Chapter 8

Examining a CSPF Failure

The ingress router determines the physical path for each label-switched path (LSP) by applying a Constrained Shortest Path First (CSPF) algorithm to the information in the traffic engineering database (TED). This chapter describes a real-world scenario in which the CSPF algorithm fails because of the incorrect association of links with administrative groups (also known as link coloring). It discusses some basic approaches to monitoring and examining a CSPF failure, including how, when, and why you use specific commands. This chapter also includes an examination of an example CSPF log file, traffic engineering database, and corrective action for the example scenario. (See Table 12.)

Table 12: Checklist for Examining a CSPF Failure

Examining a CSPF Failure Tasks	
Case Study for a CSPF Failure on page 88	
1. Verify That the LSP Is Established on page 89	show mpls lsp extensive
2. Check the Administrative Group Configuration on page 90	show configuration protocols mpls show mpls interface show ted database extensive *nodeID*
Examining a CSPF Failure on page 94	
1. Verify the CSPF Failure on page 94	clear mpls lsp show mpls lsp extensive
2. Examine the CSPF Log File on page 95	monitor start *filename* show log *filename* monitor stop
3. Examine the Traffic Engineering Database on page 97	show ted database extensive For output filtered for color: show ted database extensive *nodeID* | match "(NodeID | To: | Color)"
4. Check the Administrative Group Configuration on R5 on page 99	edit [edit protocols mpls] show delete interface so-0/0/1 admin-group set interface so-0/0/0 admin-group red show commit

Case Study for a CSPF Failure

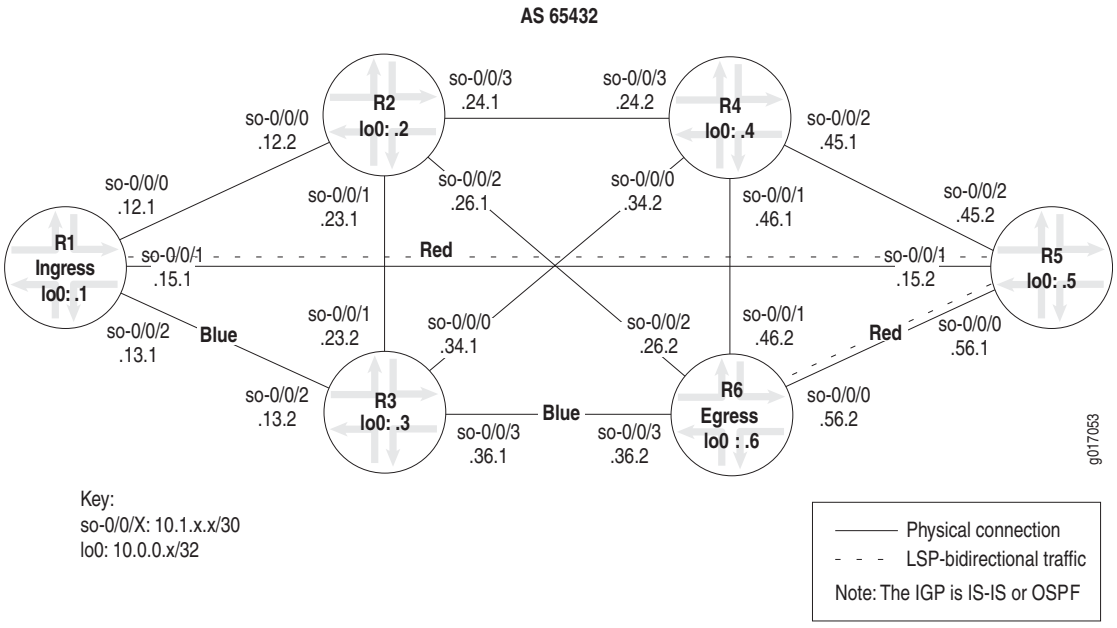
Purpose This case study presents a Multiprotocol Label Switching (MPLS) network topology and CSPF failure scenario designed to demonstrate techniques and commands that are particularly useful when addressing CSPF problems in your network. The focus of the study is the incorrect association of user-provided constraints, specifically administrative groups (also known as link coloring).

