



Multi Router APS on ISE ATM Line Cards

This feature provides 1+1 multirouter automatic protection switching (MR-APS) on the Cisco 12000 series ISE ATM line cards (Engine 3). APS refers to the mechanism of using a Protection interface in the SONET network as the backup for a Working interface. When the Working interface fails, the Protection interface quickly assumes its traffic load. In a multirouter environment, this feature allows the Protection interface to reside in a different router from the Working interface. This feature supports High Availability.

Feature History for Multirouter APS on ISE ATM Line Cards

Release	Modification
11.1 CC	This feature was introduced for Cisco 12000 Series Packet-over-SONET line cards.
12.0(23)SX	This feature was introduced on the OC3ATM and OC12ATM line cards for the Cisco 10000 series.
12.0(26)S	This feature was integrated into Cisco IOS Release 12.0(26)S, and support was added for the CHOC12, CHSTM1, OC3POS, and OC12POS line cards for the Cisco 10000 series.
12.0(30)S	This feature was integrated into Cisco IOS Release 12.0(30)S for the Cisco 12000 Series OC-12c/STM-4c and OC-3/STM-1 ATM ISE Line Cards (Engine 3). New CLI commands were introduced to support these line cards.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

Contents

- [Prerequisites for Multirouter APS for the Cisco 12000 Series ISE ATM Line Cards, page 2](#)
- [Restrictions for Multirouter APS for the Cisco 12000 Series ISE ATM Line Cards, page 2](#)
- [Information About Multirouter APS for the Cisco 12000 Series ISE ATM Line Cards, page 3](#)
- [How to Configure Multirouter APS for the Cisco 12000 Series ISE ATM Line Cards, page 5](#)
- [Configuration Example for Multirouter APS for the Cisco 12000 Series ISE ATM Line Cards, page 14](#)
- [Additional References, page 15](#)
- [Command Reference, page 16](#)

Prerequisites for Multirouter APS for the Cisco 12000 Series ISE ATM Line Cards

This feature is supported on the following Cisco 12000 series line cards for Cisco IOS Release 12.0(30)S:

- Cisco 12000 Series 4-Port OC-12/STM-4 ATM ISE Multimode Line Card
PN: 4OC12X/ATM-MM-SC
- Cisco 12000 Series 4-Port OC-12/STM-4 ATM ISE Single Mode Line Card
PN: 4OC12X/ATM-IR-SC
- Cisco 12000 Series 4-port OC-3/STM-1 ATM ISE Multimode Line Card
PN: 4OC3X/ATM-MM-SC
- Cisco 12000 Series 4-port OC-3/STM-1 ATM ISE Single Mode Line Card
PN: 4OC3X/ATM-IR-SC

Restrictions for Multirouter APS for the Cisco 12000 Series ISE ATM Line Cards

- The CLI for Packet-Over-SONET (POS) MR-APS is not supported for the Cisco 12000 Series ISE ATM line cards.
- Multirouter APS on ISE ATM Line Cards does not support the reflector channel currently supported on several POS interfaces across different Cisco platforms. ATM interfaces usually connect to an ATM switch, and POS interfaces connect to a router. Reflector channel is useful only when connected to a router.
- Bidirectional mode is recommended for Multirouter APS.
- In the 1+1 mode, no actual bridging of transmit traffic occurs.
- APS switch initiation and completion times are typically less than 10 milliseconds and 50 milliseconds respectively. The Cisco Protect Group Protocol (PGP) uses UDP packets; queuing delays incurred on these can result in longer Protection switching times.
- Although the Working and Protection interfaces can be configured on the same router, it is recommended that MR-APS be used only in multirouter configuration.

Information About Multirouter APS for the Cisco 12000 Series ISE ATM Line Cards

To implement multirouter APS, you should understand the following concepts:

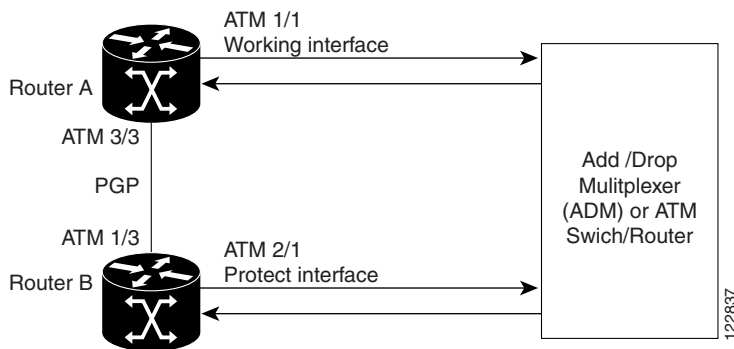
- [Multirouter APS Overview, page 3](#)
- [MR-APS Alarms and Statistics, page 4](#)
- [SNMP Trap Support, page 5](#)
- [High Availability Support for MR-APS on the Cisco 12000 Series Router, page 5](#)

Multirouter APS Overview

This feature allows switchover of ATM circuits in the event of circuit failure and is often required when connecting SONET equipment to telephone company equipment. APS refers to the mechanism of using a “Protection” ATM interface in the SONET network as the backup for a “working” ATM interface. When the Working interface fails, the Protection interface quickly assumes its traffic load.

