Chapter 1

MPLS FRR Protection Overview

Multiprotocol Label Switching (MPLS) fast reroute (FRR) refers to local protection methods such as one-to-one and many-to-one (facility) backup. In the general networking community, the term FRR has become a shorthand way of describing the entire spectrum of MPLS traffic protection mechanisms. This should not be confused with the JUNOS software fast reroute feature. In this book, the acronym FRR is used to describe general MPLS traffic protection, while the distinct JUNOS software feature is described as fast reroute.

In the JUNOS software, general MPLS traffic protection for Resource Reservation Protocol (RSVP)-signaled label-switched path (LSP) failures is provided by several complementary mechanisms. These protection mechanisms include local protection (fast reroute, link protection, and node-link protection), and path protection (primary and secondary paths). Local protection in conjunction with path protection can provide minimum packet loss for an LSP, and control the way the LSP is rerouted after a failure.

Traditionally, both types of protection rely on fast detection of connectivity failure at the physical level. However, for transmission media without fast physical level detection, the JUNOS software supports the configuration of bidirectional forwarding detection (BFD) and MPLS ping for fast-failure detection. It is beyond the scope of this document to cover BFD or MPLS ping. For more information on BFD and MPLS ping, see the *JUNOS MPLS Applications Configuration Guide*.

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

MPLS Protection Background

During network failure, MPLS FRR protects against link or node failure in the path of an RSVP-signaled LSP with local protection at the level of the link or node, and path protection at the level of the entire LSP.

Local Protection

Local protection includes two methods:

- One-to-one (fast reroute) backup is one dedicated detour that protects one LSP.
- Many-to-one (facility) backup is one bypass path that protects many LSPs.

In the Juniper Networks implementation, one-to-one backup corresponds to the fast-reroute statement, while many-to-one (facility) backup corresponds to the link-protection and node-link-protection statements. This implementation is based on RFC 4090 *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*. Local protection is included at the MPLS and RSVP hierarchy levels, as illustrated in the sample output below. It is not recommended that you configure both types of local protection (fast reroute and facility backup) together. They are included together for illustration purposes only.

The following sample output shows the configuration of the fast-reroute statement:

```
[edit]
protocols {
    mpls {
        label-switched-path lsp-path-name {
            fast-reroute ;
        }
    }
}
```

The following sample output shows the configuration of link protection (many-to-one or facility backup):

```
[edit]
protocols {
    rsvp {
        interface type-fpc/pic/port {
            link-protection;
        }
    }
    mpls {
        label-switched-path lsp-path-name {
            link-protection;
        }
    }
}
```

The following sample output shows the configuration of node-link protection (many-to-one or facility backup):

```
[edit]
protocols {
    rsvp {
        interface type-fpc/pic/port {
            link-protection;
        }
    }
    mpls {
        label-switched-path lsp-path-name {
            node-link-protection;
        }
    }
}
```

Local protection in the JUNOS software is described as follows:

- One-to-one (fast reroute) backup—A router upstream from a failure quickly builds a detour LSP around the failure to the router downstream from the failure, providing protection against link or node failure. The upstream router then signals the outage to the ingress router, thereby maintaining connectivity before a new LSP is established. You can configure one-to-one backup by including the fast-reroute statement at the [edit protocols mpls label-switched-path *path-name*] hierarchy level. For more information about configuring and verifying one-to-one backup, see "Configuring and Verifying One-to-One Backup" on page 29.

- Link protection (many-to-one or facility backup)—Each router establishes a bypass LSP to its neighbor, avoiding the link connecting them, and ensuring traffic flow for the LSP when a link connecting two nodes fails. You can configure many-to-one backup by including the link-protection statement at the [edit protocols mpls label-switched-path *path-name*] hierarchy level. For more information about configuring and verifying link protection, see "Configuring and Verifying Link Protection" on page 38.

- Node-link protection (many-to-one or facility backup)—Each router dynamically signals a bypass LSP and determines if the protected LSP needs a node bypass or a link bypass, thereby ensuring traffic flow when a node or link in the LSP fails. You can configure node-link protection by including the node-link-protection statement at the [edit protocols mpls label-switched-path *path-name*] hierarchy level. To enable node-link protection, you must also include the link-protection statement at the [edit protocols rsvp interface *interface-name*] hierarchy level. For more information about configuring and verifying node-link protection, see "Node-Link Protection Overview" on page 44.

