Chapter 3

Local Protection in an MPLS Network

The JUNOS software implementation of Multiprotocol Label Switching (MPLS) provides several complementary mechanisms for protecting against Resource Reservation Protocol (RSVP)-signaled LSP failures, including path protection (primary and secondary paths), and local protection (fast reroute, link protection, and node-link protection). This chapter describes local protection supported by the JUNOS software. (See Table 6.)

The terms *node* and *router* are used interchangeably throughout this book.

Table 6: Local Protection Checklist

Local Protection Tasks	Command or Action
Local Protection Overview on page 27	
One-to-One Backup Overview on page 28	
Configuring and Verifying One-to-One Backup on page 29	
1. Configure One-to-One Backup on page 29	[edit] edit protocols mpls [edit protocols mpls] set label-switched-path *lsp-path-name* to *address* set label-switched-path *lsp-path-name* fast-reroute (optional) set label-switched-path *lsp-path-name* primary *primary-name* (optional) set path *path-name address* loose show commit
2. Verify One-to-One Backup on page 31	show mpls lsp ingress extensive show rsvp session
Many-to-One Link Protection (Facility Backup) Overview on page 37	
Configuring and Verifying Link Protection on page 38	
1. Configure Link Protection on page 38	[edit] edit protocols rsvp interface *type-fpc/pic/port* [edit protocols rsvp interface *type-fpc/pic/port*] set link-protection show top edit protocols mpls label-switched-path *lsp-path-name* [edit protocols mpls label-switched-path *lsp-path-name*] set link-protection show commit

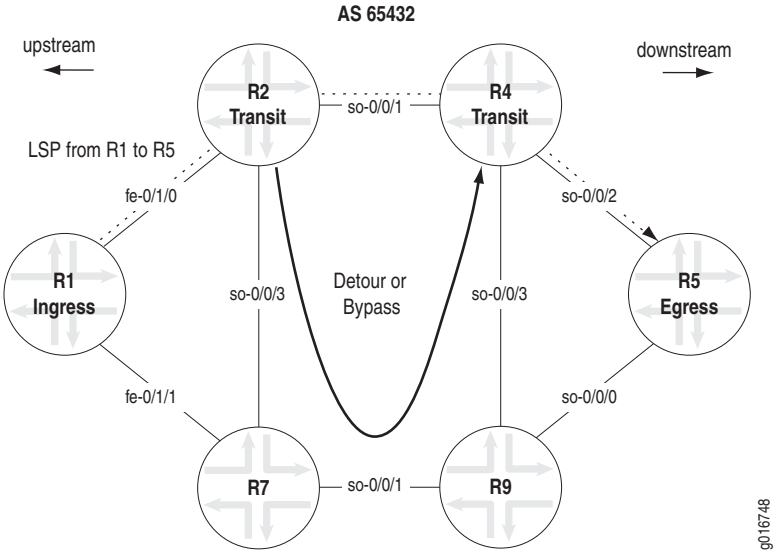
Local Protection Tasks	Command or Action
2. Verify That Link Protection Is Up on page 40	show mpls lsp extensive show rsvp session detail show rsvp interface
Node-Link Protection Overview on page 44	
Configuring and Verifying Node-Link Protection on page 45	
1. Configure Node-Link Protection on page 45	[edit] edit protocols mpls label-switched-path *lsp-path-name* [edit protocols mpls label-switched-path *lsp-path-name*] set node-link-protection show edit protocols rsvp interface *type-fpc/pic/port* [edit protocols rsvp interface *type-fpc/pic/port*] set link-protection show commit Include the node-link-protection statement on any other ingress routers that have LSPs requiring use of the bypass path. Include the link-protection statement on routers with outgoing interfaces in the LSP.
2. Verify That Node-Link Protection Is Up on page 47	show mpls lsp show mpls lsp extensive show rsvp interface show rsvp interface extensive show rsvp session detail
Conclusion on page 52	
Related Information on page 52	

Local Protection Overview

Local protection attempts to address the disadvantages of path protection by focusing on a single resource at a time (link or node), in contrast to path protection which attempts to provide protection for the entire path from the ingress router to the egress router. Double-booking of resources, unnecessary protection and nondeterministic switchover times are the main disadvantages of path protection, arising from protection at the ingress router for the entire path. By providing focused protection from the ingress of a single resource at a time, local protection addresses the disadvantages of path protection, minimizing the amount of time during which traffic is lost, while utilizing resources efficiently.

In Figure 4, if the LSP from R1 to R5 fails on the link between R2 and R4, a detour or bypass path is pre-established quickly, and traffic is redirected around the failure, until the ingress router moves the LSP to a new path that does not use the failed link.

Figure 4: Local Protection



In the Juniper Networks implementation, local protection methods are defined by the number of LSPs protected by the backup path. When one LSP is protected by one backup path, the backup path is referred to as a detour and the protection method is called fast reroute (one-to-one backup). When many LSPs are protected by one backup path, the backup path is referred to as a bypass and the protection method is called facility backup. The purpose of facility backup is to protect a link or node (facility). Facility backup can be used for protecting either a link or a node (and its associated links), also referred to as node-link protection.

The following local protection methods are discussed in this section:

- One-to-One Backup Overview on page 28
- Many-to-One Link Protection (Facility Backup) Overview on page 37
- Node-Link Protection Overview on page 44

One-to-One Backup Overview

Fast reroute or one-to-one backup is a short-term solution to reduce packet loss associated with a particular LSP. One-to-one backup is appropriate under the following circumstances:

- Protection of a small number of LSPs relative to the total number of LSPs.
- Path selection criteria, such as bandwidth, priority, and link coloring for detour paths is critical.
- Control of individual LSPs is important.

In one-to-one backup, the ingress router adds the fast reroute object to the RSVP Path message requesting that downsteam routers establish detours. Downstream routers generate Path messages and establish detours to avoid the downstream link or node. Detours are always calculated to avoid the immediate downstream link and node, providing against both link and node failure, as shown in Figure 5.

Figure 5: One-to-One Backup Detours

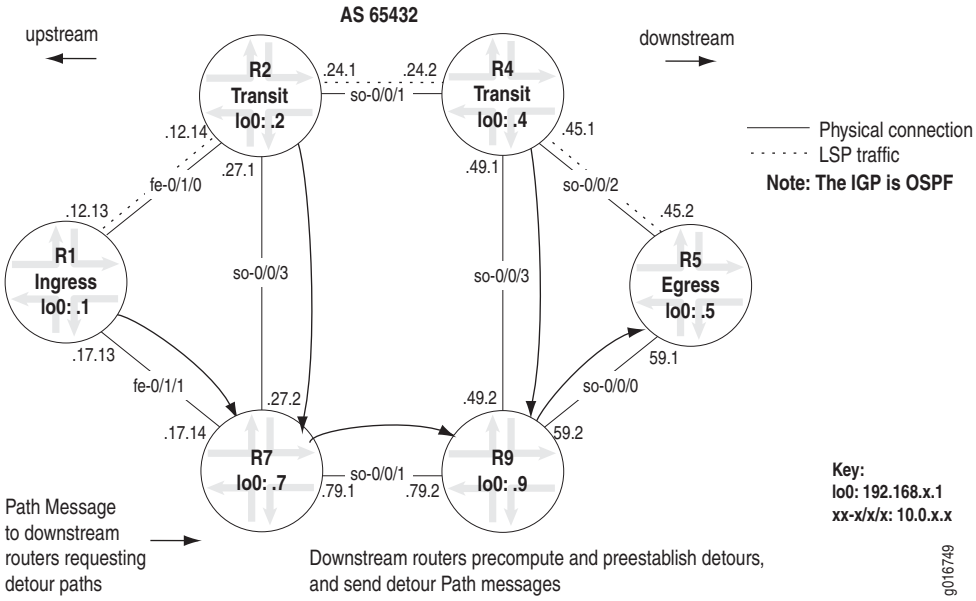


Figure 5 shows a network with one LSP configured from the ingress router R1 to the egress router R5, transiting R2 and R4. The following detours are established:

- R1 creates a detour to R5 via R7 and R9
- R2 creates a detour to R5 via R7 and R9
- R4 creates a detour to R5 via R9

Each detour is dedicated to a particular LSP traversing the router (one detour to one LSP). If the network topology has insufficient links and nodes, it may be impossible to establish a detour. Also, detour paths are not meant for long-term use because they may provide inadequate bandwidth and can result in congestion on the links. As soon as the ingress router calculates a new path avoiding the failure, traffic is redirected along the new path, detours are torn down, and new detours established.

