Configuring Automatic Protection Switching
Contents

Purpose ................................................................. 3
Requirement ......................................................... 3
Procedure ........................................................... 4
Confirm ................................................................. 5
Additional Notes .................................................... 7
  Configuration Statement Priority .................................. 7
  SONET K1 and K2 Bytes ............................................. 8
References ............................................................ 9

List of Figures

Figure 1: Two routers connected to one ADM using SONET links ....................... 3
Purpose

This application note explains how to configure Automatic Protection Switching (APS) to secure against circuit failures between an Add-Drop Multiplexer (ADM) and two routers.

Requirement

The configuration in this application note uses the routers and ADM shown in Figure 1. In this figure, two routers are connected to the ADM using SONET links. The two routers are also connected to each other using SONET links.

Figure 1: Two routers connected to one ADM using SONET links

The working router has a working circuit configured that carries traffic during normal operation. If the circuit fails, if the working circuit performance degrades, or if the working router fails, the ADM and the protect router switch the traffic to the protect circuit.

For normal APS operation, the working and protect routers communicate over the directly connected link. This traffic between the two routers can traverse over other links if the direct link is down. However, this traffic should not flow through the interface on which APS is configured, or instability may result.

Configure APS under the SONET-options statement in the configuration hierarchy for the specific SONET interface.
Configuring Automatic Protection Switching (APS)

Procedure

1. Associate the working circuit and the protect circuit by configuring the same group name.
2. Configure the same authentication key for the working and protect circuits.
3. To enable APS communication between the two routers, configure the IP address of the other router. When you choose the IP address, keep in mind that this traffic should not flow through the interface on which APS is configured. You have to configure the neighbor address only on the protect router.

**NOTE**  For channelized SONET interfaces, you must configure APS on channel 0

**Working Router Configuration**

```
[edit interfaces so-0/0/0 SONET-options]
aps {
    working-circuit group-name;
    authentication-key key;
}
```

**Protect Router Configuration**

```
[edit interfaces so-1/0/0 SONET-options]
aps {
    protect-circuit group-name;
    authentication-key key;
    neighbor 192.168.1.1
}
```

4. By default, APS is nonrevertive. To configure revertive mode, specify the amount of time that the protect router should wait after the working circuit is functional again before switching the traffic back.

**Protect Router Configuration**

```
[edit interfaces so-1/0/0 SONET-options aps]
user@router2# set revert-time seconds
```

5. You can specify the advertisement interval of the packets between the APS neighbors and the duration of time to wait for an advertisement before declaring the neighbor down.

**NOTE**  The advertisement-interval and hold-time does not need to be the same on both the protect and working router.

**Protect Router Configuration**

```
[edit interfaces so-1/0/0 SONET-options aps]
user@router2# set advertise-interval milliseconds
user@router2# set hold-time milliseconds
```

**Working Router Configuration**

```
[edit interfaces so-0/0/0 SONET-options aps]
user@router1# set advertise-interval milliseconds
user@router1# set hold-time milliseconds
```
Configuring Automatic Protection Switching (APS)

Confirm

1. To check the APS status for the router, use the `show aps` command. The example output below displays which interfaces are configured for APS, the APS group that each interface belongs to, whether the interface is a working or a protect circuit, and the state of the interface.

Example output:

```
user@router> show aps
Interface  Group                        Circuit  Intf   State
so-0/0/0   aps-group-1                  Working  enabled, up
so-1/0/0   aps-group-2                  Protect  disabled, up
so-2/0/0   aps-group-3                  Protect  disabled, up
```

2. For extensive APS information, use the `show aps extensive` command. In addition to showing the status of the local interface, this command displays the IP address of the APS neighbor, the status of the adjacency to the APS neighbor router, and the status of the neighbor interface.

Example output:

```
user@router> show aps extensive
Interface  Group                           Circuit  Intf State
so-0/0/0   aps-group-1                    Working  enabled, up
    Neighbor 192.168.1.1, adj up, neighbor interface disabled, dead 24.100
    Channel state Working
    Req K1 0x00, rcv K1 0x00, xmit K1 0x00, nbr K1 0x00, nbr paired req 0
    Revert time 0, neighbor revert time 0
    Hello due in 2.176
so-1/0/0   aps-group-2                    Protect disabled, up
    Neighbor 192.168.1.1, adj up, neighbor interface enabled, dead 25.370
    Channel state Working
    Req K1 0x00, rcv K1 0x00, xmit K1 0x00, nbr K1 0x00, nbr paired req 0
    Revert time 0, neighbor revert time 0
    Hello due in 6.553
so-2/0/0   aps-group-3                    Protect disabled, up
    Neighbor 192.168.1.1, adj up, neighbor interface enabled, dead 28.960
    Channel state Working
    Req K1 0x00, rcv K1 0x10, xmit K1 0x20, nbr K1 0x00, nbr paired req 0
    Revert time 0, neighbor revert time 0
    Hello due in 4.509
```

3. To display the transmitted and received K1 and K2 bytes for APS, use the `show interface <interface-name> extensive` command. The transmitted and received K1 and K2 bytes are listed in the Received and Transmitted SONET overhead sections.