[Figure 1](#) shows a basic multirouter APS configuration where the Working and Protection circuits terminate on different line cards installed in two different routers. Interfaces in a multirouter APS configuration are configured with SONET framing. An out-of-band (OOB) connection is established between the two routers independent of the Working and Protection links.

Figure 1 Multirouter APS Configuration



1+1 Protection Switching

In multirouter APS 1+1 Protection switching, each Working interface has an exclusive protection interface. The Protection and Working interfaces are connected to an ATM switch or a SONET ADM (Add/Drop Multiplexer) and the Working and Protection circuits terminate in different line cards in different routers. 1+1 Protection Switching is described in the Bellcore publication TR-TSY-000253, SONET Transport Systems; Common Generic Criteria, Section 5.3.

On the Protection circuit, the K1K2 bytes from the line overhead (LOH) of the SONET frame indicate the current status of the MR-APS connection and convey any requests for action. This signalling channel is used by the two ends of the connection to maintain synchronization.

The 1+1 protection switching may be bidirectional or unidirectional, and revertive or non-revertive. In bidirectional mode, the receive and transmit channels are switched as a pair. In unidirectional mode, the transmit and receive channels are switched independently. For example, in bidirectional mode, if the

receive channel on the Working interface has a loss of channel signal, both the receive and transmit channels are switched. The revertive option causes the switched channel to switch back to the original Working circuit when the line fault is removed. The default attributes for MR-APS are non-revertive and bidirectional.

Cisco Protect Group Protocol

Protect Group Protocol (PGP) runs over UDP and controls the MR-APS states of the Working and Protection interfaces over an out-of-band connection between the two routers. This independent, OOB channel may be a different SONET connection, or a lower-bandwidth connection.



Note

An out-of-band connection between the Working and Protection routers should be established before configuring MR-APS.

In MR-APS, the protection switching decision is made by the router hosting the Protection interface. The decision logic considers factors such as K1K2 data, signal failure (SF) notifications, signal degrade (SD) notifications, manual switching requests, and the state of the two routers.

Using PGP, the process controlling the Protection interface directs the process containing the Working interface to activate or deactivate the Working circuit. Hello packets are sent by the Protection router, and acknowledged by the Working router at specific intervals. If the Working router does not receive hello packets within a specified interval, it assumes full control of the Working circuit as if no Protection circuit existed. If a Protection router does not receive acknowledgements from the Working router within a specified interval, a switchover can occur.

In a router configured for MR-APS, the configuration for the Protection interface includes the IP address of the router hosting Working interface (normally the router's loopback address). PGP uses this address to send PGP packets to the Working router. The Working router replies to the source address of the PGP packets.

MR-APS Alarms and Statistics

The following statistics are reported in MR-APS:

- APS switchover count—Indicates the number of times a line is switched.
- PSBF count—Indicates the number of times the Protection Switching Byte Failure alarm is generated.

When a node receives an invalid K1 byte from the remote node, it reports a PSBF condition. An alarm is generated when the condition persists for 2.5 seconds (plus or minus 0.5 seconds). When the PSBF condition is cleared for 10 seconds (plus or minus 0.5 seconds), the alarm is cleared.

- Channel Mismatch count—Indicates the number of times the Channel Mismatch alarm is generated.
- Mode Mismatch count—Indicates the number of times the Mode Mismatch alarm is generated.

A channel mismatch is when a node receives a channel number in the K2 byte that is different than its transmitted channel number. An alarm is generated when the channel mismatch condition persists for 2.5 seconds (plus or minus 0.5 seconds). When the channel mismatch is cleared for 10 seconds (plus or minus 0.5 seconds), the alarm is cleared.

If the protection switching class of the local node is configured for 1+1 APS and the remote node is configured for 1:n APS, this alarm would be generated. If the received APS architecture differs from the local APS architecture, it would result in mode mismatch alarm. If the mode mismatch persists for 2.5(+/- 0.5)seconds, this alarm will be generated. The alarm is cleared, once the mode mismatch is absent for 10(+/- 0.5)seconds.

- FEPLF count—Indicates the number of times the Far End Protection Line Failure alarm is generated.

The Far End Protection Line Failure alarm is generated when a node receives three consecutive K1 bytes that indicate signal failure (SF) on the Protection line.

SNMP Trap Support

The following traps are defined for Multirouter APS on ISE ATM Line Cards:

- APS switchover
- FEPLF
- Mode mismatch
- Channel mismatch
- APS interface add/delete

High Availability Support for MR-APS on the Cisco 12000 Series Router

The Route Processor card (RP) provides support for RPR, RPR+ or SSO modes of Route Processor redundancy. The APS redundancy infrastructure supports each of these RP redundancy modes.

