



## Backups, Upgrades, and Node Critical Commands

---

This chapter describes embedded software utility functions and contains the following sections:

- System Database Backup, page 14-2
  - Backing Up the System Database, page 14-2
- Cisco 6732 Embedded Software Image Upgrade, page 14-5
  - Identifying Active and Standby MCC Cards, page 14-6
  - Placing Standby MCC Card Out of Service, page 14-7
  - Upgrading the Standby MCC Card, page 14-8
  - Resetting the Standby MCC Card, page 14-9
  - Verifying the Upgrade, page 14-11
  - Placing the Standby MCC Card In Service, page 14-11
  - Upgrading the Active MCC Card, page 14-11
  - Performing MCC Card Switchover, page 14-12
  - Resetting the Line Cards, page 14-13
- Cisco 6705 Embedded Software Image Upgrade, page 14-14
  - Upgrading the MCC INT Embedded Software Image, page 14-15
  - Resetting the MCC INT Card, page 14-16
- Cisco IAD1101 Embedded Software Image Upgrade, page 14-18
  - Upgrading the Cisco IAD1101 Embedded Software Image, page 14-19
  - Resetting the Internal MCC Card, page 14-21
- Node Critical Commands, page 14-23
  - Launching Node Critical Commands Utilities, page 14-23
  - Restoring a Database, page 14-24
  - Erasing a Database, page 14-25
  - Resetting the MCC Card, page 14-27
  - Resetting Line Cards, page 14-27
  - Changing a Password, page 14-28

# System Database Backup

The EMS database backup utility allows you to back up the existing configuration of a node to a TFTP server. After the database has been backed up, you can restore the node configuration, if needed. The database restore procedure is described in the “Restoring a Database” on page 14-24.

## Before You Begin

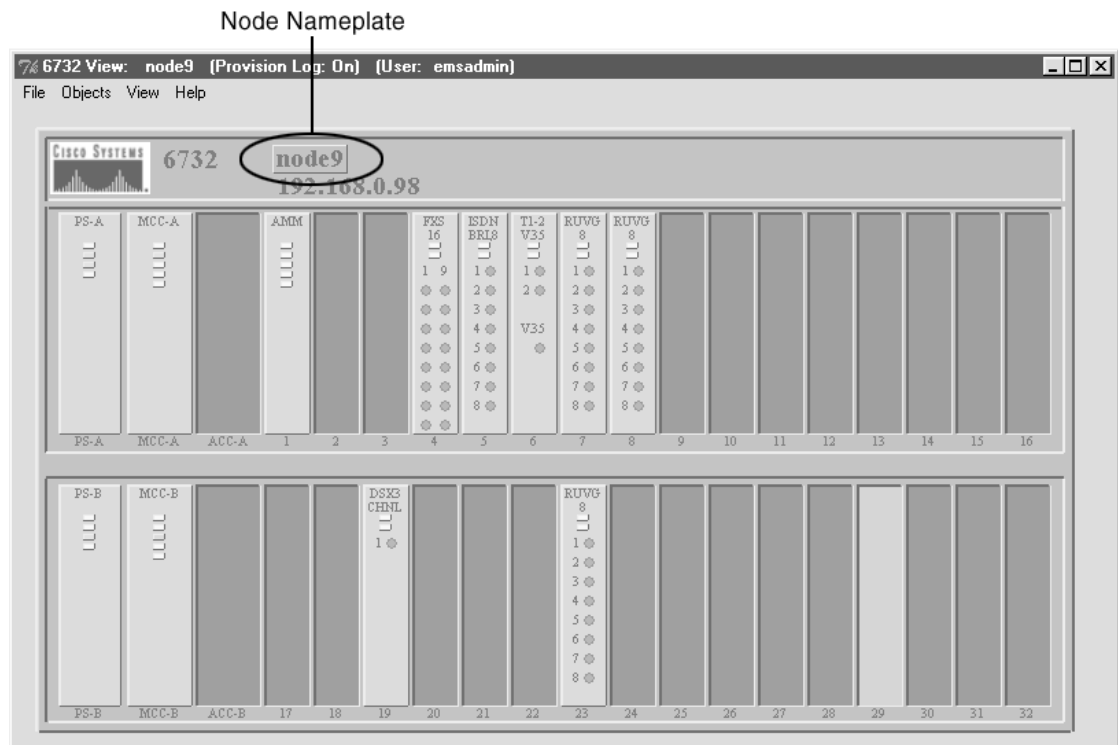
Before beginning the database backup, complete the following tasks:

- Connect a local EMS workstation to the NE chassis.
- Verify that a TFTP server is online and available to receive the database backup information. TFTP server verification can be confirmed by pinging the TFTP host (confirms that the Cisco 6700 Series NE is properly routed to the TFTP host).

## Backing Up the System Database

**Step 1** From Cisco 6700 NetView, double-click the node to open Cisco 6700 NodeView. (See Figure 14-1.)

**Figure 14-1** Cisco 6700 NodeView



37184

**Step 2** Double-click the node nameplate to launch the NE provision window. (See Figure 14-2.)

**Figure 14-2** NE Provision Window

**NE Provision for 6732 node: node9**

System Basic Provisioning	<b>NE Name:</b> 6732
IP Address Configuration	<b>Alias:</b>
IP & Datalink Route Configuration	<b>NE Location:</b> Central Office
Ping Node	<b>NE Node Type:</b> NetworkNode
Node ID Configuration	<b>NE Time Of Day:</b> 2000-04-27,17:29:17.0
IP & Inter Node Link Configuration	<b>NE Uptime:</b> 0d 9:26:16
Timing Source Selection & Control	<b>NE Backplane Version:</b> 1.3
Timing Distribution Provisioning	<b>NE Loaded Software Version:</b> 1.3(2)
NE Time Of Day Set	<b>NE CLEI Code:</b> SBMAFGODRA
Alarm Provisioning	<b>NE Serial Number:</b> 6861
Common Control Card Switch Over	<b>NE Backplane Type:</b> Unknown
Software Upgrade	<b>Alarm Status:</b> normal
Database Backup/Restore	<b>Problem List:</b>
Error Log Retrieval	
Exit	

Apply Refresh

9-5-820

**Step 3** Select **Database Backup** from the function bar. (See Figure 14-3.)

**Figure 14-3 Database Backup Window**

The screenshot shows a software window titled "NE Provision for 6732 node: node9". On the left is a vertical menu with the following items: System Basic Provisioning, IP Address Configuration, IP & Datalink Route Configuration, Ping Node, Node ID Configuration, IP & Inter Node Link Configuration, Timing Source Selection & Control, Timing Distribution Provisioning, NE Time Of Day Set, Alarm Provisioning, Common Control Card Switch Over, Software Upgrade, Database Backup, Error Log Retrieval, and Exit. The "Database Backup" option is highlighted. The main content area on the right contains the following fields and labels:

- Database Image Host IP Address:** 0 0 0 0
- Database Image Path on the Host:** [Empty text box]
- Database on Main Common Control Card:** A [Dropdown arrow]
- Active Main Common Control Card:** A
- Database Action Status:** unknownState

At the bottom right of the main area are three buttons: "Apply", "Backup", and "Refresh". A small number "37197" is visible in the bottom right corner of the window frame.

