CICM Fault Management

This document provides the fault management strategy and procedures for Centrex IP Client Manager (CICM) nodes (gateways) and their element managers (CICM-EMs). This document is part of the CICM customer documentation suite. The complete list of documents in the suite is identified in *CICM Basics*, NN0044-111.

The software releases that this document supports are indicated in the running footer of the document, for example, (I)SN08.

The topics of this document include:

What's new in fault management

The following changes have occurred for this version of the document:

- updated Architectural resilience to add the affects of ACF and SRG
- updated User interfaces for CICM with new interfaces
- updated Alarms for CICM with the behavior of LEDs in a SAM16 architecture
- updated the purpose of Card fault and recovery guidelines
- updated the section Card replacement to distinguish the SAM16 from the SAM21 hardware platforms
- revised the procedure Copying files to or from a CICM-EM or its CICM nodes (formerly known as "Copy files from one machine to another")
- updated the procedure Querying the state of a service

- renamed the procedure “Powering up and down a node (hard reboot)” to Rebooting (hard) a SAM16 with CPV5370 cards to emphasize the purpose of the procedure
- added the procedure Rebooting (hard) a SAM21 with CPN5385 cards
- updated the procedure Rebooting (soft) the node to clarify command entries
- updated the procedure Restoring the CICM node registries
- added the procedure Retrieving logs from a CICM-EM or a CICM node
- updated both procedures in Starting a service running on a node
- updated the procedure Shutting down a CICM node and its supporting information in the sections CICM node failures and Network adapter failures
- updated the procedure Troubleshooting a CPU card in a SAM16
- added the procedure Troubleshooting a CPU card in a SAM21
- updated the procedure Verifying IP network connectivity to clarify command entries
- updated the procedure Viewing the list of back-up files and logs to clarify command entries
- moved service-affecting or potentially service-affecting procedures from Fault management troubleshooting procedures for CICM into Fault management guidelines and correction procedures for CICM
- alphabetized the sequence of procedures in Fault management troubleshooting procedures for CICM and Fault management guidelines and correction procedures for CICM
- removed the obsolete procedure “View members of a group”
- removed the obsolete procedure “Use a remote machine”
- removed the obsolete procedure “View servers in a network”
- removed the obsolete procedure “View services running on a node”
- merged the procedure “View the details of a service” with Querying the state of a service
- removed the obsolete procedure “View the details of an error message”
- removed all steps asking to busy a VMG since one cannot be busied

Fault management strategy

The Centrex IP Client Manager (CICM) component accomplishes fault management by providing alarm surveillance, correlation and reporting, event log collection and reporting, troubleshooting procedures, and fault correction procedures.

Although the design of the CICM products is to minimize the customer service impact for any single point of failure, a set of specific failures may cause a degradation in the service provided.

Architectural resilience

The CICM nodes can be run on a SAM16 or SAM21 hardware platform. The CICM-EM nodes can be run on a CPX1204 or SAM21 hardware platform.

Each CICM node is partitioned into two identical independent physical nodes: Node A and Node B. The SAM21 hardware platform has a dual cPCI backplane.

The CPN5385 cards for the Nodes A and B of each CICM or CICM-EM must have been installed in different SAM21 chassis.

Towards the gateway controller (GWC), the two nodes present themselves as a single network entity with one CPU as the master and the other as a warm-standby slave. Similarly, the client sees one UNIStim IP interface which is assigned to the master CPU card. When a switchover between nodes occurs, stable calls are maintained. Calls being set up are dropped. Neither the client nor the gateway controller should see a loss of service.

When the optional Survivable Remote Gateway (SRG) feature is configured, CICM terminals (clients) that lose their connection to the CICM nodes will restart and connect to the SRG. The SRG acts a s a basic call server to route calls between terminals on the local network.

Refer to Alarms for CICM for the description of LED behaviors for SAM16 cards.

Software resilience

Only the core components of the operating system are used, for which reliability has been tested and proved definitively. No graphical user interface is provided, thus reducing the number and complexity of the components running on the system and therefore the likelihood of unexpected failure conditions.

Third party components (drivers and applications) were chosen with care and limited to those required to manage the resource cards and chassis. Both are strictly controlled and thoroughly tested in the OS configuration. This provides a highly stable platform for the CICM software.

