

Chapter 9

MPLS LSP Link Protection and Node-Link Protection

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 can only protect LSPs on a one-to-one basis, link protection and node-link protection can protect multiple LSPs by using only a single, logical bypass LSP. Link protection can provide robust backup support for a link, node-link protection can bypass 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.

This feature guide covers these topics:

Overview on page 372

System Requirements on page 375

Terms and Acronyms on page 375

Configuring MPLS LSP Link Protection or Node-Link Protection on page 376

Example: MPLS LSP Link Protection Configuration on page 379

Checking Your Work on page 386

Example: Node-Link Protection Configuration on page 402

Checking Your Work on page 412

For More Information on page 415

Revision History on page 416

Overview

Prior to JUNOS Release 5.4, the two mechanisms used to enable rapid MPLS LSP reroutes in Juniper Networks routers were Packet Forwarding Engine local repair and fast reroute. Packet Forwarding Engine local repair is an infrastructure-based solution and fast reroute provides a single backup LSP for every protected primary LSP. However, configuring backup LSPs on a one-to-one basis can become a scaling challenge for a growing MPLS network.

Scalable solutions for LSP redundancy include link protection and node-link protection. Both approaches are explained in the Internet Engineering Task Force (IETF) Internet draft draft-ietf-mpls-rsvp-lsp-fastreroute-07.txt, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels* (expires February 2005). In general, these are facility-based methods that quickly reroute traffic from multiple LSPs. They also reduce the amount of configuration necessary to implement LSP protection.

You can configure either link protection or node-link protection by itself, fast reroute by itself, or both fast reroute and one of the protection methods. Whenever one or more of these reroute options are enabled, Packet Forwarding Engine local repair is activated by default.

To enable any of Juniper Networks MPLS LSP reroute options, you must first install the LSP as a valid next hop in the main inet.0 routing table on the ingress PE router. You can accomplish this in one of several of ways:

- Enable the BGP learned routes to use the LSP.

- Set the `bgp-igp` or `bgp-igp-both-ribs` parameters at the [edit protocols mpls traffic engineering] hierarchy level.

- Configure install *prefix* active at the [edit protocols mpls lsp *lsp-name*] hierarchy level.

- Configure a static route with an indirect next hop that goes to the LSP end.

- Configure a static route with an LSP next hop.

- Configure IS-IS support for bidirectional LSPs.

To summarize, the MPLS LSP reroute options available in JUNOS are as follows:

Packet Forwarding Engine local repair—This data plane method adds enhanced capabilities to the Packet Forwarding Engine subsystem and reduces the time needed for path switchover. With local repair, the Packet Forwarding Engine can correct a path failure before it receives recomputed paths from the Routing Engine. The Routing Engine pre-computes backup routes for every MPLS path and provides this information to the Packet Forwarding Engine before any failure. Packet Forwarding Engine local repair is enabled by default and requires no additional configuration.

Fast reroute—The original control plane method for fast reroute of individual LSPs is described as “one-to-one” protection in the IETF Internet draft *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*. JUNOS software calculates LSP detours for LSPs and implements the rerouted paths as needed. You can configure the command `fast-reroute` at the `[edit protocols mpls lsp-name]` hierarchy level. For more information about MPLS LSP fast reroute, see the *JUNOS MPLS Applications Configuration Guide*.

Link protection—Another control plane method discussed in this guide. In general, link protection is useful when you wish to protect LSPs after a supporting link is lost.

Node-link protection—This is also a control plane method and is discussed in this guide. In general, link protection is useful when you wish to protect LSPs after a supporting node fails.

Link Protection

Link protection offers per-link traffic protection. It supports fast rerouting of user traffic over one mission-critical link. It does this on a per-LSP basis, much like the fast reroute option. However, it can also aggregate several protected LSPs over a single bypass LSP.

This flexible approach to single-link, rapid reroute does not require any new protocol modification beyond the RSVP-TE specification. Bypass LSPs efficiently aggregate traffic from multiple LSPs when the reroute occurs.

When link protection is enabled on a router interface and a protected LSP traverses this protected interface, JUNOS software creates a trunk-like, bypass LSP to provide an alternate path to the RSVP neighbor. Each bypass LSP keeps track of all protected LSPs that are associated with the neighbor. In case of a neighbor failure, the protected LSPs are rerouted over the bypass LSP. Bypass LSPs use label stacking to protect user traffic.

At the interface level, the router keeps track of bypass LSP characteristics. Whenever an interface enables or disables link protection, the changes are saved at the interface level and then propagated to the RSVP neighbor. When a neighbor requires link protection, the router checks the associated interface structure to determine how to create a bypass LSP.

On a per-RSVP neighbor basis, the router keeps track of all the LSP sessions passing through a neighbor as well as the bypass LSP status. For the bypass LSP, the router maintains information about protected neighbors. For regular LSPs, the router watches all threads containing the LSP. When a regular LSP is lost, the bypass LSP reroutes user traffic by using next-hop, egress Explicit Route Object (ERO), interface, and peer-address information.



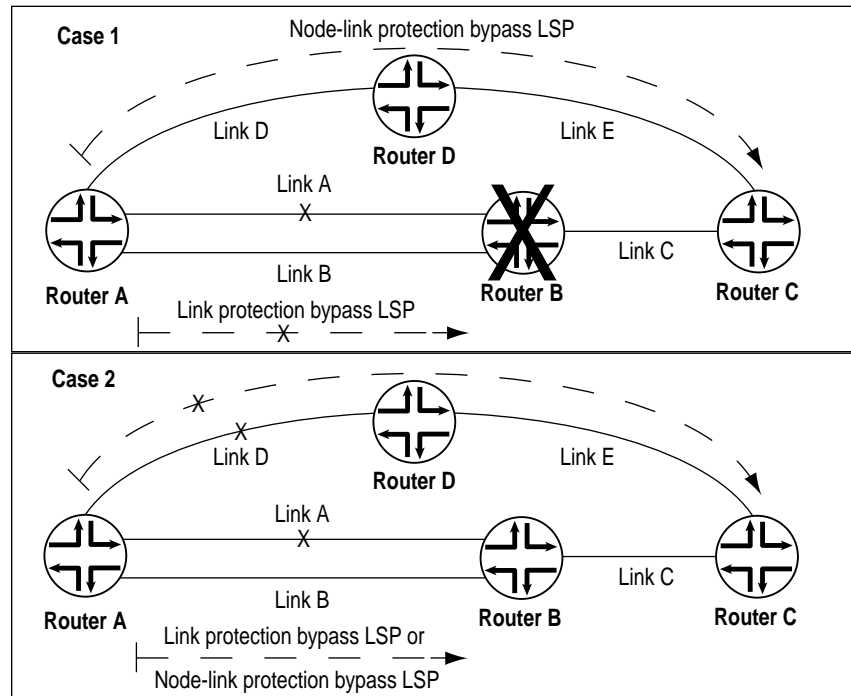
NOTE: Fast reroute, link protection, and node-link protection all rely on Constrained Shortest Path First (CSPF) to select bypass LSPs. The CSPF computation attempts to find an LSP that bypasses an affected node first, but can select an alternate link through the affected node if a node bypass LSP is not available.

Node-Link Protection

While link protection is useful for selecting an alternate path to the same router when a link fails, node-link protection establishes a bypass LSP through a different router altogether. For Case 1 in Figure 37, link protection allows an LSP to switch to link B and immediately bypass failed link A. However, if Router B fails, link B will fail and the link-protected LSP will be lost.

With node-link protection, the backup LSP can switch to link D instead and bypass the failed links and router. Another benefit of node-link protection shown in Case 2 is that a node-link-protected LSP can act like a link-protected LSP and switch to link B if link D is unavailable.

Figure 37: Link Protection and Node-Link Protection Comparison



9003130

JUNOS software signals bypass LSPs dynamically when a protected LSP transverses the protected link. The software determines if the protected LSP needs a node bypass or a link bypass and prepares the necessary bypass LSP automatically. The bypass LSP is torn down automatically when a protected LSP does not use the link.

Because the creation and removal of bypass LSPs is automatic, network resources can be used for other purposes when the bypass LSP is not needed. Likewise, network administrators do not need to configure bypass LSPs statically and can focus their maintenance efforts elsewhere.

System Requirements

To implement MPLS LSP link protection or node-link protection, your system must meet these minimum requirements:

JUNOS Release 7.1 or later for multiple bypass LSPs, manual bypass LSPs, and link protection priority

JUNOS Release 7.0 or later for link protection of point-to-multipoint LSPs

JUNOS Release 5.4 or later for link protection

JUNOS Release 6.0 and later for node-link protection

Three Juniper Networks M-series or T-series routing platforms

Terms and Acronyms

backup LSP—A redundant LSP used to reroute a single, primary LSP. Backup LSPs are found in link protection, node-link protection, and fast reroute redundancy methods.

bypass LSP—A logical trunk used to reroute multiple backup LSPs over a single connection protected with link protection.

link protection—A method of establishing bypass LSPs to provide rapid reroute capability for primary LSPs on a per-link basis. For more information about link protection, see the *JUNOS MPLS Applications Configuration Guide*.

node-link protection—A method of establishing bypass LSPs to provide rapid reroute capability for primary LSPs on a per-node basis. If node protection is unavailable, the LSP attempts to use link protection. For more information about node-link protection, see the *JUNOS MPLS Applications Configuration Guide*.