**Step 4** Complete the following fields to begin the database backup procedure:

- **Database Image Host IP Address**—Enter the IP address of the TFTP host.
- **Database Image Path on the Host**—Enter the file name to be used for the database backup file.
- **Database on Main Common Control Card**—Select the MCC (**A** or **B**) to be backed up. The active MCC is shown in the **Active Main Common Control Card** field.

**Step 5** Click **Apply** to save the backup configuration.

**Step 6** Click **Backup** to begin the database backup.

# Cisco 6732 Embedded Software Image Upgrade

The following sections describe the Stratum 3 or Stratum 4 MCC embedded software upgrade procedure for the Cisco 6732:

- Identifying Active and Standby MCC Cards, page 14-6
- Placing Standby MCC Card Out of Service, page 14-7
- Upgrading the Standby MCC Card, page 14-8
- Resetting the Standby MCC Card, page 14-9
- Placing the Standby MCC Card In Service, page 14-11
- Upgrading the Active MCC Card, page 14-11
- Performing MCC Card Switchover, page 14-12
- Resetting the Line Cards, page 14-13

**Note**

Reset procedures are also covered in the “Node Critical Commands” on page 14-23.

**Caution**

For a successful upgrade, follow all procedures, and all steps, in sequence.

**Caution**

If for any reason EMS is unable to complete the embedded software upgrade, *do not reset the MCC card*. You must restart the embedded software upgrade process. Resetting the MCC with a partial software image corrupts the MCC. If there is an error, an error message displays in the Software Upgrade Status field, or at the bottom of the NE provision window, as well as in the problem list of the MCC card (if the card is functional).

## Before You Begin

Before beginning the embedded software upgrade, complete the following tasks:

**Caution**

Be certain you are *not* upgrading to embedded software Version 1.4. Embedded software Version 1.4 *only* operates with the Cisco IAD1101. Check with your system administrator, if necessary.

- Contact your network administrator to ensure that the EMS password files are properly installed. The software upgrade procedure requires the password files and corresponding password.
- For a local upgrade, use a crossover Ethernet cable to connect the EMS workstation to the Ethernet management port on the alarm maintenance and monitoring (AMM) module. If the Cisco 6732 chassis does not contain an AMM module, use the Ethernet port on the active Main Common Control (MCC) module. Alternately, you can use straight Ethernet cables to connect the EMS workstation and Cisco 6732 to a local hub.
- For a remote upgrade, you must have a DS0-type inter node data link (INDL) between the local node and the remote node.
- Verify that INDLs to all remote nodes are working. A software upgrade cannot be done over an FDL INDL. For more information, see Chapter 8, “Inter Node Links.”

- Verify that a TFTP server is online and available to receive the database backup information. TFTP server verification can be confirmed by pinging the TFTP host (this confirms that the Cisco 6732 is properly routed to the TFTP host).
- Verify that the TFTP server contains the correct embedded software file, such as **SwLoad.iad**, in the TFTP directory.
- Back up the system database before starting the software upgrade. Before backing up the database, refer to the “Backing Up the System Database” on page 14-2, and the “Restoring a Database” on page 14-24.

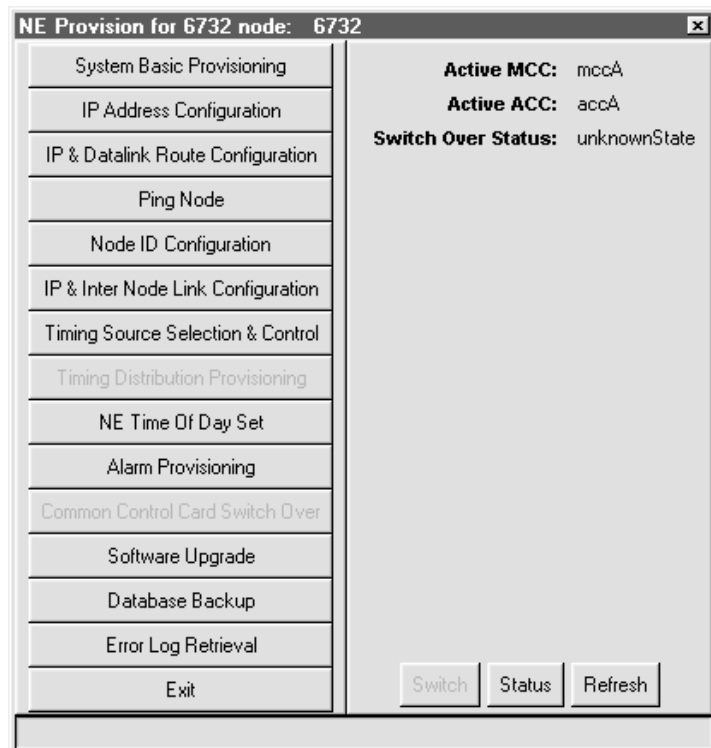
**Caution**

When upgrading multiple nodes in a network, always start from the far end of the network, one node at a time. In a typical network, a number of remote nodes (subscriber nodes) are connected to a central office terminal (COT) node. If the upgrade of COT is mishandled, the entire network can be lost. Upgrade tests and sample enhancements should be made at the edge node. If the upgrade tests fail on the edge nodes, do not attempt to upgrade the COT node.

## Identifying Active and Standby MCC Cards

- Step 1** From Cisco 6700 NodeView of the Cisco 6732 to be backed up, double-click the node nameplate to launch the NE provision window. (See Figure 14-2 on page 14-3.)
- Step 2** Click **Common Control Card Switch Over** in the function bar to view the switchover window. (See Figure 14-4.)