In addition, the CICM software is programmed to constantly perform sanity checks on software operations for unexpected or rare conditions. Failures generate “informational,” “warning,” or “error” logs, which provide assistance in resolving any problem.

User interfaces for CICM

The basic user interfaces for CICM fault management are:

- a web-based CICM element manager (CICM-EM) interface
- a web-based interface through the integrated element manager system (IEMS)
- secure telnet (SSH)

Interfacing through the web-based CICM-EM

This interface uses a web browser to access the CICM-EM web pages. The web pages enable you to:

- monitor the status of the CICM nodes and CICM-EMs
- retrieve logs from the CICM nodes and the CICM-EMs
- change the software configuration

Refer to “Element Manager web pages procedures” in *CICM Security and Administration*, NN10252-611.

Interfacing through the IEMS

The IEMS enables access to the CICM-EM and CICM nodes web pages. IEMS also collects and stores the CICM traps and system logs where they can be monitored. (IEMS is the main interface to VoIP networks.)

The CICM nodes can send SNMP traps to the IEMS or a generic SNMP trap receiver. The IEMS uses SNMP traps to indicate alarm states. Typically there is an SNMP trap for every noteworthy alarm state, so CICM alarms are echoed at the IEMS.

Interfacing through an SSH

The SSH can be used to:

- check the overall status of the CICM-EM or CICM nodes
- start and stop the service on the CICM nodes
- power up and down the CICM-EM or CICM nodes
- verify the connection of a terminal on the client LAN
- participate in the rollback of an upgrade
- facilitate troubleshooting by Nortel support personnel
- do other troubleshooting activities

Alarms for CICM

CICM alarms indicate faults with the hardware or software operation of the CICM nodes or the CICM-EMs on either the SAM16 or SAM21 hardware platforms. The status of hardware is indicated by LEDs. The status of hardware and software activities is indicated by alarms that appear at a maintenance page of the web view.

There are CICM alarms reported to the CICM-EM for both the nodes and the EMs. There are also CICM system logs reported to the IEMS. The system logs have identifiers CICMnnn.

A fault can do one or more of the following:

- record a log in the CICM debug log
- record a log in the CICM event log
- send an SNMP trap
- raise an alarm with severity critical, major, or minor

All of the current active alarm states are viewable from the CICM-EM web page interface. The EMs report the alarm states that are stored on each CICM node.

The following sections relate only to a CICM hosted in a SAM16. (When run in a SAM21, the LEDs are controlled by the SAM21 Shelf Controller and the behavior is different.)

- Alarms overview of CICM software
- Domain control
- Telco alarm LEDs
- System Status LEDs
- Fan and chassis alarm monitoring

With the SAM16 platform, the A and B nodes are installed in different chassis. For example, CICM-001A and CICM002-B are in one chassis while CICM-001B and CICM002-A are in another. This means the alarm LEDs on one chassis might apply to either node. For example, when CICM-002B has a fault, an alarm is indicated on the web pages for CICM-002B and indicated by the LEDs on the chassis with CICM-001A.

Alarms overview of CICM hardware

Fault alarms are indicated on the physical CICM chassis through a series of lights (LEDs) on the front panel (the CICM alarm panel). This physical alarm panel is reproduced on the CICM-EM web pages as a virtual alarm panel for remote monitoring of alarms.

During runtime, the CICM alarm panel is directly updated from the software controlling each CompactPCI card. Any status changes which occur in the physical hardware state (for example, loss of a mate node) is reported as a fault alarm above the corresponding CompactPCI card.

This alarm panel displays an **active**, **maintenance**, and **fault** status. Once a card is initialized, the alarm panel displays an **active** status unless all activity on that card stops.

Domain control

Domain A controls the system and telco chassis LEDs. Only Domain A has the ability to access the alarm panel LED settings and to update both the chassis and system alarm status for both domains. Domain A, as the controlling domain, shows the state of both itself and Domain B. Domain B does not have the ability to update any system of chassis alarms on its own.

If Domain A is unable to determine the state of Domain B, it will make a pessimistic assumption and show a Domain B failure. In this case, the **Component out of Service** LED will be illuminated along with a **Major** Telecom alarm LED.

