CHAPTER 5

Redundancy and SONET APS Configuration

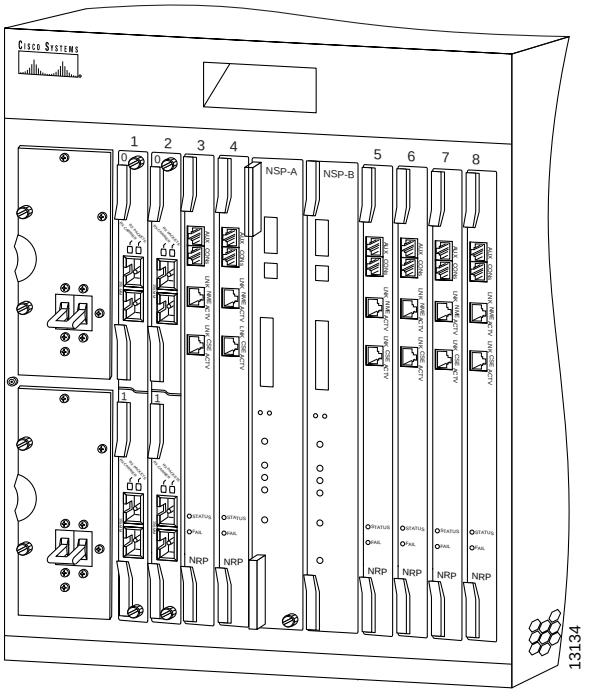
The Cisco 6400 contains two slots for node switch processors (NSPs) and eight slots for node line cards (NLCs) or node route processors (NRPs), as shown in Figure 5-1. Each slot can contain one full-height or two half-height cards. NRPs and NSPs support enhanced high system availability (EHSA) redundancy, and NLCs support SONET automatic protection switching (APS) redundancy at the port-level.

Redundancy can be configured between:

- NSPs (always assumed when two NSPs are installed in the chassis)
- NRPs and full-height NLCs installed in the following slot pairs:
  - Slots 1 and 2, 3 and 4, 5 and 6, or 7 and 8
- Half-height NLCs installed in adjacent subslot pairs:
  - Subslots 0 (top) in slots 1 and 2, 3 and 4, 5 and 6, or 7 and 8
  - Subslots 1 (bottom) in slots 1 and 2, 3 and 4, 5 and 6, or 7 and 8

This chapter contains the following sections:

Figure 5-1 Cisco 6400 Carrier-Class Broadband Aggregator



Memory Requirements

When configuring redundancy between two NRPs or two NSPs, the two cards must have identical hardware configurations. Check each card in a redundant pair, and make sure they share the following parameters:

- DRAM size
- Flash memory size
- PCMCIA disk size (NSP only)
- Hardware version (module part number)

If redundancy is configured between two cards with different amounts of memory or disk capacity, the Cisco 6400 will display a warning message. Depending on which card is identified as the primary card, the Cisco 6400 will perform the following actions:

- Primary card has more memory than secondary card—The Cisco 6400 shuts down the secondary card.
- Secondary card has more memory than primary card—The Cisco 6400 displays a message, indicating that the secondary card has more memory than the primary card. This configuration will cause redundancy to be disabled if the secondary card is activated.

Note This approach allows for memory upgrades on a redundant pair of NRPs or NSPs. For information about performing memory upgrades, see the *Cisco 6400 UAC FRU Installation and Replacement* document.

NSP Redundancy

Both NSP slots are numbered slot 0 for consistent interface identification between primary and secondary devices. Nevertheless, the left NSP slot is labeled slot A and the right slot is labeled slot B to distinguish between the two slots, when required.

You can use EHSA redundancy for simple hardware backup or for software error protection. Hardware backup protects against NSP card failure because you configure both NSP cards with the same software image and configuration information. Additionally, you configure the system to automatically synchronize configuration information on both cards when changes occur.

Software error protection protects against critical Cisco IOS software errors in a particular release because you configure the NSP cards with different software images, but use the same configuration. If you are using new or experimental Cisco IOS software, consider using the software error protection method.

This section includes:

Configuring Redundant NSPs

If two NSPs are installed in the Cisco 6400, they automatically act as a redundant pair. No configuration is necessary.

Verifying NSP Redundancy

To verify NSP redundancy, use the **show redundancy** EXEC command:

```
Switch# show redundancy
NSP A:Primary
NSP B:Secondary

Secondary NSP information:
Secondary is up
Secondary has 131072K bytes of memory.

User EHSA configuration (by CLI config):
secondary-console = off
keepalive     = on
config-sync modes:
  standard   = on
  start-up   = on
  boot-var   = on
  config-reg = on
  calendar   = on

Debug EHSA Information:
```

```
Primary   (NSP A) ehsa state:SANTA_EHSA_PRIMARY
Secondary (NSP B) ehsa state:SANTA_EHSA_SECONDARY

EHSA pins:
peer present = 1
peer state   = SANTA_EHSA_SECONDARY
crash status:this-nsp=NO_CRASH(0x1) peer-nsp=NO_CRASH(0x1)

EHSA related MAC addresses:
this bpe mac-addr = 0000.0c00.0003
peer bpe mac-addr = 0000.0c00.0004


Switch#
```

Synchronizing Redundant NSPs

To ensure that the configuration is consistent between redundant NSPs or NRPs, you can configure automatic synchronization between the two devices. You have the option of synchronizing just the startup configuration, the boot variables, the configuration register, or all three configurations (standard). When configuration is complete, you can disable autoconfiguration using the **no** command.