**Figure 14-4** Common Control Card Switch Over Option



- Step 3** Look at the **Active MCC** field. EMS identifies the active MCC:
- The MCC in the top shelf of the chassis is **MCC-A (mccA)**.
  - The MCC in the bottom shelf of the chassis is called **MCC-B (mccB)**.
- Step 4** Identify the standby MCC. The screen does not show the standby MCC. The MCC that is not active is called the standby MCC. For example, if MCC-A is active, then MCC-B is the standby MCC.
- Step 5** Click **Exit** to return to NodeView.
- 

## Placing Standby MCC Card Out of Service

---

- Step 1** From Cisco 6700 NodeView (see Figure 14-1 on page 14-2), double-click the icon of the standby MCC card (in this example, the standby MCC is on the lower shelf). EMS launches the plugin card provision window.
- Step 2** Set the **Admin Status** field to **OutOfService**.
- Step 3** Click **Apply** to place the MCC card out of service.
- Step 4** Click **Exit** to return to Cisco 6700 NodeView.
-

## Upgrading the Standby MCC Card

- Step 1** From Cisco 6700 NodeView, double-click the node nameplate to launch the NE provision window. (See Figure 14-2 on page 14-3)
- Step 2** Click **Software Upgrade** in the function bar to view the software upgrade window. (See Figure 14-5.)

Figure 14-5 Cisco 6732 Software Upgrade Window

NE Provision for 6732 node: node9

System Basic Provisioning	<b>Software Image Host IP Address:</b> 0 0 0 0
IP Address Configuration	<b>Software Image File Name:</b> <input type="text"/>
IP & Datalink Route Configuration	<b>Card Side:</b> A
Ping Node	<b>Target Card:</b> No card selected
Node ID Configuration	<b>Active MCC:</b> A
IP & Inter Node Link Configuration	<b>Software Upgrade Status:</b> unknownState
Timing Source Selection & Control	
Timing Distribution Provisioning	
NE Time Of Day Set	
Alarm Provisioning	
Common Control Card Switch Over	
Software Upgrade	
Database Backup	
Error Log Retrieval	
Exit	

Apply Upgrade Refresh

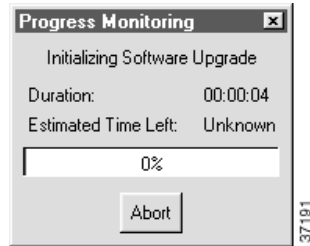
37190

- Step 3** In the **Software Image Host IP Address** field, enter the IP address of the TFTP server.
- Step 4** In the **Software Image File Name** field, enter **SwLoad.iad**.
- Step 5** From the **Card Side** drop-down menu, select the shelf (A = top shelf, B = bottom shelf) containing the standby MCC card (in this example, the bottom shelf).
- Step 6** Click **Apply** to confirm the host IP address and path to the image filename.
- Step 7** Click **Upgrade**. The backup LED on the standby MCC flashes as the embedded software image downloads into the card's Flash memory.



- Step 8** Observe the progress bar. (See Figure 14-6.) When the Software Upgrade Status field in the Software Upgrade Window reads: “passed”, the upgrade is complete.

**Figure 14-6** MCC Upgrade Progress Bar



- Step 9** Click **Exit** to return to Cisco 6700 NodeView.
- Step 10** Reset the Standby MCC card (see the next procedure, “Resetting the Standby MCC Card”).

## Resetting the Standby MCC Card



### Caution

Do not power down the NE or remove the MCC during an MCC reset. The MCC must finish loading the system software before the MCC can be safely powered down, removed, reset, or reprovioned.



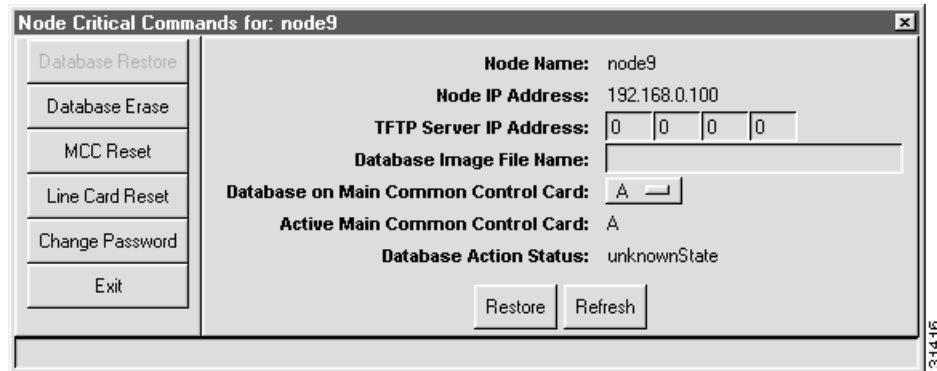
### Note

Performing an MCC reset erases the internal clock on the NE. To set the time of day on the NE, see the “Provision NE Clock” section of Chapter 4, “Initial Node Provisioning.”

- Step 1** From Cisco 6700 NetView, right-click the Cisco 6732 you are upgrading and select **Node Critical Commands** from the popup menu.

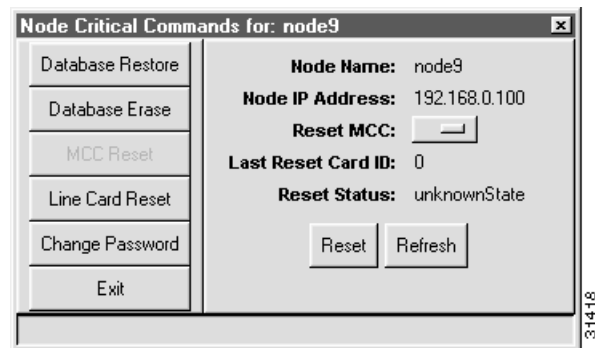
- Step 2** Enter the node critical commands password. The node critical commands window opens, displaying the database restore function. (See Figure 14-7.) If necessary, contact your EMS administrator to obtain the correct node critical commands password.

**Figure 14-7 Node Critical Commands Window**



- Step 3** Click **MCC Reset** in the function bar to open the MCC reset window. (See Figure 14-8.)

**Figure 14-8 MCC Reset**



- Step 4** In the **Reset MCC** field, select the standby MCC (**A** or **B**)
- Step 5** Click the **Reset** button and respond **Yes** to the prompt. Allow at least 45 seconds for the MCC to reset and reload the system software.
- Step 6** Click **Refresh**. The Reset Status field should read “reset”.
- Step 7** Click **Exit** to return to NetView.