Since Domain A controls the alarm panel, when Domain A is down there are no alarms available on the chassis. However, the CICM-EM virtual alarm panel is still correctly updated.

The Fault, Active and Maintenance LEDs above each of the slots are controlled by the Hot Swap Controller and CPU card for the domain on which the slot lies.

Telco alarm LEDs

The telco alarm LEDs are used to signify faults on the CICM cards and components. Minor, major and critical alarms are consistent with CS2000 alarms, and are defined as:

- **Minor chassis alarm LED**

  A minor chassis alarm is an occurrence when one, but not both, domains are reporting a minor alarm.

- **Major chassis alarm LED**

  A major chassis alarm is defined as an occurrence when both domains are reporting a minor alarm, or one (but not both) domains are reporting a major alarm.

- **Critical chassis alarm LED**

  A critical chassis alarm is defined as an occurrence when a critical alarm is raised on either or both domains, or when both domains are reporting a major alarm.

System Status LEDs

The System Status LEDs signify:

- **System Out of Service LED**

  One or more critical alarms have been reported.

- **Component Out of Service LED**

  One or more minor or major chassis alarms have been reported.

- **System In Service LED**

  No alarms are raised on the CICM.

Fan and chassis alarm monitoring

In SN08, the chassis control software dynamically controls fan speed. Chassis status, including card status, fan speed, and CPU temperature, is shown on the CICM Element Manager status web pages.

For fan replacement in the CICM chassis, refer to the Motorola documentation and procedures on *www.motorola.com/computer*.

For the CICM-EM chassis, refer to the *CPX1200SA/IH1 CompactPCI CPX1200 Series System Installation and Reference Guide*.

For the CICM node (gateway) chassis, refer to the *CPX8216A/IH4 CPX8000 Series CPX8216 and CPX8216T CompactPCI System Installation and Use*.

The table Fan speed settings provides different chassis error conditions.

Table 1 Fan speed settings

Chassis Condition	Fan Speed
Normal	LOW
Loss of any fans	HIGH
CPU temperature exceeds 50 degrees Celsius	HIGH
General Cooling System fault	HIGH

Fault management troubleshooting procedures for CICM

This section contains general procedures for troubleshooting. The procedures are arranged in alphabetical order for easy reference.

Backup and restore procedures

The backup and restore procedures included in this section are:

- “Backing up the CICM nodes” in *Upgrading CICM*, NN10230-461
- “Backing up the CICM-EM nodes” in *Upgrading CICM*, NN10230-461
- Viewing the list of back-up files and logs
- Restoring the CICM node registries from manually or automatically backed up files

Copying files to or from a CICM-EM or its CICM nodes

Copy files to a CICM-EM from:

- a CICM node
- another CICM-EM
- another computer on the same network

For example, copy the autogenerated daily backup files before they get over-written by the system.

The files are copied to or from this PC home directory on either the master or the slave CICM-EM:

D:\CentrexIP\support

You must use a secured FTP session to copy files from a CICM-EM (but not from a CICM node to its EM).

You must have a working knowledge of UNIX.

At a PC on the administration LAN

1 Telnet to the CICM node that contains the files to be copied. Refer to the *Telnet to a CICM node* procedure.

At the command line interface

2 Enter the path of directories to get to the files to be copied by entering:

cd /<directory_name>/<directory_name>

Example
cd /debuglog

3 Start an FTP session to the CICM-EM that is to receive copies of the files. Refer to the *Telnet to a CICM node* procedure.

4 Go to the directory on the CICM-EM where the EM upgrade files are to be copied:

cd /centrexip/support

5 When the files are executable files or are in binary format (for example, the UNIStim or H.248 log files), enter:

bin

Otherwise skip this step.

6 While at the CICM-EM through the FTP session, enter:

put <file_name> /<file_name>/

where

file_name
is the name of a file to be copied. More than one file can be copied at a time using the syntax shown. Using “*.log” gets all file file names ending in “.log”.

Example
get *.log //47.160.43.10/support

The recommended location for event logs and related information is the folder named *support* on the root directory of the FTP server on the CICM-EM. This makes the files make readily accessible by GNPS or Nortel support.

