

Chapter 8

Configure Miscellaneous MPLS Properties

This chapter discusses the following topics:

Configure Traffic Engineering for LSPs on page 77

Configure MPLS to Gather Statistics on page 77

Control MPLS Syslog Messages and SNMP Traps on page 78

Trace MPLS Protocol Packets and Operations on page 79

Configure Traffic Engineering for LSPs

Establishing an LSP installs a host route (a 32-bit mask) in the ingress router toward the egress router. The address of the host route is the destination address of the LSP. By default, only BGP can use LSPs in its route calculations. On the ingress router, to enable both BGP and the IGP to use an LSP in forwarding traffic destined for the egress router of that LSP, include the traffic-engineering statement at the [edit protocol mpls] hierarchy level:

```
[edit protocol mpls]
traffic-engineering bgp-igp;
```

Configure MPLS to Gather Statistics

You can configure MPLS so that it periodically gathers traffic statistics about all MPLS sessions, including transit sessions. To do this, include the statistics statement at the [edit protocol mpls] hierarchy level:

```
[edit protocol mpls]
statistics {
  file filename <size size files number>;
  interval seconds;
}
```

The default interval is 300 seconds.

The statistics are placed in a file, with one entry per LSP. At the end of each periodic report, a summary shows the current time, total number of sessions, numbers of sessions read, number of sessions ignored, and read errors, if any. Ignored sessions are typically those not in the up state or those with a reserved (0-15) incoming label (typically the egress point of an LSP). The reason for a read error appears on the same line as the entry for the LSP on which the error occurred. Gathering statistics is an unreliable process; occasional read errors might affect their accuracy. The following is a sample of the information included in the output file:

```

lsp6                0 pkt                0 Byte        0 pps         0 Bps        0%
lsp5                0 pkt                0 Byte        0 pps         0 Bps        0%
lsp6.1              34845 pkt           2926980 Byte  1049 pps     88179 Bps   132%
lsp5.1              0 pkt                0 Byte        0 pps         0 Bps        0%
lsp4                0 pkt                0 Byte        0 pps         0 Bps        0%
Dec 7 17:28:38 Total 6 sessions: 5 success, 0 fail, 1 ignored

```

Control MPLS Syslog Messages and SNMP Traps

Whenever an LSP makes a transition from up to down, or vice versa, and whenever an LSP switches from one active path to another, the ingress router generates a syslog message and sends an SNMP trap. The following shows a sample syslog message:

```

MPLS lsp sheep1 up on primary(any) Route 192.168.1.1 192.168.1.2 192.168.1.3
MPLS lsp sheep1 change on primary(any) Route 192.168.1.1 192.168.1.2
192.168.1.3
MPLS lsp sheep1 down on primary(any)
MPLS lsp sheep1 up on secondary(any) Route 192.168.1.1 192.168.1.2 192.168.1.3
MPLS lsp sheep1 change on secondary(any) to primary(any), Route 192.168.1.1
192.168.1.2 192.168.1.3

```

For information about the MPLS SNMP traps, see the *JUNOS Internet Software Configuration Guide: Installation and System Management Configuration Guide*.

For information about the proprietary MPLS MIB, see the *JUNOS Internet Software Configuration Guide: Installation and System Management Configuration Guide*.

To disable both the generation of syslog messages and SNMP traps, include the following log-updown statement at the [edit protocols mpls] hierarchy level:

```

[edit protocols mpls]
log-updown {
  no-syslog;
  no-trap;
}

```

To disable only the generation of syslog messages, configure the following:

```

[edit]
user@host# set protocols mpls log-updown no-syslog

```

For scalability reasons, only the ingress router generates SNMP traps. By default, MPLS issues traps for all configured LSPs. If you have many LSPs, the number of traps can become quite large. To disable the generation of SNMP traps, configure the following:

```

[edit]
user@host# set protocols mpls log-updown no-trap

```

Trace MPLS Protocol Packets and Operations

To trace MPLS protocol packets and operations, include the traceoptions statement at the [edit routing-options] and [edit protocol mpls] hierarchy levels:

```
[edit protocol mpls]
traceoptions {
  file filename <replace> <size size> <files number> <no-stamp>
    <(world-readable | no-world-readable)>;
  flag filename <flag-modifier> <disable>;
}
```

You can specify the following MPLS-specific flags in the MPLS traceoptions statement:

connection—Trace all Circuit Cross Connect (CCC) activity.

connection-detail—Trace detailed CCC activity.

cspf—Trace CSPF computations.

cspf-link—Trace links visited during CSPF computations.

cspf-node—Trace nodes visited during CSPF computations.

error—Trace MPLS error conditions.

state—Trace all LSP state transitions.

For general information about tracing and global tracing options, see the *JUNOS Internet Software Configuration Guide: Routing and Routing Protocols*.