Configuring MPLS LSP Link Protection or Node-Link Protection

To implement MPLS LSP link protection or node-link protection, perform the following:

Configuring Link Protection or Node-Link Protection on the LSP on page 376

Configuring Link Protection on the RSVP Interfaces Traversed by the LSP on page 377

Option: Configuring Multiple Bypass LSPs, Manual Bypass LSPs, and Link Protection Priority on page 377

To view a full configuration example, see these sections:

Example: MPLS LSP Link Protection Configuration on page 379

Checking Your Work on page 386

Example: Node-Link Protection Configuration on page 402

Checking Your Work on page 412

Configuring Link Protection or Node-Link Protection on the LSP

You enable the level of LSP protection you want on the ingress router. Link protection redirects LSP traffic to a bypass LSP that can traverse the same router that contains the affected link, while node-link protection sends LSP traffic to a bypass LSP that circumvents the affected router. To enable link protection for an LSP or point-to-multipoint LSP, include the link-protection statement at the [edit protocols mpls label-switched-path *lsp-name*] hierarchy level. To enable node-link protection for an LSP, include the node-link-protection statement at the [edit protocols mpls label-switched-path *lsp-name*] hierarchy level.

```
[edit]
protocols {
  mpls {
    label-switched-path lsp-name {
      ( link-protection | node-link-protection );
    }
  }
}
```

After link protection or node-link protection is established, the LSP marks the desired link protection bit in the RSVP Session Attribute (SA) object. To disable link protection or node-link protection for an LSP, delete the link-protection or node-link-protection statements at the [edit protocols mpls label-switched-path *lsp-name*] hierarchy level.

For more information about point-to-multipoint LSPs, see the *JUNOS MPLS Applications Configuration Guide*.

Configuring Link Protection on the RSVP Interfaces Traversed by the LSP

To complete your link protection or node-link protection configuration, configure RSVP interface-level link protection at the [edit protocols rsvp interface *interface-name*] hierarchy level. Include the link protection statement on every RSVP interface the LSP uses to exit each router found in the LSP path. As an option, you can configure a loose or strict path for all bypass LSPs with the path statement at the [edit protocols rsvp interface *interface-name* link-protection] hierarchy level.

```
[edit]
protocols {
  rsvp {
    interface interface-name {
      link-protection {
        path ip-address {
          (loose | strict);
        }
      }
    }
  }
}
```

To disable link protection on an RSVP interface, include the disable statement at the [edit protocols rsvp interface *interface-name* link-protection] hierarchy level.

Option: Configuring Multiple Bypass LSPs, Manual Bypass LSPs, and Link Protection Priority

You can configure multiple bypass LSP paths for a link-protected RSVP LSP. When you enable this option, RSVP signals multiple bypasses concurrently for a link-protected LSP. To configure, start by enabling link protection or node-link protection by including the link-protection or node-link-protection statement at the [edit protocols mpls label-switched-path *lsp-name*] hierarchy level. To configure an RSVP interface to include multiple bypasses, specify how much bandwidth the bypasses should consume by including the bandwidth statement at the [edit protocols rsvp interface *interface-name* link-protection] hierarchy level. To limit the total number of bypasses that can be created, include the max-bypasses statement at the [edit protocols rsvp interface *interface-name* link-protection] hierarchy level.

Other bypass options include limiting the maximum number of hops a bypass LSP will traverse, selectively disallowing node-link protection, setting a timer to redistribute data periodically across the bypass LSPs, requiring strict or loose paths for the bypass LSPs, and establishing the percentage of bandwidth required for the bypass LSPs. To configure, include the hop-limit, no-node-protection, optimize-timer, path, and subscription statements, respectively, at the [edit protocols rsvp interface *interface-name* link-protection] hierarchy level.

Another option is to specify bypass LSPs manually. To configure, include the to and bandwidth statements at the [edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*] hierarchy level. Optionally, you can specify the hop limit and path type for the manual bypass LSP. To configure the options, include the hop-limit and path statements at the [edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*] hierarchy level.

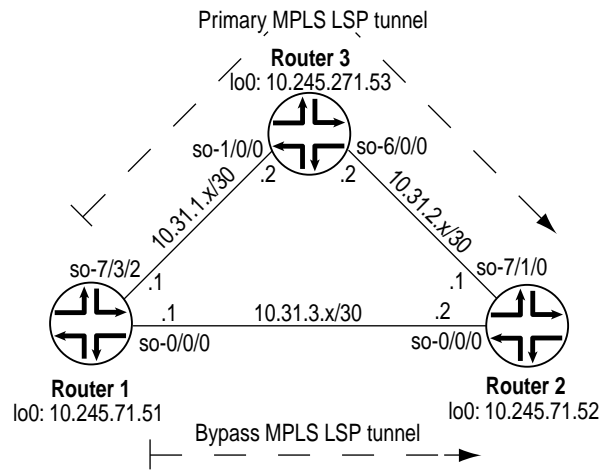
Link protection priority enables you to provide preferred combinations of priority and class in a traffic engineering class matrix. When selecting a bypass LSP, the routing platform selects the bypass containing the lowest priority. To configure link protection priority for all bypass LSP paths, include the priority statement at the [edit protocols rsvp interface *interface-name* link-protection] hierarchy level. To configure link protection priority for a manually specified bypass LSP path, include the priority statement at the [edit protocols rsvp interface *interface-name* link-protection bypass *bypass-name*] hierarchy level.

```
[edit protocols]
mpls {
  label-switched-path lsp-name {
    ( link-protection | node-link-protection );
  }
}
rsvp {
  interface interface-name {
    link-protection {
      bandwidth bps;
      bypass bypass-name {
        to ip-address;
        bandwidth bps;
        hop-limit maximum-hops; # The default value is 255 hops.
        path ip-address {
          (loose | strict);
        }
        priority priority;
      }
      hop-limit maximum-hops; # The range is 2 hops to the default (255 hops).
      max-bypasses number; # The range for this statement is 1 to 99.
      no-node-protection;
      optimize-timer seconds; # The default value of 0 disables this option.
      path ip-address {
        (loose | strict);
      }
      subscription percent; # The range for this statement is 1 to 65535.
    }
  }
}
```

For more information about multiple bypass LSPs for link-protected LSPs, manually configured bypass LSPs, and link protection priority, see the *JUNOS MPLS Applications Configuration Guide*.

Example: MPLS LSP Link Protection Configuration

Figure 38: MPLS LSP Link Protection Topology Diagram



In Figure 38, a primary MPLS LSP is established from Router 1 through Router 3 to destination Router 2. To implement link protection, include the link-protection statement on the primary LSP at the ingress point and on the appropriate downstream RSVP interfaces you wish to protect. In this case, the primary LSP named Protected_LSP on Router 1 requires link protection, as does the so-7/3/2 RSVP interface of Router 1 and the so-6/0/0 RSVP interface of Router 3. After link protection is enabled for the protected LSP, bypass LSPs are established automatically for the LSP-traversed interfaces of Routers 1 and 3.

On Router 1, configure an interior gateway protocol (IGP) routing protocol (in this case, IS-IS), RSVP, and MPLS on the so-0/0/0 and so-7/3/2 interfaces. Next, configure the primary LSP on Router 1 to point to the loopback address of Router 2. The primary LSP's strict path must travel through Router 3.

Enable link protection on both the LSP itself and the outgoing RSVP interface traversed by the primary LSP (in this case, the so-7/3/2 RSVP interface of Router 1). After you enable link protection, the router notices that the primary LSP is protected and prepares a bypass LSP.

Configure a static route of 10.31.5.1 in the LSP on Router 1. You can use this route for testing purposes. Also, if you want to enable Packet Forwarding Engine local repair, establish a policy that requires all traffic to use per-packet load balancing. Once this policy is configured, export it to the neighboring routers with the export statement at the [edit routing-options forwarding-table] hierarchy level.

```

Router 1 [edit]
interfaces {
  so-0/0/0 {
    unit 0 {
      family inet {
        address 10.31.3.1/30;
      }
      family iso;
      family mpls;
    }
  }
  so-7/3/2 {
    unit 0 {
      family inet {
        address 10.31.1.1/30;
      }
      family iso;
      family mpls;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.245.71.51/32;
      }
      family iso {
      }
    }
  }
}

```

```

protocols {
  rsvp {
    interface so-7/3/2.0 {
      link-protection; # Enable link protection on the interface carrying the main LSP
    }
    interface so-0/0/0.0 {
    }
  }
  mpls {
    label-switched-path Protected_LSP {
      to 10.245.71.52;
      install 10.31.5.1/32 active; # This route is used for testing the LSPs.
      link-protection; # Enable link protection on the protected LSP
      primary path1;
    }
    path path1 {
      10.31.1.2 strict;
    }
    interface so-0/0/0.0;
    interface so-7/3/2.0;
  }
  isis {
    level 2 wide-metrics-only;
    interface so-0/0/0.0 {
      level 1 disable;
      level 2 {
        metric 100;
        te-metric 100;
      }
    }
    interface so-7/3/2.0 {
      level 1 disable;
      level 2 {
        metric 10;
        te-metric 10;
      }
    }
    interface lo0.0 {
      passive;
    }
  }
}
routing-options {
  forwarding-table { # Apply this policy to the forwarding table only
    export pplb; # if Packet Forwarding Engine local repair is needed.
  }
}
policy-options {
  policy-statement pplb {
    then { # Configure this policy only if
      load-balance per-packet; # Packet Forwarding Engine local repair is needed.
    }
  }
}

```

On Router 2, no link protection configuration is needed. However, you should configure MPLS, RSVP, and IS-IS to communicate with the other routers.

```
Router 2 [edit]
interfaces {
  so-0/0/0 {
    unit 0 {
      family inet {
        address 10.31.3.2/30;
      }
      family iso;
      family mpls;
    }
  }
  so-7/1/0 {
    unit 0 {
      family inet {
        address 10.31.2.1/30;
      }
      family iso;
      family mpls;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.245.71.53/32;
      }
      family iso {
      }
    }
  }
}
```

```
protocols {
  rsvp {
    interface so-0/0/0.0;
    interface so-7/1/0.0;
  }
  mpls {
    interface so-0/0/0.0;
    interface so-7/1/0.0;
  }
  isis {
    level 2 wide-metrics-only;
    interface so-0/0/0.0 {
      level 1 disable;
      level 2 {
        metric 100;
        te-metric 100;
      }
    }
    interface so-7/1/0.0 {
      level 1 disable;
      level 2 {
        metric 10;
        te-metric 10;
      }
    }
    interface lo0.0 {
      passive;
    }
  }
}
```

On Router 3, include IS-IS, RSVP, and MPLS on the so-1/0/0 and so-6/0/0 interfaces. Enable link protection on the remaining RSVP interface traversed by the primary LSP (in this case, the so-6/0/0 RSVP interface). After you enable link protection, the router notices the primary LSP is protected and prepares a bypass LSP.