To automatically synchronize the configurations between redundant NSPs, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Switch(config)# redundancy`	Enters redundancy configuration mode.
Step 2	`Switch(config-r)# main-cpu`	Enters main-cpu configuration mode.
Step 3	`Switch(config-r-mc)# auto-sync [standard | bootvar | config-register | startup-config]`	Synchronizes the configuration between redundant NSPs.

Boot variables are ROM monitor (ROMMON) environment variables used to control the booting process. The configuration register, stored in NVRAM, contains startup time parameters for the system. For more information about the booting process, see the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Example

In the following example, the configuration is synchronized between redundant NSPs:

```
!
redundancy
 main-cpu
  auto-sync standard
  !
```

Verifying Synchronized NSPs

To verify that NVRAM and sec-NVRAM contain identical startup configurations, compare the output of the following command entries:

Switch# **cd nvram:** Switch# **dir** Switch# **more startup-config**	Switch# **cd sec-nvram:** Switch# **dir** Switch# **more startup-config**

The displayed output should be identical.

Erasing Startup Configurations on Redundant NSPs

To erase the startup configuration on redundant NSPs, complete the following steps beginning in EXEC mode:

	Command	Purpose
Step 1	Switch# **erase nvram:**	Erases the primary NSP's startup configuration.
Step 2	Switch# **erase sec-nvram:**	Erases the secondary NSP's startup configuration.

Note If you only erase the startup configuration on the primary NSP, and the primary and secondary NSPs reverse roles, the new primary NSP will use the old startup configuration.

Verifying Erased Startup Configurations

To verify that you erased the startup configuration on redundant NSPs, use the **dir nvram:** and **dir sec-nvram:** EXEC commands and check that the startup-config size is zero:

```
NSP# dir nvram:
Directory of nvram:/

  1  -rw-           0              <no date>  startup-config

129016 bytes total (129016 bytes free)
```

You can also use the **show startup** EXEC command and make sure that a valid configuration file does not appear:

```
NSP# show startup
%% Non-volatile configuration memory is being written, Try again later
```

PCMCIA Disk Mirroring

Introduced in Cisco IOS Release 12.1(5)DB, the PCMCIA disk mirroring enables automatic data synchronization between the PCMCIA disks of two redundant NSPs. Disk synchronization is the act of copying data from one disk to another.

Disk mirroring provides full NSP redundancy for the NRP-2, which depends on the NSP for image and file storage. Without disk mirroring, there is no guarantee of NRP-2 support after an NSP failover (user intervention might be required to restore the NRP2 state to that prior to the failover). With disk mirroring enabled, NRP-2 has continued support from the NSP, except during the relatively short NSP failover period.

When PCMCIA disk mirroring is enabled, as it is by default, disk synchronization is initiated each time that:

- The primary or secondary NSP boots or reloads
- The secondary NSP is inserted into the Cisco 6400 chassis
- A PCMCIA disk is inserted into disk slot 0 of the primary or secondary NSP
- The PCMCIA disk in disk slot 0 of either NSP is formatted
- A command is entered to:
  - Re-enable disk mirroring (**mirror**)
  - Explicitly initiate disk synchronization (**redundancy sync**)
  - Modify or reorganize the files on the disks (**copy**, **rename**, **delete**, **mkdir**, **format**)

Note PCMCIA disk mirroring is not supported in Cisco IOS Release 12.1(4)DB and earlier releases. Use the **dir**, **mkdir**, and **copy** EXEC commands to manually copy files from the primary NSP's PCMCIA disks to the secondary NSP's PCMCIA disks.

PCMCIA disk mirroring also introduced new labels for pairs of mirrored disks:

- **mir-disk0**—PCMCIA disks in disk slot 0 of both NSPs
- **mir-disk1**—PCMCIA disks in disk slot 1 of both NSPs

The **mir-disk0** and **mir-disk1** labels enable you to perform any integrated file system (IFS) operation (such as **copy**, **rename**, and **delete**) on the same file on both the primary and secondary disks.

Restrictions and Recommendations

- If an NSP failover occurs during disk synchronization, the file that is being copied is deleted from the receiving disk, instead of only partially copied. This means that the file is no longer available to the NRP-2. The amount of time it takes to complete disk synchronization varies for each system, but depends on the number and sizes of files being copied.
- Disk mirroring (automatic data synchronization between a pair of disks) is not supported between:
  - Two disks on a single NSP
  - Two disks with mismatched slot numbers (disk0: and disk1:)

  You can, however, initiate disk synchronization between disk0: and disk1: on the active NSP, even in a single-NSP system.
- Cisco recommends that you use PCMCIA disks of the same memory capacity.

Disabling PCMCIA Disk Mirroring

Disk mirroring is enabled by default. To disable disk mirroring, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Switch(config)# redundancy`	Enters redundancy configuration mode.
Step 2	`Switch(config-r)# main-cpu`	Enters main-cpu configuration mode.
Step 3	`Switch(config-r-mc)# no mirror`	Disables data synchronization between the NSP PCMCIA disks.