How to Configure Multirouter APS for the Cisco 12000 Series ISE ATM Line Cards

This section contains the following procedures for implementing MR-APS with the Cisco 12000 Series ISE ATM line cards:

- [Configuring the Working and Protect Interfaces, page 5](#)
- [Performing Manual Protection Switching, page 10](#)
- [Configuring Bit Error Rate Thresholds, page 11](#)
- [Monitoring MR-APS, page 13](#)

Configuring the Working and Protect Interfaces

In the following configuration, MR-APS is configured on two routers, the Working router that hosts the Working interface, and the Protect router that hosts the standby interface. It is assumed that the out-of-band PGP connection between the routers has already been established.

SUMMARY STEPS

Configure the Working Router

1. **enable**
2. **configure terminal**
3. **redundancy**

4. **port-group** *port-groupID* **aps multi-router**
5. **member port** *slot/port* {**working** | **protection** [*working-ip-address*]}
6. **timers hello** *hello-interval hold-interval* [*hello-fail-revert-interval*]
7. **authentication** *authentication-phrase*
8. **end**

Configure the Protect Router

9. Repeat Step 1 to Step 4 on the Protect router.
10. **member port** *slot/port* {**working** | **protection** [*working-ip-address*]}
11. **timers hello** *hello-interval hold-interval* [*hello-fail-revert-interval*]
12. **revertive** *timeout*
13. **authentication** *authentication-phrase*
14. **end**

DETAILED STEPS

Command or Action	Purpose
Configure the Working router. Step 1 enable Example: Router1> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: Router1# configure terminal	Enters global configuration mode.
Step 3 redundancy Example: Router1(config)# redundancy	Enters redundancy configuration mode.
Step 4 port-group <i>portgroupID</i> aps multi-router Example: Router1(config-red)# port-group 1 aps multi-router	Enters redundancy port configuration mode to create the multirouter APS port-group with the ID "1." The multi-router keyword must be used if one member of the redundancy group is on a different router. Once a MR-APS port group is created, Working and Protection ports (interfaces) can then be added to that port group.
Step 5 member port <i>slot/port</i> { primary secondary working protection } [<i>working-ip-address</i>] Example: Router1(config-red-port)# member port 2/0 working	Configures a Working interface within the port group. In this example the slot/port is 2/0, designating that the first port of the line card in slot 2 is assigned to MR-APS port group 1.
Step 6 timers hello <i>hello-interval</i> <i>hold-interval</i> [<i>fail-revert-interval</i>] Example: Router1(config-red-port)# timers hello 3 9 120	(Optional) Specifies the time intervals used by PGP. To return to the default timers, use the no form of the command. <ul style="list-style-type: none"> • The hello interval is the number of seconds between hello packets. The default is 1 second. • The hold interval is the number of seconds to wait to receive a response from a hello packet before the interface is declared down. The default is 3 seconds. The hold interval should be three times as long as the hello interval. • The fail revert interval is the number of seconds the Protection interface waits before reverting to the Working interface (when the revert option is configured). The default is 120 seconds. • The PGP hello timers can be configured individually for the Working and Protect routers.

Command or Action	Purpose
<p>Step 7 <code>authentication authentication-phrase</code></p> <p>Example: Router1(config-red-port)# authentication squeegee</p>	<p>(Optional) Configures the authentication phrase to permit each router to accept PGP packets. The authentication phrase must be the same on both routers. To disable authentication, use the no form of this command.</p> <ul style="list-style-type: none"> Enter 1 to 8 alphanumeric characters.
<p>Step 8 <code>end</code></p> <p>Example: Router1(config-red-port)# end</p>	<p>Exits Redundancy Port Configuration command mode to privileged Exec command mode.</p>
<p>Configure the Protection router.</p>	
<p>Step 9 Repeat Step 1 to Step 4 on the Protection router.</p>	<p>To configure the Protection interfaces on the Protection router, Perform Steps 1 through 5 on the Protect router, then skip to Step 12.</p>
<p>Step 10 <code>member port slot/port {primary secondary working protection} [working-ip-address]</code></p> <p>Example: Router2(config-red-port)# member port 3/0 protection 1.1.1.1</p>	<p>PGP uses the Working router's IP address to send hello packets from the Protection to the Working router. The Working router replies to the source address of the PGP packets.</p>
<p>Step 11 <code>revertive timeout</code></p> <p>Example: Router2(config-red-port)# revertive 200</p>	<p>(Optional) Specifies the time interval in which the Protection circuit is switched back to the Working circuit if the Working interface becomes operational. To make the circuit non-revertive, use the no form of the command. MR-APS groups are non-revertive by default.</p> <ul style="list-style-type: none"> Enter 1–86,400 seconds.
<p>Step 12 <code>timers hello hello-interval hold-interval [fail-revert-interval]</code></p> <p>Example: Router2(config-red-port)# timers hello 3 9 120</p>	<p>(Optional) Specifies the time intervals used by PGP. To return to the default timers, use the no form of the command.</p> <ul style="list-style-type: none"> The hello interval is the number of seconds between hello packets. The default is 1 second. The hold interval is the number of seconds to wait to receive a response from a hello packet before the interface is declared down. The default is 3 seconds. The hold interval should be three times as long as the hello interval. The fail revert interval is the number of seconds the Protection interface waits before reverting to the Working interface (when the revertive operation is configured). The default is 120 seconds. The PGP hello timers can be configured individually for the Working and Protect routers.