Configuring and Verifying One-to-One Backup

The following sections describe the steps you must take to configure and verify one-to-one backup.

- Configure One-to-One Backup on page 29
- Verify One-to-One Backup on page 31

Step 1: Configure One-to-One Backup

The following steps show the commands you must issue to configure a LSP with fast reroute and a primary path. The show command output includes bandwidth and hop limit for your information only. Bandwidth and hop limit are not configured on R1. You can configure bandwidth and hop limit using the bandwidth and hop-limit statements at the [edit protocols mpls lsp *lsp-path-name*] hierarchy level.

NOTE: It is not necessary to issue the fast-reroute statement on the transit or egress routers.

Action To configure one-to-one backup on the ingress router, follow these steps:

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

   ```
   [edit]
   user@R1# edit protocols mpls
   ```

2. Configure the LSP:

   ```
   [edit protocols mpls]
   user@R1# set label-switched-path  lsp-path-name to address
   ```

   For example:

   ```
   [edit protocols mpls]
   user@R1# set label-switched-path r1-to-r5 to 192.168.5.1
   ```

3. Configure one-to-one backup (fast reroute):

   ```
   [edit protocols mpls]
   user@R1# set label-switched-path lsp-path-name fast-reroute
   ```

   For example:

   ```
   [edit protocols mpls]
   user@R1# set label-switched-path r1-to-r5 fast-reroute
   ```

4. (Optional) Configure a primary path:

   [edit protocols mpls]
   user@R1# **set label-switched-path** *lsp-path-name* **primary** *primary-name*

   For example:

   [edit protocols mpls]
   user@R1# **set label-switched-path r1-to-r5 primary via-r2**

5. (Optional) Configure the primary ERO list:

   [edit protocols mpls]
   user@R1# **set path** *path-name address* **loose**

   For example:

   [edit protocols mpls]
   user@R1# **set path via-r2 10.0.12.14 loose**

6. Verify and commit the configuration:

   [edit protocols mpls]
   user@R1# **show**
   user@R1# **commit**

Sample Output

```
[edit protocols mpls]
user@R1# show
label-switched-path r1-to-r5 {
    to 192.168.5.1;
    fast-reroute;
    primary via-r2;
    bandwidth bps; # Bandwidth for the LSP
    hop-limit number; # Maximum number of routers the LSP can
                                          traverse
}
path via-r2 {
    10.0.12.14 loose;
}
[...Output truncated...]

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

What It Means

When the fast-reroute statement is configured, the ingress router signals all downstream routers to compute and preestablish a detour path for the LSP, using the Constrained Shortest Path First (CSPF) algorithm on the information in the local router's traffic engineering database (TED). By default, when the detour path is calculated by CSPF, the detour path inherits the same administrative group constraints (link coloring or resource classes) as the main LSP.

Step 2: Verify One-to-One Backup

You can verify that one-to-one backup is established by examining the ingress router and the other routers in the network.

Action To verify one-to-one backup, enter the following JUNOS CLI operational mode commands:

```
user@host> show mpls lsp ingress extensive
user@host> show rsvp session
```

Sample Output The following sample output is from the ingress router R1 in the network shown in Figure 5 on page 28:

```
user@R1> show mpls lsp ingress extensive
Ingress LSP: 1 sessions

192.168.5.1
  From: 192.168.1.1, State: Up, ActiveRoute: 0, LSPname: r1-to-r5
  ActivePath: via-r2 (primary)
  FastReroute desired
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
 *Primary   via-r2           State: Up
    SmartOptimizeTimer: 180
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 3)
 10.0.12.14 S 10.0.24.2 S 10.0.45.2 S
    Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node
10=SoftPreempt):
          10.0.12.14(flag=9) 10.0.24.2(flag=1) 10.0.45.2
    8 May 11 14:51:46 Fast-reroute Detour Up
    7 May 11 14:50:55 Record Route:  10.0.12.14(flag=9) 10.0.24.2(flag=1)
10.0.45.2
    6 May 11 14:50:55 Record Route:  10.0.12.14(flag=9) 10.0.24.2 10.0.45.2
    5 May 11 14:50:52 Selected as active path
    4 May 11 14:50:52 Record Route:  10.0.12.14 10.0.24.2 10.0.45.2
    3 May 11 14:50:52 Up
    2 May 11 14:50:52 Originate Call
    1 May 11 14:50:52 CSPF: computation result accepted
  Created: Thu May 11 14:50:52 2006
Total 1 displayed, Up 1, Down 0
```

What It Means The sample output from R1 shows that the FastReroute desired object was included in the Path messages for the LSP, allowing R1 to select the active path for the LSP and establish a detour path to avoid R2.

In line 8, Fast-reroute Detour Up shows that the detour is operational. Lines 6 and 7 indicate that transit routers R2 and R4 have established their detour paths.

R2, 10.0.12.14, includes (flag=9), indicating that node protection is available for the downstream node and link. R4, 10.0.24.2, includes (flag=1), indicating that link protection is available for the next downstream link. In this case, R4 can protect only the downstream link because the node is the egress router R5, which cannot be protected. For more information about flags, see the *JUNOS Feature Guide*.

The output for the show mpls lsp extensive command does not show the actual path of the detour. To see the actual links used by the detour paths, you must use the show rsvp session ingress detail command.

Sample Output The following sample output is from the ingress router R1 in the network shown in Figure 5 on page 28.

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

192.168.5.1
  From: 192.168.1.1, LSPstate: Up, ActiveRoute: 0
  LSPname: r1-to-r5, LSPpath: Primary
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: 100848
  Resv style: 1 FF, Label in: -, Label out: 100848
  Time left:    -, Since: Thu May 11 14:17:15 2006
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 1 receiver 9228 protocol 0
  FastReroute desired
  PATH rcvfrom: localclient
  Adspec: sent MTU 1500
  Path MTU: received 1500
  PATH sentto: 10.0.12.14 (fe-0/1/0.0) 35 pkts
  RESV rcvfrom: 10.0.12.14 (fe-0/1/0.0) 25 pkts
  Explct route: 10.0.12.14 10.0.24.2 10.0.45.2
  Record route: <self> 10.0.12.14 10.0.24.2 10.0.45.2
    Detour is Up
    Detour Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
    Detour adspec: sent MTU 1500
    Path MTU: received 1500
    Detour PATH sentto: 10.0.17.14 (fe-0/1/1.0) 23 pkts
    Detour RESV rcvfrom: 10.0.17.14 (fe-0/1/1.0) 20 pkts
    Detour Explct route: 10.0.17.14 10.0.79.2 10.0.59.1
    Detour Record route: <self> 10.0.17.14 10.0.79.2 10.0.59.1
    Detour Label out: 100848
Total 1 displayed, Up 1, Down 0
```

What It Means The sample output from R1 shows the RSVP session of the main LSP. The detour path is established, Detour is Up. The physical path of the detour is displayed in Detour Explct route. The detour path uses R7 and R9 as transit routers to reach R5, the egress router.

Sample Output The following sample output is from the first transit router R2 in the network shown in Figure 5 on page 28:

```
user@R2> show rsvp session transit detail
Transit RSVP: 1 sessions

192.168.5.1
  From: 192.168.1.1, LSPstate: Up, ActiveRoute: 1
  LSPname: r1-to-r5, LSPpath: Primary
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: 100448
  Resv style: 1 FF, Label in: 100720, Label out: 100448
  Time left:  126, Since: Wed May 10 16:12:21 2006
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 5 receiver 9216 protocol 0
  FastReroute desired
  PATH rcvfrom: 10.0.12.13 (fe-0/1/0.0) 173 pkts
  Adspec: received MTU 1500 sent MTU 1500
  PATH sentto: 10.0.24.2 (so-0/0/1.0) 171 pkts
  RESV rcvfrom: 10.0.24.2 (so-0/0/1.0) 169 pkts
  Explct route: 10.0.24.2 10.0.45.2
  Record route: 10.0.12.13 <self> 10.0.24.2 10.0.45.2
```

```
    Detour is Up
    Detour Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
    Detour adspec: received MTU 1500 sent MTU 1500
    Path MTU: received 1500
    Detour PATH sentto: 10.0.27.2 (so-0/0/3.0) 169 pkts
    Detour RESV rcvfrom: 10.0.27.2 (so-0/0/3.0) 167 pkts
    Detour Explct route: 10.0.27.2 10.0.79.2 10.0.59.1
    Detour Record route: 10.0.12.13 <self> 10.0.27.2 10.0.79.2 10.0.59.1
    Detour Label out: 100736
Total 1 displayed, Up 1, Down 0
```

What It Means The sample output from R2 shows the detour is established (Detour is Up) and avoids R4, and the link connecting R4 and R5 (10.0.45.2). The detour path is through R7 (10.0.27.2) and R9 (10.0.79.2) to R5 (10.0.59.1), which is different from the explicit route for the detour from R1. R1 has the detour passing through the 10.0.17.14 link on R7, while R1 is using the 10.0.27.2 link. Both detours merge at R9 through the 10.0.79.2 link to R5 (10.0.59.1).