To enable Packet Forwarding Engine local repair, establish a policy that requires traffic to use per-packet load balancing. Once this policy is configured, export it to the neighboring routers.

```

Router 3 [edit]
interfaces {
  so-1/0/0 {
    unit 0 {
      family inet {
        address 10.31.1.2/30;
      }
      family iso;
      family mpls;
    }
  }
  so-6/0/0 {
    unit 0 {
      family inet {
        address 10.31.2.2/30;
      }
      family iso;
      family mpls;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.245.271.53/32;
      }
      family iso {
      }
    }
  }
}

```

```

protocols {
  rsvp {
    interface so-1/0/0.0;
    interface so-6/0/0.0 { # Primary interface going to Router 2.
      link-protection;
    }
  }
  mpls {
    interface so-1/0/0.0;
    interface so-6/0/0.0;
  }
  isis {
    level 2 wide-metrics-only;
    interface so-1/0/0.0 {
      level 1 disable;
      level 2 {
        metric 10;
        te-metric 10;
      }
    }
    interface so-6/0/0.0 {
      level 1 disable;
      level 2 {
        metric 10;
        te-metric 10;
      }
    }
    interface lo0.0 {
      passive;
    }
  }
}
policy-options {
  policy-statement pplb {
    then {
      load-balance per-packet; # If Packet Forwarding Engine local repair is needed.
    }
  }
}
routing-options {
  forwarding-table {
    export pplb; # If Packet Forwarding Engine local repair is needed.
  }
}

```

Checking Your Work

To verify proper operation of MPLS LSP link protection, use the following commands:

```
show mpls lsp
show route
show route forwarding-table
show rsvp interface detail
show rsvp neighbor detail
show rsvp session detail
```

The following sections show the output of these commands used with the configuration example:

Case 1: Normal Operation on page 386

Case 2: When the Link from Router 1 to Router 3 Is Disabled on page 394

Case 3: When the Link from Router 3 to Router 2 Is Disabled on page 397

Case 1: Normal Operation

Once link protection is enabled on the required RSVP interfaces and primary LSP, the bypass LSPs are prepared.

```
Router 1 user@Router1> show mpls lsp
Ingress LSP: 1 sessions
To      From      State Rt ActivePath  P  LSPname
10.245.71.52 10.245.71.51 Up  1 path1    *  Protected_LSP

# This is the main LSP

Total 1 displayed, Up 1, 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
10.245.71.52 10.245.271.53 Up  1 1 SE 100003 0
Bypass->10.31.2.1

# This is the bypass LSP from Router 3 to Router 2.

Total 1 displayed, Up 1, Down 0
```

```
user@Router1> show rsvp session detail
```

```
Ingress RSVP: 2 sessions
```

```
10.245.71.52
```

```
From: 10.245.71.51, LSPstate: Up, ActiveRoute: 1  
LSPname: Protected_LSP
```

```
# This is the main LSP. Notice that a backup LSP is not signaled when the main LSP is still up.
```

```
Resv style: 1 SE, Label in: -, Label out: 100007  
Time left: -, Since: Thu Aug 8 12:13:24 2002  
Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500  
Port number: sender 2 receiver 33 protocol 0  
Link protection desired  
Type: Link protected LSP  
PATH rcvfrom: localclient  
PATH sentto: 10.31.1.2 (so-7/3/2.0) 36 pkts  
RESV rcvfrom: 10.31.1.2 (so-7/3/2.0) 38 pkts  
Explct route: 10.31.1.2 10.31.2.1  
Record route: <self> 10.31.1.2 10.31.2.1
```

```
10.245.271.53
```

```
From: 10.245.71.51, LSPstate: Up, ActiveRoute: 0  
LSPname: Bypass->10.31.1.2
```

```
# This is the bypass from Router 1 to Router 2. This also appears in show mpls lsp above.
```

```
Resv style: 1 SE, Label in: -, Label out: 100000  
Time left: -, Since: Thu Aug 8 12:14:31 2002  
Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500  
Port number: sender 1 receiver 51 protocol 0  
Type: Bypass LSP  
PATH rcvfrom: localclient  
PATH sentto: 10.31.3.2 (so-0/0/0.0) 32 pkts  
RESV rcvfrom: 10.31.3.2 (so-0/0/0.0) 32 pkts  
Explct route: 10.31.3.2 10.31.2.2  
Record route: <self> 10.31.3.2 10.31.2.2  
Total 2 displayed, Up 2, Down 0
```

```
Egress RSVP: 0 sessions
```

```
Total 0 displayed, Up 0, Down 0
```

```
Transit RSVP: 1 sessions
```

```
10.245.71.52
```

```
From: 10.245.271.53, LSPstate: Up, ActiveRoute: 1  
LSPname: Bypass->10.31.2.1
```

```
Resv style: 1 SE, Label in: 100003, Label out: 0  
Time left: 52, Since: Thu Aug 8 12:03:27 2002  
Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500  
Port number: sender 1 receiver 19 protocol 0  
PATH rcvfrom: 10.31.1.2 (so-7/3/2.0) 76 pkts  
PATH sentto: 10.31.3.2 (so-0/0/0.0) 77 pkts  
RESV rcvfrom: 10.31.3.2 (so-0/0/0.0) 78 pkts  
Explct route: 10.31.3.2  
Record route: 10.31.1.2 <self> 10.31.3.2  
Total 1 displayed, Up 1, Down 0
```

```

user@Router1> show RSVP interface detail
RSVP interface: 2 active
fxp0.0 Index 1, State Dis/Up
NoAuthentication, NoAggregate, NoReliable, NoLinkProtection
HelloInterval 9(second)
Address 192.168.71.52
PacketType      Total          Last 5 seconds
      Sent Received      Sent Received
Path            0          0          0          0
PathErr         0          0          0          0
PathTear        0          0          0          0
Resv            0          0          0          0
ResvErr         0          0          0          0
ResvTear        0          0          0          0
Hello           0          0          0          0
Ack             0          0          0          0
Srefresh        0          0          0          0
EndtoEnd RSVP  0          0          0          0

so-0/0/0.0 Index 8, State Ena/Up
NoAuthentication, NoAggregate, NoReliable, NoLinkProtection
HelloInterval 20(second)
Address 10.31.3.1, 10.245.71.51
ActiveResv 2, PreemptionCnt 0, Update threshold 10%
Subscription 100%, StaticBW 622.08Mbps, AvailableBW 622.08Mbps
PacketType      Total          Last 5 seconds
      Sent Received      Sent Received
Path            441          0          0          0
PathErr         0          0          0          0
PathTear        3          0          0          0
Resv            0          431         0          0
ResvErr         0          0          0          0
ResvTear        0          0          0          0
Hello           489          487         0          0
Ack             0          0          0          0
Srefresh        0          0          0          0
EndtoEnd RSVP  0          0          0          0

so-7/3/2.0 Index 11, State Ena/Up
NoAuthentication, NoAggregate, NoReliable, LinkProtection

# Link protection is enabled.

HelloInterval 3(second)
Address 10.31.1.1, 10.245.71.51
ActiveResv 1, PreemptionCnt 0, Update threshold 10%
Subscription 100%, StaticBW 2.48832Gbps, AvailableBW 2.48832Gbps
PacketType      Total          Last 5 seconds
      Sent Received      Sent Received
Path            225          138         0          0
PathErr         12          4          0          0
PathTear        5          3          0          0
Resv            134          216         0          1
ResvErr         0          0          0          0
ResvTear        3          1          0          0
Hello           750          799         1          1
Ack             0          0          0          0
Srefresh        0          0          0          0
EndtoEnd RSVP  0          0          0          0

```

```

user@Router1> show RSVP neighbor detail
RSVP neighbor: 2 learned
Address: 10.31.1.2 via: so-7/3/2.0 status: Up
Last changed time: 38:17, Idle: 5 sec, Up cnt: 1, Down cnt: 0
Message received: 329
Hello: sent 747, received: 747, interval: 3 sec
Remote instance: 0x41b21a47, Local instance: 0x238fa919
Refresh reduction: not operational
Link protection: enabled # This should be enabled
LSP name: Bypass->10.31.1.2
Bypass LSP: operational, Backup routes: 2, Backup LSPs: 0

```

The number of backup routes equals 2 because the main LSP is already considered for protection.

```

Bypass explicit route: 10.31.3.2 10.31.2.2

Address: 10.31.3.2 via: so-0/0/0.0 status: Up
Last changed time: 17:46, Idle: 5 sec, Up cnt: 4, Down cnt: 3
Message received: 430
Hello: sent 506, received: 486, interval: 20 sec
Remote instance: 0x194fa7af, Local instance: 0x507b7c2a
Refresh reduction: not operational
Link protection: disabled
Bypass LSP: does not exist, Backup routes: 0, Backup LSPs: 0

