper    G    60   11   backbone2
                                                   41   none - remote
```

4.5 Step 5: Check FEC-to-LDP Binding

To verify a specific LSP that does not appear in the output of the **show ldp neighbor** command, check the FECs that the LDP has learned by using the **show ldp binding** command, which results in the following output. A missing FEC could provide information to further investigate the problem. Use the **detail** keyword to display detailed information. If the LDP binding is not active, see Step 6: Troubleshoot Inactive LDP Binding.

```
[local]R1#show ldp binding
 active binding, Local/In - local/input label binding
 From - source of remote label, Remote/Out - remote/output
label binding
Prefix/FEC          Learned-From    Local/In   Remote/Out Interface
10.21.1.0/24        local           3
                    100.1.1.2:0                3
                    100.1.1.4:0                3
                    100.1.1.3:0                3
100.1.1.1/32        local           3
                    100.1.1.2:0                524291
                    100.1.1.4:0                524291
                    100.1.1.3:0                524292
100.1.1.2/32        100.1.1.2:0     524291     3           backbone1
                    100.1.1.4:0                524292
                    100.1.1.3:0                524293
100.1.1.3/32        100.1.1.2:0     524295     524295      backbone1
                    100.1.1.4:0                524295      backbone2
                    100.1.1.3:0                3
100.1.1.4/32        100.1.1.2:0     524296     524296
                    100.1.1.4:0                3           backbone2
                    100.1.1.3:0                524294
192.168.1.0/30      local            3
                    100.1.1.2:0                3
                    100.1.1.4:0                524294
                    100.1.1.3:0                524295
192.168.1.4/30      local           3
                    100.1.1.2:0                524297
                    100.1.1.4:0                3
                    100.1.1.3:0                524296
192.168.1.8/30      100.1.1.2:0     524293     3           backbone1
                    100.1.1.4:0                524293
                    100.1.1.3:0                3
192.168.1.12/30     100.1.1.4:0     524294     3           backbone2
                    100.1.1.2:0                524294
                    100.1.1.3:0                3
192.168.16.24/30    local           3
```

4.6 Step 6: Troubleshoot Inactive LDP Binding

When the LDP binding is not active, use the **`show ip route`** and **`show ip route registered prefix`** commands to isolate the fault.

When the LDP binding is not active, check the following:

- Does the route up time indicate flapping issues?
- Does the route version in the output from both of these **`show ip route`** commands match?

In the following example, the **`show ip route`** output displays the version, `6871`, in decimal format in the `Best match Routing entry for` field. However, the **`show ip route registered prefix`** | **`begin`** output displays the version in a hexadecimal format (`0x1AD7`) in the `Return pfx ver` field. To determine if these versions match, convert the hexadecimal format into the decimal format. In decimal format of`0x1AD7` is `6871`, which matches the version in the **`show ip route`** output. This indicates that the RIB is operating correctly and has correctly updated LDP. If the versions do not match, contact your local technical support representative. You can also see the `Route Uptime` for evidence of flapping issues.

```
[local]R1#show ip route 172.16.57.5/24
    Best match Routing entry for 172.16.57.5/24  is
 172.16.8.6/24 , version 6871

    Route Uptime 1d05h

     Paths: total 2, best path count 2

    Route has been downloaded to following slots
     01/0, 04/0, 10/0

    Path information :

      Active path :
      Known via ospf 1, type-OSPF intra area, distance 110,
metric 2,
      Tag 0, Next-hop 26.1.1.1, NH-ID 0x30E00001, Adj ID: 0x1,
Interface to-tb2-
a
      Circuit 1/11:1023:63/1/1/18

      Active path :
      Known via ospf 1, type-OSPF intra area, distance 110,
metric 2,
      Tag 0, Next-hop 27.1.1.1, NH-ID 0x30E00001, Adj ID: 0x2,
Interface to-tb2-
b
      Circuit 1/12:1023:63/1/1/20