When calculating a path, the CSPF algorithm factors in user–provided constraints. The ingress router determines the physical path for each LSP by applying a CSPF algorithm to the information in the traffic engineering database. CSPF is a shortest-path-first (SPF) algorithm that has been modified to take into account constraints when calculating the shortest path across the network. Links that do not comply with the restrictions are removed from the tree and cannot be factored into the resulting SPF calculations.

CSPF integrates topology link-state information that is learned from interior gateway protocol (IGP) traffic engineering extensions and is maintained in the traffic engineering database. The information stored in the traffic engineering database includes attributes associated with the state of network resources.

The network topology shown in Figure 4 illustrates a network in which the LSP is constrained by administrative group coloring (also known as link coloring), and CSPF tracing is configured on the ingress router R1. In this example, the LSP is forced to transit R5 in accordance with the restrictions imposed.

Figure 4: CSPF Topology with Administrative Group Coloring



The network shown in Figure 4 is an MPLS router-only network with SONET interfaces. For more details about the MPLS network topology, see “Configuring CSPF Tracing” on page 73.

The MPLS network shown in Figure 4 on page 88 is configured with administrative group coloring as follows:

- The LSP R1-to-R6 is established with R1 as the ingress router and R6 as the egress router.
- The required path to R6 transits R5 on the red links. The inclusion of red coloring is not strictly necessary. To force the LSP to transit R5, you could color the links on R3 and R2 blue and then exclude the blue links.
- Both red and blue colors are used with the include and exclude statements to ensure that the LSP always transits R5. For information on configuring administrative group coloring, see the *JUNOS MPLS Applications Configuration Guide*.

Steps To Take To check that the network is configured correctly and the LSP is established, follow these steps:

1. Verify That the LSP Is Established on page 89
2. Check the Administrative Group Configuration on page 90

Step 1: Verify That the LSP Is Established

Purpose Check that the LSP shown in Figure 4 on page 88 is established and traversing the path from R1 to R6 through the red links.

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

```
user@host> show mpls lsp extensive
user@host> show mpls lsp
```

Sample Output

```
user@R1> show mpls lsp extensive | no-more
Ingress LSP: 1 sessions

10.0.0.6
  From: 10.0.0.1, State: Up, ActiveRoute: 1, LSPname: R1-to-R6
  ActivePath:  (primary)
  LoadBalance: Random
  Metric: 100
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
 *Primary                    State: Up
          Include: red    Exclude: blue
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 20)
 10.1.15.2 S 10.1.56.2 S
    Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node
10=SoftPreempt):
          10.1.15.2 10.1.56.2
    6 May 11 19:31:42 Selected as active path
    5 May 11 19:31:42 Record Route:  10.1.15.2 10.1.56.2
    4 May 11 19:31:42 Up
    3 May 11 19:31:42 Originate Call
    2 May 11 19:31:42 CSPF: computation result accepted
    1 May 11 19:31:12 CSPF failed: no route toward 10.0.0.6[5 times]
  Created: Wed May 11 19:29:17 2005
Total 1 displayed, Up 1, Down 0
[...Output truncated...]
```

Sample Output 2

```
[edit protocols mpls]
user@R5# run show mpls lsp
Ingress LSP: 0 sessions
Total 0 displayed, Up 0, Down 0

Egress LSP: 0 sessions
Total 0 displayed, Up 0, Down 0

Transit LSP: 2 sessions
To              From            State   Rt Style Labelin Labelout LSPname
10.0.0.1        10.0.0.6        Up       1  1 FF  100352        3 R6-to-R1
10.0.0.6        10.0.0.1        Up       1  1 FF  100384        3 R1-to-R6
Total 2 displayed, Up 2, Down 0
```

What It Means Sample Output 1 from ingress router R1 shows that LSP R1-to-R6 is successfully established as indicated by the Explicit Route Object (ERO) 10.1.15.2 S 10.1.56.2 S, the log message CSPF: computation result accepted, and State: Up. Also, the LSP is routing packets correctly over the red links, avoiding the blue links or the links without any coloring. See Step 3 in "Configuring CSPF Tracing" on page 73 for information on the steps CSPF takes to select a path.