Example

In the following example, PCMCIA disk mirroring is disabled:

```
!
redundancy
 main-cpu
  auto-sync standard
  no mirror
  !
```

Verifying that Disk Mirroring is Disabled

To verify that disk mirroring is disabled, use the **show redundancy sync-status** EXEC command:

```
Switch# show redundancy sync-status
 Disk Mirror is disabled in configuration
 Peer Secondary NSP is present
 disk1 or sec-disk1 is wrong or missing

Switch#
```

Enabling PCMCIA Disk Mirroring

If disk mirroring is disabled, and you want to re-enable it, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Switch(config)# redundancy`	Enters redundancy configuration mode.
Step 2	`Switch(config-r)# main-cpu`	Enters main-cpu configuration mode.
Step 3	`Switch(config-r-mc)# mirror`	Enables data synchronization between the NSP PCMCIA disks.

Example

In the following example, PCMCIA disk mirroring is enabled:

```
!
redundancy
 main-cpu
  auto-sync standard
  mirror
  !
```

Verifying that Disk Mirroring is Enabled

To verify that disk mirroring is enabled, complete one or both of the following steps:

Step 1 Use the **show redundancy sync-status** EXEC command to check that disk mirroring is enabled:

```
Switch# show redundancy sync-status
→ Disk Mirror is enabled in configuration:proper sync
(Mirror threshold is 0 MB:smaller files will be copied blindly)

 Peer Secondary NSP is present
 disk1 or sec-disk1 is wrong or missing

 mir-disk0 (disk0 -> sec-disk0):in sync.
 mir-disk1 (disk1 -> sec-disk1):out of sync.

Switch#
```

Step 2 Use the **dir** command to verify matching file names and file sizes on the mirrored PCMCIA disks.

```
Switch# dir disk0:
Switch# dir sec-disk0:

Switch# dir disk1:
Switch# dir sec-disk1:
```

Specifying the File Size Threshold

By default, when performing disk synchronization (either through disk mirroring or user initiation), the system compares files between the PCMCIA disks. The system does not copy files with matching file names, sizes, and time stamps. You can, however specify a file size threshold below which files are copied without comparison.

To specify the file size threshold, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Switch(config)# redundancy`	Enters redundancy configuration mode.
Step 2	`Switch(config-r)# main-cpu`	Enters main-cpu configuration mode.
Step 3	`Switch(config-r-mc)# mirror threshold` *size*	Specifies the file size threshold below which files are copied without comparison.

Example—File Size Threshold

In the following example, PCMCIA disk mirroring is enabled with a specified file size threshold of 2 MB:

```
!
redundancy
 main-cpu
  auto-sync standard

  mirror threshold 2
  !
```

Verifying the File Size Threshold

To verify the file size threshold, use the **show redundancy sync-status** EXEC command, and check the Mirror Threshold field:

```
Switch# show redundancy sync-status
Disk Mirror is enabled in configuration:proper sync
 (Mirror threshold is 2 MB:smaller files will be copied blindly)

 Peer Secondary NSP is present
 disk1 or sec-disk1 is wrong or missing

 mir-disk0 (disk0 -> sec-disk0):out of sync.
 mir-disk1 (disk1 -> sec-disk1):out of sync.

 Disk Mirror full sync is in progress (disk0 to sec-disk0, 23%)

Switch#
```

Specifying to Copy All Files Blindly

Instead of specifying a file size threshold below which files are copied without comparison, you can choose to copy *all* files blindly (without comparing sizes or time stamps).

To copy all files blindly, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Switch(config)# redundancy`	Enters redundancy configuration mode.
Step 2	`Switch(config-r)# main-cpu`	Enters main-cpu configuration mode.
Step 3	`Switch(config-r-mc)# mirror all`	Specifies to copy all files blindly when performing disk synchronization.

Example—Copying Blindly

In the following example, PCMCIA disk mirroring is enabled and set to copy all files blindly:

```
!
redundancy
 main-cpu
  auto-sync standard

  mirror all
  !
```

Verifying Blind Copying

To verify blind copying, use the **show redundancy sync-status** EXEC command to check the configured synchronization type. The first line displayed should end with “full sync” instead of “proper sync.”

```
Switch# show redundancy sync-status
Disk Mirror is enabled in configuration:full sync
 (Mirror threshold is 0 MB:smaller files will be copied blindly)

 Peer Secondary NSP is present
 disk1 or sec-disk1 is wrong or missing

 mir-disk0 (disk0 -> sec-disk0):out of sync.
 mir-disk1 (disk1 -> sec-disk1):out of sync.
```

```
 Disk Mirror full sync is in progress (disk0 to sec-disk0, 23%)

Switch#
```

Initiating PCMCIA Disk Synchronization

Disk synchronization copies the data from one PCMCIA disk to another. To initiate disk synchronization, use one of the following commands in global configuration mode:

Command	Purpose
Switch# **redundancy sync disk0** [**all**][1]	Copies data from disk0:[2] of the primary NSP to disk0: of the secondary NSP.
Switch# **redundancy sync disk1** [**all**]	Copies data from disk1:[3] of the primary NSP to disk1: of the secondary NSP.
Switch# **redundancy sync disk0 reverse** [**all**]	Copies data from disk0: of the secondary NSP to disk0: of the primary NSP.
Switch# **redundancy sync disk1 reverse** [**all**]	Copies data from disk1: of the secondary NSP to disk1: of the primary NSP.
Switch# **redundancy sync local** [**all**]	Copies data from disk0: of the primary NSP to disk1: of the primary NSP. Can be used with single-NSP systems.