[local]R1show ip route registered prefix | begin 172.16.57.5/24
172.16.57.5/24      ldp
Version         : 0xE5       Lookup type     : 0x2
Return pfx ver : 0x1AD7     Return pfx      : 172.16.57.5/24
```

4.7 Step 7: Collect LDP Debug Information

If you have performed the troubleshooting steps in this section and the problem persists, you can collect debug information for further analysis by technical support representatives using the following **debug** commands:

- **debug ldp all**
- **debug ip routing all**
- **debug ip routing libso**
- **debug ip routing message**
- **debug ldp filter {interface if-name | neighbor ip-addr | prefix ip-addr/prefix-length [exact-match]}**—Use the **interface**, **neighbor**, or **prefix** keywords to enable the LDP debugging filter on an interface, for neighbors, or for prefixes.
- **debug ldp message {msg-type [detail] | {dump | receive | send}}**

For the full syntax for these commands, see the *Command List*.

Run these commands for a few minutes, save the output, and send it to technical support representatives. For more information, see *Data Collection Guideline for the SmartEdge Router*.

5 Troubleshoot RSVP Signaling

When packets are not being forwarded on an RSVP LSP, but signaling appears to be functioning properly, you should test whether the RSVP LSPs are up. Focus on the LSP that is reported as a problem to examine the problem in more detail.

To troubleshoot RSVP signaling issues, use the commands in Table 4.

Table 4 Tasks to Troubleshoot RSVP Issues

Task	Command	Notes	Checked ?
Step 1: Check Packet Forwarding	**ping mpls rsvp** ***lsp-name***		
Step 2: Verify that LSPs Exist and Determine Their States	**show mpls lsp** **show rsvp lsp**		
Step 3: Examine RSVP LSP Counters	**show rsvp counters**		
Step 4: Check the state of RSVP neighbors	**show rsvp neighbor**		
Step 5: Display Information About a Specific RSVP LSP	**show rsvp lsp** ***lsp-name***		
Step 6: Verify an ERO was Correctly Learned	**show rsvp explicit-route** ***er-name*** **show configuration rsvp**		
Step 7: Display information about an LSP route	**show ip route** ***end-ip-addr*** **detail**		
Step 8: Display Detailed RSVP Information	**show mpls lsp detail**		

Table 4 Tasks to Troubleshoot RSVP Issues

Task	Command	Notes	Checked ?
Step 9: Troubleshoot CSPF Route Calculations	**debug cspf** **show configuration** **show cspf database**		
Step 10: Collect Debug Information for Technical Support Representatives	**debug ip routing all** **debug lm download** **debug lm in-label** **debug lm lsp** **debug lm msg** **debug rsvp**	Run these commands for a short time only.	

5.1 Step 1: Check Packet Forwarding

To verify an RSVP LSP, use the **`ping mpls rsvp`** ***`lsp-name`*** command.

Enter the command on the ingress LSR for the LSP being tested. The name of the target LSP should be an LSP that originates on your node and ends on another node. (The number of transit hops is not important.) You cannot ping an egress or transit RSVP LSP.

The following example shows the ping response for the LSP `Crossed-primary-R2-R3`. A positive response verifies that a packet can pass through the LSP.

```
[local]R1#ping mpls rsvp Crossed-primary-R2-R3
Sending 5 100-byte MPLS echos to Crossed-primary-R2-R3, source 172.16.10.5,
    timeout is 1 second, send interval is 0 msec:
!!!!!
```

To view the path that the LSP takes, run the **`show rsvp lsp`** command as in the following example, which shows the explicit route, `R2-R6-R5-R4-R3` that has been learned for this LSP.