Sample Output The following sample output is from the second transit router R4 in the network shown in Figure 5 on page 28:

```
user@R4> show rsvp session transit detail
Transit RSVP: 1 sessions

192.168.5.1
  From: 192.168.1.1, LSPstate: Up, ActiveRoute: 1
  LSPname: r1-to-r5, LSPpath: Primary
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: 3
  Resv style: 1 FF, Label in: 100448, Label out: 3
  Time left:  155, Since: Wed May 10 16:15:38 2006
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 5 receiver 9216 protocol 0
  FastReroute desired
  PATH rcvfrom: 10.0.24.1 (so-0/0/1.0) 178 pkts
  Adspec: received MTU 1500 sent MTU 1500
  PATH sentto: 10.0.45.2 (so-0/0/2.0) 178 pkts
  RESV rcvfrom: 10.0.45.2 (so-0/0/2.0) 175 pkts
  Explct route: 10.0.45.2
  Record route: 10.0.12.13 10.0.24.1 <self> 10.0.45.2
    Detour is Up
    Detour Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
    Detour adspec: received MTU 1500 sent MTU 1500
    Path MTU: received 1500
    Detour PATH sentto: 10.0.49.2 (so-0/0/3.0) 176 pkts
    Detour RESV rcvfrom: 10.0.49.2 (so-0/0/3.0) 175 pkts
    Detour Explct route: 10.0.49.2 10.0.59.1
    Detour Record route: 10.0.12.13 10.0.24.1 <self> 10.0.49.2 10.0.59.1
    Detour Label out: 100352
Total 1 displayed, Up 1, Down 0
```

What It Means The sample output from R4 shows the detour is established (Detour is Up) and avoids the link connecting R4 and R5 (10.0.45.2). The detour path is through R9 (10.0.49.2) to R5 (10.0.59.1). Some of the information is similar to that found in the output for R1 and R2. However, the explicit route for the detour is different, going through the link connecting R4 and R9 (so-0/0/3 or 10.0.49.2.

Sample Output The following sample output is from R7, which is used in the detour path in the network shown in Figure 5 on page 28:

```
user@R7> show rsvp session transit detail
Transit RSVP: 1 sessions, 1 detours

192.168.5.1
  From: 192.168.1.1, LSPstate: Up, ActiveRoute: 1
  LSPname: r1-to-r5, LSPpath: Primary
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: 100368
  Resv style: 1 FF, Label in: 100736, Label out: 100368
  Time left:  135, Since: Wed May 10 16:14:42 2006
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 5 receiver 9216 protocol 0
  Detour branch from 10.0.27.1, to skip 192.168.4.1, Up
    Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
    Adspec: received MTU 1500
    Path MTU: received 0
    PATH rcvfrom: 10.0.27.1 (so-0/0/3.0) 179 pkts
    Adspec: received MTU 1500 sent MTU 1500
    PATH sentto: 10.0.79.2 (so-0/0/1.0) 177 pkts
    RESV rcvfrom: 10.0.79.2 (so-0/0/1.0) 179 pkts
    Explct route: 10.0.79.2 10.0.59.1
    Record route: 10.0.12.13 10.0.27.1 <self> 10.0.79.2 10.0.59.1
    Label in: 100736, Label out: 100368
  Detour branch from 10.0.17.13, to skip 192.168.2.1, Up
    Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
    Adspec: received MTU 1500
    Path MTU: received 0
    PATH rcvfrom: 10.0.17.13 (fe-0/1/1.0) 179 pkts
    Adspec: received MTU 1500
    PATH sentto: 10.0.79.2 (so-0/0/1.0) 0 pkts
    RESV rcvfrom: 10.0.79.2 (so-0/0/1.0) 0 pkts
    Explct route: 10.0.79.2 10.0.59.1
    Record route: 10.0.17.13 <self> 10.0.79.2 10.0.59.1
    Label in: 100752, Label out: 100368
Total 1 displayed, Up 1, Down 0
```

What It Means The sample output from R7 shows the same information as for a regular transit router used in the primary path of the LSP: the ingress address (192.168.1.1), the egress address (192.168.5.1), and the name of the LSP (r1-to-r5). Two detour paths are displayed; the first to avoid R4 (192.168.4.1) and the second to avoid R2 (192.168.2.1). Because R7 is used as a transit router by R2 and R4, R7 can merge the detour paths together as indicated by the identical Label out value (100368) for both detour paths. Whether R7 receives traffic from R4 with a label value of 100736 or from R2 with a label value of 100752, R7 forwards the packet to R5 with a label value of 100368.

Sample Output The following sample output is from R9, which is a router used in the detour path in the network shown in Figure 5 on page 28:

```
user@R9> show rsvp session transit detail
Transit RSVP: 1 sessions, 1 detours

192.168.5.1
  From: 192.168.1.1, LSPstate: Up, ActiveRoute: 1
  LSPname: r1-to-r5, LSPpath: Primary
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: 3
  Resv style: 1 FF, Label in: 100352, Label out: 3
```

```
  Time left:  141, Since: Wed May 10 16:16:40 2006
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 5 receiver 9216 protocol 0
  Detour branch from 10.0.49.1, to skip 192.168.5.1, Up
    Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
    Adspec: received MTU 1500
    Path MTU: received 0
    PATH rcvfrom: 10.0.49.1 (so-0/0/3.0) 183 pkts
    Adspec: received MTU 1500 sent MTU 1500
    PATH sentto: 10.0.59.1 (so-0/0/0.0) 182 pkts
    RESV rcvfrom: 10.0.59.1 (so-0/0/0.0) 183 pkts
    Explct route: 10.0.59.1
    Record route: 10.0.12.13 10.0.24.1 10.0.49.1 <self> 10.0.59.1
    Label in: 100352, Label out: 3
  Detour branch from 10.0.27.1, to skip 192.168.4.1, Up
    Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
    Adspec: received MTU 1500
    Path MTU: received 0
  Detour branch from 10.0.17.13, to skip 192.168.2.1, Up
    Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
    Adspec: received MTU 1500
    Path MTU: received 0
    PATH rcvfrom: 10.0.79.1 (so-0/0/1.0) 181 pkts
    Adspec: received MTU 1500
    PATH sentto: 10.0.59.1 (so-0/0/0.0) 0 pkts
    RESV rcvfrom: 10.0.59.1 (so-0/0/0.0) 0 pkts
    Explct route: 10.0.59.1
    Record route: 10.0.12.13 10.0.27.1 10.0.79.1 <self> 10.0.59.1
    Label in: 100368, Label out: 3
Total 1 displayed, Up 1, Down 0
```

What It Means The sample output from R9 shows that R9 is the penultimate router for the detour path, the explicit route includes only the egress link address (10.0.59.1), and the Label out value (3) indicates that R9 has performed penultimate-hop label popping. Also, the detour branch from 10.0.27.1 does not include path information because R7 has merged the detour paths from R2 and R4. Notice that the Label out value in the detour branch from 10.0.17.13 is 100368, the same value as the Label out value on R7.