Sample Output 2 from transit router R5 shows that LSP R1-to-R6 is transiting R5 as expected.

Step 2: Check the Administrative Group Configuration

Action To check the administrative group configuration, enter the following JUNOS CLI operational mode commands, or issue the show command at the [edit protocols mpls] hierarchy level, as shown in the example below:

```
user@host> show configuration protocols mpls
user@host> show mpls interface
user@host> show ted database extensive nodeID
```

Sample Output 1

```
[edit protocols mpls]
user@R1# show
traceoptions {
    file cspf;
    flag cspf;
    flag cspf-node;
    flag cspf-link;
}
admin-groups {
    blue 4;
    red 8;
}
label-switched-path R1-to-R6 {
    to 10.0.0.6;
    metric 100;
    admin-group {
        include red;
        exclude blue;
    }
}
interface so-0/0/0.0;
interface so-0/0/1.0 {
    admin-group red;
}
```

```
interface so-0/0/2.0 {
    admin-group blue;
}
interface fxp0.0 {
    disable;
}

[edit protocols mpls]
user@R3# show
admin-groups {
    blue 4;
}
interface fxp0.0 {
    disable;
}
interface so-0/0/0.0;
interface so-0/0/1.0;
interface so-0/0/2.0 {
interface so-0/0/3.0 {
    admin-group blue;
}

[edit protocols mpls]
user@R5# show
admin-groups {
    red 8;
}
interface fxp0.0 {
    disable;
}
interface so-0/0/0.0 {
    admin-group red;
}
interface so-0/0/1.0;
interface so-0/0/2.0;

[edit protocols mpls]
user@R6# show
admin-groups {
    blue 4;
    red 8;
}
label-switched-path R6-to-R1 {
    to 10.0.0.1;
}
interface so-0/0/0.0 {
    admin-group red;
}
interface so-0/0/1.0;
interface so-0/0/2.0;
interface so-0/0/3.0 {
    admin-group blue;
}
```

Sample Output 2

```
useruser@R1> show mpls interface
Interface        State       Administrative groups
so-0/0/0.0       Up         <none>
so-0/0/1.0       Up          red
so-0/0/2.0       Up          blue
```

```
user@R1> show mpls interface
Interface        State       Administrative groups
so-0/0/0.0       Up          <none>
so-0/0/1.0       Up          red
so-0/0/2.0       Up          blue

user@R3> show mpls interface
Interface        State       Administrative groups
so-0/0/0.0       Up          <none>
so-0/0/1.0       Up          <none>
so-0/0/2.0       Up          <none>
so-0/0/3.0       Up          blue

user@R5> show mpls interface
Interface        State       Administrative groups
so-0/0/0.0       Up          red
so-0/0/1.0       Up          <none>
so-0/0/2.0       Up          <none>

user@R6> show mpls interface
Interface        State       Administrative groups
so-0/0/0.0       Up          red
so-0/0/1.0       Up          <none>
so-0/0/2.0       Up          <none>
so-0/0/3.0       Up          blue
```

Sample Output 3

```
user@R1> show ted database extensive R1
TED database: 6 ISIS nodes 6 INET nodes
NodeID: R1.00(10.0.0.1)
  Type: Rtr, Age: 665 secs, LinkIn: 3, LinkOut: 3
  Protocol: IS-IS(2)
    To: R2.00(10.0.0.2), Local: 10.1.12.1, Remote: 10.1.12.2
      Color: 0 <none>
      Metric: 10
      Static BW: 155.52Mbps
      Reservable BW: 155.52Mbps
      Available BW [priority] bps:
          [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
          [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
      Interface Switching Capability Descriptor(1):
        Switching type: Packet
        Encoding type: Packet
        Maximum LSP BW [priority] bps:
          [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
          [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
    To: R5.00(10.0.0.5), Local: 10.1.15.1, Remote: 10.1.15.2
      Color: 0x100 red
      Metric: 10
      Static BW: 155.52Mbps
      Reservable BW: 155.52Mbps
      Available BW [priority] bps:
          [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
          [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
      Interface Switching Capability Descriptor(1):
        Switching type: Packet
        Encoding type: Packet
        Maximum LSP BW [priority] bps:
          [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
          [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
    To: R3.00(10.0.0.3), Local: 10.1.13.1, Remote: 10.1.13.2
      Color: 0x10 blue
      Metric: 10
      Static BW: 155.52Mbps
```

```
Reservable BW: 155.52Mbps
Available BW [priority] bps:
    [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
    [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
Interface Switching Capability Descriptor(1):
  Switching type: Packet
  Encoding type: Packet
  Maximum LSP BW [priority] bps:
    [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
    [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
```