```
[local]R1#show rsvp lsp Crossed-primary-R2-R3

                --- RSVP LSP Crossed-primary-R2-R3 (Tunnel ID: 11) ---

Ingress             : 172.16.10.5     Endpoint            : 172.16.8.6
Origin              : Ingress         LSP State           : Up
Extended Tunnel ID  : 172.16.10.5     LSP ID              : 1
Traffic-Eng         : default         State Transitions   : 9
Downstream Nhop     : 192.168.210.54  Downstream Intf     : 192.168.210.53
Downstream Intf Name: ge-2/2
Downstream Nbr      : 192.168.210.54  Downstream Label    : 458761
Setup Priority      : 7               Holding Priority    : 0
Last Downstream Tx  : 4               Last Downstream Rx  : 6
Next Timer in (sec) : 9               Lifetime (sec)      : 157
Time to Die (sec)   : 150             B/W (Bytes/sec)     : 0
LSP cct             : 255/3:1023:63/0/1/34
IGP Shortcut        : Disabled        Exclusive Mapping   : No
Nnhop Label         : 458779
Nnhop Addr:         : 172.16.57.6
Session Attr        : Local-Protect Node-Protect May-Reroute Record-Label

Path Error messages :
Time: 2d01h, Node Address: 192.168.210.42, Code: Routing Problem,
      Flags: 0x0, Value: 0x5, Repeat cnt: 10
Time: 2d03h, Node Address: 192.168.210.57, Code: Routing Problem,
      Flags: 0x0, Value: 0x5, Repeat cnt: 7
Time: 2d03h, Node Address: 192.168.210.53, Code: Routing Problem,
      Flags: 0x0, Value: 0x7, Repeat cnt: 4
Time: 2d03h, Node Address: 192.168.210.57, Code: Notify Error,
      Flags: 0x0, Value: 0x3
Time: 2d03h, Node Address: 192.168.210.57, Code: Routing Problem,
      Flags: 0x0, Value: 0x5, Repeat cnt: 10

Use Explicit Route  : Yes             Record Route        : Yes
Explicit Route      : R2-R6-R5-R4-R3
LSP protected by LSP Crossed-backup-R2-R3
Recorded Route (hops: 4):
        172.16.10.6/32 (Protection Available), Label flags 1, value 458761
        172.16.57.6/32  Label flags 1, value 458779
        172.16.57.5/32 (Protection Available), Label flags 1, value 458780
        172.16.8.6/32  Label flags 1, value 0
```

5.2 Step 2: Verify that LSPs Exist and Determine Their States

You can run the **show mpls lsp** command to see whether LSPs have been created. You can also run this command to identify a specific LSP to ping or investigate further.

The following example shows details about the RSVP LSPs:

```
[local]R1#show mpls lsp
Codes : S - MPLS-Static, R - RSVP, L - LDP, B - BGP

Type Endpoint            Direct Next-hop  Out Label      Adjacency Id
R    172.16.8.5/32       192.168.210.54   458767         0x130006d
R    172.16.8.5/32       192.168.210.54   458762         0x1300070
R    172.16.8.5/32       192.168.210.1    0              0x1300010
R    172.16.8.6/32       192.168.210.54   458761         0x1300071
R    172.16.8.6/32       192.168.210.1    458754         0x1300040
R    172.16.57.5/32      192.168.210.54   458757         0x1300062
R    172.16.57.5/32      192.168.210.1    458764         0x1300064
R    172.16.57.6/32      192.168.210.54   458758         0x1300025
R    172.16.57.6/32      192.168.210.1    458769         0x1300066
```

You should see LSPs listed with type `R`. Use the `Endpoint` IP address and prefix length to investigate further.

You can also list the RSVP LSPs by running the **show rsvp lsp** command. Use this command to determine the LSP name to use to ping the LSP; the command produces output similar to the following:

```
[local]R1#show rsvp lsp
LSP                    TID Ingress         Endpoint        State FRR O Prtct
Local-backup-R2-R3     1   172.16.8.5      172.16.8.6      Up        T None
Straight-primary-R2-R1 3   172.16.8.5      172.16.10.5     Up        E None
Straight-backup-R2-R1  3   172.16.8.5      172.16.10.5     Up        E None
Bypass-link-R2-R1      5   172.16.8.5      172.16.10.5     Up        E None
::::
::::
Straight-backup-R3-R6  8   172.16.8.6      172.16.10.6     Up        T None
Bypass-link-R3-R6      10  172.16.8.6      172.16.10.6     Up        T None
Crossed-primary-R3-R1 11   172.16.8.6      172.16.10.5     Up        E None
Crossed-backup-R3-R1  11   172.16.8.6      172.16.10.5     Up        E None
Local-backup-R1-R6     1   172.16.10.5     172.16.10.6     Up        I Back
Local-primary-R1-R6    1   172.16.10.5     172.16.10.6     Up        I Prim
Straight-backup-R1-R4  3   172.16.10.5     172.16.57.5     Up        I Back
Straight-primary-R1-R4 3   172.16.10.5     172.16.57.5     Up    5   I Prim
```

Use this command to collect the following information for further investigation.

- `LSP`—Name of the LSP. Each RSVP LSP has a specific name.
- `ID`—Tunnel ID of the LSP.
- `Ingress`—IP address of the router from which the LSP originates, usually the loopback address of the router in the local context.
- `Endpoint`—Destination address of the LSP, usually the IP address of the destination router to which the packet is sent. It can be a loopback address configured on the destination router.
- `State`—State of the LSP: Up, Down, Shut, or Stale.

- `FRR`—If the LSP has an FRR bypass LSP that can protect it, this field displays the tunnel ID of that bypass LSP. Otherwise, this field is empty.
- `Origin`—Origin for the type of LSP relative to the location of the local router in the path: I (or Ingress) for ingress, E (or Egress) for egress, or T (or Transit) for transit.
- `Prtct`—Protection characteristic of the LSP. For example, if an LSP does not protect other LSPs but is protected by other LSPs, `Prim` (for primary LSP) is listed. If an LSP protects other LSPs (a backup, or a backup of a backup), `Back` is listed. If an LSP has no protection characteristic, `None` is listed. If an LSP is a bypass LSP, it is pre-established to protect an LSP that traverses either a specific link (link bypass LSP) or a specific node (node bypass LSP), and `Bypass` is listed.

5.3 Step 3: Examine RSVP LSP Counters

Use the **`show rsvp counters lsp`** command to display evidence about the state of RSVP LSPs.

In this example, the counter `Stale LSPs` is the number of LSPs that moved to the Stale state due to local or neighbor restarts. `Stale LSPs Recovered` shows the number of previously stale LSPs that returned to the Up state.

```
[local]R1#show rsvp counters lsp
                --- Global RSVP Counters ---
         LSP Counters
      Total Sessions:         26           Total LSPs:          27
        Ingress LSPs:          7          Egress LSPs:          18
        Transit LSPs:          2          Backup LSPs:          1
             Up LSPs:         23            Down LSPs:          4
         Active LSPs:         23         Backup2 LSPs:          0
         Bypass LSPs:          0        Rerouted LSPs:          0
          Stale LSPs:          5 Stale LSPs Recovered:          5
```

5.4 Step 4: Check the State of RSVP Neighbors

Use the **`show rsvp neighbor`** command to display information about the state of the neighbors on all interfaces, as in the following example:

```
[local]R1#show rsvp neighbor

         --- All RSVP Neighbors ---

Nbr Address      GR    Rest-Time  Recov-Time State
192.168.210.1    No    0          0          Up
192.168.210.54   No    0          0          Up
192.168.210.57   No    0          0          Up
```

This summary includes the following information for all RSVP neighbors:

- `Nbr Address`—Neighbor address: IP Address
- `GR`—Graceful Restart Enabled: Yes or No
- `Rest-Time`—Number of seconds in which the Nbr must send a Hello message after restarting
- `Recov-Time`—Number of seconds that Nbr must refresh LSPs after restarting
- `State`—`Up`, `Down`, `Hello Disabled`, or `Restarting`.

5.5 Step 5: Display Information About a Specific RSVP LSP

If you ping an LSP and receive no response, you can display information on the LSP using the **show rsvp lsp *lsp-name*** command, which produces the following output:

```
[local]R1#show rsvp lsp Crossed-primary-R2-R3

                --- RSVP LSP Crossed-primary-R2-R3 (Tunnel ID: 11) ---

Ingress             : 172.16.10.5     Endpoint            : 172.16.8.6
Origin              : Ingress         LSP State           : Up
Extended Tunnel ID  : 172.16.10.5     LSP ID              : 1
Traffic-Eng         : default         State Transitions   : 9
Downstream Nhop     : 192.168.210.54  Downstream Intf     : 192.168.210.53
Downstream Intf Name: ge-2/2
Downstream Nbr      : 192.168.210.54  Downstream Label    : 458761
Setup Priority      : 7               Holding Priority    : 0
Last Downstream Tx  : 4               Last Downstream Rx  : 6
Next Timer in (sec) : 9               Lifetime (sec)      : 157
Time to Die (sec)   : 150             B/W (Bytes/sec)     : 0
LSP cct             : 255/3:1023:63/0/1/34
IGP Shortcut        : Disabled        Exclusive Mapping   : No
Nnhop Label         : 458779
Nnhop Addr:         : 172.16.57.6
Session Attr        : Local-Protect Node-Protect May-Reroute Record-Label

Path Error messages :
Time: 2d01h, Node Address: 192.168.210.42, Code: Routing Problem,
      Flags: 0x0, Value: 0x5, Repeat cnt: 10
Time: 2d03h, Node Address: 192.168.210.57, Code: Routing Problem,
      Flags: 0x0, Value: 0x5, Repeat cnt: 7
Time: 2d03h, Node Address: 192.168.210.53, Code: Routing Problem,
      Flags: 0x0, Value: 0x7, Repeat cnt: 4
Time: 2d03h, Node Address: 192.168.210.57, Code: Notify Error,
      Flags: 0x0, Value: 0x3
Time: 2d03h, Node Address: 192.168.210.57, Code: Routing Problem,
      Flags: 0x0, Value: 0x5, Repeat cnt: 10

Use Explicit Route  : Yes             Record Route        : Yes
Explicit Route      : R2-R6-R5-R4-R3
LSP protected by LSP Crossed-backup-R2-R3
Recorded Route (hops: 4):
        172.16.10.6/32 (Protection Available), Label flags 1, value 458761
        172.16.57.6/32  Label flags 1, value 458779
        172.16.57.5/32 (Protection Available), Label flags 1, value 458780
        172.16.8.6/32  Label flags 1, value 0
```

Look for an LSP state of `Up`. Use the data about the neighboring nodes to understand the LSP path from the ingress to the egress node, as well as other useful information. For example, use the `Endpoint` IP address (`172.16.8.6`) from this command in the **show ip route *ip-addr* detail** command to verify that the route is in the RIB; see Section 5.7 on page 29.

5.6 Step 6: Verify an ERO Was Correctly Learned

To confirm that the Explicit Route Object (ERO) in the **show rsvp lsp *name*** command has been correctly learned and is consistent with the configuration, use the **show rsvp explicit-route** command to see the explicit route. Verify the EROs with the **show configuration rsvp** command. The following example shows the output for the explicit route of interest, R2-R6-R5-R4-R3:

```
[local]R1#show rsvp explicit-route R2-R6-R5-R4-R3
Explicit Route: R2-R6-R5-R4-R3 Hop Count: 4 ID: 10
  Length: 8 Addr: 192.168.210.54/32
  Length: 8 Addr: 192.168.210.42/32
  Length: 8 Addr: 192.168.210.57/32
  Length: 8 Addr: 192.168.210.25/32
```

This is consistent with the ERO configuration for RSVP in the excerpt from the output of the **show configuration rsvp** command:

```
. . .
   explicit-route R2-R6-R5-R4-R3
   next-hop 192.168.210.54
   next-hop 192.168.210.42
   next-hop 192.168.210.57
   next-hop 192.168.210.25
. . .
```

5.7 Step 7: Display Information About an LSP Route

To examine the LSP Crossed-primary-R2-R3, from Section 5.5 on page 28, enter the **show ip route *end-ip-addr* detail** command. In the output, look for LSPs in the RIB that were downloaded to the various slots and known through RSVP. The endpoint address we're interested in is the loopback address of the egress LSR, in this case, R3.