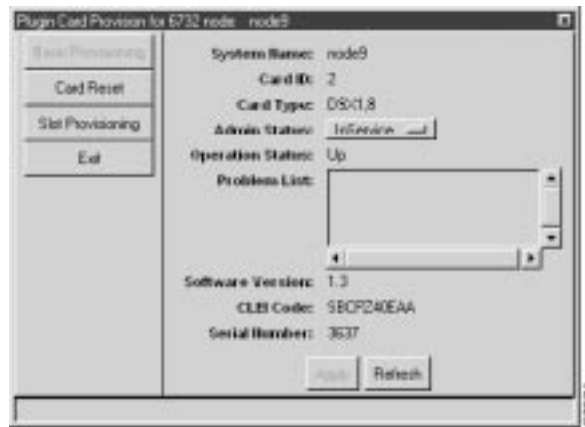
## Verifying the Upgrade

- 
- Step 1 From Cisco 6700 NodeView, double-click the icon of the standby MCC card to open the Plugin Card Provisioning window. (See Figure 14-9.)
  - Step 2 Confirm that the version number in the Software Version field is correct.
- 

## Placing the Standby MCC Card In Service

- 
- Step 1 From Cisco 6700 NodeView, double-click the standby MCC card. EMS launches the plugin card provisioning window. (See Figure 14-9.)

*Figure 14-9 Plugin Card Provisioning Window*



- Step 2 Set the **Admin Status** field to **InService** (you can safely dismiss the warning message).
  - Step 3 Click **Apply** to place the card in service.
  - Step 4 Click **Exit** to return to NodeView.
- 

## Upgrading the Active MCC Card

- 
- Step 1 From Cisco 6700 NodeView, double-click the node nameplate to launch the NE provision window. (See Figure 14-2 on page 14-3).
  - Step 2 Click **Software Upgrade** in the function bar to view the software upgrade window. (See Figure 14-5 on page 14-8.)
  - Step 3 In the **Software Image Host IP Address** field, enter the IP address of the TFTP server.
  - Step 4 In the **Software Image File Name** field, enter **SwLoad.fbx**.
  - Step 5 From the **Card Side** drop-down menu, select the shelf (A = top shelf, B = bottom shelf) containing the active MCC card.

- Step 6** From the **Target Card** drop-down menu, select the active MCC card.
- Step 7** Click **Apply** to confirm the host IP address and path to the image filename.
- Step 8** Click **Upgrade** to download the embedded software image into the Flash memory of the MCC card. EMS displays a progress bar. (See Figure 14-6 on page 14-9.) Wait until the software upgrade is complete and the Software Upgrade Status field reads: “passed”.
- Step 9** Click **Exit** to return to NodeView.



**Note** The MCC switchover (described in the next procedure) automatically resets the active MCC. You do not have to perform an independent reset.

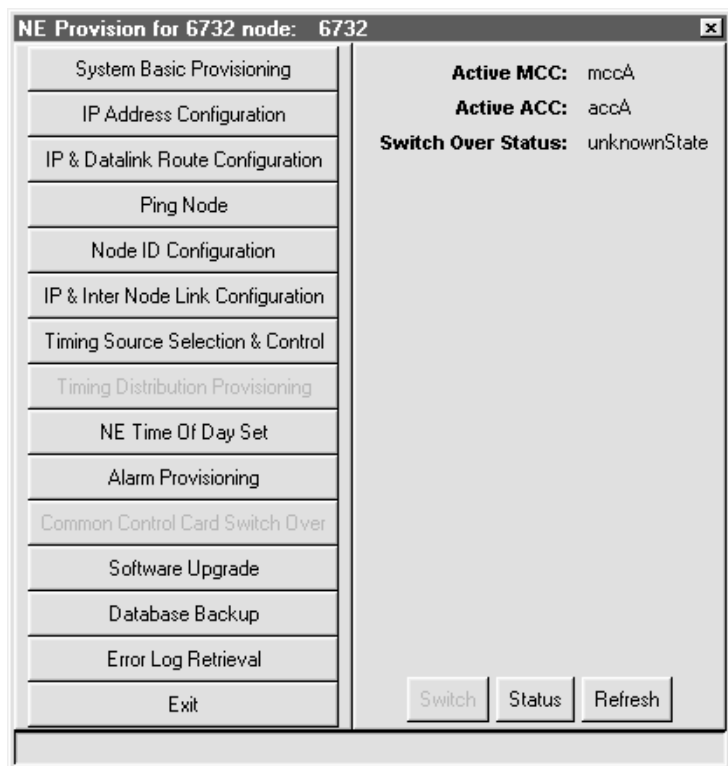


**Note** Performing an MCC reset erases the internal clock on the NE. To set the time of day on the NE, see “Setting the NE Clock” on page 4-14.

## Performing MCC Card Switchover

- Step 1** From Cisco 6700 NodeView, double-click the node nameplate to launch the NE provision window.
- Step 2** Click **Common Control Card Switch Over** in the function bar. (See Figure 14-10.)

*Figure 14-10 Common Control Card Switch Over Option*



- Step 3 Click **Switch** to switch control from the active MCC to the standby MCC.
- Step 4 Respond **Yes** to the confirmation prompt. EMS switches traffic to the standby MCC.
- Step 5 Click **Exit** to return to NodeView.

## Resetting the Line Cards



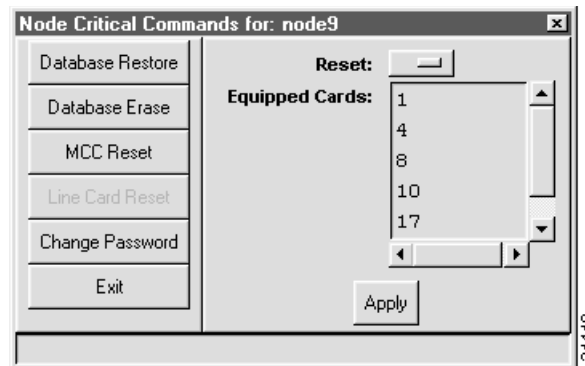
**Note** The line card reset procedure applies to all Cisco 6700 series platforms. BPS-HP and AMM service modules do not need to be reset.



**Caution** The line card reset procedure reboots the line interface modules and effectively takes them out of service. Any traffic carried on the line cards is lost or dropped. To eliminate or reduce the potential for interrupted subscriber service, plan and coordinate this activity carefully.

- Step 1 From Cisco 6700 NetView, right-click the icon of the NE you are upgrading and select **Node Critical Commands** from the popup menu.
- Step 2 Enter the node critical commands password. The node critical commands window opens, displaying the database restore function. (See Figure 14-7 on page 14-10.) If necessary, contact your EMS administrator to obtain the correct node critical commands password.
- Step 3 Click **Line Card Reset** in the function bar to open the line card reset window. (See Figure 14-11.)

**Figure 14-11** Line Card Reset



- Step 4 From the **Equipped Cards** list, either select a line card to be reset, then in the **Reset** field, choose **Selected**, or, in the **Reset** field, choose **All**.
- Step 5 Click **Apply** to reset either the selected line card, or all line cards.
- Step 6 Repeat Step 4 and Step 5 for each card that you want to reset.