```

```

user@Router1> show route 10.31.5.1 extensive

inet.0: 24 destinations, 24 routes (22 active, 0 holddown, 2 hidden)
10.31.5.1/32 (1 entry, 1 announced)
State: <FlashAll>
TSI:
KRT in-kernel 10.31.5.1/32 -> {0.0.0.0, 0.0.0.0}
*RSVP Preference: 7
Next hop: via so-7/3/2.0 weight 1, selected

```

This is the main LSP

```

Label-switched-path Protected_LSP
Label operation: Push 100007
Next hop: via so-0/0/0.0 weight 20001

```

This is a backup route, though the backup LSP has not been signaled yet.

```

Label-switched-path Bypass->10.31.1.2
Label operation: Push 100007, Push 100000(top)[0]
State: <Active Int>
Local AS: 69
Age: 8:34 Metric: 20
Task: RSVP
Announcement bits (1): 0-KRT
AS path: I

```

```
user@Router1> show route forwarding-table destination 10.31.5.1 extensive
```

```
Routing table: inet [Index 0]
```

```
Internet:
```

```
Destination: 10.31.5.1/32
```

```
Route type: user      Route reference: 0
```

```
Flags: sent to PFE
```

```
Next-hop type: unilist      Index: 39      Reference: 1
```

```
Next-hop type: Push 100007
```

```
Next-hop interface: so-7/3/2.0      Weight: 1
```

```
# Packet Forwarding Engine local repair is enabled (otherwise, only one entry appears for Next-hop).
```

```
Next-hop type: Push 100007, Push 100000(top)[0]
```

```
Next-hop interface: so-0/0/0.0      Weight: 20001
```

```
# The Weight value for the backup starts at 20000.
```

```

Router 3 user@Router3> show mpls lsp
Ingress LSP: 0 sessions

# The ingress bypass LSP to Router 2 does not appear here.

Total 0 displayed, Up 0, Down 0

Egress LSP: 1 sessions
To      From      State Rt Style Labelin Labelout LSPname
10.245.271.53 10.245.71.51 Up  0 1 SE  3    -
Bypass->10.31.1.2
Total 1 displayed, Up 1, Down 0

Transit LSP: 1 sessions
To      From      State Rt Style Labelin Labelout LSPname
10.245.71.52 10.245.71.51 Up  1 1 SE 100000 0 Protected_LSP
Total 1 displayed, Up 1, Down 0

user@Router3> show RSVP session detail
Ingress RSVP: 1 sessions

10.245.71.52
From: 10.245.271.53, LSPstate: Up, ActiveRoute: 0
LSPname: Bypass->10.31.2.1

# The ingress bypass session to Router 2 from Router 1.

Suggested label received: -, Suggested label sent: -
Recovery label received: -, Recovery label sent: 100004
Resv style: 1 SE, Label in: -, Label out: 100004
Time left: -, Since: Thu Aug 8 12:27:07 2002
Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
Port number: sender 1 receiver 16 protocol 0
Type: Bypass LSP
PATH rcvfrom: localclient
PATH sentto: 10.31.1.1 (so-1/0/0.0) 3 pkts
RESV rcvfrom: 10.31.1.1 (so-1/0/0.0) 3 pkts
Explot route: 10.31.1.1 10.31.3.2
Record route: <self> 10.31.1.1 10.31.3.2
Total 1 displayed, Up 1, Down 0

Egress RSVP: 1 sessions

10.245.271.53
From: 10.245.71.51, LSPstate: Up, ActiveRoute: 0
LSPname: Bypass->10.31.1.2

# The bypass from Router 1 to Router 3, arriving by way of Router 2.

Suggested label received: -, Suggested label sent: -
Recovery label received: -, Recovery label sent: -
Resv style: 1 SE, Label in: 3, Label out: -
Time left: 54, Since: Thu Aug 8 12:26:48 2002
Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
Port number: sender 1 receiver 52 protocol 0
PATH rcvfrom: 10.31.2.1 (so-6/0/0.0) 5 pkts
PATH sentto: localclient
RESV rcvfrom: localclient
Record route: 10.31.3.1 10.31.2.1 <self>
Total 1 displayed, Up 1, Down 0

```

```

Transit RSVP: 1 sessions

10.245.71.52
From: 10.245.71.51, LSPstate: Up, ActiveRoute: 1
LSPname: Protected_LSP

# This is the main LSP

Suggested label received: -, Suggested label sent: -
Recovery label received: -, Recovery label sent: 0
Resv style: 1 SE, Label in: 100000, Label out: 0
Time left: 41, Since: Thu Aug 8 12:26:39 2002
Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
Port number: sender 2 receiver 33 protocol 0
Link protection desired
Type: Link protected LSP
PATH rcvfrom: 10.31.1.1 (so-1/0/0.0) 9 pkts
PATH sentto: 10.31.2.1 (so-6/0/0.0) 11 pkts
RESV rcvfrom: 10.31.2.1 (so-6/0/0.0) 10 pkts
Explot route: 10.31.2.1
Record route: 10.31.1.1 <self> 10.31.2.1
Total 1 displayed, Up 1, Down 0

user@Router3> show RSVP neighbor detail
RSVP neighbor: 2 learned
Address: 10.31.2.1 via: so-6/0/0.0 status: Up
Last changed time: 27, Idle: 0 sec, Up cnt: 1, Down cnt: 0
Message received: 19
Hello: sent 6, received: 6, interval: 9 sec
Remote instance: 0x625d2852, Local instance: 0x327317df
Refresh reduction: not operational
Link protection: enabled
LSP name: Bypass->10.31.2.1
Bypass LSP: operational, Backup routes: 1, Backup LSPs: 0

# Backup routes = 1

Bypass explicit route: 10.31.1.1 10.31.3.2

Address: 10.31.1.1 via: so-1/0/0.0 status: Up
Last changed time: 41, Idle: 0 sec, Up cnt: 1, Down cnt: 0
Message received: 15
Hello: sent 17, received: 17, interval: 3 sec
Remote instance: 0x2ebdcf43, Local instance: 0x643d9e23
Refresh reduction: not operational
Link protection: disabled
Bypass LSP: does not exist, Backup routes: 0, Backup LSPs: 0

```

```

user@Router3> show RSVP interface detail
RSVP interface: 2 active
fxp0.0 Index 1, State Dis/Up
NoAuthentication, NoAggregate, NoReliable, NoLinkProtection
HelloInterval 9(second)
Address 192.168.6.64
PacketType      Total          Last 5 seconds
      Sent  Received      Sent  Received
Path            0           0         0       0
PathErr         0           0         0       0
PathTear        0           0         0       0
Resv            0           0         0       0
ResvErr         0           0         0       0
ResvTear        0           0         0       0
Hello           0           0         0       0
Ack             0           0         0       0
Srefresh        0           0         0       0
EndtoEnd RSVP  0           0         0       0

so-1/0/0.0 Index 6, State Ena/Up
NoAuthentication, NoAggregate, NoReliable, NoLinkProtection
HelloInterval 3(second)
Address 10.31.1.2, 10.245.271.53
ActiveResv 1, PreemptionCnt 0, Update threshold 10%
Subscription 100%, StaticBW 2.48832Gbps, AvailableBW 2.48832Gbps
PacketType      Total          Last 5 seconds
      Sent  Received      Sent  Received
Path            5           14         0       1
PathErr         0           0         0       0
PathTear        0           0         0       0
Resv            8           9          0       0
ResvErr         0           0         0       0
ResvTear        0           0         0       0
Hello           23          25         2       2
Ack             0           0         0       0
Srefresh        0           0         0       0
EndtoEnd RSVP  0           0         0       0

so-6/0/0.0 Index 9, State Ena/Up
NoAuthentication, NoAggregate, NoReliable, LinkProtection

# Link protection is enabled.

HelloInterval 9(second)
Address 10.31.2.2, 10.245.271.53
ActiveResv 1, PreemptionCnt 0, Update threshold 10%
Subscription 100%, StaticBW 9.95328Gbps, AvailableBW 9.95328Gbps
PacketType      Total          Last 5 seconds
      Sent  Received      Sent  Received
Path            12           8          0       0
PathErr         0           0         0       0
PathTear        0           1         0       0
Resv            9           14         0       1
ResvErr         0           0         0       0
ResvTear        0           0         0       0
Hello           8           8          1       1
Ack             0           0         0       0
Srefresh        0           0         0       0
EndtoEnd RSVP  0           0         0       0

```

```

user@Router3> show route forwarding-table family mpls
Routing table: ccc
MPLS:
Destination  Type RtRef Next hop      Type Index NhRef Netif
default      perm  0          dsced  1  1
0            user  0          recv   3  3
1            user  0          recv   3  3
2            user  0          recv   3  3
100000      user  0          ulst   77  1

```

This is the main LSP.

```

Swap 0 so-6/0/0.0
Swap 100004[0] so-1/0/0.0
100000(S=0)  user  0          ulst   78  1
Pop so-6/0/0.0
Swap 100004[0] so-1/0/0.0
100007      user  0          ulst   71  1

```

The bypass LSP from Router 1 to Router 2.

```

Swap 0 so-6/0/0.0
Swap 100003[0] so-1/0/0.0
100007(S=0)  user  0          ulst   73  1
Pop so-6/0/0.0
Swap 100003[0] so-1/0/0.0