1. Optional **all** keyword specifies to copy all files blindly (without comparing file sizes and time stamps).
2. disk0: = PCMCIA disk in NSP disk slot 0
3. disk1: = PCMCIA disk in NSP disk slot 1

Example—Disk Synchronization

```
Switch# redundancy sync disk0

00:29:52:%DISKMIRROR-6-PROGRS:Disk Sync in Progress (disk0 to sec-disk0, 0%)
Switch#
```

Example—Reverse Disk Synchronization

```
Switch# redundancy sync disk0 reverse

00:32:13:%DISKMIRROR-6-PROGRS:Disk Sync in Progress (sec-disk0 to disk0, 0%)
Switch#
```

Example—Local Disk Synchronization

```
Switch# redundancy sync local

00:32:13:%DISKMIRROR-6-PROGRS:Disk Sync in Progress (disk0 to disk1, 0%)
Switch#
```

Verifying Disk Synchronization

To verify disk synchronization, complete one or both of the following steps:

Step 1 Use the **show redundancy sync-status** EXEC command to check that the disk content is synchronized:

```
Switch# show redundancy sync-status
Disk Mirror is enabled in configuration:proper sync
 (Mirror threshold is 0 MB:smaller files will be copied blindly)

 Peer Secondary NSP is present
 disk1 or sec-disk1 is wrong or missing

→ mir-disk0(disk0/sec-disk0):in sync.
 mir-disk1(disk1/sec-disk1):out of sync.
```

Step 2 Use the **dir** command to verify matching file names and file sizes on the mirrored PCMCIA disks.

```
Switch# dir disk0:
Switch# dir sec-disk0:

Switch# dir disk1:
Switch# dir sec-disk1:
```

Performing Mirrored IFS Operations

When disk mirroring is enabled and disk synchronization is complete, avoid performing IFS operations (such as **copy**, **rename**, and **delete**) using the labels **disk0:**, **disk1:**, **sec-disk0:**, or **sec-disk1:**. Modifying a file using these labels can break disk synchronization without affecting the output of the **show redundancy sync-status** EXEC command. In other words, the **show redundancy sync-status** command output can declare disks to be "in sync," even after disk synchronization is broken using the improper labels.

Because the **dir** command does not *modify* any files, you can use the **dir** command with the **disk0:**, **disk1:**, **sec-disk0:**, or **sec-disk1:** labels at any time to check disk contents, as shown in the previous sections.

Cisco recommends that you perform *mirrored* IFS operations by using the labels **mir-disk0:** and **mir-disk1:**. These new labels target the PCMCIA disks in the specified slot of both NSPs, and ensure that the files affected by the IFS operations are still mirrored.

Note If you want to save a file on only one PCMCIA disk and not have that file mirrored, use the [**sec-**]**disk0:/non-mirror** or [**sec-**]**disk1:/non-mirror** directory.

Examples

The following examples show mirrored IFS operations:

```
Switch# copy tftp://10.1.1.1/test-config mir-disk0:test-config
Switch# rename mir-disk0:test-config mir-disk0:test-config1
Switch# delete mir-disk0:test-config1
```

The following example shows an intentional nonmirrored IFS operation:

```
Switch# copy tftp://10.1.1.1/test-config2 sec-disk0:/non-mirror/test-config2
```

Troubleshooting and Monitoring PCMCIA Disk Mirroring

Use the **show redundancy sync-status** EXEC command to display all status information on disk mirroring and synchronization.

Use the **debug disk-mirror** EXEC command to display debug messages for IFS call events, disk write events, and disk synchronization events.

Using NSP Redundancy for Hardware Backup

For simple hardware backup, the redundant NSPs must have the same system image.To ensure that the redundant NSPs run the same image, complete the following steps:

Step 1 Use the **show bootvar** EXEC command to display the current booting parameters for the primary and secondary NSPs. Check that the secondary NSP is up.

```
Switch# show bootvar
BOOT variable =
CONFIG_FILE variable =
Current CONFIG_FILE variable =
BOOTLDR variable does not exist
Configuration register is 0x0

→ Secondary is up.
Secondary BOOT variable =
Secondary CONFIG_FILE variable =
Secondary BOOTLDR variable does not exist
Secondary Configuration register is 0x0
```

Step 2 Use the **dir** {**bootflash:** | **disk0:** | **disk1:** | **sec-bootflash:** | **sec-disk0:** | **sec-disk1:**} EXEC command to verify the location and version of the primary and secondary NSP software image.

```
Switch# dir disk0:
Directory of disk0:/

  3  -rw-      628539   Jan 01 2000 00:08:55  c6400s-wp-mz.120-5.DB

109760827 bytes total (108228293 bytes free)

Switch# dir sec-disk0:
Directory of sec-disk0:/

  8  -rw-      628224   Jul 01 1999 00:08:55  c6400s-wp-mz.120-4.DB

109760512 bytes total (108228608 bytes free)
```

Step 3 If the primary and secondary NSPs contain the same image version in the same location, the NSPs are already configured for hardware backup. Do not proceed to the next step.