Sample Output The following sample output is from the egress router R5 in the network shown in Figure 5 on page 28:

```
user@R5> show rsvp session egress detail
Egress RSVP: 1 sessions, 1 detours

192.168.5.1
  From: 192.168.1.1, LSPstate: Up, ActiveRoute: 0
  LSPname: r1-to-r5, LSPpath: Primary
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: -
  Resv style: 1 FF, Label in: 3, Label out: -
  Time left:  119, Since: Thu May 11 14:44:31 2006
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 1 receiver 9230 protocol 0
  FastReroute desired
  PATH rcvfrom: 10.0.45.1 (so-0/0/2.0) 258 pkts
  Adspec: received MTU 1500
  PATH sentto: localclient
  RESV rcvfrom: localclient
  Record route: 10.0.12.13 10.0.24.1 10.0.45.1 <self>
  Detour branch from 10.0.49.1, to skip 192.168.5.1, Up
```

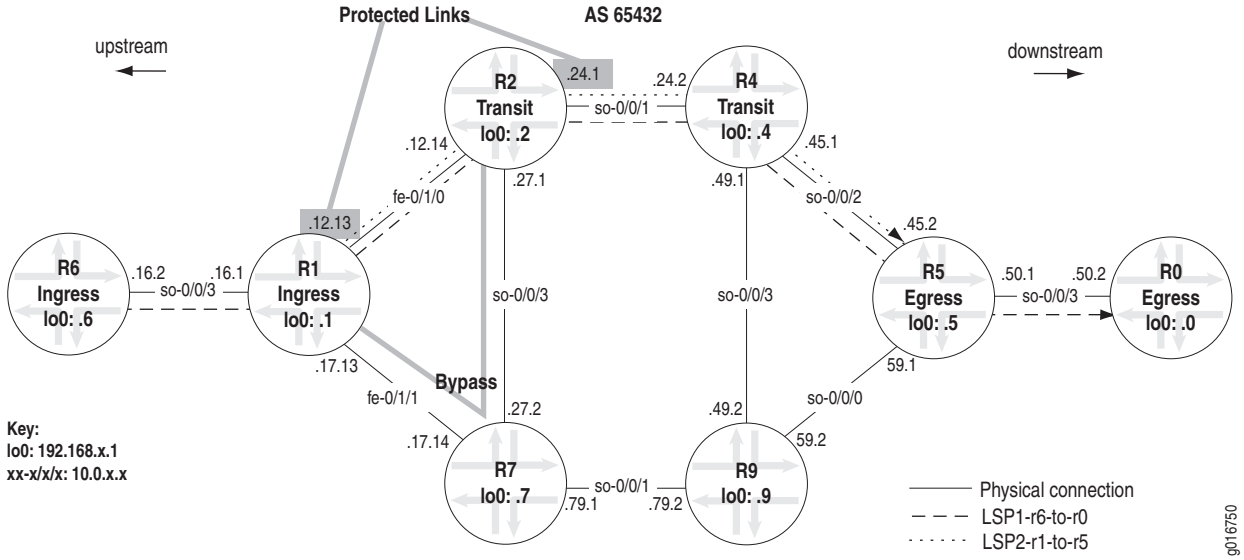
```
    Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
    Adspec: received MTU 1500
    Path MTU: received 0
  Detour branch from 10.0.27.1, to skip 192.168.4.1, Up
    Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
    Adspec: received MTU 1500
    Path MTU: received 0
  Detour branch from 10.0.17.13, to skip 192.168.2.1, Up
    Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
    Adspec: received MTU 1500
    Path MTU: received 0
    PATH rcvfrom: 10.0.59.2 (so-0/0/0.0) 254 pkts
    Adspec: received MTU 1500
    PATH sentto: localclient
    RESV rcvfrom: localclient
    Record route: 10.0.12.13 10.0.24.1 10.0.49.1 10.0.59.2 <self>
    Label in: 3, Label out: -
Total 1 displayed, Up 1, Down 0
```

What It Means The sample output from R5 shows the main LSP in the Record route field and the detours through the network.

Many-to-One Link Protection (Facility Backup) Overview

Many-to-one (facility backup) is based on interface rather than on LSP. While fast reroute protects interfaces or nodes along the entire path of a LSP, many-to-one protection can be applied on interfaces as needed, as shown in Figure 6. In Figure 6, a bypass path is set up around the link to be protected (10.0.12.14) using an alternate interface to forward traffic. The bypass path is shared by all protected LSPs traversing the failed link (many LSPs protected by one bypass path).

Figure 6: Many-to-One or Link Protection



In Figure 6, two LSPs (lsp1-r6-to-r0 and lsp2-r1-to-r5) are protected by one preestablished bypass path from R1 to R2 through R7. Both LSPs have strict paths configured that go through interface fe-0/1/0. On R1, the interface 10.0.12.13 has link protection configured that protects the next hop 10.0.12.14.

Link protection (many-to-one or facility backup) allows a router immediately upstream from a link failure to use an alternate interface to forward traffic to its downstream neighbor. This is accomplished by preestablishing a bypass path that is shared by all protected LSPs traversing the failed link. A single bypass path can safeguard a set of protected LSPs. When an outage occurs, the router immediately upstream from the link outage switches protected traffic to the bypass link, then signals the link failure to the ingress router.

Like fast reroute, link protection provides local repair and restores connectivity faster than the ingress router switching traffic to a standby secondary path. However, unlike fast reroute, link protection does not provide protection against the failure of the downstream neighbor.

Link protection is appropriate in the following situations:

- The number of LSPs to be protected is large.
- Satisfying path selection criteria (priority, bandwidth, and link coloring) for bypass paths is less critical.
- Control at the granularity of individual LSPs is not required.

Configuring and Verifying Link Protection

The following sections describe the steps you must take to configure and verify link protection (many-to-one backup):

1. Configure Link Protection on page 38
2. Verify That Link Protection Is Up on page 40

Step 1: Configure Link Protection

Purpose Configuring link protection is a two-part process. The first part involves configuring link protection on the RSVP interface, and the second part sets link protection for any LSPs traversing the protected link that require use of the bypass path.

Action To configure link protection, follow these steps:

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

   ```
   [edit]
   user@R1# edit protocols rsvp interface type-fpc/pic/port
   ```

   For example:

   ```
   [edit]
   user@R1# edit protocols rsvp interface fe-0/1/0
   ```

2. Configure link protection for the interface:

   ```
   [edit protocols rsvp interface type-fpc/pic/port]
   user@R1# set link-protection
   ```

3. Verify the link protection configuration for the interface:

   ```
   [edit protocols rsvp interface type-fpc/pic/port]
   user@R1# show
   ```

4. Configure link protection for LSPs requiring use of the bypass path:

   [edit protocols rsvp interface fe-0/1/0.0]
   user@R1# **top**

   [edit]
   user@R1# **edit protocols mpls label-switched-path** *lsp-path-name*

   For example:

   [edit]
   user@R1# **edit protocols mpls label-switched-path lsp2-r1-to-r5**

5. Configure link protection for the LSP:

   [edit protocols mpls label-switched-path *lsp-path-name*]
   user@R1# **set link-protection**

6. Verify and the link protection configuration for the LSP:

   [edit protocols mpls label-switched-path *lsp-path-name*]
   user@R1# **show**
   user@R1# **commit**

Sample Output The following sample output illustrates the configuration of the link protection on ingress router R1 in the network shown in Figure 6 on page 37:

```
[edit protocols rsvp]
user@R1# show
interface fe-0/1/0.0 {
    link-protection; #Protection for the RSVP interface
}

[edit protocols mpls label-switched-path lsp2-r1-to-r5]
user@R1# up

[edit protocols mpls]
user@R1# show
label-switched-path lsp2-r1-to-r5 { #Path level of the hierarchy
    to 192.168.5.1;
    link-protection;

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

What It Means The sample output shows link protection for a specific interface. After link protection is configured, a bypass path is signaled to avoid that link in case of a failure. Having a bypass path available does not in itself provide protection for LSPs that traverse the protected link. You must configure link protection on the ingress router for each LSP that will benefit from the bypass path.

Step 2: Verify That Link Protection Is Up

When you verify link protection, you must check that the bypass LSP is up. You can also check the number of LSPs protected by the bypass. In the network shown in Figure 6 on page 37, a bypass path should be up to protect the link between R1 and R2, or next-hop 10.0.12.14, and the two LSPs traversing the link, lsp2-r1-to-r5 and lsp1-r6-to-r0.

Action To verify link protection (many-to-one backup), enter the following JUNOS CLI operational mode commands on the ingress router:

```
user@host> show mpls lsp extensive
user@host> show rsvp session detail
user@host> show rsvp interface
```

Sample Output

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

192.168.5.1
  From: 192.168.1.1, State: Up, ActiveRoute: 0, LSPname: lsp2-r1-to-r5
  ActivePath: via-r2 (primary)
  Link protection desired
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
 *Primary   via-r2           State: Up
    SmartOptimizeTimer: 180
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 3)
 10.0.12.14 S 10.0.24.2 S 10.0.45.2 S
    Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node
10=SoftPreempt):
          10.0.12.14(Label=101264) 10.0.24.2(Label=100736) 10.0.45.2(Label=3)
    6 Jun 16 14:06:33 Link-protection Up
    5 Jun 16 14:05:39 Selected as active path
    4 Jun 16 14:05:39 Record Route:  10.0.12.14(Label=101264)
10.0.24.2(Label=100736) 10.0.45.2(Label=3)
    3 Jun 16 14:05:39 Up
    2 Jun 16 14:05:39 Originate Call
    1 Jun 16 14:05:39 CSPF: computation result accepted
  Created: Fri Jun 16 14:05:38 2006
Total 1 displayed, Up 1, Down 0

[...Output truncated...]

Transit LSP: 2 sessions

192.168.0.1
  From: 192.168.6.1, LSPstate: Up, ActiveRoute: 0
  LSPname: lsp1-r6-to-r0, LSPpath: Primary
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: 101296
  Resv style: 1 SE, Label in: 100192, Label out: 101296
  Time left:  116, Since: Mon Jun 19 10:26:32 2006
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 1 receiver 58739 protocol 0
  Link protection desired
  Type: Link protected LSP, using Bypass->10.0.12.14
      1 Jun 19 10:26:32 Link protection up, using Bypass->10.0.12.14
  PATH rcvfrom: 10.0.16.2 (so-0/0/3.0) 579 pkts
  Adspec: received MTU 1500 sent MTU 1500
  PATH sentto: 10.0.12.14 (fe-0/1/0.0) 474 pkts
  RESV rcvfrom: 10.0.12.14 (fe-0/1/0.0) 501 pkts
```

```
  Explct route: 10.0.12.14 10.0.24.2 10.0.45.2 10.0.50.2
  Record route: 10.0.16.2 <self> 10.0.12.14 10.0.24.2 10.0.45.2 10.0.50.2
[...Output truncated...]
```

What It Means The sample output from ingress router R1 shows that lsp2-r1-to-r5 and lsp1-r6-to-r0 have link protection up, and both LSPs are using the bypass path, 10.0.12.14. However, the show mpls lsp command does not list the bypass path. For information about the bypass path, use the show rsvp session command.

Sample Output

```
user@R1> show rsvp session detail
Ingress RSVP: 2 sessions

192.168.2.1
  From: 192.168.1.1, LSPstate: Up, ActiveRoute: 0
  LSPname: Bypass->10.0.12.14
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: 101456
  Resv style: 1 SE, Label in: -, Label out: 101456
  Time left:    -, Since: Fri May 26 18:38:09 2006
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 1 receiver 18709 protocol 0
  Type: Bypass LSP
    Number of data route tunnel through: 2
    Number of RSVP session tunnel through: 0
  PATH rcvfrom: localclient
  Adspec: sent MTU 1500
  Path MTU: received 1500
  PATH sentto: 10.0.17.14 (fe-0/1/1.0) 51939 pkts
  RESV rcvfrom: 10.0.17.14 (fe-0/1/1.0) 55095 pkts
  Explct route: 10.0.17.14 10.0.27.1
  Record route: <self> 10.0.17.14 10.0.27.1

192.168.5.1
  From: 192.168.1.1, LSPstate: Up, ActiveRoute: 0
  LSPname: lsp2-r1-to-r5, LSPpath: Primary
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: 101264
  Resv style: 1 SE, Label in: -, Label out: 101264
  Time left:    -, Since: Fri Jun 16 14:05:39 2006
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 1 receiver 18724 protocol 0
  Link protection desired
  Type: Link protected LSP
  PATH rcvfrom: localclient
  Adspec: sent MTU 1500
  Path MTU: received 1500
  PATH sentto: 10.0.12.14 (fe-0/1/0.0) 8477 pkts
  RESV rcvfrom: 10.0.12.14 (fe-0/1/0.0) 8992 pkts
  Explct route: 10.0.12.14 10.0.24.2 10.0.45.2
  Record route: <self> 10.0.12.14 10.0.24.2 10.0.45.2
Total 2 displayed, Up 2, Down 0

Egress RSVP: 1 sessions

192.168.1.1
  From: 192.168.5.1, LSPstate: Up, ActiveRoute: 0
  LSPname: r5-to-r1, LSPpath: Primary
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: -
  Resv style: 1 FF, Label in: 3, Label out: -
  Time left:  159, Since: Mon May 22 22:08:16 2006
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
```

```
  Port number: sender 1 receiver 64449 protocol 0
  PATH rcvfrom: 10.0.17.14 (fe-0/1/1.0) 63145 pkts
  Adspec: received MTU 1500
  PATH sentto: localclient
  RESV rcvfrom: localclient
  Record route: 10.0.59.1 10.0.79.2 10.0.17.14 <self>
Total 1 displayed, Up 1, Down 0

Transit RSVP: 2 sessions

192.168.0.1
  From: 192.168.6.1, LSPstate: Up, ActiveRoute: 0
  LSPname: lsp1-r6-to-r0, LSPpath: Primary
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: 101296
  Resv style: 1 SE, Label in: 100192, Label out: 101296
  Time left:  129, Since: Mon Jun 19 10:26:32 2006
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 1 receiver 58739 protocol 0
  Link protection desired
  Type: Link protected LSP
  PATH rcvfrom: 10.0.16.2 (so-0/0/3.0) 3128 pkts
  Adspec: received MTU 1500 sent MTU 1500
  PATH sentto: 10.0.12.14 (fe-0/1/0.0) 2533 pkts
  RESV rcvfrom: 10.0.12.14 (fe-0/1/0.0) 2685 pkts
  Explct route: 10.0.12.14 10.0.24.2 10.0.45.2 10.0.50.2
  Record route: 10.0.16.2 <self> 10.0.12.14 10.0.24.2 10.0.45.2 10.0.50.2

192.168.6.1
  From: 192.168.0.1, LSPstate: Up, ActiveRoute: 0
  LSPname: r0-to-r6, LSPpath: Primary
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: 3
  Resv style: 1 FF, Label in: 100128, Label out: 3
  Time left:  143, Since: Thu May 25 12:30:26 2006
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 1 receiver 4111 protocol 0
  PATH rcvfrom: 10.0.17.14 (fe-0/1/1.0) 57716 pkts
  Adspec: received MTU 1500 sent MTU 1500
  PATH sentto: 10.0.16.2 (so-0/0/3.0) 54524 pkts
  RESV rcvfrom: 10.0.16.2 (so-0/0/3.0) 50534 pkts
  Explct route: 10.0.16.2
  Record route: 10.0.50.2 10.0.59.1 10.0.79.2 10.0.17.14 <self> 10.0.16.2
Total 2 displayed, Up 2, Down 0
```

What It Means The sample output from ingress router R1 shows the ingress, egress, and transit LSPs for R1. Some information is similar to that found in the show mpls lsp command. However, because link protection is an RSVP feature, information about bypass paths is provided. The bypass path appears as a separate RSVP ingress session for the protected interface, as indicated by the Type field.

The bypass path name is automatically generated. By default, the name appears as Bypass > *interface-address*, where the interface address is the next downstream router's interface (10.0.12.14). The explicit route 10.0.17.14 10.0.27.1 for the session shows R7 as the transit node and R2 as the egress node.

Within the ingress RSVP section of the output, the LSP originating at R1 (lsp2-r1-to-r5) is shown requesting link protection. Since a bypass path is in place to protect the downstream link, lsp2-r1-to-r5 is associated with the bypass, as indicated by the Link protected LSP field.

The egress section of the output shows the return LSP r5-to-r1, which is not protected.

The transit section of the output shows link protection requested by lsp1-r6-to-r0. Since a bypass path is in place to protect the downstream link, lsp1-r6-to-r0 is associated with the bypass, as indicated by the Link protected LSP field. Also included in the transit section of the output is the return LSP r0-to-r6, which is not protected.