# Cisco 6705 Embedded Software Image Upgrade

The following section describes the MCC INT embedded software upgrade procedure for the Cisco 6705:

- Upgrading the MCC INT Embedded Software Image, page 14-15
- Resetting the MCC INT Card, page 14-16



Note

The Cisco 6705 has only one MCC card, identified as “MCC INT”.



Note

Reset procedures are also covered in the “Node Critical Commands” on page 14-23.



Caution

For a successful upgrade, follow all procedures, and all steps, in sequence.



Caution

If for any reason EMS is unable to complete the embedded software upgrade, *do not reset the MCC card*. You must restart the embedded software upgrade process. Resetting the MCC with a partial software image corrupts the MCC. If there is an error, an error message displays in the Software Upgrade Status field, or at the bottom of the NE provision window, as well as in the problem list of the MCC card (if the card is functional).

## Before You Begin

Before beginning the embedded software upgrade, complete the following tasks:



Caution

Be certain you are *not* upgrading to embedded software Version 1.4. Embedded software Version 1.4 *only* operates with the Cisco IAD1101. Check with your system administrator, if necessary.

- Contact your network administrator to ensure that the EMS password files are properly installed. You cannot complete the software upgrade procedure without the password files and corresponding password.
- For a local upgrade, use a crossover Ethernet cable to connect the EMS workstation to the Ethernet management port on the main common control (MCC) module. Alternately, you can use straight Ethernet cables to connect the EMS workstation and Cisco 6705 to a local hub.
- For a remote upgrade, you must have a DS0-type inter node data link (INDL) between the local node and the remote node. Verify that INDLs to all remote nodes are working. A software upgrade cannot be done over an FDL INDL. For more information, see Chapter 8, “Inter Node Links.”
- Verify that a TFTP server is online and available to receive the database backup information. TFTP server verification can be confirmed by pinging the TFTP host (this confirms that the Cisco 6705 is properly routed to the TFTP host).

- Verify that the TFTP server contains the correct embedded software file, such as **SwLoad.iad**, in the TFTP directory.
- Back up the system database before starting the software upgrade. Before backing up the database, refer to the “Backing Up the System Database” on page 14-2, and the “Restoring a Database” on page 14-24.

**Note**

When upgrading multiple nodes in a network, always start from the far end of the network, one node at a time. In a typical network, a number of remote nodes (subscriber nodes) are connected to a central office terminal (COT) node. If the upgrade of COT is mishandled, the entire network can be lost. Upgrade tests and sample enhancements should be made at the edge node. If the upgrade tests fail on the edge nodes, do not attempt to upgrade the COT node.

## Upgrading the MCC INT Embedded Software Image

- Step 1** From Cisco 6700 NodeView of the Cisco 6705 that you intend to upgrade, double-click the node nameplate to launch the NE provision window. (See Figure 14-2 on page 14-3.)
- Step 2** Select **Software Upgrade** from the function bar to view the software upgrade window. (See Figure 14-12.)

*Figure 14-12 Cisco 6705 Software Upgrade Window*

NE Provision for 6705 node: 6705	
System Basic Provisioning	Software Image Host IP Address: 0 0 0 0
IP Address Configuration	Software Image File Name: <input type="text"/>
IP & Datalink Route Configuration	Target Card: No card selected <input type="text"/>
Ping Node	Software Upgrade Status: unknownState
Node ID Configuration	
IP & Inter Node Link Configuration	
IP RIP Configuration	
IP Network Address Translation (NAT)	
IP Access Lists	
Timing Source Selection & Control	
Timing Distribution Provisioning	
NE Time Of Day Set	
Alarm Provisioning	
Software Upgrade	
Database Backup	
Error Log Retrieval	
Exit	

Apply Upgrade Refresh

35483

- Step 3** In the **Software Image Host IP Address** field, enter the IP address of the TFTP server.
- Step 4** In the **Software Image File Name** field, enter **SwLoad.fbx**.
- Step 5** Click **Apply** to confirm the host IP address and path to the image filename.
- Step 6** Click **Upgrade** to download the embedded software image into the Flash memory of the MCC card. EMS displays a progress bar. (See Figure 14-6 on page 14-9.) Wait until the software upgrade is complete and the Software Upgrade Status field reads: “passed.”
- 

## Resetting the MCC INT Card

The MCC INT card must be reset before the new embedded software becomes active.



### Caution

Resetting the MCC INT card resets all line cards in the Cisco 6705, momentarily placing the line cards out of service. Any traffic carried on the line cards is lost or dropped. To eliminate or reduce the potential for interrupted subscriber service, plan and coordinate this activity carefully.

---



### Caution

Do not power down the NE or remove the MCC during an MCC reset. The MCC must finish loading the system software before the MCC can be safely powered down, removed, reset, or reprovisioned.

---



### Note

Performing an MCC reset erases the internal clock on the NE. To set the time of day on the NE, see “Setting the NE Clock” on page 4-14.

---

There are two ways to reset the MCC card: physically, or through the software.

## Physical Reset

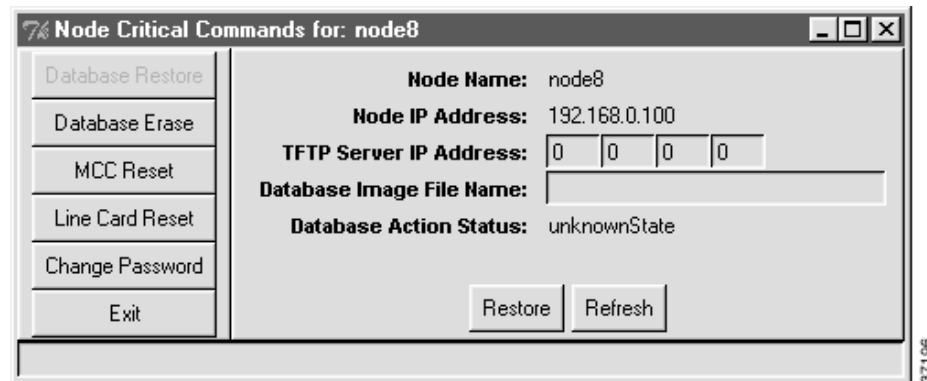
- Step 1** Physically unlock the MMC card by lifting the lever on the face of the card.
- Step 2** Gently slide the MCC card away from the NE chassis backplane.
- Step 3** Reinstall the MCC card by carefully sliding it forward until the lever touches the front of the chassis.
- Step 4** Secure the MCC card by pressing the lever down. See the *Cisco 6705 Hardware Installation Guide* for handling procedures. Allow at least 45 seconds for the MCC to reset and reload the system software.
-