	Command or Action	Purpose
Step 13	authentication <i>authentication-phrase</i> Example: Router2(config-red-port)# authentication squeegee	(Optional) Configures the authentication phrase to permit each router to accept PGP packets. The authentication phrase must be the same on both routers. To disable authentication, use the no form of this command. <ul style="list-style-type: none"> • Enter 1 to 8 alphanumeric characters.
Step 14	end Example: Router2(config-red-port)# end	Exits Redundancy Port Configuration command mode to Privileged Exec command mode.

Examples

In the following example, Router1 is a Working router with loopback address 1.1.1.1. Router 2 is the Protection router. The MR-APS circuit is a default circuit (non-revertive, bidirectional) identified as port group 1.

Configure the Working router.

```
Router1# configure terminal
Router1(config)# redundancy
Router1(config-red)# port-group 1 aps multi-router
Router1(config-red-port)# member port 2/0 working
Router1(config-red-port)# timers hello 3 9 200
Router1(config-red-port)# authentication squeegee
Router1(config-red-port)# end
Router1#
```

Configure the Protection router.

```
Router2> enable
Router2# configure terminal
Router2(config)# redundancy
Router2(config-red)# port-group 1 aps multi-router
Router2(config-red-port)# member port 3/0 protection 1.1.1.1
Router2(config-red-port)# timers hello 3 9 120
Router2(config-red-port)# revertive 200
Router2(config-red-port)# authentication squeegee
Router2(config-red-port)# end
Router2#
```

Troubleshooting Tips

- If the interfaces appear to be down, use the **show interfaces** command to check connectivity.
- Check that the ADM is sourcing the SONET clocking.
- Use the **show controllers atm slot/port** command to obtain hardware-related information.
- Use the **show running-config** command to display the configuration parameters of all of the commands that the current user has modified. The **show running-config** interface command is useful when there are multiple interfaces and you want to look at the configuration of a specific interface.
- Use the **show aps** command to check the current APS configuration for each interface.

- Use the **debug aps** command to check specific interface APS activity.

Performing Manual Protection Switching

The following commands are used to perform the various switch requests. These commands are again available only on the Protection router because that is where the K1K2 processing takes place.

Manual Protection Switching

In MR-APS, you can manually switch a channel signal from one path to another, or you can lock out a switchover altogether while performing system maintenance. A switchover from the Working path to Protection path is useful when upgrading or maintaining the system, or in cases where a signal failure caused a switchover. When the MR-APS circuit is configured for non-revertive operation, the system does not automatically revert to the original Working circuit when the fault has been corrected. The switchover to the formerly failed interface must be requested through the CLI. The interface originally configured as the Working path might be preferred because of its link loss characteristics.

There are three types of manual switchover requests:

- Lockout requests—Have the highest priority and take effect regardless of the condition of the Protection signal. A lockout prevents the active signal from switching over from the Working path to the Protection path.
- Forced switchover requests—Have the next highest priority and are only prevented if there is an existing lockout on the Protection path, or the signal on the Protection path has failed when switching from Working to Protection.
- Manual switchover requests—Have the lowest priority and only occur if there is no Protection path lockout, a forced switchover, or the signal has failed or degraded.

The priority order for switchover are a follows (from higher to lower priority):

1. Lockout
2. Signal failure on the Protection path
3. Forced switchover
4. Signal failure on the Working path
5. Signal degrade on the Working or Protection path
6. Manual switchover

If a request or condition of a higher priority is in effect, a lower priority request is rejected.

Use the **clear** option to remove all manual switching requests. For **manual** and **force**, requests, **clear** only eliminates the precedence effect of these commands and does not cause another switchover.



Note

Redundancy port-group *groupID* force and **redundancy port-group *groupID* manual** are privileged exec commands that take effect at the time they are entered. The commands are not written to NVRAM and do not appear when you display the running configuration.

Table 1 MR-APS Manual Protection Switching Commands

Manual Protection Switching Task	Command
Force the specified circuit to switch from the Protection circuit to the Working circuit, unless a request of equal or higher priority is in effect.	redundancy port-group <i>groupID</i> force 0
Force the specified circuit to switch from the Working circuit to the Protection circuit, unless a request of equal or higher priority is in effect.	redundancy port-group <i>groupID</i> force 1
Manually request the specified circuit to switch from the Protection circuit to the Working circuit, unless a request of equal or higher priority is in effect.	redundancy port-group <i>groupID</i> manual 0
Manually request the specified circuit to switch from the Working circuit to the Protection circuit, unless a request of equal or higher priority is in effect.	redundancy port-group <i>groupID</i> manual 1
Prevent a Working circuit from switching to a Protection circuit.	redundancy port-group <i>groupID</i> lockout
Clear all existing switch requests.	redundancy port-group <i>groupID</i> clear