Sample Output

```
user@R1> show rsvp interface
RSVP interface: 4 active
                  Active Subscr- Static      Available   Reserved    Highwater
Interface   State resv   iption  BW          BW          BW          mark
fe-0/1/0.0  Up         2   100%  100Mbps     100Mbps     0bps        35Mbps
fe-0/1/1.0  Up         1   100%  100Mbps     100Mbps     0bps        0bps
fe-0/1/2.0  Up         0   100%  100Mbps     100Mbps     0bps        0bps
so-0/0/3.0  Up         1   100%  155.52Mbps  155.52Mbps  0bps        0bps
```

What It Means

The sample output from ingress router R1 shows the number of LSPs going through the interfaces configured on R1. The Active resv field shows the number of LSPs for each interface. For example, interface fe-0/1/0.0 between R1 and R2 has two active reservations, lsp1-r6-to-r0 and lsp2-r1-to-r5; interface fe-0/1/1.0 between R1 and R7 has one, the bypass (10.0.12.14); interface fe-0/1/2.0 between R6 and R1 has no LSP reservations; and interface so-0/0/3.0 between R6 and R1 has one LSP reservation, lsp1-r6-to-r0.

Node-Link Protection Overview

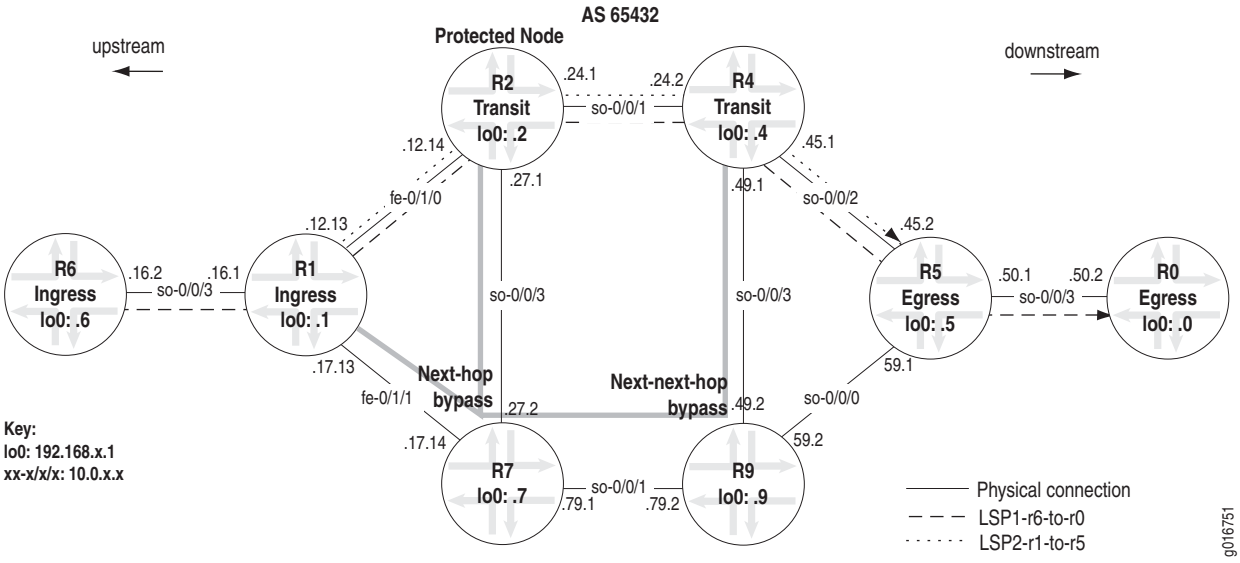
Node-link protection (many-to-one or facility backup) extends the capabilities of link protection and provides slightly different protection from fast reroute. While link protection is useful for selecting an alternate path to the same router when a specific link fails, and fast reroute protects interfaces or nodes along the entire path of an LSP, node-link protection establishes a bypass path that avoids a particular node in the LSP path.

When you enable node-link protection for an LSP, you must also enable link protection on all RSVP interfaces in the path. Once enabled, the following types of bypass paths are established:

- Next-hop bypass LSP—Provides an alternate route for an LSP to reach a neighboring router. This type of bypass path is established when you enable either node-link protection or link protection.
- Next-next-hop bypass LSP—Provides an alternate route for an LSP through a neighboring router en route to the destination router. This type of bypass path is established exclusively when node-link protection is configured.

Figure 7 illustrates the example MPLS network topology used in this section. The example network uses OSPF as the interior gateway protocol (IGP) and a policy to create traffic.

Figure 7: Node-Link Protection



The MPLS network in Figure 7 illustrates a router-only network that consists of unidirectional LSPs between R1 and R5, (lsp2-r1-to-r5) and between R6 and R0 (lsp1-r6-to-r0). Both LSPs have strict paths configured that go through interface fe-0/1/0.

In the network shown in Figure 7 on page 44, both types of bypass paths are preestablished around the protected node (R2). A next-hop bypass path avoids interface fe-0/1/0 by going through R7, and a next-next-hop bypass path avoids R2 altogether by going through R7 and R9 to R4. Both bypass paths are shared by all protected LSPs traversing the failed link or node (many LSPs protected by one bypass path).

Node-link protection (many-to-one or facility backup) allows a router immediately upstream from a node failure to use an alternate node to forward traffic to its downstream neighbor. This is accomplished by preestablishing a bypass path that is shared by all protected LSPs traversing the failed link.

When an outage occurs, the router immediately upstream from the outage switches protected traffic to the bypass node, and then signals the failure to the ingress router. Like fast reroute, node-link protection provides local repair, restoring connectivity faster than the ingress router can establish a standby secondary path or signal a new primary LSP.

Node-link protection is appropriate in the following situations:

- Protection of the downstream link and node is required.
- The number of LSPs to be protected is large.
- Satisfying path selection criteria (priority, bandwidth, and link coloring) for bypass paths is less critical.
- Control at the granularity of individual LSPs is not required.

Configuring and Verifying Node-Link Protection

The following section describes the steps you must take to configure and verify many-to-one backup.

1. Configure Node-Link Protection on page 45
2. Verify That Node-Link Protection Is Up on page 47

Step 1: Configure Node-Link Protection

Configuring node-link protection is a two-part process. The first part involves configuring node-link protection for any LSPs traversing the protected node that require use of the bypass path, and the second part sets link protection on the outgoing RSVP interface on routers in the LSP.

Action To configure node-link protection, follow these steps:

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

   ```
   [edit]
   user@R1# edit protocols mpls label-switched-path lsp-path-name
   ```

For example:

```
[edit]
user@R1# edit protocols mpls label-switched-path lsp2-r1-to-r5
```

2. Configure node-link protection for the LSP:

   ```
   [edit protocols mpls label-switched-path lsp-path-name]
   user@R1# set node-link-protection
   ```

3. Verify the node-link protection configuration for the LSP:

   ```
   [edit protocols mpls label-switched-path lsp-path-name]
   user@R1# show
   ```

4. Configure link protection for the interface:

   ```
   [edit protocols]
   user@R1# edit protocols rsvp interface interface-name
   ```

   For example:

   ```
   [edit protocols]
   user@R1# edit protocols rsvp interface fe-0/1/0
   ```

5. Configure link protection:

   ```
   [edit protocols rsvp interface interface-name]
   user@R1# set link-protection
   ```

6. Verify the link protection configuration for the interface, and commit both configurations:

   ```
   [edit protocols rsvp interface interface-name]
   user@R1# show
   user@R1# commit
   ```