## Software Reset

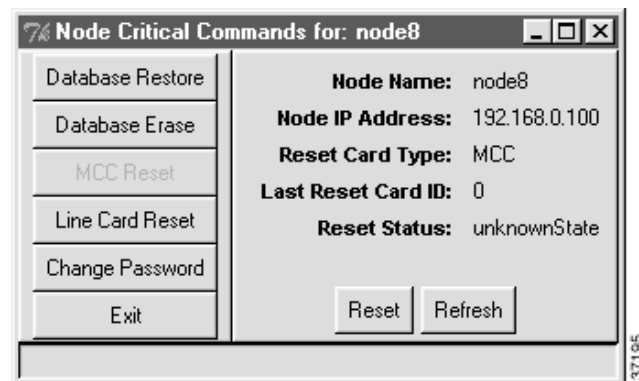
- Step 1** From the Cisco 6700 NetView, right-click the icon of the Cisco 6705 you are upgrading and select **Node Critical Commands**.
- Step 2** Enter the node critical commands password. The node critical commands window opens, displaying the database restore function. (See Figure 14-13.) If necessary, contact your EMS administrator to obtain the correct node critical commands password.

*Figure 14-13 Cisco 6705 and IAD1101 Node Critical Commands Window*



- Step 3** Click **MCC Reset** in the function bar to view the MCC Reset window. (See Figure 14-14.)

*Figure 14-14 Cisco 6705 and IAD1101 MCC Reset Window*



- Step 4** Click the **Reset** button and respond **Yes** to the prompt. Allow at least 45 seconds for the MCC to reset and reload the system software.
- Step 5** Click **Exit** in the function bar to return to Cisco 6700 NetView.

# Cisco IAD1101 Embedded Software Image Upgrade

The following section describes the software upgrade procedure for the Cisco IAD1101, and includes the following sections:

- Upgrading the Cisco IAD1101 Embedded Software Image, page 14-19
- Resetting the Internal MCC Card, page 14-21



## Note

The Cisco IAD1101 has an internal MCC card. The MCC card is always the target of the upgrade procedure.



## Caution

The software upgrade procedure requires a reset of the Cisco IAD1101 internal MCC card. This causes all lines and cards to reset, momentarily placing the lines out of service. Any traffic carried on the line cards is lost or dropped. To eliminate or reduce the potential for interrupted subscriber service, plan and coordinate this activity carefully.



## Caution

For a successful upgrade, follow all procedures, and all steps, in sequence.



## Caution

If for any reason EMS is unable to complete the embedded software upgrade, *do not reset the MCC card*. You must restart the embedded software upgrade process. Resetting the MCC with a partial software image corrupts the MCC. If there is an error, an error message displays in the Software Upgrade Status field, or at the bottom of the NE provision window, as well as in the problem list of the MCC card (if the card is functional).

## Before You Begin

Before beginning the embedded software upgrade, complete the following tasks:



## Caution

Be certain you are upgrading to embedded software Version 1.4. Check with your system administrator, if necessary.

- Contact your network administrator to ensure that the EMS password files are properly installed. You cannot complete the software upgrade procedure without the password files and corresponding password.
- For a local upgrade, use a crossover Ethernet cable to connect the EMS workstation to the Ethernet port on the Cisco IAD1101. Alternately, you can use straight Ethernet cables to connect the EMS workstation and Cisco IAD1101 to a local hub.
- For a remote upgrade, you must have a DS0-type inter node data link (INDL) between the local node and the remote node. Verify that INDLs to all remote nodes are working. A software upgrade cannot be done over an FDL INDL. For more information, see Chapter 8, “Inter Node Links.”
- Verify that a TFTP server is online and available to receive the database backup information. TFTP server verification can be confirmed by pinging the TFTP host (this confirms that the Cisco IAD1101 is properly routed to the TFTP host).

- Verify that the TFTP server contains the correct embedded software file, such as **SwLoad.iad**, in the TFTP directory.
- Back up the system database before starting the software upgrade. Before backing up the database, refer to the “Backing Up the System Database” on page 14-2, and the “Restoring a Database” on page 14-24.

**Note**

When upgrading multiple nodes in a network, always start from the far end of the network, one node at a time. In a typical network, a number of remote nodes (subscriber nodes) are connected to a central office terminal (COT) node. If the upgrade of COT is mishandled, the entire network can be lost. Upgrade tests and sample enhancements should be made at the edge node. If the upgrade tests fail on the edge nodes, do not attempt to upgrade the COT node.

## Upgrading the Cisco IAD1101 Embedded Software Image

- Step 1** From Cisco 6700 NodeView of the Cisco IAD1101 you intend to upgrade, double-click the node nameplate to launch the NE provision window. (See Figure 14-15.)

*Figure 14-15 Cisco IAD1101 NE Provision Window*

System Basic Provisioning	<b>NE Name:</b> IAD1101
IP Address Configuration	<b>Alias:</b>
IP & Datalink Route Configuration	<b>NE Location:</b> Central Office
Ping Node	<b>NE Node Type:</b> NetworkNode
Node ID Configuration	<b>NE Time Of Day:</b> 1970-01-03,15:06:16.0
IP & Inter Node Link Configuration	<b>NE Uptime:</b> 2d 23:06:16
IP RIP Configuration	<b>NE Backplane Version:</b> 1.255
IP Network Address Translation (NAT)	<b>NE Loaded Software Version:</b> 1.5.1.15
IP Access Lists	<b>NE SBMAF0DRA:</b> ██████████
Timing Source Selection & Control	<b>6513 Serial Number:</b> -1
Timing Distribution Provisioning	<b>NE Backplane Type:</b> Unknown
NE Time Of Day Set	<b>Alarm Status:</b> normal
Alarm Provisioning	<b>Problem List:</b>
Software Upgrade	
Database Backup	
Error Log Retrieval	
Exit	Apply Refresh

- Step 2** Select **Software Upgrade** from the function bar to view the software upgrade window.  
(See Figure 14-16.)

*Figure 14-16 Cisco IAD1101 Software Upgrade Window*

- Step 3** In the **Software Image Host IP Address** field, enter the IP address of the TFTP server.
- Step 4** In the **Software Image File Name** field, enter **SwLoad.iad**.
- Step 5** Set the **Target Card** field to **MCC**.
- Step 6** Click **Apply** to confirm the host IP address and path to the image filename.
- Step 7** Click **Upgrade** to download the embedded software image into the Flash memory of the MCC card. EMS displays a progress bar. (See Figure 14-6 on page 14-9.) Wait until the software upgrade is complete and the Software Upgrade Status field reads: “passed.”
- Step 8** Respond to the reboot prompt by dismissing it and resetting the internal MCC card (see “Resetting the Internal MCC Card” on page 14-21).