Examples

This example manually switches traffic from the Working interface to the Protect interface.

```
Router2# redundancy port-group 10 manual 1
```

This example manually switches traffic from the Protect interface to the Working interface.

```
Router2# redundancy port-group 10 manual 0
```

The following two commands are used to force switch the traffic.

```
Router2# redundancy port-group 10 force 1
Router2# redundancy port-group 10 force 0
```

This example prevents a manual switching from a Working to a Protection interface.

```
Router2# redundancy port-group 10 lockout
```

This example clears all existing switch requests.

```
Router2# redundancy port-group 10 clear
```

Configuring Bit Error Rate Thresholds

The following commands permit the configuration of threshold values for raising SONET alarms. Exceeding the bit error rate (BER) thresholds will result in a signal degrade (SD) request or a signal failure (SF) request.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm slot/port**
4. **sonet threshold sd-ber bit-error-rate**
5. **sonet threshold sf-ber bit-error-rate**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface atm slot/port Example: Router(config)# interface atm 1/0	Enters interface command mode. In this example, port 0 of the ATM line card in slot 1 is being configured.
Step 4	sonet threshold sd-ber bit-error-rate Example: Router(config-if)# sonet-threshold sd-ber 5	Sets the Signal Degrade bit error rate threshold. 5–9 (10 to the minus n)
Step 5	sonet threshold sf-ber bit-error-rate Example: Router(config-if)# sonet-threshold sf-ber 5	Sets the Signal Fail bit error rate threshold. 3–5 (10 to the minus n)
Step 6	end Example: Router1(config-if)# end	Exits Interface Configuration command mode to privileged Exec command mode.

Examples

In the following example, the Working router's (router1) atm interface is set to BER values other than the default values. The Protection router (router2) is set with the same values.

```
Router1> enable
Router1# configure terminal
Router1(config)# interface atm 1/0
Router1(config-if)# sonet-threshold sd-ber 7
Router1(config-if)# sonet-threshold sf-ber 5
Router1(config-if)# end
```

```

Router1#

Router1> enable
Router2# configure terminal
Router2(config)# interface atm 1/0
Router2(config-if)# sonet-threshold sd-ber 7
Router2(config-if)# sonet-threshold sf-ber 5
Router2(config-if)# end
Router2#

```

Monitoring MR-APS

The following show command can be used to monitor and verify MR-APS configurations:

- **show aps**
- **show running-config**
- **show controllers atm slot/port**
- **show interface atm slot/port**

Examples

```

Router1# show aps
ATM2/2 APS Group 3:working channel 1 (Active)
  Protect at 3.3.1.2
  PGP timers (from protect):hello time=1; hold time=3
  SONET framing
  Remote APS configuration:(null)

Router2# show running-config
. . .
port-group 3 aps multi-router
  member port 2/2 working
. . .

Router2# show controller atm 2/2
ATM2/2
SECTION
  LOF = 0          LOS = 0          RDOOL = 0          BIP(B1) = 93
  Active Alarms:None
LINE
  AIS = 0          RDI    = 0          FEBE = 0          BIP(B2) = 0
  Active Alarms:None
PATH
  AIS = 0          RDI    = 2          FEBE = 2513       BIP(B3) = 405
  LOP = 0          NEWPTR = 0          PSE = 304        NSE = 0
  Active Alarms:None

SF-BER Threshold =3      SD-BER Threshold =6 ATM
Correctable HCS errors = 0      Uncorrectable HCS errors = 0
LCD = 0
Active Alarms: None

Router2# show interfaces atm 2/2
ATM2/2 is up, line protocol is up  Hardware is PM622 OC-12c ATM, address is 000c.85e4.3126
(bia 000c.86f4.3156)
MTU 4470 bytes, sub MTU 4470, BW 622000 Kbit, DLY 80 usec, rely 255/255, load 1/255
Encapsulation ATM, loopback not set

```

```

Carrier delay is 8 msec
Encapsulation(s):AAL5, PVC mode
4095 maximum active VCs, 8 current VCCs
Max vpi bits:8
VC idle disconnect time:300 seconds
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Queueing strategy:fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
    Available Bandwidth 598962 kilobits/sec
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 output buffer failures, 0 output buffers swapped out

```

Configuration Example for Multirouter APS for the Cisco 12000 Series ISE ATM Line Cards

Using the configuration shown in [Figure 1 on page 3](#), the following example shows the configuration of multirouter APS. Router A is configured with the Working interface, and Router B is configured with the Protection interface. If the Working interface on Router A becomes unavailable, the connection will automatically switch over to the Protection interface on Router B.

Router A, the Working router, can use the following minimum redundancy configuration:

```

interface Loopback0
 ip address 21.21.21.21 255.255.255.255
 no ip directed-broadcast
 no clns route-cache
!
redundancy
mode rpr
 port-group 20 aps multi-router
  member port 1/1 working
!

```

Router B, the Protect router, can use the following minimum redundancy configuration:

```

redundancy
mode rpr
 port-group 20 aps multi-router
  member port 2/1 protection 21.21.21.21
 direction bidirectional

```

Additional References

The following sections provide references related to multirouter APS.