7 Confirm all copied files are present:

ls -al

8 This procedure is complete.

Querying a registry key

Query a particular key in the Windows registry of CICM static data.

At a PC on the administration LAN

1 Telnet to the CICM node.

At the command line interface

2 Enter the command:

reg query <registry><path>

Example
reg query “hklm\software\nortel networks\centrexip international gateway\8.10”

Note: Using the option **/s** allows all subkeys to be displayed.

Example
reg query “hklm\software\nortel networks\centrexip international gateway\8.10” /s

Information about the registry key is displayed.

3 This procedure is complete.

Querying the state of a service

Query the state of a service on a CICM node, for example, to determine the dependencies a service needs to start or to confirm if a CICM node is running when the CICM-EMs are unavailable.

At a PC on the administration LAN

1 Telnet to the CICM node. Refer to the *Telnet to a CICM node* procedure.

At the command line interface

2 Enter the command:

sc query <service_name>

or

sc qc <service_name>

where

service_name
is the name of the service to start.

Example
sc query cxip09

The details of the state of the service is displayed. When STATE indicates STOPPED, there is no service running on that CICM-EM or CICM node. When STATE indicates RUNNING, there is service on the CICM node

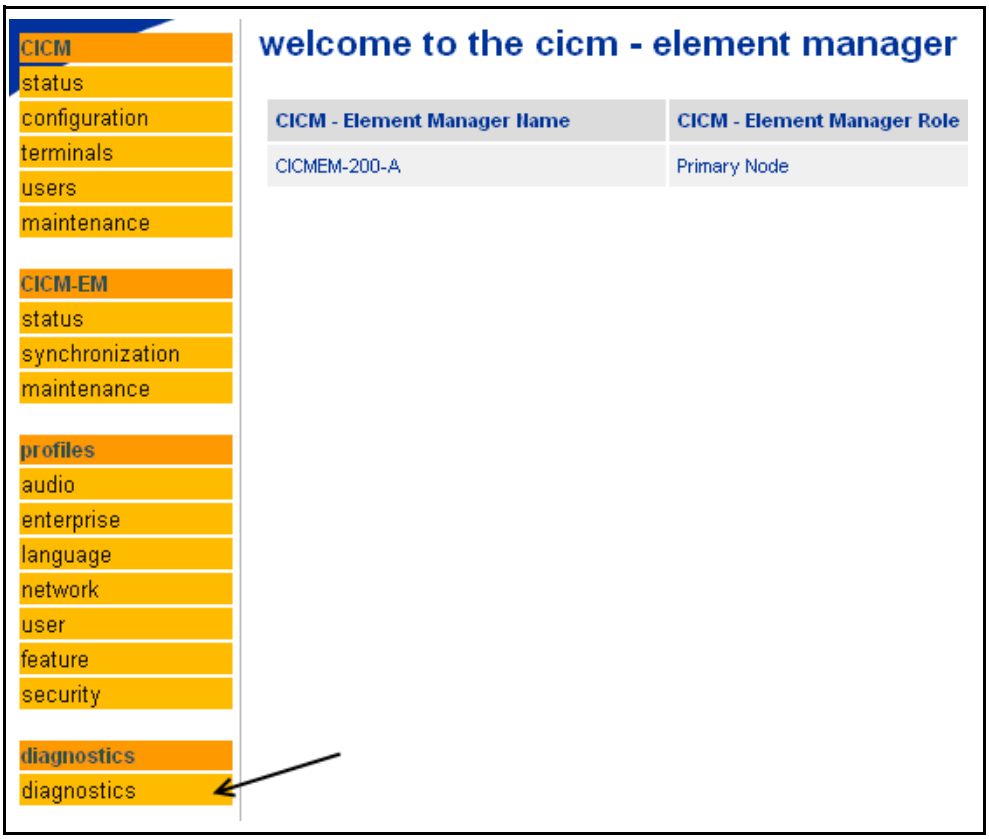
3 This procedure is complete.