Step 4 If the secondary NSP does not contain the same image in the same location, use the **delete** and **squeeze** EXEC commands to delete the secondary NSP software image.

```
Switch# delete sec-disk0:c6400s-wp-mz.120-4.DB
Switch# squeeze sec-disk0:
```

Step 5 Copy the primary NSP image to the same location on the secondary NSP.

```
Switch# copy disk0:c6400s-wp-mz.120-5.DB sec-disk0:c6400s-wp-mz.120-5.DB
```

Verifying NSP Redundancy for Hardware Backup

To verify that the NSP redundancy is configured for hardware backup, use the **show bootvar** and **dir** EXEC commands from Step 1 and Step 2. Check that both NSPs use the same system image and store the image in identical locations.

Using NSP Redundancy for Software Error Protection

For software error protection, the primary and secondary NSPs should have different system images. Cisco recommends using NSP redundancy for software error protection when you are using new or experimental Cisco IOS software.

To specify different startup images for the primary and secondary NSPs, complete the following steps, beginning in EXEC mode:

Step 1 Use the **dir** {**bootflash:** | **disk0:** | **disk1:** | **sec-bootflash:** | **sec-disk0:** | **sec-disk1:**} EXEC command to verify the locations and versions of the primary and secondary NSP software images.

```
Switch# dir disk0:
Directory of disk0:/

  3  -rw-      628539   Jan 01 2000 00:08:55  c6400s-wp-mz.120-5.DB
376  -rw-        2134   Jan 05 2000 22:05:27  startup.config

109760827 bytes total (108228293 bytes free)

Switch# dir sec-disk0:
Directory of sec-disk0:/

  8  -rw-      628224   Jul 01 1999 00:08:55  c6400s-wp-mz.120-5.DB
184  -rw-        2134   Jan 05 2000 22:05:27  startup.config

109760512 bytes total (108228608 bytes free)
```

Step 2 If necessary, copy the desired system images to the primary and secondary NSPs. Make sure the primary and secondary NSPs use different image versions.

```
Switch# copy tftp://10.1.1.1/c6400s-wp-mz.120-7.DB disk0:c6400s-wp-mz.120-7.DB
Switch# copy tftp://10.1.1.1/c6400s-wp-mz.120-5.DB sec-disk0:c6400s-wp-mz.120-5.DB
```

Step 3 From global configuration mode, use the **boot system** global configuration command to boot the images from the appropriate locations. Enter the image for the primary NSP first.

```
Switch# configure terminal
Switch(config)# boot system flash disk0:c6400s-wp-mz.120-7.DB
Switch(config)# boot system flash disk0:c6400s-wp-mz.120-5.DB
```

Step 4 Set the configuration register to load the system image from Flash.

```
Switch (config)# config-register 0x2101
```

Step 5 Enable automatic synchronization of the redundant NSPs.

```
Switch(config)# redundancy
Switch(config-r)# main-cpu
Switch(config-r-mc)# auto-sync standard
Switch(config-r-mc)# end
```

Step 6 Save the configuration file to the startup configuration in NVRAM. Because automatic synchronization is enabled, this step saves the **boot system** commands to both NSP startup configurations.

```
Switch# copy system:running-config nvram:startup-config
```

Step 7 If the primary NSP is not running the correct image, reset both NSPs.

```
Switch# hw-module nsp A reset
Switch# hw-module nsp B reset
```

Step 8 If the primary NSP is running the earlier software version, perform a switchover from the current primary to the secondary NSP.

```
Switch# redundancy force-failover main-cpu
```

Verifying NSP Redundancy for Software Error Protection

To verify that NSP redundancy is configured for software error protection, use the **show bootvar** EXEC command. Check that the secondary NSP is up, that the BOOT variables identify different software images, and that all other variables match.

```
Switch# show bootvar
BOOT variable = tftp:dir/c6400s-wp-mz.121-5.DC.bin 10.255.254.254,12;
CONFIG_FILE variable =
BOOTLDR variable =
Configuration register is 0x2000 (will be 0x1 at next reload)

Secondary is up.
Secondary BOOT variable = tftp:dir/c6400s-wp-mz.121-4.DC.bin 10.255.254.254,12;
Secondary CONFIG_FILE variable =
Secondary BOOTLDR variable =
Secondary Configuration register is 0x1
```

Booting Redundant NSPs from a Network Server

To boot a dual-NSP system from a network server (also called *netbooting*), the network management interface (Ethernet 0/0/0 on the NSP) must be configured for Dynamic Host Configuration Protocol (DHCP) IP address acquisition. To do this, complete the following steps beginning in global configuration mode:

	Command	Purpose

Step 1	`Switch(config)# redundancy`
	`Switch(config-r)# main-cpu`
	`Switch(config-r-mc)# auto-sync standard`
		Enables automatic synchronization between the redundant NSPs.

Step 2	`Switch(config-r-mc)# exit` `Switch(config-r)# exit`	Returns to global configuration mode.
Step 3	`Switch(config)# interface ethernet0/0/0` `Switch(config-if)# ip address negotiated`	Configures the NSP network management interface for DHCP IP address acquisition.
Step 4	`Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 5	`Switch# copy system:running-config nvram:startup-config`	Saves the configuration to the startup configuration.