## Resetting the Internal MCC Card

**Caution**

The Cisco IAD1101 internal MCC card must be reset before the new embedded software becomes active. This momentarily places the lines out of service. Any traffic being carried on an installed line card is lost or dropped.

**Caution**

Do not power down the NE or remove the MCC during an MCC reset. The MCC must finish loading the system software before the MCC can be safely powered down, removed, reset, or reprovisioned.

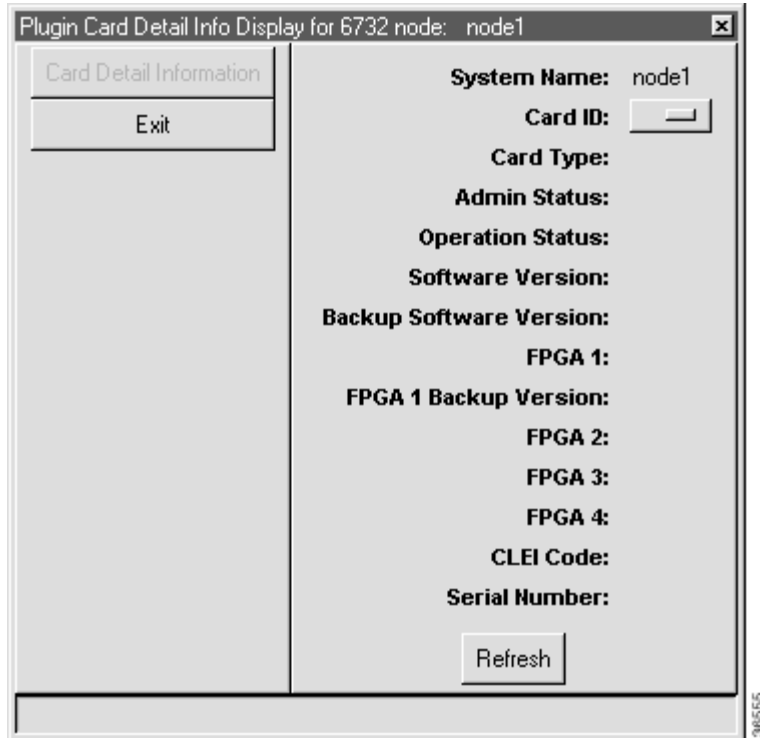
**Note**

Performing an MCC reset erases the internal clock on the NE. To set the time of day on the NE, see the “Provision NE Clock” section of Chapter 4, “Initial Node Provisioning.”

- 
- Step 1** From the Cisco 6700 NetView, right-click the icon of the Cisco IAD1101 you are upgrading and select **Node Critical Commands**.
  - Step 2** Enter the node critical commands password. The node critical commands window opens, displaying the database restore function. (See Figure 14-13 on page 14-17.) If necessary, contact your EMS administrator to obtain the correct node critical commands password.
  - Step 3** Select **MCC Reset** in the function bar on the left side of the window to open the MCC Reset window. (See Figure 14-14 on page 14-17.)
  - Step 4** Click the **Reset** button and respond **Yes** to the prompt. Allow at least 45 seconds for the MCC to reset and reload the system software.
  - Step 5** Click **Exit**.

- Step 6** From Cisco 6700 NodeView Objects menu, select **Plugin Card Details**. EMS displays the Plugin Card Detail Info Display window. (See Figure 14-17.)

*Figure 14-17 Plugin Card Detail Window*



- Step 7** In the Card ID field, select **MCC** and verify the software version number.

# Node Critical Commands

This section describes the embedded software utilities that are launched from the node critical commands window:

- Restoring a Database, page 14-24
- Erasing a Database, page 14-25
- Resetting the MCC card:
  - For the Cisco 6732, refer to page 14-9
  - For the Cisco 6705, refer to page 14-16
  - For the Cisco IAD1101, refer to page 14-21
- Resetting Line Cards, refer to page 14-13
- Changing a Password, page 14-28

**Caution**

---

These commands affect service; *any user traffic passing through the node will be dropped*. To eliminate or reduce the potential for interrupted subscriber service, plan and coordinate these activities carefully.

---

## Launching Node Critical Commands Utilities

To launch the node critical commands window, complete the following steps:

- 
- Step 1** From Cisco 6700 NetView, right-click a node icon and select **Node Critical Commands** from the drop-down menu.
- Step 2** Enter the node critical commands password. The node critical commands window opens, displaying the database restore function.
- 

**Note**

---

Your EMS workstation requires a special password file to launch the node critical commands window. If EMS cannot locate the password file, you cannot launch the node critical commands window. Contact your EMS administrator to obtain the password file.

---

## Restoring a Database

Use the database restore function to restore a backedup database to an MCC on the Cisco 6732, Cisco 6705, or Cisco IAD1101. See the “Backing Up the System Database” on page 14-2 for the database backup procedure.

### Cisco 6732 Database Restoration

- 
- Step 1** From Cisco 6700 NetView, right-click a node icon and select **Node Critical Commands** from the drop-down menu.
- Step 2** Enter the node critical commands password. The node critical commands window opens, displaying the database restore function. See Figure 14-18.)

*Figure 14-18 Cisco 6732 Database Restore Window*

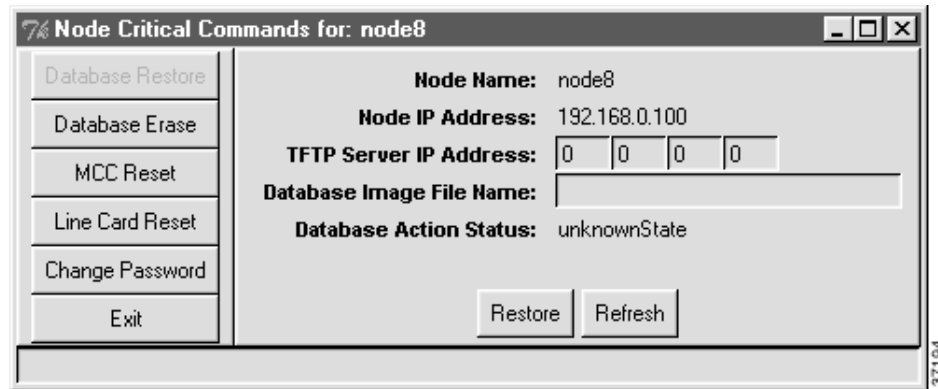
- Step 3** Complete the following fields:
- **TFTP Server IP Address**—Enter the IP address of the TFTP server that contains the database backup file. For the default, leave all zeros.
  - **Database Image File Name**—Enter the file name of the database backup file on the TFTP server.
  - **Database on Main Common Control Card**—Select the MCC to be restored (**A** or **B**). The active MCC is indicated in the **Active Main Common Control Card** field.
- Step 4** Click **Restore** to upload the database file from the TFTP server to the selected MCC.
-



## Cisco 6705 and Cisco IAD1101 Database Restoration

- Step 1** From Cisco 6700 NetView, right-click a node icon and select **Node Critical Commands** from the drop-down menu.
- Step 2** Enter the node critical commands password. The node critical commands window opens, displaying the database restore function. (See Figure 14-19.)