What It Means Sample Output 1 shows that administrative group coloring is correctly configured on all relevant routers. Administrative groups red and blue are configured at the [edit protocols mpls] hierarchy level, and relevant interfaces are associated with each administrative group correctly.

R3 is configured with blue coloring and the include and exclude statements are included in the configuration of R1 to ensure that LSP R1-to-R6 always transits R5. The inclusion of red coloring is not strictly necessary. To force the LSP to transit R5, you could color the links on R2 and R3 blue and then exclude the blue links. Red coloring is included in this example to demonstrate the fact that the CSPF algorithm excludes links that do not have a color configured, when the include statement is configured at the [edit protocols mpls] hierarchy level.

In addition, ingress router R1 has CSPF tracing configured in preparation for gathering information when the CSPF algorithm fails later in this example.

Sample Output 2 shows that the correct interfaces are associated with the red and blue administration groups on R1, R3, R5, and R6.

Sample Output 3 confirms that link coloring is correctly reported in the traffic engineering database for R1. Not shown is the traffic engineering database output for the remaining routers, which is similar to the R1 output, and correct.

Examining a CSPF Failure

Purpose When a local CSPF failure indicates that no path meets the constraints configured for the LSP, you must perform CSPF-based tracing and be familiar with the contents of the traffic engineering database to resolve the problem. See "Examine the Traffic Engineering Database" on page 97 for an analysis of the traffic engineering database.

NOTE: If an LSP does not establish immediately, wait at least a minute or so before taking diagnostic or corrective action. This is because the RSVP retry timer is set to a 30-second default, resulting in a slight delay before the correct state of the LSP is available.

Steps To Take To examine a CSPF failure, follow these steps:

1. Verify the CSPF Failure on page 94
2. Examine the CSPF Log File on page 95
3. Examine the Traffic Engineering Database on page 97
4. Check the Administrative Group Configuration on R5 on page 99

Step 1: Verify the CSPF Failure

Purpose To simulate a configuration error on the network, router R5 has the administrative group coloring removed from interface so-0/0/0. The result is a CSPF failure at R5 because there is no longer a path between R1 and R6 that includes the red color.

Action To confirm that the LSP is down and verify the configuration on routers R1 and R5, enter the following JUNOS CLI operational mode commands:

```
user@host> clear mpls lsp
user@host> show mpls lsp extensive
```

Sample Output 1

```
user@R1> clear mpls lsp

[edit protocols mpls]
user@R1# run show mpls lsp extensive
Ingress LSP: 1 sessions

10.0.0.6
  From: 0.0.0.0, State: Dn, ActiveRoute: 0, LSPname: R1-to-R6
  ActivePath: (none)
  LoadBalance: Random
  Metric: 100
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
  Primary                  State: Dn
          Include: red    Exclude: blue
    Will be enqueued for recomputation in 24 second(s).
    9 May 11 20:12:28 CSPF failed: no route toward 10.0.0.6
    8 May 11 20:12:28 Clear Call
    7 May 11 20:12:28 Deselected as active
    6 May 11 19:31:42 Selected as active path
    5 May 11 19:31:42 Record Route:  10.1.15.2 10.1.56.2
```

```
    4 May 11 19:31:42 Up
    3 May 11 19:31:42 Originate Call
    2 May 11 19:31:42 CSPF: computation result accepted
    1 May 11 19:31:12 CSPF failed: no route toward 10.0.0.6[5 times]
  Created: Wed May 11 19:29:17 2005
Total 1 displayed, Up 0, Down 1
[...Output truncated...]
```