Related Documents

Related Topic	Document Title
APS and SONET commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<i>Cisco IOS Interface Command Reference</i> , Release 12.0
APS and SONET configuration	<i>Cisco IOS Interface Configuration Guide</i> , Release 12.0
APS on the Cisco 7500 and Cisco 12000 series routers	<i>Automatic Protection Switching of Packet-over-SONET Circuits</i> feature document, Release 11.2

Standards

Standards	Title
Bellcore SONET linear 1+1 architecture	TR-TSY-000253, SONET Transport Systems; Common Generic Criteria, Section 5.3.

MIBs

MIBs	MIBs Link
CISCO-APS-MIB (Also used for APS on POS interfaces. This MIB is a Cisco version of the IETF APS MIB)	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0S command reference publications.

authentication

To set the authentication phrase for Cisco Protect Group Protocol (PGP) communications on the peer routers in a multirouter APS configuration, use the authentication command in redundancy port configuration mode. To disable authentication, use the **no** form of this command.

authentication *authentication-phrase*

no authentication

Syntax Description

authentication-phrase 1 to 8 alphanumeric characters.
Sets authentication phrase for PGP communications.

Defaults

The default is no authentication.

Command Modes

Redundancy port configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.

Usage Guidelines

This command is applicable only to multirouter APS.

Authentication must be enabled on the peer routers in multirouter APS configurations so that they may receive PGP packets on the out-of-band (OOB) communications channel.

Examples

The following example specifies squeegee as the PGP authentication phrase on router1 (repeat for the other router):

```
router1(config)# redundancy
router1(config-red)# port group 1 aps multirouter
router1(config-red-port)# authentication squeegee
router1(config-red-port)# end
```

Related Commands

Command	Description
port group	Creates a port redundancy group.
show running-config	Displays the running configuration file.

direction

To designate a multirouter APS circuit as unidirectional or bidirectional, use the **direction** command in redundancy port configuration mode.

direction {unidirectional | bidirectional}

Syntax Description	unidirectional	bidirectional
	Specifies that the receive and transmit lines of the Working and Protection interfaces are switched over independently should either or both fail.	Specifies that the receive and transmit lines are switched over together to the Protection circuit should either fail.

Defaults Bidirectional is the default for multirouter APS.

Command Modes Redundancy port configuration

Command History	Release	Modification
	12.0(30)S	This command was introduced.

Usage Guidelines In bidirectional mode, a failure on a Working Tx or Rx line triggers an APS switchover of the Working Tx and Rx lines to the Protection interface Tx and Rx lines.

In unidirectional mode, failure on a Working Tx or Rx line triggers an APS switchover of only the failed line to the corresponding line of the Protection interface.

We do not recommend that multirouter APS be configured as unidirectional. Use the **direction unidirectional** command only when you must interoperate with SONET network equipment, such as Add Drop Multiplexors (ADMs) that only support unidirectional mode.

If the local mode is bidirectional and the remote end is configured as unidirectional APS, the local router functions in unidirectional mode. This is reported in the **show aps** command output which displays the provisioned mode as bidirectional and the operational mode as unidirectional.

Examples The following example shows how to configure and ATM interface for unidirectional mode>:

```
Router2> enable
Router2# configure terminal
Router2(config)# redundancy
Router2(config-red)# port-group 1 aps multi-router
Router2(config-red-port)# member port 3/0 protection 1.1.1.1
Router2(config-red-port)# direction unidirectional
Router2((config-red-port)# end
Router2#
```

Related Commands

Command	Description
revertive	Sets the time interval after which the Protection circuit reverts to the Working circuit when the Working circuit becomes available.
show aps	Displays information about the current automatic protection switching (APS) feature.
show running-config	Displays the running configuration file.

member port

To add members to a redundancy port group, use the **member port** command in redundancy port configuration mode. To remove a member, use the **no** form of this command.

member port *slot/port* { **protection** [*working-ip-address*] | **working** }

no member port *slot/port*

Syntax Description

<i>slot/port</i>	Specifies the slot and port number of a line card.
protection	Specifies that the port (interface) being configured is a Protection port.
<i>working-ip-address</i>	Specifies the IP address of the Working router in a multirouter APS configuration.
working	Specifies that the port (interface) being configured is a Protection port.

Defaults

No default behavior or values

Command Modes

Redundancy port configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.

Usage Guidelines

Above commands are used to add port members to the redundancy group.

For the multirouter APS, the redundancy role of the member port can be configured as either working or protection.