*Figure 14-19 Cisco 6705 and Cisco IAD1101 Database Restore Window*



- Step 3** Complete the following fields:
- **TFTP Server IP Address**—Enter the IP address of the TFTP server that contains the database backup file. For the default, leave all zeros.
  - **Database Image File Name**—Enter the file name of the database backup file on the TFTP server.
- Step 4** Click **Restore** to upload the database file from the TFTP server to the selected MCC.

## Erasing a Database



### Caution

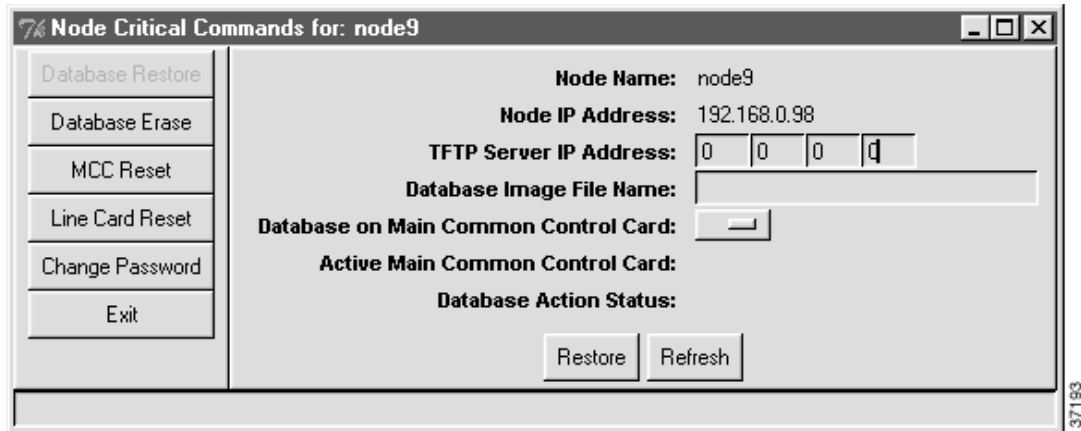
Erasing the database removes all card and line provisioning, including cross connects and inter node connections.

## Cisco 6732

- Step 1** Launch the node critical commands window. (See “Launching Node Critical Commands Utilities” on page 14-23.)

**Step 2** Click **Database Erase** in the function bar to open the database erase window. (See Figure 14-20.)

*Figure 14-20 Cisco 6732 Database Erase Window*



**Step 3** Select the MCC to be erased in the **Database on Main Common Control Card** field.

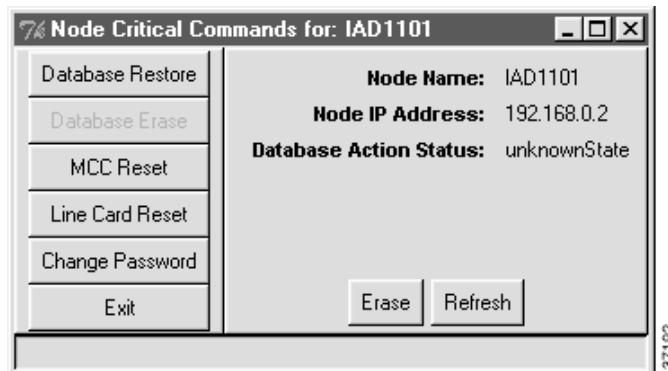
**Step 4** Click **Erase**.

## Cisco 6705 and Cisco IAD1101

**Step 1** Launch the node critical commands window. (See “Launching Node Critical Commands Utilities” on page 14-23.)

**Step 2** Click **Database Erase** in the function bar to open the database erase window. (See Figure 14-21.)

*Figure 14-21 Cisco 6705 and Cisco IAD1101 Database Erase Window*



**Step 3** Click **Erase**.

## Resetting the MCC Card

The MCC reset function resets the main control card (MCC) and reloads the embedded software.

**Caution**

---

Resetting the MCC causes all lines and cards in the NE to be reset as well, momentarily placing the line cards out of service. Any traffic being carried on the line cards is lost or dropped. To eliminate or reduce the potential for interrupted subscriber service, plan and coordinate this activity carefully.

---

**Caution**

---

Do not power down the NE or remove the MCC during an MCC reset. The MCC must finish loading the system software before the MCC can be safely powered down, removed, reset, or reprovisioned.

---

### Cisco 6732 MCC

Refer to “Resetting the Standby MCC Card” on page 14-9.

### Cisco 6705 MCC INT

Refer to “Resetting the MCC INT Card” on page 14-16.

### Cisco IAD1101 Internal MCC

Refer to “Resetting the Internal MCC Card” on page 14-21.

**Note**

---

Performing an MCC reset erases the internal clock on the NE. To set the time of day on the NE, see the “Provision NE Clock” section of Chapter 4, “Initial Node Provisioning.”

---

## Resetting Line Cards

The line card reset function resets all selected cards in the NE.

**Caution**

---

The line card reset procedure reboots the selected line cards and effectively takes them out of service. Any traffic carried on the line cards is lost or dropped. To eliminate or reduce the potential for interrupted subscriber service, plan and coordinate this activity carefully.

---

To reset line cards in a Cisco 6700 series NE, refer to the “Resetting the Line Cards” on page 14-13.

## Changing a Password

You can use the change password function to change the node critical commands password. This password is used to launch the node critical commands window. (See Figure 14-22.)



**Note** The node critical commands password is not the password used to log in to EMS. To change the EMS login password for a particular user, see “Provisioning EMS User Security” on page 15-2.

- Step 1** Launch the node critical commands window. (See “Launching Node Critical Commands Utilities” on page 14-23.)
- Step 2** Click **Change Password** on the function bar to open the change password window. (See Figure 14-22.)

*Figure 14-22 Change Node Critical Commands Password*

- Step 3** Complete the following fields to change the node critical commands password:
- **Old Password**—Enter the old (existing) password.
  - **New Password**—Enter an alphanumeric string (of at least five characters in length). This string will replace the old password.
  - **Repeat New Password**—Retype the new password to confirm the password change.
- Step 4** Click **Save**.