7. Repeat Step 1 through Step 3 on any other ingress routers that have LSPs requiring use of the bypass path.

8. Repeat Step 4 and Step 5 on routers with outgoing interfaces in the LSP.

Sample Output The following sample output shows the configuration of node-link protection on ingress router R1 in the network shown in Figure 6 on page 37:

```
[edit protocols mpls label-switched-path lsp2-r1-to-r5]
user@R1# up

[edit protocols mpls]
user@R1# show
label-switched-path lsp2-r1-to-r5 { #Label-switched-path level of the hierarchy
    to 192.168.5.1;
    node-link-protection; #LSP node-link protection

[edit protocols rsvp]
user@R1# show
interface fe-0/1/0.0 {
    link-protection; #Link protection for the RSVP interface
}

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

What It Means The sample output shows the configuration of node-link protection for an LSP. After node-link protection is configured, bypass paths are signaled to avoid the protected link or node in case of failure. Having bypass paths available does not in itself provide protection for LSPs that traverse the protected node. You must include the node-link-protection statement on the ingress router for each LSP that will benefit from the bypass path.

Step 2: Verify That Node-Link Protection Is Up

After you configure node-link protection, you must check that bypass paths are up. You can also check the number of LSPs protected by the bypass paths. In the network shown in Figure 7 on page 44, two bypass paths should be up: one next-hop bypass path protecting the link between R1 and R2 (or next-hop 10.0.12.14), and a next-next-hop bypass path avoiding R2.

Action To verify node-link protection (many-to-one backup), enter the following JUNOS CLI operational mode commands on the ingress router. You can also issue the commands on transit routers and other routers used in the bypass path for slightly different information.

- **show mpls lsp** (See Sample Output on page 47)
- **show mpls lsp extensive** (See Sample Output on page 48)
- **show rsvp interface** (See Sample Output on page 49)
- **show rsvp interface extensive** (See Sample Output on page 49)
- **show rsvp session detail** (See Sample Output on page 50)

Sample Output

```
user@R1> show mpls lsp
Ingress LSP: 1 sessions
To              From            State Rt ActivePath       P     LSPname
192.168.5.1     192.168.1.1     Up     0 via-r2           *     lsp2-r1-to-r5
Total 1 displayed, Up 1, Down 0

Egress LSP: 1 sessions
To              From            State   Rt Style Labelin Labelout LSPname
192.168.1.1     192.168.5.1     Up       0  1 FF       3        - r5-to-r1
Total 1 displayed, Up 1, Down 0

Transit LSP: 2 sessions
To              From            State   Rt Style Labelin Labelout LSPname
```

```
192.168.0.1     192.168.6.1     Up       0  1 FF 100464   101952 lsp1-r6-to-r0
192.168.6.1     192.168.0.1     Up       0  1 FF  100448        3 r0-to-t6
Total 2 displayed, Up 2, Down 0
```

What It Means Sample output from R1 for the show mpls lsp command shows a brief description of the state of configured and active LSPs for which R1 is the ingress, transit, and egress router. All LSPs are up. R1 is the ingress router for lsp2-r1-to-r5, and the egress router for return LSP r5-to-r1. Two LSPs transit R1, lsp1-r6-to-r0 and the return LSP r0-to-t6. For more detailed information about the LSP, include the extensive option when you issue the show mpls lsp command.

Sample Output

```
user@R1> show mpls lsp extensive
Ingress LSP: 1 sessions

192.168.5.1
  From: 192.168.1.1, State: Up, ActiveRoute: 0, LSPname: lsp2-r1-to-r5
  ActivePath: via-r2 (primary)
  Node/Link protection desired
  LoadBalance: Random
  Encoding type: Packet, Switching type: Packet, GPID: IPv4
 *Primary   via-r2           State: Up
    SmartOptimizeTimer: 180
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 3)
 10.0.12.14 S 10.0.24.2 S 10.0.45.2 S
    Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node
10=SoftPreempt):
          10.0.12.14(Label=101872) 10.0.24.2(Label=101360) 10.0.45.2(Label=3)
   11 Jul 11 14:30:58 Link-protection Up
   10 Jul 11 14:28:28 Selected as active path
    [...Output truncated...]
  Created: Tue Jul 11 14:22:58 2006
Total 1 displayed, Up 1, Down 0

Egress LSP: 1 sessions

192.168.1.1
  From: 192.168.5.1, LSPstate: Up, ActiveRoute: 0
  LSPname: r5-to-r1, LSPpath: Primary
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: -
  Resv style: 1 FF, Label in: 3, Label out: -
  Time left:  146, Since: Tue Jul 11 14:28:36 2006
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 1 receiver 29228 protocol 0
  PATH rcvfrom: 10.0.12.14 (fe-0/1/0.0) 362 pkts
  Adspec: received MTU 1500
  PATH sentto: localclient
  RESV rcvfrom: localclient
  Record route: 10.0.45.2 10.0.24.2 10.0.12.14 <self>
Total 1 displayed, Up 1, Down 0

Transit LSP: 2 sessions

192.168.0.1
  From: 192.168.6.1, LSPstate: Up, ActiveRoute: 0
  LSPname: lsp1-r6-to-r0, LSPpath: Primary
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: 101952
  Resv style: 1 SE, Label in: 100464, Label out: 101952
  Time left:  157, Since: Tue Jul 11 14:31:38 2006
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 1 receiver 11131 protocol 0
```

```
  Node/Link protection desired
  Type: Node/Link protected LSP, using Bypass->10.0.12.14->10.0.24.2
      1 Jul 11 14:31:38 Node protection up, using Bypass->10.0.12.14->10.0.24.2
  PATH rcvfrom: 10.0.16.2 (so-0/0/3.0) 509 pkts
  Adspec: received MTU 1500 sent MTU 1500
  PATH sentto: 10.0.12.14 (fe-0/1/0.0) 356 pkts
  RESV rcvfrom: 10.0.12.14 (fe-0/1/0.0) 358 pkts
  Explct route: 10.0.12.14 10.0.24.2 10.0.45.2 10.0.50.2
  Record route: 10.0.16.2 <self> 10.0.12.14 10.0.24.2 10.0.45.2 10.0.50.2

192.168.6.1
  From: 192.168.0.1, LSPstate: Up, ActiveRoute: 0
  LSPname: r0-to-t6, LSPpath: Primary
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: 3
  Resv style: 1 FF, Label in: 100448, Label out: 3
  Time left:  147, Since: Tue Jul 11 14:31:36 2006
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 1 receiver 23481 protocol 0
  PATH rcvfrom: 10.0.12.14 (fe-0/1/0.0) 358 pkts
  Adspec: received MTU 1500 sent MTU 1500
  PATH sentto: 10.0.16.2 (so-0/0/3.0) 350 pkts
  RESV rcvfrom: 10.0.16.2 (so-0/0/3.0) 323 pkts
  Explct route: 10.0.16.2
  Record route: 10.0.50.2 10.0.45.2 10.0.24.2 10.0.12.14 <self> 10.0.16.2
Total 2 displayed, Up 2, Down 0
```

What It Means Sample output from R1 for the show mpls lsp extensive command shows detailed information about all LSPs for which R1 is the ingress, egress, or transit router, including all past state history and the reason why an LSP failed. All LSPs are up. The main two LSPs lsp2-r1-to-r5 and lsp1-r6-to-r0 have node-link protection as indicated by the Node/Link protection desired field in the ingress and transit sections of the output. In the ingress section of the output, the Link-protection Up field shows that lsp2-r1-to-r5 has link protection up. In the transit section of the output, the Type: Node/Link protected LSP field shows that lsp1-r6-to-r0 has node-link protection up, and in case of failure will use the bypass LSP Bypass->10.0.12.14->10.0.24.2.

Sample Output

```
user@R1> show rsvp interface
RSVP interface: 4 active
                    Active Subscr- Static      Available   Reserved    Highwater
Interface   State resv   iption  BW          BW          BW          mark
fe-0/1/0.0  Up         2   100%  100Mbps     100Mbps     0bps        0bps
fe-0/1/1.0  Up         1   100%  100Mbps     100Mbps     0bps        0bps
fe-0/1/2.0  Up         0   100%  100Mbps     100Mbps     0bps        0bps
so-0/0/3.0  Up         1   100%  155.52Mbps  155.52Mbps  0bps        0bps
```

What It Means Sample output from R1 for the show rsvp interface command shows four interfaces enabled with RSVP (Up). Interface fe-0/1/0.0 has two active RSVP reservations (Active resv) that might indicate sessions for the two main LSPs, lsp1-r6-to-r0 and lsp2-r1-to-r5. Interface fe-0/1/0.0 is the connecting interface between R1 and R2, and both LSPs are configured with a strict path through fe-0/1/0.0. For more detailed information about what is happening on interface fe-0/1/0.0, issue the show rsvp interface extensive command.

Sample Output

```
user@R1> show rsvp interface extensive
RSVP interface: 3 active
fe-0/1/0.0 Index 67, State Ena/Up
  NoAuthentication, NoAggregate, NoReliable, LinkProtection
  HelloInterval 9(second)
```