Note Make sure the DHCP server is properly set up with appropriate dynamic and static pools of IP addresses.

Example

In the following example, the NSP network management interface is configured for DHCP IP address acquisition. This allows you to boot redundant NSPs from a network server.

```
!
redundancy
 main-cpu
  auto-sync standard
  !
interface ethernet0/0/0
 ip address negotiated
 !
```

Verifying Booting Redundant NSPs from a Network Server

To verify that the NSPs are prepared for netbooting, use the **more sec-nvram:startup-config** EXEC command. The presence of the correct commands in the secondary startup configuration confirms that both NSPs are configured properly.

NRP Redundancy

For two NRPs to act as a redundant pair, they must be installed in one the following slot pairs:

- 1 and 2
- 3 and 4
- 5 and 6
- 7 and 8

Configuring Redundant NRPs

To configure NRP redundancy, complete the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	`Switch(config)# redundancy`	Enters the redundancy configuration submode.
Step 2	`Switch(config-r)# associate slot` *slot* [*slot*]	Configures the two slots as a redundant pair. You need specify only the first slot of the redundant pair. The second slot is assumed to be the adjacent slot.

Example

In the following example, the NRPs in slots 1 and 2 are configured as a redundant pair.

```
!
redundancy
 associate slot 1 2
 main-cpu
  auto-sync standard
```

Verifying NRP Redundancy

To verify NRP redundancy, use the **show redundancy** EXEC command on the NRP:

```
Router# show redundancy
Primary   NRP in slot 2, system configured non redundant

User EHSA configuration (by CLI config):
slave-console = off
keepalive     = on
config-sync modes:
standard   = on
start-up   = on
boot-var   = on
config-reg = on

NSP EHSA configuration (via pam-mbox):
redundancy         = off
preferred (slot 2) = yes

Debug EHSA Information:
NRP specific information:
Backplane resets       = 0
NSP mastership changes = 0

print_pambox_config_buff: pmb_configG values:
valid            = 1
magic            = 0xEBDDBE1 (expected 0xEBDDBE1)
nmacaddrs        = 1
run_redundant    = 0x0
preferred_master = 0x1
macaddr[0][0]    = 0010.7b79.af93
macaddr[1][0]    = 0000.0000.0000

EHSA pins:
peer present = 0
peer state   = SANTA_EHSA_SECONDARY
crash status: this-nrp=NO_CRASH(1) peer-nrp=NO_CRASH(1)

EHSA related MAC addresses:
peer bpe mac-addr = 0010.7b79.af97
my   bpe mac-addr = 0010.7b79.af93
```

Erasing Startup Configurations on Redundant NRPs

To erase the startup configuration on redundant NRPs, complete the following steps beginning in EXEC mode:

	Command	Purpose
Step 1	`Router# erase nvram:`	Erases the primary NRP's startup configuration.
Step 2	`Router# erase sec-nvram:`	Erases the secondary NRP's startup configuration.

Note If you erase the startup configuration on the primary NRP only, and the primary and secondary NRPs reverse roles, the new primary NRP will use the old startup configuration.

Verifying Erased Startup Configurations

To verify that you erased the startup configuration on redundant NRPs, use the **dir nvram:** and **dir sec-nvram:** EXEC commands and check that the startup-config size is zero:

```
NRP# dir nvram:
Directory of nvram:/

  1  -rw-           0              <no date>  startup-config

129016 bytes total (129016 bytes free)
```

You can also use the **show startup** EXEC command and make sure that a valid configuration file does not appear:

```
NRP# show startup
%% Non-volatile configuration memory is being written, Try again later
```

NLC Redundancy

When a node line card (NLC) is configured for redundancy, all ports on that card are automatically configured to operate in redundant mode using SONET automatic protection switching (APS). For more information on SONET APS, see the "SONET APS for NLC Port Redundancy" section on page 5-19.

Configuring Redundant Full-Height NLCs

For two full-height NLCs to act as a redundant pair, they must be installed in one the following slot pairs:

- 1 and 2
- 3 and 4
- 5 and 6
- 7 and 8

Note By default, the NLC in the lower slot number is the working device, and the NLC in the higher slot number is the protection device.

To configure redundant full-height NLCs, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Switch(config)# redundancy`	Enters the redundancy configuration submode.
Step 2	`Switch(config-r)# associate slot` *slot* [*slot*]	Configures the two slots as a redundant pair. You need specify only the first slot of the redundant pair. The second slot is assumed to be the adjacent slot.

Example

In the following example, the OC-12s in slots 5 and 6 are configured for redundancy:

```
!
redundancy
 associate slot 5 6
!
```

Configuring Redundant Half-Height NLCs

For two half-height NLCs to act as a redundant pair, they must be installed in one of the following slot/subslot pairs:

- 1/0 and 2/0, or 1/1 and 2/1
- 3/0 and 4/0, or 3/1 and 4/1
- 5/0 and 6/0, or 5/1 and 6/1
- 7/0 and 8/0, or 7/1 and 8/1

Note By default, the NLC in the lower slot number is the working device, and the NLC in the higher slot number is the protection device.