Sample Output 2

```
[edit protocols mpls]
user@R5# run show mpls lsp
Ingress LSP: 0 sessions
Total 0 displayed, Up 0, Down 0

Egress LSP: 0 sessions
Total 0 displayed, Up 0, Down 0

Transit LSP: 1 sessions
To              From            State   Rt Style Labelin Labelout LSPname
10.0.0.1        10.0.0.6        Up       1  1 FF  100352        3 R6-to-R1
Total 1 displayed, Up 1, Down 0
```

What It Means

Sample Output 1 from ingress router R1 shows that the clear mpls lsp command was issued to confirm that R1 cannot reestablish LSP R1-to-R6. The sample output from the show mpls lsp extensive command shows that LSP R1-to-R6 is down, State: Dn and ActivePath: (None); and that the CSPF has failed, CSPF failed: no route toward 10.0.0.6.

Sample Output 2 from transit router R5 shows that LSP R1-to-R6 is not included in the output, indicating that the LSP is not transiting R5.

Most network problems appear as a local CSPF failure, as shown in the sample output. The CSPF failure indicates that no path meeting the constraints for the LSP can be found in the router's traffic engineering database. To resolve these problems effectively, use CSPF tracing on the ingress router, and analyze the traffic engineering database to locate the node that should meet the constraints.

Step 2: Examine the CSPF Log File

Purpose

After you have confirmed that the LSP is down, obtain more information about the possible cause of the failure.

NOTE: To obtain useful information from the CSPF log file, make sure that CSPF tracing is configured on the ingress router. For more information on configuring CSPF tracing, see "Configuring CSPF Tracing" on page 73.

Action

To examine the CSPF log file, enter the following JUNOS CLI operational mode commands:

```
user@host> monitor start filename
user@host> show log filename
```

NOTE: To stop monitoring CSPF, issue the monitor stop command.

Sample Output `user@R1> monitor start cspf`

```
[edit protocols mpls]
user@R1# run show log cspf-failed3
May 27 10:22:23 trace_on: Tracing to "/var/log/cspf" started
May 27 10:22:29 CSPF adding path R1-to-R6(primary ) to CSPF queue 1
May 27 10:22:29 CSPF creating CSPF job
May 27 10:22:29
May 27 10:22:29 CSPF for path R1-to-R6(primary ), begin at R1.00 , starting
May 27 10:22:29         path include: 0x00000100    << administration group red
May 27 10:22:29         path exclude: 0x00000010    << administration group blue
May 27 10:22:29         bandwidth: CT0=0bps ; setup priority: 0; random
May 27 10:22:29 CSPF final destination 10.0.0.6
May 27 10:22:29 CSPF starting from R1.00 (10.0.0.1) to 10.0.0.6, hoplimit 254
May 27 10:22:29         constraint include 0x00000100
May 27 10:22:29         constraint exclude 0x00000010
May 27 10:22:29    Node R1.00 (10.0.0.1) metric 0, hops 0, avail 32000 32000 32000 32000
May 27 10:22:29      Link 10.1.12.1->10.1.12.2(R2.00/10.0.0.2) metric 10 color 0x00000000 bw 155.52Mbps
May 27 10:22:29         Reverse Link for 10.1.12.1->10.1.12.2 is 10.1.12.2->10.1.12.1
May 27 10:22:29         link fails include 0x00000100
May 27 10:22:29      Link 10.1.15.1->10.1.15.2(R5.00/10.0.0.5) metric 10 color 0x00000100 bw 155.52Mbps
May 27 10:22:29         Reverse Link for 10.1.15.1->10.1.15.2 is 10.1.15.2->10.1.15.1
May 27 10:22:29         link's interface switch capability descriptor #1
May 27 10:22:29           encoding: Packet, switching: Packet
May 27 10:22:29         link passes constraints
May 27 10:22:29      Link 10.1.13.1->10.1.13.2(R3.00/10.0.0.3) metric 10 color 0x00000010 bw 155.52Mbps
May 27 10:22:29         Reverse Link for 10.1.13.1->10.1.13.2 is 10.1.13.2->10.1.13.1
May 27 10:22:29         link fails include 0x00000100
May 27 10:22:29    Node R5.00 (10.0.0.5) metric 10, hops 1, avail 32000 32000 32000 32000
May 27 10:22:29      Link 10.1.15.2->10.1.15.1(R1.00/10.0.0.1) metric 10 color 0x00000100 bw 155.52Mbps
May 27 10:22:29         skipped: end point already visited
May 27 10:22:29      Link 10.1.45.2->10.1.45.1(R4.00/10.0.0.4) metric 10 color 0x00000000 bw 155.52Mbps
May 27 10:22:29         Reverse Link for 10.1.45.2->10.1.45.1 is 10.1.45.1->10.1.45.2
May 27 10:22:29         link fails include 0x00000100
May 27 10:22:29      Link 10.1.56.1->10.1.56.2(R6.00/10.0.0.6) metric 10 color 0x00000000 bw 155.52Mbps
May 27 10:22:29         Reverse Link for 10.1.56.1->10.1.56.2 is 10.1.56.2->10.1.56.1
May 27 10:22:29         link fails include 0x00000100
May 27 10:22:29 CSPF completed in 0s
May 27 10:22:29 CSPF couldn't find a route to 10.0.0.6
May 27 10:22:29 CSPF for R1-to-R6 done!
monitor stop
```