```
  Address 10.0.12.13
  ActiveResv 2, PreemptionCnt 0, Update threshold 10%
  Subscription 100%,
  bc0 = ct0, StaticBW 100Mbps
  ct0: StaticBW 100Mbps, AvailableBW 100Mbps
    MaxAvailableBW 100Mbps = (bc0*subscription)
    ReservedBW [0] 0bps[1] 0bps[2] 0bps[3] 0bps[4] 0bps[5] 0bps[6] 0bps[7] 0bps
  Protection: On, Bypass: 2, LSP: 2, Protected LSP: 2, Unprotected LSP: 0
      2 Jul 14 14:49:40 New bypass Bypass->10.0.12.14
      1 Jul 14 14:49:34 New bypass Bypass->10.0.12.14->10.0.24.2
    Bypass: Bypass->10.0.12.14, State: Up, Type: LP, LSP: 0, Backup: 0
      3 Jul 14 14:49:42 Record Route:  10.0.17.14 10.0.27.1
      2 Jul 14 14:49:42 Up
      1 Jul 14 14:49:42 CSPF: computation result accepted
    Bypass: Bypass->10.0.12.14->10.0.24.2, State: Up, Type: NP, LSP: 2, Backup:0
      4 Jul 14 14:50:04 Record Route:  10.0.17.14 10.0.79.2 10.0.59.1 10.0.45.1
      3 Jul 14 14:50:04 Up
      2 Jul 14 14:50:04 CSPF: computation result accepted
      1 Jul 14 14:49:34 CSPF failed: no route toward 10.0.24.2
[...Output truncated...]
```

What It Means Sample output from R1 for the show rsvp interface extensive command shows more detailed information about the activity on all RSVP interfaces (3). However, only output for fe-0/1/0.0 is shown. Protection is enabled (Protection: On), with two bypass paths (Bypass: 2) protecting two LSPs (Protected LSP: 2). All LSPs are protected, as indicated by the Unprotected LSP: 0 field. The first bypass Bypass->10.0.12.14 is a link protection bypass path (Type: LP), protecting the link between R1 and R2, fe-0/1/0.0. The second bypass path 10.0.12.14->10.0.24.2 is a node-link protected LSP, avoiding R2 in case of node failure.

Sample Output

```
user@R1> show rsvp session detail
Ingress RSVP: 2 sessions

192.168.4.1
  From: 192.168.1.1, LSPstate: Up, ActiveRoute: 0
  LSPname: Bypass->10.0.12.14->10.0.24.2
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: 102000
  Resv style: 1 SE, Label in: -, Label out: 102000
  Time left:    -, Since: Tue Jul 11 14:30:53 2006
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 1 receiver 60120 protocol 0
  Type: Bypass LSP
    Number of data route tunnel through: 2
    Number of RSVP session tunnel through: 0
  PATH rcvfrom: localclient
  Adspec: sent MTU 1500
  Path MTU: received 1500
  PATH sentto: 10.0.17.14 (fe-0/1/1.0) 336 pkts
  RESV rcvfrom: 10.0.17.14 (fe-0/1/1.0) 310 pkts
  Explct route: 10.0.17.14 10.0.79.2 10.0.59.1 10.0.45.1
  Record route: <self> 10.0.17.14 10.0.79.2 10.0.59.1 10.0.45.1

192.168.5.1
  From: 192.168.1.1, LSPstate: Up, ActiveRoute: 0
  LSPname: lsp2-r1-to-r5, LSPpath: Primary
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: 101872
  Resv style: 1 SE, Label in: -, Label out: 101872
  Time left:    -, Since: Tue Jul 11 14:28:28 2006
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
```

```
  Port number: sender 2 receiver 60118 protocol 0
  Node/Link protection desired
  Type: Node/Link protected LSP
  PATH rcvfrom: localclient
  Adspec: sent MTU 1500
  Path MTU: received 1500
  PATH sentto: 10.0.12.14 (fe-0/1/0.0) 344 pkts
  RESV rcvfrom: 10.0.12.14 (fe-0/1/0.0) 349 pkts
  Explct route: 10.0.12.14 10.0.24.2 10.0.45.2
  Record route: <self> 10.0.12.14 10.0.24.2 10.0.45.2
Total 2 displayed, Up 2, Down 0

Egress RSVP: 1 sessions

192.168.1.1
  From: 192.168.5.1, LSPstate: Up, ActiveRoute: 0
  LSPname: r5-to-r1, LSPpath: Primary
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: -
  Resv style: 1 FF, Label in: 3, Label out: -
  Time left:  147, Since: Tue Jul 11 14:28:36 2006
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 1 receiver 29228 protocol 0
  PATH rcvfrom: 10.0.12.14 (fe-0/1/0.0) 348 pkts
  Adspec: received MTU 1500
  PATH sentto: localclient
  RESV rcvfrom: localclient
  Record route: 10.0.45.2 10.0.24.2 10.0.12.14 <self>
Total 1 displayed, Up 1, Down 0

Transit RSVP: 2 sessions

192.168.0.1
  From: 192.168.6.1, LSPstate: Up, ActiveRoute: 0
  LSPname: lsp1-r6-to-r0, LSPpath: Primary
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: 101952
  Resv style: 1 SE, Label in: 100464, Label out: 101952
  Time left:  134, Since: Tue Jul 11 14:31:38 2006
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 1 receiver 11131 protocol 0
  Node/Link protection desired
  Type: Node/Link protected LSP
  PATH rcvfrom: 10.0.16.2 (so-0/0/3.0) 488 pkts
  Adspec: received MTU 1500 sent MTU 1500
  PATH sentto: 10.0.12.14 (fe-0/1/0.0) 339 pkts
  RESV rcvfrom: 10.0.12.14 (fe-0/1/0.0) 343 pkts
  Explct route: 10.0.12.14 10.0.24.2 10.0.45.2 10.0.50.2
  Record route: 10.0.16.2 <self> 10.0.12.14 10.0.24.2 10.0.45.2 10.0.50.2

192.168.6.1
  From: 192.168.0.1, LSPstate: Up, ActiveRoute: 0
  LSPname: r0-to-t6, LSPpath: Primary
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: 3
  Resv style: 1 FF, Label in: 100448, Label out: 3
  Time left:  158, Since: Tue Jul 11 14:31:36 2006
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 1 receiver 23481 protocol 0
  PATH rcvfrom: 10.0.12.14 (fe-0/1/0.0) 344 pkts
  Adspec: received MTU 1500 sent MTU 1500
  PATH sentto: 10.0.16.2 (so-0/0/3.0) 337 pkts
  RESV rcvfrom: 10.0.16.2 (so-0/0/3.0) 310 pkts
```

```
  Explct route: 10.0.16.2
  Record route: 10.0.50.2 10.0.45.2 10.0.24.2 10.0.12.14 <self> 10.0.16.2
Total 2 displayed, Up 2, Down 0
```

What It Means Sample output from R1 shows detailed information about the RSVP sessions active on R1. All sessions are up, with two ingress sessions, one egress session, and two transit sessions.

Within the ingress section, the first session is a bypass path, as indicated by the Type: Bypass LSP field; and the second session is a protected LSP (lsp2-r1-to-r5) originating on R1, as indicated by the Type: Node/Link protected LSP field.

Conclusion

Multiprotocol Label Switching (MPLS) label-switched path (LSP) link protection and node-link protection are facility-based methods used to reduce the amount of time needed to reroute LSP traffic. These protection methods are often compared to fast reroute—the other JUNOS software LSP protection method.

While fast reroute protects LSPs on a one-to-one basis, link protection and node-link protection protect multiple LSPs by using a single, logical bypass LSP. Link protection provides robust backup support for a link, node-link protection bypasses a node or a link, and both types of protection are designed to interoperate with other vendor equipment. Such functionality makes link protection and node-link protection excellent choices for scalability, redundancy, and performance in MPLS-enabled networks.

Related Information

For additional information about MPLS fast reroute and MPLS protection methods, see the following:

- *JUNOS Feature Guide*
- *JUNOS MPLS Applications Configuration Guide*
- Semeria, Chuck. *RSVP Signaling Extensions for MPLS Traffic Engineering.* White paper. 2002
- Semeria, Chuck. *IP Dependability: Network Link and Node Protection*. White paper. 2002
- RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*