Examples

The following example adds port 2/0 on router1 as a member of port group 1:

```
Router1# configure terminal
Router1(config)# redundancy
Router1(config-red)# port-group 1 aps multi-router
Router1(config-red-port)# member port 2/0 working
Router1(config-red-port)# end
Router1#
```

The following example deletes port 2/0 as a member of port group 1, then deletes port group 1:

```
Router2> enable
Router2# configure terminal
Router2(config)# redundancy
Router2(config-red)# port-group 1 aps multi-router
Router2(config-red-port)# no member port 2/0
Router2((config-red-port)# exit
Router2(config-red)# no port-group 1
Router2(config-red)# end
Router2#
```

Related Commands

Command	Description
port group	Creates a port redundancy group.
show running-config	Displays the running configuration file.

port-group

To create a port redundancy group, use the **port-group** command in redundancy configuration mode. To delete a port redundancy group, use the **no** form of this command.

port-group *groupID* **aps** [**multi-router**]

no port-group *groupID*

Syntax Description

<i>groupID</i>	1–255. Specifies a unique number to identify the port group to be created.
aps	Specifies that the port group is an APS circuit.
multi-router	Indicates that the Working and Protection ports in an APS port group are installed in different routers.

Defaults

The following defaults apply when a port group is first created:

- APS redundancy class is 1+1.
- APS port redundancy groups are non-revertive.

Command Modes

Redundancy configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.

Usage Guidelines

Use the **port-group** command to create or delete a redundancy group wherein the redundant members are line card ports. Executing the **port-group** command enters the port redundancy group configuration mode (config-red-port). Use the **no** form of the command to delete the port redundancy group and free the associated group identifier for reuse. Delete all members of a port group before deleting the port group, otherwise, the port group is not deleted and an error message displays.

Examples

The following example creates a multirouter APS port group identified as port-group 10:

```
Router1# config terminal
Router1(config)# redundancy
Router1(config-red)# port-group 10 aps multi-router
Router1(config-red-port)#
```

Related Commands

Command	Description
member port	Creates a member port within a redundancy port group.
show running-config	Displays the running configuration file.

redundancy port-group

To manually initiate redundancy switching of port groups, use the **redundancy port-group** command in privileged EXEC configuration mode.

```
redundancy port-group groupID {clear | force {1 | 0} | lockout | manual {1 | 0}}
```

Syntax Description	groupID	1–255. Specifies the identifier of the port group.
	clear	Removes all force and manual switching requests.
	force	Requests switch over of Working and Protection circuits. It is a higher priority request than manual .
	1	Switches the Working circuit to the Protection circuit.
	0	Switches the Protection circuit to the Working circuit.
	lockout	Prevents a switchover
	manual	Requests switch over of Working and Protection circuits. It is a lower priority request than force .

Defaults No default behavior or values

Command Modes Privileged exec command

Command History	Release	Modification
	12.0(30)S	This command was introduced.

Usage Guidelines In MR-APS, you can manually switch a channel signal from one path to another, or you can lock out a switchover altogether while performing system maintenance. A switchover from the Working path to Protection path is useful when upgrading or maintaining the system, or in cases where a signal failure caused a switchover. When the MR-APS circuit is configured for non-revertive operation, the system does not automatically revert to the original Working circuit when the fault has been corrected. The switchover to the formerly failed interface must be requested through the CLI. The interface originally configured as the Working path might be preferred because of its link loss characteristics or because of its distance advantage.

There are three types of manual switchover requests:

- Lockout requests—Have the highest priority and take effect regardless of the condition of the Protection signal. A lockout prevents the active signal from switching over from the Working path to the Protection path.
- Forced switchover requests—Have the next highest priority and are only prevented if there is an existing lockout on the Protection path, or the signal on the Protection path has failed when switching from Working to Protection.
- Manual switchover requests—Have the lowest priority and only occur if there is no Protection path lockout, a forced switchover, or the signal has failed or degraded.

The priority order for switchover are as follows (from higher to lower priority):

1. Lockout
2. Signal failure on the Protection path
3. Forced switchover
4. Signal failure on the Working path
5. Signal degrade on the Working or Protection path
6. Manual switchover

If a request or condition of a higher priority is in effect, a lower priority request is rejected.

Use the **clear** option to remove all manual switching requests. For **manual** and **force**, requests, **clear** only eliminates the precedence effect of these commands and does not cause another switchover.

Examples

This example manually switches traffic from the Working interface to the Protect interface.

```
Router2# redundancy port-group 10 manual 1
```

This example manually switches traffic from the Protect interface to the Working interface.

```
Router2# redundancy port-group 10 manual 0
```

The following two commands are used to force switch the traffic.

```
Router2# redundancy port-group 10 force 1
Router2# redundancy port-group 10 force 0
```

This example prevents a manual switching from a Working to a Protection interface.

```
Router2# redundancy port-group 10 lockout
```

This example clears all existing switch requests.

```
Router2# redundancy port-group 10 clear
```

Related Commands

Command	Description
show running-config	Displays the running configuration file.

revertive

To enable automatic switchover from the Protection interface to the Working interface after the Working interface becomes available, use the **revertive** command in redundancy port configuration mode. To disable automatic switchover, use the no form of this command.

revertive *timeout*

no revertive

Syntax Description

<i>timeout</i>	Optional. 1 to 86,400 seconds. Sets the time interval after which the Protection circuit reverts to the Working circuit when the Working circuit becomes available.
----------------	--

Defaults

There is no timeout default value.
MR-APS is non-revertive by default.

Command Modes

Redundancy port configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.