```

Case 2: When the Link from Router 1 to Router 3 Is Disabled

```

[edit]
user@Router1# set interfaces so-7/3/2 disable

```

The primary interface from Router 1 to Router 3 is disabled.

```

[edit]
user@Router1# commit
commit complete

```

```

Router 1 user@Router1> show mpls lsp
Ingress LSP: 1 sessions
To      From      State Rt ActivePath  P  LSPname
10.245.71.52 10.245.71.51 Up  0 path1      *  Protected_LSP

# The main LSP is up.

Total 1 displayed, Up 1, 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
10.245.71.52 10.245.271.53 Up  0 1 SE 100004  0
Bypass->10.31.2.1

# The bypass LSP from Router 3 to Router 2.

Total 1 displayed, Up 1, Down 0

user@Router1> show RSVP session detail
Ingress RSVP: 3 sessions

10.245.71.52
From: 10.31.3.1, LSPstate: Up, ActiveRoute: 0
LSPname: Protected_LSP

# The newly signaled backup LSP, as indicated by the To/From field.

Resv style: 1 SE, Label in: -, Label out: 100000
Time left: -, Since: Thu Aug 8 12:29:16 2002
Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
Port number: sender 2 receiver 33 protocol 0
Link protection desired
Type: Backup LSP at Point-of-Local-Repair
PATH rcvfrom: localclient
PATH sentto: 10.31.1.2 (so-0/0/0.0) 4 pkts
RESV rcvfrom: 10.31.2.2 (so-0/0/0.0) 3 pkts
Explct route: 10.31.2.2 10.31.2.1
Record route: <self> 10.31.2.2 10.31.2.1

10.245.71.52
From: 10.245.71.51, LSPstate: Dn, ActiveRoute: 0

# The original LSP is now down.

LSPname: Protected_LSP
Resv style: 0 -, Label in: -, Label out: -
Time left: -, Since: Thu Aug 8 12:13:24 2002
Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
Port number: sender 2 receiver 33 protocol 0
Link protection desired
Type: Link protected LSP
PATH rcvfrom: localclient
PATH sentto: [no route]
Explct route: 10.31.1.2 10.31.2.1
Record route: <self> ...incomplete

10.245.271.53
From: 10.245.71.51, LSPstate: Up, ActiveRoute: 1
LSPname: Bypass->10.31.1.2

```

The bypass LSP from Router 1 to Router 2.

```

Resv style: 1 SE, Label in: -, Label out: 100001
Time left: -, Since: Thu Aug 8 12:26:48 2002
Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
Port number: sender 1 receiver 52 protocol 0
Type: Bypass LSP
PATH rcvfrom: localclient
PATH sentto: 10.31.3.2 (so-0/0/0.0) 13 pkts
RESV rcvfrom: 10.31.3.2 (so-0/0/0.0) 13 pkts
Explct route: 10.31.3.2 10.31.2.2
Record route: <self> 10.31.3.2 10.31.2.2
Total 3 displayed, Up 2, Down 1

```

```

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

```

```

Transit RSVP: 1 sessions

```

```

10.245.71.52
From: 10.245.271.53, LSPstate: Up, ActiveRoute: 0
LSPname: Bypass->10.31.2.1

```

The bypass LSP from Router 3 to Router 2, which will fail in the next case.

```

Resv style: 1 SE, Label in: 100004, Label out: 0
Time left: 38, Since: Thu Aug 8 12:27:07 2002
Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
Port number: sender 1 receiver 16 protocol 0
PATH rcvfrom: 10.31.1.2 (so-7/3/2.0) 11 pkts
PATH sentto: 10.31.3.2 (so-0/0/0.0) 12 pkts
RESV rcvfrom: 10.31.3.2 (so-0/0/0.0) 12 pkts
Explct route: 10.31.3.2
Record route: 10.31.1.2 <self> 10.31.3.2
Total 1 displayed, Up 1, Down 0

```

```

user@Router1> show rsvp neighbor detail
RSVP neighbor: 2 learned
Address: 10.31.1.2 via: so-7/3/2.0 status: Down

```

The neighbor is down.

```

Last changed time: 25, Idle: 25 sec, Up cnt: 2, Down cnt: 2
Message received: 397
Hello: sent 900, received: 890, interval: 3 sec
Remote instance: 0x0, Local instance: 0x41b41b17
Refresh reduction: not operational
Link protection: enabled
  LSP name: Bypass->10.31.1.2
  Bypass LSP: operational, Backup routes: 2, Backup LSPs: 1
  Bypass explicit route: 10.31.3.2 10.31.2.2

Address: 10.31.3.2 via: so-0/0/0.0 status: Up
Last changed time: 25:40, Idle: 5 sec, Up cnt: 4, Down cnt: 3
Message received: 502
Hello: sent 558, received: 538, interval: 20 sec
Remote instance: 0x194fa7af, Local instance: 0x507b7c2a
Refresh reduction: not operational
Link protection: disabled
  Bypass LSP: does not exist, Backup routes: 0, Backup LSPs: 0

```

```
user@Router1> show route 10.31.5.1
```

```
inet.0: 23 destinations, 23 routes (22 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both
```

```
10.31.5.1/32   *[RSVP/7] 00:03:04, metric 20
               > via so-0/0/0.0, label-switched-path Bypass->10.31.1.2
```

```
# The route can be reached by way of the backup LSP
```

```
user@Router1> show route forwarding-table destination 10.31.5.1
```

```
Routing table: inet
```

```
Internet:
```

Destination	Type	RtRef	Next hop	Type	Index	NhRef	Netif
10.31.5.1/32	user	0	Push 100000, Push 100001(top)[0]				
so-0/0/0.0							

```
# Double-stacked labels appear on the backup LSP from Router 1 to 2 to 3.
```

```
Before proceeding to Case 3, re-enable the so-7/3/2 interface on Router 1.
```

```
[edit]
```

```
user@Router1# delete interfaces so-7/3/2 disable
```

```
[edit]
```

```
user@Router1# commit
```

```
commit complete
```

Case 3: When the Link from Router 3 to Router 2 Is Disabled

```
[edit]
```

```
user@Router3# set interfaces so-6/0/0 disable
```

```
# The primary interface from Router 3 to Router 2 is disabled.
```

```
[edit]
```

```
user@Router3# commit
```

```
commit complete
```

```

Router 3 user@Router3> show rsvp session
Ingress RSVP: 2 sessions
To      From      State Rt Style Labelin Labelout LSPName
10.245.71.52 10.245.271.53 Up   1 1 SE   - 100005
Bypass->10.31.2.1
10.245.71.52 10.31.1.2   Up   0 1 SE   -   0 Protected_LSP

# The backup is signaled from Router 3 to Router 2.

Total 2 displayed, Up 2, Down 0

Egress RSVP: 1 sessions
To      From      State Rt Style Labelin Labelout LSPName
10.245.271.53 10.245.71.51 Up   0 1 SE   3   -
Bypass->10.31.1.2
Total 1 displayed, Up 1, Down 0

Transit RSVP: 1 sessions
To      From      State Rt Style Labelin Labelout LSPName
10.245.71.52 10.245.71.51 Dn   0 0 - 100000 - Protected_LSP

# The main LSP is down.

Total 1 displayed, Up 0, Down 1

user@Router3> show rsvp session detail
Ingress RSVP: 2 sessions

10.245.71.52
From: 10.245.271.53, LSPstate: Up, ActiveRoute: 1
LSPName: Bypass->10.31.2.1
Suggested label received: -, Suggested label sent: -
Recovery label received: -, Recovery label sent: 100005
Resv style: 1 SE, Label in: -, Label out: 100005
Time left: -, Since: Thu Aug 8 12:31:09 2002
Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
Port number: sender 1 receiver 17 protocol 0
Type: Bypass LSP
PATH rcvfrom: localclient
PATH sentto: 10.31.1.1 (so-1/0/0.0) 6 pkts
RESV rcvfrom: 10.31.1.1 (so-1/0/0.0) 6 pkts
Explot route: 10.31.1.1 10.31.3.2
Record route: <self> 10.31.1.1 10.31.3.2

10.245.71.52
From: 10.31.1.2, LSPstate: Up, ActiveRoute: 0
LSPName: Protected_LSP
Suggested label received: -, Suggested label sent: -
Recovery label received: -, Recovery label sent: 0
Resv style: 1 SE, Label in: -, Label out: 0
Time left: -, Since: Thu Aug 8 12:31:59 2002
Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
Port number: sender 2 receiver 33 protocol 0
Link protection desired
Type: Backup LSP at Point-of-Local-Repair

# This is the backup LSP

```

```

PATH rcvfrom: localclient
PATH sentto: 10.31.2.1 (so-1/0/0.0) 5 pkts
RESV rcvfrom: 10.31.3.2 (so-1/0/0.0) 2 pkts
Explct route: 10.31.3.2
Record route: <self> 10.31.3.2
Total 2 displayed, Up 2, Down 0

```

Egress RSVP: 1 sessions

```

10.245.271.53
From: 10.245.71.51, LSPstate: Up, ActiveRoute: 0
LSPname: Bypass->10.31.1.2
Suggested label received: -, Suggested label sent: -
Recovery label received: -, Recovery label sent: -
Resv style: 1 SE, Label in: 3, Label out: -
Time left: 31, Since: Thu Aug 8 12:26:48 2002
Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
Port number: sender 1 receiver 52 protocol 0
PATH rcvfrom: 10.31.2.1 (so-6/0/0.0) 23 pkts
PATH sentto: localclient
RESV rcvfrom: localclient
Record route: 10.31.3.1 10.31.2.1 <self>
Total 1 displayed, Up 1, Down 0