To configure redundant half-height NLCs, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Switch(config)# redundancy`	Enters the redundancy configuration submode.
Step 2	`Switch(config-r)# associate subslot` *slot/subslot* [*slot/subslot*]	Configures the two subslots as a redundant pair. You need only specify the first subslot of the redundant pair. The second subslot is assumed to be the adjacent slot.

Example

In the following example, the OC-3s in subslots 3/0 and 4/0 are configured as a redundant pair:

```
!
redundancy
 associate subslot 3/0 4/0
 !
```

Verifying NLC Redundancy

To verify NLC redundancy, use the **show aps** EXEC command on the NSP. The **show aps** command displays the status for all NLCs configured for port redundancy.

```
Switch# show aps
ATM7/0/0: APS Lin NR Uni, Failure channel: Protection
          Active Channel: CHANNEL7/0/0, Channel stat: Good
          Port stat (w,p): (Good, Good)
ATM7/0/1: APS Lin NR Uni, Failure channel: Protection
          Active Channel: CHANNEL7/0/1, Channel stat: Good
          Port stat (w,p): (Good, Good)
```

SONET APS for NLC Port Redundancy

SONET automatic protection switching (APS) provides a mechanism to support redundant transmission interfaces (circuits) between SONET devices. Automatic switchover from the working (primary) circuit to the protection (secondary) circuit happens when the working circuit fails or degrades.

The Cisco 6400 supports SONET APS operation that is:

- 1+1— There is one working interface and one protection interface, and the same payload from the transmitting end is sent to both the receiving ends. The receiving end decides which interface to use. The line overhead (LOH) bytes (K1 and K2) in the SONET frame indicate both status and action.
- Linear—Back-to-back connection (as opposed to a ring topology), as defined in the *Telcordia GR-253-CORE* document.
- Unidirectional—Transmit and receive channels are switched independently.
- Nonreverting—Nonreverting channels continue to operate after a failure has been corrected, thus preventing data from flowing back to the working channel.

Note By default, the NLC in the lower slot number is the working device, and the NLC in the higher slot number is the protection device.

Enabling and Disabling SONET APS

In the Cisco 6400, a pair of redundant ports is represented as a single interface. APS commands are accepted only for an interface that represents a pair of redundant ports.

For APS operation, the APS mode must be specified for each interface associated with a redundant pair of ports. To enable SONET APS, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Switch(config)# interface atm slot/subslot/port`	Specifies the interface (that represents a pair of redundant NLC ports).
Step 2	`Switch(config-if)# aps mode linear 1+1 nonreverting unidirectional`	Enables SONET APS on the interface. This command must be entered before the other **aps** commands.

Note SONET APS is enabled by default when you install an NLC in a slot already configured for redundancy.

If the redundant NLC configuration is disabled by using the **no associate slot** or **no associate subslot** redundancy configuration commands, two interface configuration sections are created, one for each port, but all of the APS configuration commands are removed.

Example—Enabling SONET APS

In the following example, SONET APS is enabled for ATM interface 1/0/0:

```
!
interface atm 1/0/0
 aps mode linear 1+1 nonreverting unidirectional
 !
```

Example—Disabling Redundancy and SONET APS

The following table shows example configurations before and after redundancy is turned off:

Redundancy On	After Redundancy Is Turned Off
redundancy associate slot 1 2 ! interface ATM1/0/0 no ip address no ip redirects no ip proxy-arp no atm auto-configuration no atm ilmi-keepalive atm uni version 4.0 aps mode linear 1+1 nonreverting unidirectional aps signal-fail BER threshold 3 !	interface ATM1/0/0 no ip address no ip redirects no ip proxy-arp no atm auto-configuration no atm ilmi-keepalive atm uni version 4.0 ! interface ATM2/0/0 no ip address no ip redirects no ip proxy-arp no atm auto-configuration no atm ilmi-keepalive atm uni version 4.0 !

Verifying SONET APS

To verify the that SONET APS is enabled or to determine if a switchover has occurred, use the **show aps** EXEC command or the **show controller atm** *slot/subslot/port* command.

In the following example, slot 7 contains the working (primary) card, and slot 8 contains the protection (secondary) card:

```
Switch# show aps
ATM7/0/0: APS Lin NR Uni, Failure channel: Protection
          Active Channel: CHANNEL7/0/0, Channel stat: Good
          Port stat (w,p): (Good, Good)
ATM7/0/1: APS Lin NR Uni, Failure channel: Protection
          Active Channel: CHANNEL7/0/1, Channel stat: Good
          Port stat (w,p): (Good, Good)
```

In the following example, the OC-3 interface ATM 5/0/0 is not configured for redundancy:

```
Switch# show controller atm 5/0/0
→ Redundancy NOT Enabled on interface
IF Name: ATM5/0/0    Chip Base Address(es): A8B08000, 0 Port type: OC3    Port rate: 155
Mbps    Port medium: SM Fiber
Port status:Good Signal    Loopback:None    Flags:8308
TX Led: Traffic Pattern    RX Led: Traffic Pattern  TX clock source:  network-derived
Framing mode:  sts-3c
Cell payload scrambling on
Sts-stream scrambling on
```

Setting SONET APS Priority Requests

APS priority requests are used to manually control the relationship between two APS ports from the EXEC mode. The APS priority levels, lockout (1), force (2), and manual (5) are defined in the *Telcordia GR-253-CORE* document.