```
[local]R1#show ip route 172.16.8.6 detail
    Longest match Routing entry for 172.16.8.6/32 is 172.16.8.6/32 , version 143
    Route Uptime 4d00h
    Paths: total 4, best path count 3 (includes 2 lsp best paths)

    Route has been downloaded to following slots
     01/0, 02/0, 03/0

    Path information :

      Active path :
      Known via isis PBN1, type-IS-IS level-2, distance 115, metric 1501,
      Tag 0, Next-hop 192.168.210.54, NH-ID 0x31100003, Adj ID: 0x1000001, Interface ge-2/2
      Circuit 2/2:1023:63/1/1/22

      Known via bgp 64512, type-Internal BGP, distance 200, metric 0,
      Tag 0, Next-hop 172.16.8.6

      Active LSP path ineligible for fib, only used for recursion
      Known via rsvp distance 6, metric 0,
      Tag 0, Next-hop 192.168.210.1, NH-ID 0x30E00002, Adj ID: 0x130004D, Interface ge-2/1
      Circuit 255/3:1023:63/0/1/17
      Label 458753

      Active LSP path ineligible for fib, only used for recursion
      Known via rsvp distance 6, metric 0,
      Tag 0, Next-hop 192.168.210.54, NH-ID 0x30E00002, Adj ID: 0x1300011, Interface ge-2/2
      Circuit 255/3:1023:63/0/1/2
      Label 458763
```

5.8 Step 8: Display Detailed RSVP Information

To display detailed information about RSVP paths, use the **`show mpls lsp detail`** command. Use the following command in combination with pinging the egress LSR to see if the `Tx Packet` and `Tx Bytes` counters increment after pinging the LSP.

```
 [local]R1#show mpls lsp detail

------------------------------------------------------------
Type                : RSVP            LSP Circuit         : 255/3:1023:63/0/1/16
Egress              : 172.16.8.5/32   Client ID           : 2
Traffic-Eng         : default         RIB Table ID        : 0x0
Direct Next Hop     : 192.168.210.1   Direct Next Hop Cct : 2/1:1023:63/1/1/20
Adjacency ID        : 0x1300048       Out Label Count     : 1
Tunnel ID           : 0x9             Flags               : 0x44010
Alt label           : 0x7001a         Alt action          : PUSH
Alt Egress          : 192.168.210.54   Alt LSP Cct         : 255/3:1023:63/0/1/15
Out Label Stack     : 0
Special Procedures  :
Tx Packets          : 0               Tx Bytes            : 0

------------------------------------------------------------
Type                : RSVP            LSP Circuit         : 255/3:1023:63/0/1/15
Egress              : 172.16.8.5/32   Client ID           : 2
Traffic-Eng         : default         RIB Table ID        : 0x0
Direct Next Hop     : 192.168.210.54  Direct Next Hop Cct : 2/2:1023:63/1/1/22
Adjacency ID        : 0x130003f       Out Label Count     : 1
Tunnel ID           : 0x80000009      Flags               : 0x84010
Out Label Stack     : 458778
Special Procedures  :
Tx Packets          : 0               Tx Bytes            : 0

------------------------------------------------------------
Type                : RSVP            LSP Circuit         : 255/3:1023:63/0/1/17
Egress              : 172.16.8.6/32   Client ID           : 2
Traffic-Eng         : default         RIB Table ID        : 0x0
Direct Next Hop     : 192.168.210.1   Direct Next Hop Cct : 2/1:1023:63/1/1/20
Adjacency ID        : 0x130004d       Out Label Count     : 1
Tunnel ID           : 0x8000000b      Flags               : 0x84010
Out Label Stack     : 458753
Special Procedures  :
Tx Packets          : 10              Tx Bytes            : 1180

------------------------------------------------------------
--(more)--
```

After entering this command, ping the LSP of interest:

```
[local]R1#ping mpls rsvp Crossed-primary-R2-R3
Sending 5 100-byte MPLS echos to Crossed-primary-R2-R3, source 172.16.10.5,
    timeout is 1 second, send interval is 0 msec:
!!!!!
```

After pinging the LSP, enter the **`show mpls lsp detail`** command again. In the following excerpt from the output, the `Tx Packets` counter has incremented to 15. The circuit `255/3:1023:63/0/1/17` was learned with the **`show ip route end-ip-addr detail`** command, as shown in Section 5.7 on page 29.