Retrieving logs from a CICM-EM or a CICM node

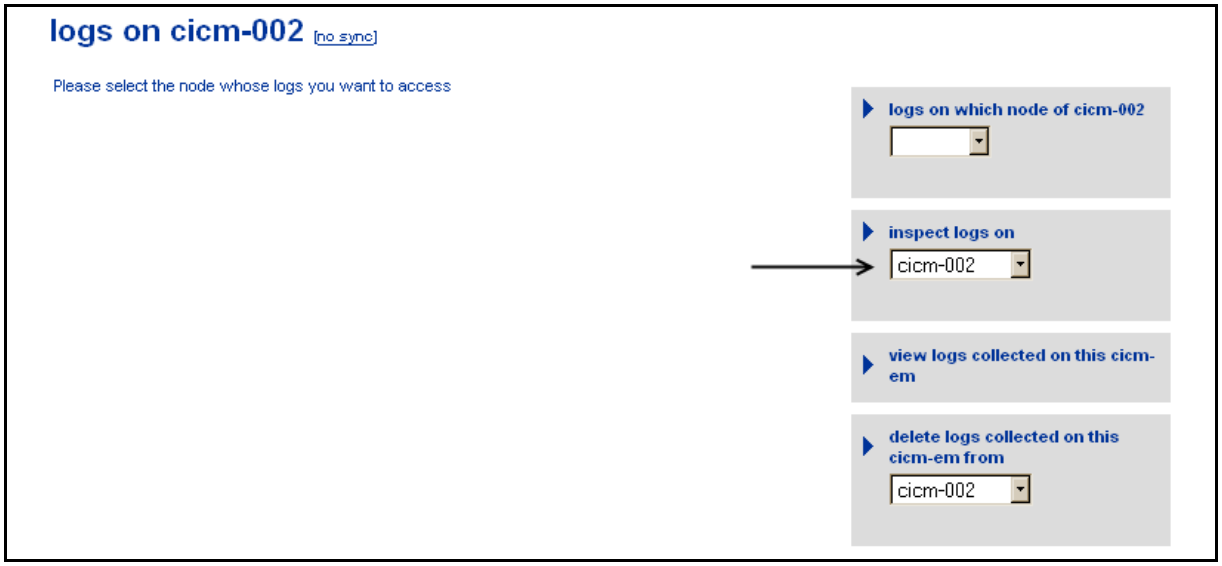
Retrieve CICM logs from a CICM-EM or a CICM node to assist troubleshooting faults.

At the home page of the CICM-EM

1 Click on **diagnostics** in the left menu.



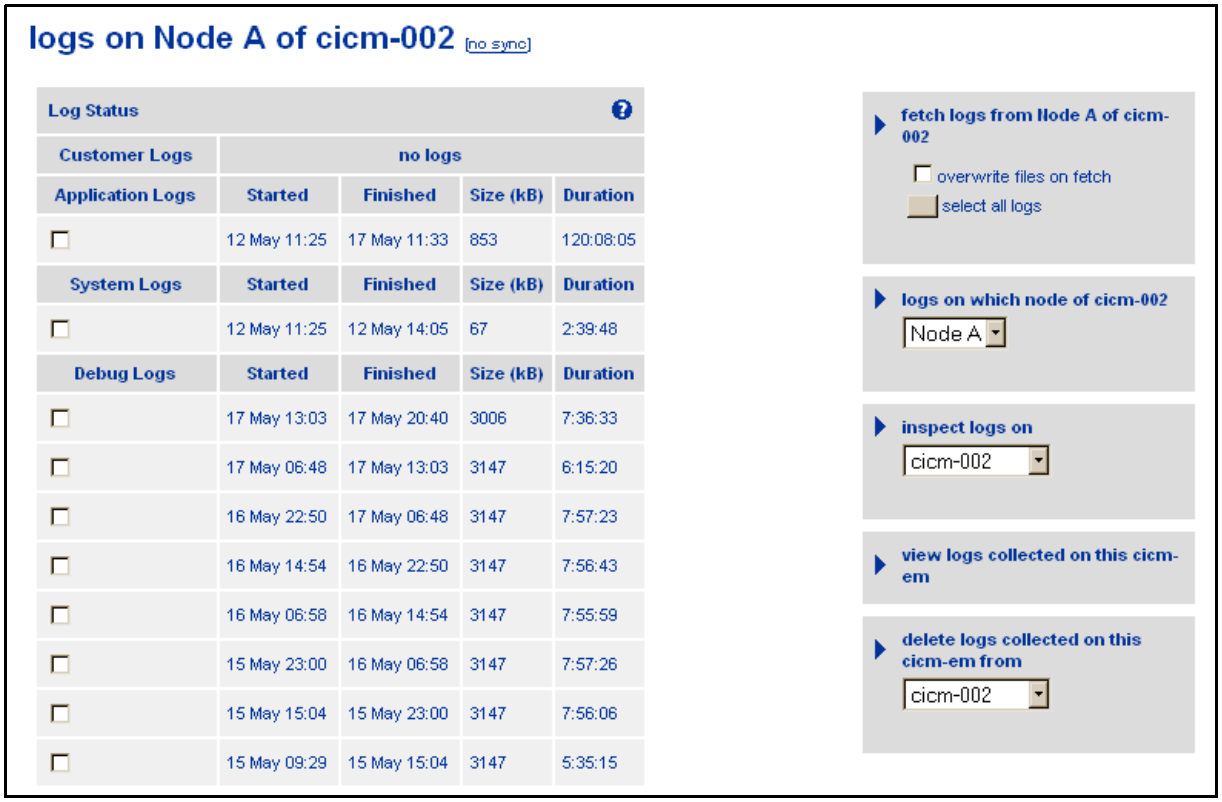
2 Select the CICM node identifier from the drop-down menu under **inspect logs on**.