What It Means The sample output shows that the monitor start cspf command was issued to start displaying entries in the cspf log file in real time. The cspf log file is generated by the routing protocol process after the file is configured with the traceoptions statement at the [edit protocols mpls] hierarchy level. In this example, the cspf log file is configured with the cspf, cspf-node, and cspf-link flags to provide the most granular information about the steps taken by the CSPF algorithm. For information on configuring CSPF tracing, see “Configuring CSPF Tracing” on page 73.

The only link that passes the color constraint is between R1 and R5, 10.1.15.0/32. The CSPF algorithm is a locally run algorithm, which makes its calculations on a given router. When the CSPF algorithm runs on R5, it prunes 10.1.15.2 and selects 10.1.56.1 to send the message to R6.The link between R5 and R6 10.1.56.0/32 does not pass the color constraints, indicating a problem with R5. At this stage, it is useful to examine the traffic engineering database to determine which link on R5 should be associated with the red color.

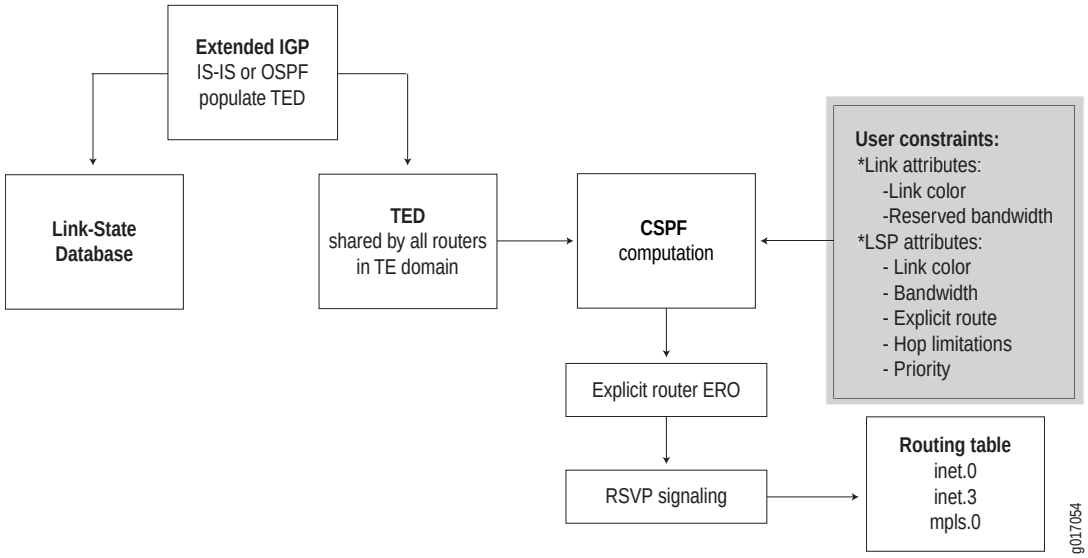
Step 3: Examine the Traffic Engineering Database