To set the APS priority requests, use the following commands in EXEC mode:

Command	Purpose
`Switch# aps lockout atm slot/subslot/port`	APS priority level 1 request. Prevents a working interface from switching to a protection interface.
`Switch# aps force atm slot/subslot/port from [protection | working]`	APS priority level 2 request. Manually forces the specified interface to the protection or working interface, unless a request of equal or higher priority is in effect. Use the **working** option to force operation from the working channel to the protection channel. Use the **protection** option to force operation from the protection channel to the working channel.
`Switch# aps manual atm slot/subslot/port from [protection | working]`	APS priority level 5 request. Manually switches an interface to the protection or working interface, unless a request of equal or higher priority is in effect. Use the **working** option to manually switch operation from the working channel to the protection channel. Use the **protection** option to manually switch operation from the protection channel to the working channel.
`Switch# aps clear atm slot/subslot/port`	Manually clears all posted APS priority requests created by any of the APS priority commands.

Example

In the following example, the system is forced to use the protection channel associated with ATM interface 1/0/0:

```
Switch# aps force atm 1/0/0 from working
```

Verifying the APS Priority Requests

To verify that you successfully set the APS priority requests, use the **show aps** EXEC command:

```
Switch# aps force atm 5/1/0 from working
Switch# show aps

ATM5/1/0:APS Lin NR Uni, Failure channel:Working
          Active Channel:CHANNEL6/1/0, Channel stat:Force Switch
          Port stat (w,p):(Good, Good)
```

Setting SONET APS Signal Thresholds

You can configure the APS signal bit error rate (BER) thresholds at which the system announces signal degradation or signal failure.

The **aps signal-degrade BER threshold** command controls the BER value at which a signal degrade is announced, indicating an unstable or error-prone connection. This BER threshold can be in the range of 10^{-5} to 10^{-9}, and there is no default threshold.

The **aps signal-fail BER threshold** command controls the BER value at which a signal failure is announced, indicating a broken connection. This BER threshold can be in the range of 10^{-3} to 10^{-5}, with a default threshold of 10^{-3}.

To configure the thresholds, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Switch(config)# interface atm slot/subslot/port`	Selects the NLC interface.
Step 2	`Switch(config-if)# aps signal-degrade BER threshold value`	Sets the BER threshold value for signal degradation for the interface.
Step 3	`Switch(config-if)# aps signal-fail BER threshold value`	Sets the BER threshold value for signal failure for the interface.

The *value* argument represents the exponent of the BER threshold. For instance, a value of 5 would set the threshold to 10^{-5}.

Example

The following example shows how to set the APS signal degradation and signal failure thresholds for ATM interface 1/0/0:

```
Switch(config)# interface atm 1/0/0
Switch(config-if)# aps signal-degrade BER threshold 7
Switch(config-if)# aps signal-fail BER threshold 5
```

Verifying SONET APS Signal Thresholds

To display the current BER threshold settings for an interface, use the **show interface atm** command:

```
Switch# show interface atm 1/0/0
interface ATM1/0/0
 description la1
 no ip address
 no ip redirects
 no ip proxy-arp
 no atm auto-configuration
 no atm ilmi-keepalive
 atm uni version 4.0
 aps mode linear 1+1 nonreverting unidirectional
 aps signal-fail BER threshold 3
 aps signal-degrade BER threshold 9
```

Primary and Secondary Role Switching

The Cisco 6400 allows you to manually force the primary and secondary devices in a redundant pair to switch roles. This capability can be important for upgrade or debug activities.

Reversing NSP and NRP Redundancy Roles

To reverse the primary and secondary roles in a redundant pair of NSPs or NRPs, use the following command in EXEC mode:

Command	Purpose
`Switch# redundancy force-failover {slot | slot/subslot | main-cpu}`	Forces the system to switch the current primary and secondary devices of the redundant pair.

Reversing NLC Redundancy Roles

To reverse the primary and secondary roles in a redundant pair of NLCs, use the **aps force** or **aps manual** EXEC commands described in the "Setting SONET APS Priority Requests" section on page 5-20.

Resetting Cards, Slots, and Subslots

On the Cisco 6400 it is often useful to reset a card in a particular slot or subslot in a redundant pair. The reset function described here is different from resetting an interface. In general, the **hw-module (reset)** command simulates card removal and insertion of the specified device. If the specified card is the primary device in a redundant pair, operation will automatically switch to the other card.

To reset a card, use the following command in EXEC mode:

Command	Purpose
`Switch# hw-module {slot slot | subslot slot/subslot | main-cpu | sec-cpu | nsp {A | B}} reset`	Simulates removal and insertion of a device installed in the Cisco 6400 chassis.

When entered in EXEC mode, this command causes an immediate reset of the device installed in the specified slot or subslot. When a port is reset, all of the input/output hardware associated with the port is reset. If a slot is reset, both of the cards installed in the associated subslots are reset. The **main-cpu** and **sec-cpu** options allow you to reset the desired NSP regardless of the one to which you are currently connected.

Note The **hw-module** command is not supported for ports. The command only supports slots and subslots.