For more detailed information about SONET K1 and K2 bytes, see Additional Notes.

Example Output:

```
user@router> show interfaces so-1/1/0 extensive
Physical interface: so-1/1/0, Enabled, Physical link is Up
    Interface index: 19, SNMP ifIndex: 15
    Description: core-01 pos4/2
    Link-level type: Cisco-HDLC, MTU: 4474, Clocking: Internal, SONET
    Speed: OC3, Loopback: None, CRC: 32, Payload scrambler: Enabled
    Device flags : Present Running
    Interface flags: Point-To-Point SNMP-Traps
```
Link flags : Keepalives
Keepalive statistics:
  Input : 44430 (last seen 00:00:02 ago)
  Output: 54279 (last seen 00:00:09 ago)
Statistics last cleared: Never
Traffic statistics:
  Input bytes : 60612218635 0 bps
  Output bytes : 762134959 0 bps
  Input packets: 285814012 0 pps
  Output packets: 2269922 0 pps
Input errors:
  Errors: 0, Drops: 0, Framing errors: 6, Runts: 0, Giants: 0
  Policed discards: 6, L3 incompletes: 0, L2 channel errors: 0
  L2 mismatch timeouts: 0, HS link CRC errors: 0, HS link FIFO overflows: 0
Output errors:
  Carrier transitions: 1, Errors: 0, Drops: 0, Aged packets: 0
  HS link FIFO underflows: 0
Active alarms : None
Active defects : None
SONET PHY:
  PLL Lock                  0        0        OK
  PHY Lock                  0        0        OK
SONET section:
  BIP-B1  0        0
  SEF     1        1        OK
  LOS     1        1        OK
  LOP     1        1        OK
  ES-S    1
  SES-S   1
  SEFS-S  1
SONET line:
  BIP-B2  0        0
  REI-L   0        0
  RDI-L   0        0        OK
  AIS-L   0        0        OK
  BERR-SF 0        0        OK
  BERR-SD 0        0        OK
  ES-L    1
  SES-L   1
  UAS-L   0
  ES-LFE  0
  SES-LFE 0
  UAS-LFE 0
SONET path:
  BIP-B3  0        0
  RET-P   0        0
  LOP-P   0        0        OK
  AIS-P   0        0        OK
  RDI-P   0        0        OK
  UNEQ-P  0        0        OK
  PLM-P   0        0        OK
  ES-P    1
  SES-P   1
  UAS-P   0
  ES-PFE  0
  SES-PFE 0
  UAS-PFE 0
Received SONET overhead:
  F1 : 0x00, J0 : 0x00, K1 : 0x00, K2 : 0x00
  S1 : 0x00, C2 : 0x16, C2(cmp) : 0xcf, P2 : 0x00
  Z3 : 0x00, Z4 : 0x00, S1(cmp) : 0x00
Transmitted SONET overhead:
Received path trace:
Host name : core-01
Interface : POS4/2
IP Address : 10.10.10.29
72 65 67 2d 63 6f 72 65 2d 30 31 00 00 00 00 00 core-01.....
00 00 00 00 00 00 00 00 50 4f 53 34 2f 32 00 00 ..POS4/2..
00 00 00 00 00 00 00 00 31 30 2e 31 30 2e 31 30 ....10.10.10.2
9.....00000800..
Transmitted path trace: router so-1/1/0
72 65 67 2d 65 64 67 65 2d 30 31 32 73 6f 2d 31 router so-1
2f 31 2f 30 00 00 00 00 00 00 00 00 00 00 00 00 00
/1/0............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...........
POS configuration:
Policing bucket: Disabled
Shaping bucket : Disabled
Giant threshold: 4486, Runt threshold: 5
PFE configuration:
Destination slot: 1, Stream number: 4, PLP byte: 1 (0x00)
CoS transmit queue bandwidth:
 Queue0: 95, Queue1: 0, Queue2: 0, Queue3: 5
CoS weighted round-robin:
 Queue0: 95, Queue1: 0, Queue2: 0, Queue3: 5
Logical interface so-1/1/0.0 (Index 10) (SNMP ifIndex 29)
Description: core-01 pos4/2
Flags: Point-To-Point SNMP-Traps, Encapsulation: Cisco-HDLC
Protocol inet, MTU: 4470, Flags: None
 Addresses, Flags: Is-Preferred Is-Primary
 Destination: 10.10.10.28/30, Local: 10.10.10.30, Broadcast:
 Unspecified
Protocol iso, MTU: 4469, Flags: None

4. For detailed APS debugging, you can look at the apsd log file using the show log apsd command. To view what is currently being written to the apsd log, use the monitor start apsd command.