Purpose Examining the traffic engineering database is another way to locate the node that should meet the constraints but does not. Once identified, you can concentrate your troubleshooting efforts on why that node is not being represented accurately in the database.

The contents of the traffic engineering database are consistent among all routers within a given traffic engineering domain. Therefore, you can issue the show ted database command from any router in the same traffic engineering domain to obtain more granular information about the CSPF failure.

CSPF integrates topology link-state information that is learned from the IGP traffic engineering extensions and maintained in the traffic engineering database. The information stored in the traffic engineering database includes attributes associated with the state of the network resources (such as total link bandwidth, reserved link bandwidth, available link bandwidth, and link color). When calculating a path, the CSPF algorithm factors in user–provided information such as bandwidth requirements, maximum allowed hop count, and administrative groups, all of which are obtained from user configuration. (See Figure 5).

Figure 5: User–Provided Constraints



Action To examine the traffic engineering database, enter the following JUNOS CLI operational mode commands:

```
user@host> show ted database extensive
user@host> show ted database extensive NodeID | match "(NodeID|To:|Color)"
```

Sample Output 1

```
[edit protocols mpls]
user@R1# run show ted database extensive
TED database: 6 ISIS nodes 6 INET nodes
[...Output truncated...]
NodeID: R5.00(10.0.0.5)
  Type: Rtr, Age: 103 secs, LinkIn: 3, LinkOut: 3
  Protocol: IS-IS(2)
    To: R1.00(10.0.0.1), Local: 10.1.15.2, Remote: 10.1.15.1
      Color: 0x100 red
      Metric: 10
      Static BW: 155.52Mbps
      Reservable BW: 155.52Mbps
      Available BW [priority] bps:
          [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
          [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
      Interface Switching Capability Descriptor(1):
        Switching type: Packet
        Encoding type: Packet
        Maximum LSP BW [priority] bps:
          [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
          [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
    To: R4.00(10.0.0.4), Local: 10.1.45.2, Remote: 10.1.45.1
      Color: 0 <none>
      Metric: 10
      Static BW: 155.52Mbps
      Reservable BW: 155.52Mbps
      Available BW [priority] bps:
          [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
          [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
      Interface Switching Capability Descriptor(1):
        Switching type: Packet
        Encoding type: Packet
        Maximum LSP BW [priority] bps:
          [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
          [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
    To: R6.00(10.0.0.6), Local: 10.1.56.1, Remote: 10.1.56.2
      Color: 0 <none>
      Metric: 10
      Static BW: 155.52Mbps
      Reservable BW: 155.52Mbps
      Available BW [priority] bps:
          [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
          [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
      Interface Switching Capability Descriptor(1):
        Switching type: Packet
        Encoding type: Packet
        Maximum LSP BW [priority] bps:
          [0] 155.52Mbps   [1] 155.52Mbps  [2] 155.52Mbps  [3] 155.52Mbps
          [4] 155.52Mbps   [5] 155.52Mbps  [6] 155.52Mbps  [7] 155.52Mbps
[...Output truncated...]
```