```

Transit RSVP: 1 sessions

```

10.245.71.52
From: 10.245.71.51, LSPstate: Dn, ActiveRoute: 0
LSPname: Protected_LSP
Suggested label received: -, Suggested label sent: -
Recovery label received: -, Recovery label sent: -
Resv style: 0 -, Label in: 100000, Label out: -
Time left: 53, Since: Thu Aug 8 12:26:39 2002
Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
Port number: sender 2 receiver 33 protocol 0
Link protection desired
Type: Link protected LSP
PATH rcvfrom: 10.31.1.1 (so-1/0/0.0) 30 pkts
PATH sentto: [no route]
Explct route: 10.31.2.1
Record route: 10.31.1.1 <self> ...incomplete
Total 1 displayed, Up 0, Down 1

```

```
user@Router3> show route forwarding-table family mpls
```

```
Routing table: ccc
```

```
MPLS:
```

Destination	Type	RtRef	Next hop	Type	Index	NhRef	Netif
default	perm	0	dscd	1	1		
0	user	0	recv	3	3		
1	user	0	recv	3	3		
2	user	0	recv	3	3		
100000	user	0	Swap	100005[0]			so-1/0/0.0

This shows label swapping for the main LSP traveling over the backup LSP through Router 2.

```

Router 1 user@Router1> show rsvp session detail
Ingress RSVP: 1 sessions

10.245.71.52
From: 10.245.71.51, LSPstate: Up, ActiveRoute: 1
LSPname: Protected_LSP

# The main LSP is not affected.

Resv style: 1 SE, Label in: -, Label out: 100000
Time left: -, Since: Thu Aug 8 12:13:24 2002
Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
Port number: sender 2 receiver 33 protocol 0
Link protection desired
PATH rcvfrom: localclient
PATH sentto: 10.31.1.2 (so-7/3/2.0) 95 pkts
RESV rcvfrom: 10.31.1.2 (so-7/3/2.0) 87 pkts
Explct route: 10.31.1.2 10.31.2.1
Record route: <self> 10.31.1.2 10.31.3.2
Total 1 displayed, Up 1, Down 0

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

Transit RSVP: 1 sessions

10.245.71.52
From: 10.245.271.53, LSPstate: Up, ActiveRoute: 0
LSPname: Bypass->10.31.2.1

# The bypass LSP is listed, because Router 1 does not know of the backup from
Router 3 to Router 2.

Resv style: 1 SE, Label in: 100005, Label out: 0
Time left: 53, Since: Thu Aug 8 12:31:09 2002
Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
Port number: sender 1 receiver 17 protocol 0
PATH rcvfrom: 10.31.1.2 (so-7/3/2.0) 11 pkts
PATH sentto: 10.31.3.2 (so-0/0/0.0) 11 pkts
RESV rcvfrom: 10.31.3.2 (so-0/0/0.0) 11 pkts
Explct route: 10.31.3.2
Record route: 10.31.1.2 <self> 10.31.3.2
Total 1 displayed, Up 1, Down 0

user@Router1> show route forwarding-table family mpls
Routing table: ccc
MPLS:
Destination      Type RtRef Next hop      Type Index NhRef Netif
default          perm  0          dscd  8  1
0                user  0          rcv   10  3
1                user  0          rcv   10  3
2                user  0          rcv   10  3
100005          user  0          Swap  0  so-0/0/0.0

# Swapping labels on the bypass LSP

100005(S=0)      user  0          Pop    so-0/0/0.0

```

```
user@Router1> show route forwarding-table destination 10.31.5.1 extensive
```

```
Routing table: inet [Index 0]
```

```
Internet:
```

```
Destination: 10.31.5.1/32
```

```
Route type: user          Route reference: 0
```

```
Flags: sent to PFE
```

```
Next-hop type: Push 100000
```

There is only one entry here. The bypass to Router 3 is broken because the connection between Router 3 and Router 2 is disabled.

```
Next-hop interface: so-7/3/2.0
```

```
user@Router1> show isis adjacency
```

Interface	System	L State	Hold (secs)	SNPA
so-0/0/0.0	Router2	2 Up	24	
so-7/3/2.0	Router3	2 Up	23	

```
user@Router1> show route 10.31.5.1 extensive
```

```
inet.0: 22 destinations, 22 routes (21 active, 0 holddown, 1 hidden)
```

```
10.31.5.1/32 (1 entry, 1 announced)
```

```
State: <FlashAll>
```

```
TSI:
```

```
KRT in-kernel 10.31.5.1/32 -> {0.0.0.0}
```

```
*RSVP Preference: 7
```

```
Next hop: via so-7/3/2.0 weight 1, selected
```

Only one entry is shown.

```
Label-switched-path Protected_LSP
```

```
Label operation: Push 100000
```

```
State: <Active Int>
```

```
Local AS: 69
```

```
Age: 2:21 Metric: 100
```

```
Task: RSVP
```

```
Announcement bits (1): 0-KRT
```

```
AS path: I
```

```
user@Router1> show rsvp neighbor detail
```

```
RSVP neighbor: 2 learned
```

```
Address: 10.31.1.2 via: so-7/3/2.0 status: Up
```

```
Last changed time: 2:58, Idle: 0 sec, Up cnt: 3, Down cnt: 2
```

```
Message received: 433
```

```
Hello: sent 965, received: 950, interval: 3 sec
```

```
Remote instance: 0x74be7c42, Local instance: 0x41b41b17
```

```
Refresh reduction: not operational
```

```
Link protection: disabled
```

```
Bypass LSP: does not exist, Backup routes: 0, Backup LSPs: 0
```

```
Address: 10.31.3.2 via: so-0/0/0.0 status: Up
```

```
Last changed time: 30:54, Idle: 0 sec, Up cnt: 4, Down cnt: 3
```

```
Message received: 533
```

```
Hello: sent 593, received: 573, interval: 20 sec
```

```
Remote instance: 0x194fa7af, Local instance: 0x507b7c2a
```

```
Refresh reduction: not operational
```

```
Link protection: disabled
```

```
Bypass LSP: does not exist, Backup routes: 0, Backup LSPs: 0
```

```

user@Router1> show rsvp session
Ingress RSVP: 1 sessions
To      From      State Rt Style Labelin Labelout LSPname
10.245.71.52 10.245.71.51 Up   1 1 SE   - 100000 Protected_LSP
Total 1 displayed, Up 1, Down 0

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

Transit RSVP: 1 sessions
To      From      State Rt Style Labelin Labelout LSPname
10.245.71.52 10.245.271.53 Up   0 1 SE 100005 0
Bypass->10.31.2.1
Total 1 displayed, Up 1, Down 0
    
```

Example: Node-Link Protection Configuration

Figure 39: Node-Link Protection Topology Diagram

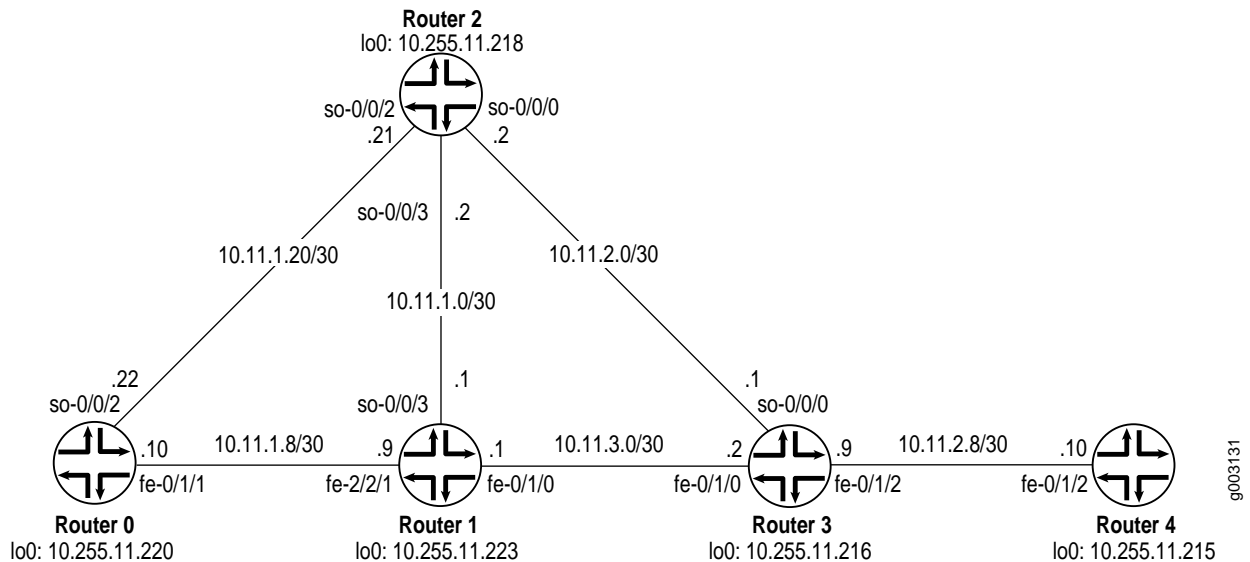


Figure 39 shows an example of how you can implement node-link protection. An LSP is initiated on Router 0 with a strict path travelling through Router 1, Router 2, Router 3, and Router 4. You configure node-link protection within the LSP and link protection on all RSVP interfaces in the path.