Usage Guidelines

The **revertive** *timeout* command configures the Wait-To-Restore (WTR) timer specified in the Bellcore GR-253 standard to determine the time interval that must elapse before the Protect circuit can switch back to Working circuit when the alarms on the Working interface clear. The **revertive** *timeout* timer starts when the alarms are cleared. The **revertive** *timeout* interval should be greater than the **hello timer** *hello-fail-revert* interval to prevent a premature reversion from Protect to Working while the *hello-fail-revert* timer is still running following a possible PGP failure.

Examples

The following example sets the APS group a revertive with a revert time of 30 seconds:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# port-group 1 aps multi-router
Router(config-red-port)# member port 3/0 protection 1.1.1.1
Router(config-red-port)# revertive 30
Router(config-red-port)# end
```

Related Commands

Command	Description
show running-config	Displays the running configuration file.

signalling

To change the signalling used for MR-APS k1k2 support, use the **signalling** command in redundancy port configuration mode.

signalling {sdh | sonet}

Syntax Description	sdh	sonet
	Specifies SDH signalling.	Specifies SONET signalling.

Defaults The default is the same signalling as the framing.

Command Modes Redundancy port configuration

Command History	Release	Modification
	12.0(30)S	This command was introduced.

Usage Guidelines This command is used to change the signalling for k1k2 byte signalling support. SDH signalling is not supported for multirouter APS in Cisco IOS Release 12.0(30)S.

Examples The following example sets the signalling type as SDH:

```
Router2> enable
Router2# configure terminal
Router2(config)# redundancy
Router2(config-red)# port-group 1 aps multi-router
Router2(config-red-port)# member port 3/0 protection 1.1.1.1
Router2((config-red-port)# signalling sdh
Router2((config-red-port)# end
```

Related Commands	Command	Description
	show running-config	Displays the running configuration file.

timers hello

To specify the time intervals used by the Cisco protect group protocol (PGP), use the **timers hello** command in redundancy port configuration mode. To reinstate the default values, use the **no** form of this command.

timers hello *hello-interval hold-interval hello-fail-revert-interval*

no timers hello

Syntax Description

<i>hello-interval</i>	Specifies the number of seconds between PGP hello packets.
<i>hold-interval</i>	Specifies the number of seconds before the interface is declared down.
<i>hello-fail-revert-interval</i>	Specifies the number of seconds to wait before reverting to the Working interface.

Defaults

The hello interval default is 1 second.

The hold interval default is 3 seconds.

The fail revert interval is 120 seconds.

Command Modes

Redundancy port configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.

Usage Guidelines

The **timers hello** command sets the PGP hello timers. The PGP protocol provides information in addition to SONET K1K2 byte alarms that the multirouter APS algorithm uses to determine if a switchover is required. PGP hello timers work together with the **revertive timeout** command (if configured) in scheduling circuit switchovers and switchbacks.

In a typical multirouter APS configuration, the Protect router sends hello packets (hellos) to the Working router over the PGP channel. The hellos are sent every *hello-interval* and the Working router immediately sends an acknowledgement. The Working router expects to receive hellos from the Protect router every *hello-interval*. If the Working router does not receive hellos for a time interval specified by the *hold-interval*, then the Working router assumes a PGP failure, and APS is suspended. Similarly, if the Protect router does not receive hello acknowledgements from the Working router before the *hold-interval* timer expires, it declares PGP failure and a switchover can occur. The *hello-fail-revert-interval* is the number of seconds the Protection interface waits before reverting to the Working interface (if the K1K2 bytes are not indicating an alarm on the Working Tx and Rx lines). The default is 120 seconds. The PGP hello timers can be configured individually for the Working and Protect routers, though typically they should have the same values. The hold interval should be three times as long as the hello interval.

PGP communication failures can occur because of the following:

- Working router failure
- Protect router failure
- PGP channel failure

Router failure typically occurs because of the following:

- Software failure
- Software reload
- CPU overload
- Resources setup delay
- Power off
- Hardware failure

PGP channel failure can occur because of the following:

- Traffic congestion
- Interface failure due to alarms
- Interface hardware failure

Some PGP channel failures can be avoided by providing higher bandwidth interfaces for PGP to minimize congestion.

The **revertive** *timeout* value should be greater than the *hello-fail-revert-interval* value. During a software reload or a power cycle of the Working router, PGP signals the need to switch to the Protect interface. As the Working router reloads or reboots, the physical layer can be operational and alarm-free before the router is capable of forwarding traffic. The *hello-fail-revert-interval* should be set to a time interval sufficient for the Working interface to become operational.

Examples

The following example configures the PGP hello timers:

```
Router2> enable
Router2# configure terminal
Router2(config)# redundancy
Router2(config-red)# port-group 1 aps multi-router
Router2(config-red-port)# member port 3/0 protection 1.1.1.1
Router1(config-red-port)# timers hello 3 9 200
Router2((config-red-port)# end
```

Related Commands

Command	Description
revertive	Enables automatic switchover from the Protection interface to the Working interface after the Working interface becomes available.
show running-config	Displays the running configuration file.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

timers hello