The important difference between using the fast-reroute statement and either of the link-protection statements is that the fast-reroute statement, regardless of whether a link or node fails, always protects one LSP with one detour path. The link-protection and node-link-protection statements always protect any LSPs crossing the node with one bypass path.

There are a couple of things to consider when deciding to configure fast reroute or link protection. The first is interoperability with equipment from other vendors, for example, Cisco Systems supports FRR, but does not support one-to-one backup. The second is that protection paths consume forwarding resources. In this regard, facility backup has better scaling because the protection paths are shared.

Path Protection

Complementary to local protection methods, JUNOS software supports the configuration of path protection with primary and secondary paths. By configuring path protection together with local protection, you can obtain minimum packet loss for an LSP while at the same time maintaining control over the path after the failure.

In the JUNOS software, path protection is included at the MPLS hierarchy level, as illustrated in the sample output below. The sample output shows the primary, secondary, and path statements you must include to an MPLS LSP configuration.

```
[edit]
protocols {
    mpls {
        label-switched-path lsp-path-name {
            primary path-name;
            secondary path-name {
                standby;
            }
        }
        path path-name {
        }
        path path-name {
        }
    }
}
```

Path protection in the JUNOS software is described as follows:

- Primary paths—Dictate the physical path for the LSP and are used in normal operations. When not configured and when Constrained Shortest Path First (CSPF) is used, the label-switched router (LSR) determines the path to reach the egress router based on user constraints, such as LSP bandwidth, link color, or other constraints. You can configure primary paths by issuing the primary *path-name* statement at the [edit protocols mpls label-switched-path *path-name*] hierarchy level. For an example and more information about configuring and verifying primary paths, see “Configuring and Verifying a Primary Path” on page 12.

- Secondary paths—Become operational when the primary path fails. There are two types of secondary paths: standby and non-standby. A standby secondary path is precomputed and pre-signaled while a non-standby secondary path is precomputed but is *not* pre-signaled. You can configure secondary paths by issuing the secondary *path-name* statement at the [edit protocols mpls label-switched-path *path-name*] hierarchy level. To configure a standby secondary path, include the standby statement at the [edit protocols mpls label-switched-path lsp-path-name secondary] hierarchy level. For an example and more information about configuring and verifying secondary paths, see “Configuring and Verifying a Secondary Path” on page 17.

Terms and Acronyms

Bypass tunnel—A label-switched path (LSP) that is used to protect multiple LSPs in many-to-one (facility) backup.

CSPF—Constrained Shortest Path First. An MPLS algorithm that has been modified to take into account specific restrictions when calculating the shortest path across the network.

Detour LSP—The LSP that is used to reroute traffic around a failure in one-to-one backup.

DMP—Detour Merge Point. In the case of one-to-one backup, this is an LSR where multiple detours converge. Only one detour is signaled beyond that LSR.

Facility backup—A local repair method in which a bypass tunnel is used to protect one or more protected LSPs that traverse the point of local repair, the resource being protected, and the merge point, in that order.

Local repair—Techniques used to repair LSP tunnels quickly when a node or link along the LSP fails.

LSP—An MPLS label-switched path (LSP). In this document, an LSP is always explicitly routed.

LSR—Label-switching router. A router on which MPLS is enabled and that can process label-switched packets.

Merge point— The LSR where one or more backup tunnels rejoin the path of the protected LSP downstream of the potential failure. The same LSR may simultaneously be a merge point and a point of local repair.

Next-hop bypass tunnel—A backup tunnel that bypasses a single link for different LSPs.

Next-next-hop bypass tunnel—A backup tunnel that bypasses a single node of the protected LSP.

One-to-one backup—A local repair method in which a detour LSP is separately created for each protected LSP at a point of local repair.

Point of local repair—The ingress (head-end) LSR of a backup tunnel or a detour LSP.

Protected LSP—An LSP is protected at a given hop if it has one or multiple detours or bypass paths.

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*