On router 0, configure an LSP to travel across routers 1, 2, 3, and 4. Include the node-link-protection statement in the LSP and configure link protection on outgoing RSVP interface fe-0/1/1. To support the LSP, configure OSPF, MPLS, and RSVP on the needed interfaces.

```

Router 0 [edit]
interfaces {
  fe-0/1/1 {
    unit 0 {
      family inet {
        address 10.11.1.10/30;
      }
      family mpls;
    }
  }
  so-0/0/2 {
    unit 0 {
      family inet {
        address 10.11.1.22/30;
      }
      family mpls;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.255.11.220/32;
      }
    }
  }
}

```

```

protocols {
  ospf {
    area 0.0.0.0 {
      interface lo0.0 {
        passive;
      }
      interface fe-0/1/1.0;
      interface so-0/0/2.0;
    }
    traffic-engineering;
  }
  mpls {
    statistics {
      file mplsStat.log size 1m;
      interval 30;
      display-id;
    }
    traffic-engineering bgp-igp-both-ribs;
    traceoptions {
      file mpls.log size 5m world-readable;
      flag cspf;
      flag cspf-link;
      flag cspf-node;
      flag state;
      flag error;
    }
    explicit-null;
    label-switched-path test_r0_r4 {
      from 10.255.11.220;
      to 10.255.11.215;
      node-link-protection; # Apply node-link protection to the LSP
      primary pathP;
    }
    path pathP { # Define the LSP path across routers 1, 2, 3, and 4.
      10.11.1.9 strict;
      10.11.1.2 strict;
      10.11.2.1 strict;
      10.11.2.10 strict;
    }
    interface fe-0/1/1.0;
    interface so-0/0/2.0;
  }
  rsvp {
    traceoptions {
      file rsvp.log size 3m files 12 world-readable;
      flag event;
      flag state;
      flag error;
      flag packets detail;
    }
    interface fe-0/1/1.0 {
      link-protection; # Apply link protection to RSVP interfaces in the LSP path.
    }
    interface so-0/0/2.0;
  }
}

```

On Router 1, configure link protection on outgoing RSVP interface so-0/0/3. Configure OSPF, MPLS, and RSVP on all transit interfaces.

```
Router 1 [edit]
interfaces {
  fe-0/1/0 {
    unit 0 {
      family inet {
        address 10.11.3.1/30;
      }
      family mpls;
    }
  }
  fe-2/2/1 {
    unit 0 {
      family inet {
        address 10.11.1.9/30;
      }
      family mpls;
    }
  }
  so-0/0/3 {
    unit 0 {
      family inet {
        address 10.11.1.1/30;
      }
      family mpls;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.255.11.223/32;
      }
    }
  }
}
```

```
protocols {
  ospf {
    area 0.0.0.0 {
      interface lo0.0 {
        passive;
      }
      interface fe-0/1/0.0;
      interface fe-2/2/1.0;
      interface so-0/0/3.0;
    }
    traffic-engineering;
  }
  mpls {
    traffic-engineering bgp-igp-both-ribs;
    explicit-null;
    interface fe-0/1/0.0;
    interface fe-2/2/1.0;
    interface so-0/0/3.0;
  }
  rsvp {
    interface fe-0/1/0.0;
    interface fe-2/2/1.0;
    interface so-0/0/3.0 {
      link-protection; # Apply link protection on all RSVP interfaces in the LSP path.
    }
  }
}
```

On Router 2, configure link protection on outgoing RSVP interface so-0/0/0. Configure OSPF, MPLS, and RSVP on all transit interfaces.

```
Router 2 [edit]
interfaces {
  so-0/0/0 {
    unit 0 {
      family inet {
        address 10.11.2.2/30;
      }
      family mpls;
    }
  }
  so-0/0/2 {
    unit 0 {
      family inet {
        address 10.11.1.21/30;
      }
      family mpls;
    }
  }
  so-0/0/3 {
    unit 0 {
      family inet {
        address 10.11.1.2/30;
      }
      family mpls;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.255.11.218/32;
      }
    }
  }
}
```

```
protocols {
  ospf {
    area 0.0.0.0 {
      interface lo0.0 {
        passive;
      }
      interface so-0/0/0.0;
      interface so-0/0/2.0;
      interface so-0/0/3.0;
    }
    traffic-engineering;
  }
  mpls {
    traffic-engineering bgp-igp-both-ribs;
    explicit-null;
    interface so-0/0/0.0;
    interface so-0/0/2.0;
    interface so-0/0/3.0;
  }
  rsvp {
    interface so-0/0/0.0 {
      link-protection; # Apply link protection to RSVP interfaces in the LSP path.
    }
    interface so-0/0/2.0;
    interface so-0/0/3.0;
  }
}
```

On Router 3, configure link protection on outgoing RSVP interface fe-0/1/2. Configure OSPF, MPLS, and RSVP on all transit interfaces.

```
Router 3 [edit]
interfaces {
  fe-0/1/0 {
    unit 0 {
      family inet {
        address 10.11.3.2/30;
      }
      family mpls;
    }
  }
  fe-0/1/2 {
    unit 0 {
      family inet {
        address 10.11.2.9/30;
      }
      family mpls;
    }
  }
  so-0/0/0 {
    unit 0 {
      family inet {
        address 10.11.2.1/30;
      }
      family mpls;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.255.11.216/32;
      }
    }
  }
}
```

```
protocols {
  ospf {
    area 0.0.0.0 {
      interface lo0.0 {
        passive;
      }
      interface fe-0/1/0.0;
      interface fe-0/1/2.0;
      interface so-0/0/0.0;
    }
    traffic-engineering;
  }
  mpls {
    traffic-engineering bgp-igp-both-ribs;
    explicit-null;
    interface fe-0/1/0.0;
    interface fe-0/1/2.0;
    interface so-0/0/0.0;
  }
  rsvp {
    interface fe-0/1/0.0;
    interface fe-0/1/2.0 {
      link-protection; # Apply link protection to RSVP interfaces in the LSP path.
    }
    interface so-0/0/0.0;
  }
}
```

Because Router 4 is the endpoint of the LSP, you can configure interfaces and protocols as usual. There is no need to configure any node-link protection or link protection statements on this router.

```

Router 4 [edit]
interfaces {
  fe-0/1/2 {
    unit 0 {
      family inet {
        address 10.11.2.10/30;
      }
      family mpls;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.255.11.215/32;
      }
    }
  }
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface lo0.0 {
        passive;
      }
      interface fe-0/1/2.0;
    }
    traffic-engineering;
  }
  mpls {
    traffic-engineering bgp-igp-both-ribs;
    explicit-null;
    interface fe-0/1/2.0;
  }
  rsvp {
    interface fe-0/1/2.0;
  }
}

```

Checking Your Work

To verify proper operation of MPLS LSP node-link protection, use the following commands:

```
show mpls lsp extensive
```

```
show route detail
```

```
show rsvp neighbor detail
```

```
show rsvp session detail
```

The following section shows the output of these commands used with the configuration example.

```
user@router0> show rsvp session detail
Ingress RSVP: 2 sessions

10.255.11.215
From: 10.255.11.220, LSPstate: Up, ActiveRoute: 5
LSPname: test_r0_r4, LSPpath: Primary
Suggested label received: -, Suggested label sent: -
Recovery label received: -, Recovery label sent: 100128
Resv style: 1 SE, Label in: -, Label out: 100128
Time left: -, Since: Thu May 8 13:36:58 2003
Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
Port number: sender 3 receiver 56517 protocol 0
Node/Link protection desired
Type: Node/Link protected LSP
PATH rcvfrom: localclient
PATH sentto: 10.11.1.9 (fe-0/1/1.0) 20 pkts
RESV rcvfrom: 10.11.1.9 (fe-0/1/1.0) 37 pkts
Explct route: 10.11.1.9 10.11.1.2 10.11.2.1 10.11.2.10
Record route: <self> 10.11.1.9 10.11.1.2 10.11.2.1 10.11.2.10

10.255.11.218
From: 10.255.11.220, LSPstate: Up, ActiveRoute: 0
LSPname: Bypass->10.11.1.9->10.11.1.2 # 2 next hops indicate node-link
protection.
Suggested label received: -, Suggested label sent: -
Recovery label received: -, Recovery label sent: 0
Resv style: 1 SE, Label in: -, Label out: 0
Time left: -, Since: Thu May 8 13:36:58 2003
Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
Port number: sender 1 receiver 56521 protocol 0
Type: Bypass LSP
Number of data route tunnel through: 4
Number of RSVP session tunnel through: 0
PATH rcvfrom: localclient
PATH sentto: 10.11.1.21 (so-0/0/2.0) 1 pkts
RESV rcvfrom: 10.11.1.21 (so-0/0/2.0) 1 pkts
Explct route: 10.11.1.21
Record route: <self> 10.11.1.21
Total 2 displayed, Up 2, Down 0

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

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

The `show mpls lsp extensive` command provides some useful information about link protection and node-link protection. The protection flag entry indicates a series of values. By adding the values together, you can learn the protection state of an LSP based on the total sum. Significant values for the flags include: 1 = Available (Link Protection), 2 = In Use, and 8 = Node Protection. Thus, a value of 9 means that node protection is available (1 + 8 = 9) and a value of A means that a node protected link is in use (8 + 2 = A, in hexadecimal).