Sample Output 2

```
[edit protocols]
user@R1# run show ted database extensive R5.00 | match "(NodeID|To:|Color)"
NodeID: R5.00(10.0.0.5)
    To: R1.00(10.0.0.1), Local: 10.1.15.2, Remote: 10.1.15.1
      Color: 0x100 red
    To: R4.00(10.0.0.4), Local: 10.1.45.2, Remote: 10.1.45.1
      Color: 0 <none>
    To: R6.00(10.0.0.6), Local: 10.1.56.1, Remote: 10.1.56.2
      Color: 0 <none>
    To: R1.00(10.0.0.1), Local: 10.1.15.2, Remote: 10.1.15.1
      Color: 0x100 red
```

```
To: R4.00(10.0.0.4), Local: 10.1.45.2, Remote: 10.1.45.1
  Color: 0 <none>
To: R6.00(10.0.0.6), Local: 10.1.56.1, Remote: 10.1.56.2
  Color: 0 <none>
```

What It Means Sample Output 1 from ingress router R1 shows a wealth of information on each node in the network, although only a portion is included in this example. The output shows the total number of IS-IS and INET nodes in the traffic engineering domain. The portion of the traffic engineering database shown represents a node (R5), and the Type field indicates Rtr (router). The Type field could also indicate Net (network) if the node were a pseudo node. The node (R5) has three input and output links that are running IS-IS Level 2, Protocol: IS-IS(2). The links lead to nodes R1, R4, and R6. The local address and remote address for each link is specified. The information on each node includes administrative groups (Color:), metrics, static bandwidth, reservable bandwidth, and available bandwidth priority level. The information contained in the traffic engineering database should be the same across all routers in the same traffic engineering domain. For a detailed description of the fields in the output of the show ted database extensive command, see the *JUNOS Routing Protocols and Policies Command Reference*.

Sample Output 2 shows filtered output that allows you to focus on exactly what is missing or incorrect.

Both outputs confirm that the link between R1 and R5, 10.1.15.0/32, is associated with the red color, while the link between R5 and R6, 10.1.56.0/32, is not associated with a color. In the network shown in Figure 4 on page 88, for the LSP to establish correctly, link 10.1.56.1 must be associated with the red color.

Step 4: Check the Administrative Group Configuration on R5

Purpose Focus on R5 to determine which interfaces are associated with the red color, and make any necessary corrections.

Action To check the administrative group configuration on R5 and make any necessary corrections, enter the following JUNOS CLI commands:

```
user@R5> edit
[edit protocols mpls]
user@R5# show
user@R5# delete interface so-0/0/1 admin-group
user@R5# set interface so-0/0/0 admin-group red
user@R5# show
user@R5# commit
```

Sample Output 1

```
user@R5> edit
Entering configuration mode

[edit protocols mpls]
user@R5# show
admin-groups {
    red 8;
}
interface fxp0.0 {
    disable;
}
interface so-0/0/0.0;
interface so-0/0/1.0 {      <<<incorrect interface configured with admin-group
    admin-group red;
}
interface so-0/0/2.0;
```

Sample Output 2

```
[edit protocols mpls]
user@R5# delete interface so-0/0/1 admin-group

[edit protocols mpls]
user@R5# set interface so-0/0/0 admin-group red

[edit protocols mpls]
user@R5# show
admin-groups {
    red 8;
    blue 4;
}
interface fxp0.0 {
    disable;
}
interface so-0/0/0.0 {      <<<correct interface configured with admin-group
    admin-group red;
}
interface so-0/0/1.0;
interface so-0/0/2.0;

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

Sample Output 3

```
user@R1> show mpls lsp
Ingress LSP: 1 sessions
To              From            State Rt ActivePath       P     LSPname
10.0.0.6        10.0.0.1        Up     1                  *     R1-to-R6
Total 1 displayed, Up 1, Down 0

Egress LSP: 1 sessions
To              From            State   Rt Style Labelin Labelout LSPname
10.0.0.1        10.0.0.6        Up       0  1 FF       3        - R6-to-R1
Total 1 displayed, Up 1, Down 0

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

What It Means Sample Output 1 from transit router R5 shows that at the [edit protocols mpls] hierarchy level, interface so-0/0/1 is incorrectly configured with the admin-group red statement. The so-0/0/0 interface should be configured with the admin-group red statement.

Sample Output 2 shows the steps taken to correct the configuration. The administration group has been deleted from so-0/0/1 and so-0/0/0 is now associated with the red color.

Sample Output 3 shows that LSP R1-to-R6 is established.