Additional Notes

Configuration Statement Priority

During normal operations, the routers and ADM automatically switch traffic between the working and protect circuits if circuit or router failures occur. The following configuration statements are available for manually switching between the working and protect circuits. They are listed in the order of priority from highest to lowest.

- Lockout
- Force
- Request

A higher priority statement overrides the lower priority command. Signal failures, signal degradations, and router failures override a Request statement but are overridden by Force and Lockout commands.
1. Configure the request and force statements at [edit interfaces
interface-name SONET-options aps] hierarchy level on the protect router, and you
specify a manual switch to the working or protect circuit.

   [edit interfaces <interface-name> SONET-options aps]
   set request (protect | working)

   [edit interfaces <interface-name> SONET-options aps]
   set force (protect | working)

2. To force a lockout of the protect circuit and force the use of the working circuit, configure
the lockout statement on the protect circuit:

   [edit interfaces <interface-name> SONET-options aps]
   set lockout

To stop asserting the particular request, you must delete the request, force, or lockout
statement from the configuration.

**SONET K1 and K2 Bytes**

SONET K1 and K2 bytes are signaled on the protect circuit between the ADM and the router to
direct the operation of APS.

The SONET K1 byte indicates the type of APS request and the channel number that made the
request. Bits 1 to 4 are for the type of request, and bits 5 to 8 are for the channel number. For
the JUNOS APS 1:1 implementation, channel 0 refers to the protect circuit and channel 1 refers
to the working circuit. The following table summarizes the mapping of bits 1 through 4.

<table>
<thead>
<tr>
<th>K1 Bits 4 through 1</th>
<th>Type of Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>1111 (0xF)</td>
<td>Lockout of Protection Request</td>
</tr>
<tr>
<td>1110 (0xE)</td>
<td>Forced Switch Request</td>
</tr>
<tr>
<td>1101 (0xD)</td>
<td>Signal Failure (SF) – high-priority request</td>
</tr>
<tr>
<td>1100 (0xC)</td>
<td>Signal Failure (SF) – low-priority request</td>
</tr>
<tr>
<td>1011 (0xB)</td>
<td>Signal Degradation (SD) – high-priority request</td>
</tr>
<tr>
<td>1010 (0xA)</td>
<td>Signal Degradation (SD) – low-priority request</td>
</tr>
<tr>
<td>1001 (0x9)</td>
<td>Not Used</td>
</tr>
<tr>
<td>1000 (0x8)</td>
<td>Manual Switch</td>
</tr>
<tr>
<td>0111 (0x7)</td>
<td>Not Used</td>
</tr>
<tr>
<td>0110 (0x6)</td>
<td>Wait to Restore Request</td>
</tr>
<tr>
<td>0101 (0x5)</td>
<td>Not Used</td>
</tr>
<tr>
<td>0100 (0x4)</td>
<td>Exercise Request</td>
</tr>
<tr>
<td>0011 (0x3)</td>
<td>Not Used</td>
</tr>
<tr>
<td>0010 (0x2)</td>
<td>Reverse Request</td>
</tr>
<tr>
<td>0001 (0x1)</td>
<td>Do Not Revert Request</td>
</tr>
<tr>
<td>0000 (0x0)</td>
<td>No Request</td>
</tr>
</tbody>
</table>
The SONET K2 byte indicates the channel number, type of architecture, and mode of operation. Bits 1 to 4 are for the channel number, bit 5 is for type of architecture, and bits 6 through 8 are for mode of operation.

For the JUNOS APS 1:1 implementation, channel 0 refers to the protect circuit and channel 1 refers to the working circuit. A zero for bit 5 indicates 1+1 architecture, and a one for bit 5 indicates 1:n architecture. See the table below for mapping of bits 6 to 8.

<table>
<thead>
<tr>
<th>K2 Bits 6 through 8</th>
<th>Mode of Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>Unidirectional mode</td>
</tr>
<tr>
<td>101</td>
<td>Bidirectional mode</td>
</tr>
<tr>
<td>110</td>
<td>Line RDI</td>
</tr>
<tr>
<td>111</td>
<td>Line AIS</td>
</tr>
</tbody>
</table>

References

JUNOS Internet Software Configuration Guide
Bellcore GR-253-CORE