```

user@router0> show mpls lsp extensive
Ingress LSP: 1 sessions

10.255.11.215
From: 10.255.11.220, State: Up, ActiveRoute: 5, LSPname: test_r0_r4
ActivePath: pathP (primary)
Node/Link protection desired
LoadBalance: Random
Encoding type: Packet, Switching type: Packet, GPID: IPv4
*Primary pathP      State: Up
  OptimizeTimer: 30
  Reoptimization in 13 second(s).
  Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 40)
10.11.1.9 S 10.11.1.2 S 10.11.2.1 S 10.11.2.10 S
  Received RRO (ProtectionFlag 1=Available 2=InUse 4=B/W 8=Node):
    10.11.1.9(flag=9 Label=100128) 10.11.1.2(flag=9 Label=100080) 10.11.2.1(flag=1 Label=100080)
10.11.2.10(Label=0)
  67 May 8 13:46:14 CSPF: computation result ignored[18 times]
  66 May 8 13:37:31 Record Route: 10.11.1.9(flag=9 Label=100128) 10.11.1.2(flag=9 Label=100080) 10.11.2.1(flag=1
Label=100080) 10.11.2.10(Label=0)
  65 May 8 13:37:28 CSPF: computation result ignored
  64 May 8 13:37:07 Record Route: 10.11.1.9(flag=9 Label=100128) 10.11.1.2(flag=1 Label=100080)
10.11.2.1(Label=100080) 10.11.2.10(Label=0)
  63 May 8 13:37:01 Record Route: 10.11.1.9(flag=9 Label=100128) 10.11.1.2(Label=100080)
10.11.2.1(Label=100080) 10.11.2.10(Label=0)
  62 May 8 13:37:01 Link-protection Up
  61 May 8 13:36:58 Selected as active path
  60 May 8 13:36:58 Record Route: 10.11.1.9(Label=100128) 10.11.1.2(Label=100080) 10.11.2.1(Label=100080)
10.11.2.10(Label=0)
  59 May 8 13:36:58 Up
  58 May 8 13:36:58 Originate Call
  57 May 8 13:36:58 CSPF: computation result accepted
  56 May 8 13:36:29 CSPF failed: no route toward 10.11.2.10[10 times]
  55 May 8 13:32:04 Clear Call
  54 May 8 13:31:40 Deselected as active
  53 May 8 13:31:40 Link-protection Down
  52 May 8 13:31:40 Down
  51 May 8 13:31:36 CSPF failed: no route toward 10.11.2.10[6 times]
  50 May 8 13:29:00 10.11.2.1: Session preempted
  49 May 8 13:28:42 Record Route: 10.11.1.9(flag=9 Label=100064) 10.11.1.2(flag=9 Label=100064)
10.11.2.1(Label=100064) 10.11.2.10(Label=0)
  48 May 8 13:28:40 CSPF failed: no route toward 10.11.2.10
  47 May 8 13:28:35 Link-protection Up
  46 May 8 13:28:35 Link-protection Down
  45 May 8 13:28:30 Link-protection Up
  44 May 8 13:28:30 Link-protection Down
  43 May 8 13:28:10 CSPF failed: no route toward 10.11.2.10
  42 May 8 13:27:44 Link-protection Up
  41 May 8 13:27:44 Link-protection Down
  40 May 8 13:27:42 Link-protection Up
  39 May 8 13:27:42 Record Route: 10.11.1.9(flag=9 Label=100064) 10.11.1.2(flag=9 Label=100064) 10.11.2.1(flag=1
Label=100064) 10.11.2.10(Label=0)
  38 May 8 13:27:41 CSPF failed: no route toward 10.11.2.10[2 times]
  37 May 8 13:27:39 CSPF: link down/deleted 10.11.2.9(eagle.00/10.255.11.216)->0.0.0.0(eagle.04/0.0.0.0)

```

```

36 May 8 13:27:39 Link-protection Down
35 May 8 13:27:39 Record Route: 10.11.1.9(Label=100064) 10.11.1.2(Label=100064) 10.11.2.1(Label=100064)
10.11.2.10(Label=0)
34 May 8 13:27:39 CSPF failed: no route toward 10.11.2.10
33 May 8 13:27:39 CSPF: link down/deleted 0.0.0.0(eagle.04/0.0.0.0)->0.0.0.0(papst.00/10.255.11.215)
32 May 8 13:27:12 CSPF: computation result ignored[16 times]
31 May 8 13:19:35 Record Route: 10.11.1.9(flag=9 Label=100064) 10.11.1.2(flag=9 Label=100048) 10.11.2.1(flag=1
Label=100048) 10.11.2.10(Label=0)
30 May 8 13:19:22 Link-protection Up
29 May 8 13:19:22 Record Route: 10.11.1.9(flag=9 Label=100064) 10.11.1.2(flag=9 Label=100048)
10.11.2.1(Label=100048) 10.11.2.10(Label=0)
28 May 8 13:19:22 Up
27 May 8 13:19:22 Link-protection Down
26 May 8 13:19:22 CSPF: computation result accepted
25 May 8 13:19:16 Link-protection Up
24 May 8 13:19:16 Link-protection Down
23 May 8 13:18:54 CSPF failed: no route toward 10.11.2.1
22 May 8 13:18:54 CSPF: link down/deleted 0.0.0.0(eagle.04/0.0.0.0)->0.0.0.0(papst.00/10.255.11.215)
21 May 8 13:18:53 CSPF failed: no route toward 10.11.2.1[2 times]
20 May 8 13:18:46 CSPF: link down/deleted 10.11.2.9(eagle.00/10.255.11.216)->0.0.0.0(eagle.04/0.0.0.0)
19 May 8 13:18:35 Record Route: 10.11.1.9(flag=9 Label=100032) 10.11.1.2(flag=9 Label=100032)
10.11.2.1(Label=100016) 10.11.2.10(Label=0)
18 May 8 13:18:35 Record Route: 10.11.1.9(flag=9 Label=100032) 10.11.1.2(Label=100032)
10.11.2.1(Label=100016) 10.11.2.10(Label=0)
Created: Thu May 8 13:13:28 2003
Total 1 displayed, Up 1, Down 0

```

```

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

```

```

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

```

```

user@router0> show rsvp neighbor detail

```

```

RSVP neighbor: 2 learned
Address: 10.11.1.9 via: fe-0/1/1.0 status: Up
Last changed time: 33:02, Idle: 5 sec, Up cnt: 1, Down cnt: 0
Message received: 130
Hello: sent 221, received: 221, interval: 9 sec
Remote instance: 0x66368e80, Local instance: 0x643f57b5
Refresh reduction: incomplete
Remote end: enabled, Ack-extension: disabled

```

```

Address: 10.11.1.21 via: so-0/0/2.0 status: Up
Last changed time: 32:41, Idle: 10 sec, Up cnt: 1, Down cnt: 0
Message received: 78
Hello: sent 218, received: 218, interval: 9 sec
Remote instance: 0x74b57f2a, Local instance: 0x66341d2f
Refresh reduction: operational
Remote end: enabled, Ack-extension: enabled

```

```

user@router0> show route 10.255.11.215 detail

```

```

inet.0: 33 destinations, 34 routes (31 active, 0 holddown, 2 hidden)
10.255.11.215/32 (2 entries, 1 announced)
State: <FlashAll>
*RSVP Preference: 7
Next hop: 10.11.1.9 via fe-0/1/1.0 weight 1, selected
Label-switched-path test_r0_r4
Label operation: Push 100128, selfID=RSVP-7
Next hop: via so-0/0/2.0 weight 20001
Label-switched-path Bypass->10.11.1.9->10.11.1.2
Label operation: Push 100080, selfID=RSVP-7, parentID=RSVP-8

```

```

State: <Active Int>
Local AS: 69
Age: 13:14 Metric: 40
Task: RSVP
Announcement bits (2): 0-KRT 3-Resolve inet.0
AS path: I
IS-IS Preference: 18
Level: 2
Next hop: 10.11.1.9 via fe-0/1/1.0, selected
State: <Int>
Inactive reason: Route Preference
Local AS: 69
Age: 13:20 Metric: 40
Task: IS-IS
AS path: I

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

10.255.11.215/32 (1 entry, 1 announced)
State: <FlashAll>
*RSVP Preference: 7
Next hop: 10.11.1.9 via fe-0/1/1.0 weight 1, selected
Label-switched-path test_r0_r4
Label operation: Push 100128, selfID=RSVP-7
Next hop: via so-0/0/2.0 weight 20001
Label-switched-path Bypass->10.11.1.9->10.11.1.2
Label operation: Push 100080, selfID=RSVP-7, parentID=RSVP-8
State: <Active Int>
Local AS: 69
Age: 13:14 Metric: 40
Task: RSVP
Announcement bits (1): 1-Resolve inet.0
AS path: I

```

For More Information

For additional information about MPLS LSP link protection or node-link protection, see the following:

JUNOS MPLS Applications Configuration Guide

P. Pan, editor, Internet draft draft-ietf-mpls-rsvp-lsp-fastreroute-07.txt, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels* (expires February 2005)

Revision History

- 2 February 2005—Added information about configuring multiple bypass LSPs, manual bypass LSPs, and link protection priority, 7.1R1 Release. Richard Hendricks.
- 6 October 2004—Added support for link protection of point-to-multipoint LSPs, 7.0R1 Release. Richard Hendricks.
- 6 July 2004—6.4R1 Release. Richard Hendricks.
- 5 April 2004—6.3R1 Release. Richard Hendricks.

- 22 December 2003—6.2R1 Release. Richard Hendricks.
- 22 September 2003—6.1R1 Release. Richard Hendricks.
- 30 June 2003—Added node-link protection, 6.0R1 Release. Richard Hendricks.
- 2 April 2003—5.7R1 Release. Richard Hendricks.
- 27 December 2002—5.6R1 Release. Richard Hendricks.
- 30 September 2002—New link protection example added for the 5.5R1 Release.
Richard Hendricks.
- 19 July 2002—5.4R1 Release. Richard Hendricks.
- 15 July 2002—Document revised based on comments from Ping Pan. Richard
Hendricks.
- 28 May 2002—Document revised and reformatted. Richard Hendricks.
- 18 March 2002—Initial document written. Greg Ketell.