```
[local]R1#show mpls lsp detail
. . .
------------------------------------------------------------
Type                : RSVP            LSP Circuit         : 255/3:1023:63/0/1/17
Egress              : 172.16.8.6/32   Client ID           : 2
Traffic-Eng         : default         RIB Table ID        : 0x0
Direct Next Hop     : 192.168.210.1   Direct Next Hop Cct : 2/1:1023:63/1/1/20
Adjacency ID        : 0x130004d       Out Label Count     : 1
Tunnel ID           : 0x8000000b      Flags               : 0x84010
Out Label Stack     : 458753
Special Procedures  :
Tx Packets          : 15              Tx Bytes            : 1770

------------------------------------------------------------
. . .
```

5.9 Step 9: Troubleshoot CSPF Route Handling

CSPF works with link-state routing protocols such as OSPF and IS-IS to automate the provisioning of label-switched paths (LSPs) in core networks and differentiate levels of quality of service (QoS) in Layer 2 and Layer 3 service applications. It calculates LSPs in an MPLS TE domain on a single path from the headend (ingress) router to the tailend (egress) router, based on a set of criteria called constraints. The headend router uses CSPF to calculate the best path; other routers in the domain do not calculate CSPF. When you use CSPF, the ingress and egress routers must be part of the same MPLS TE domain. When the constraints are not met for any links, CSPF removes these links from its network topology and then runs the Shortest Path First (SPF) algorithm on the remaining LSP links. For example, if the bandwidth constraint is not met, all the TE LSP links that do not meet this constraint are removed from the network topology. CSPF then calculates the SPF on the remaining LSP links and generates a list of nodes called a path list. This path list of explicit routes provides the shortest path (that meets the constraints) through the network to the destination. The CSPF calculation creates an ordered set of IP addresses mapping to the next-hop addresses in the TE LSP, and the Explicit Route Object (ERO), which defines the path that RSVP must take from the ingress router to the egress router. CSPF sends these results to RVSP; RSVP then uses this path to signal the LSP to reserve resources.

Use the following steps to troubleshoot problems with the CSPF route calculations:

1. Before beginning to troubleshoot CSPF problems, enable CSPF debug messages using the **`debug cspf`** command.

2. Check the CSPF configuration by entering the **`show configuration`** command. Ensure that the following requirements are met:

   - A global router ID is configured with the **`router-id`** command.
   - The ingress and egress routers for CSPF are both part of the same MPLS TE domain.
   - CSPF is enabled with the **`cspf`** command

3. Also in the configuration, examine the following constraint settings for the CSPF links and correct them if necessary:

   - Administrative group (**admin-group** command)
   - Nodes and links to exclude from the CSPF path computation (**exclude** command)
   - Next-hop entry for an RSVP explicit route (**next-hop** command)
   - Maximum number of routers that the tunnel can traverse, including ingress and egress routers (**hop-limit** command)
   - Minimum bandwidth required for an LSP to be applied (**minimum-bandwidth** command
   - Priority of a tunnel (**priority** command).

4. Examine the CSPF database with the **show cspf database** command.

5.10 Step 10: Collect Debug Information for Technical Support Representatives

If you have performed the troubleshooting steps in this section and the problem persists, you can use the following commands to collect debug information for further analysis by your local technical support representative:

- **debug ip routing all**
- **debug lm download**
- **debug lm in-label**
- **debug lm lsp [*ip-addr/prefix-length*]**
- **debug lm msg [*ip-addr/prefix-length*]**
- **debug lm rib**
- **debug rsvp**

For the full syntax for these commands, see *Command List*.

Run these commands for a few minutes.and save the output to send to customer support. For more information, see *Data Collection Guideline for the SmartEdge Router*.