3 Click on **inspect logs on**.

4 Select the CICM node A or B from the drop-down menu under **on which node of cicm-nnn**.

A clock indicates time lapse until the display of logs appears.

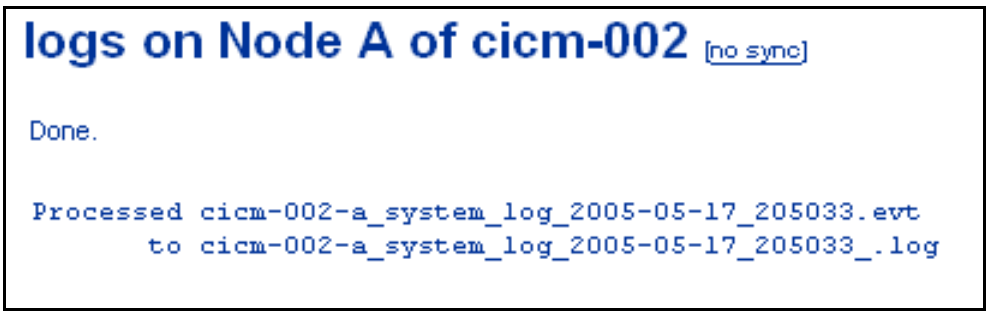


5 Click on each box of the logs you wish to have collected.

6 Click on the box *overwrite files on fetch* to get updated the contents of logs that are already collected.

7 Click on **fetch logs from node A/B cicm-nnn**.

A clock indicates time lapse until the list of logs appears.



8 This procedure is complete.

Tracing a route

Display the route taken from your computer to the computer you want to connect to. If there are any routers between you and the destination computer, they will reply as a hop.

At a PC on the administration LAN

1 Telnet to the CICM node. Refer to the *Telnet to a CICM node* procedure.

At the command line interface

2 Enter the command:
tracert <IP_address>

where

IP_address
is the IP address of the computer to route the connection to.

Example
tracert 47.160.168.173

Response: Verification of the route tracing is displayed, with the number of hops and their IP addresses.

```
Tracing route to REM3A [47.160.168.173
over a maximum of 30 hops:

1 <10ms 10ms <10ms tmdhrd07.europe.nortel.com
[47.160.42.1]
2 <10ms 10ms <10ms tmdhrd07.europe.nortel.com
[47.160.249.33]
3 <10ms 10ms <10ms tmdhrd07.europe.nortel.com
[47.160.168.173]

Trace complete.
```

3 This procedure is complete.

Troubleshooting a CPU card in a SAM16

Troubleshoot the faults of a CPV5370 CPU card in a SAM16 chassis when the CICM-EM cannot indicate the status of itself or its CICM nodes. For example, troubleshoot when:

- a CICM-EM reports an unreachable mate
- a CICM-EM reports the web page cannot be loaded
- the service on a CICM node is unavailable

At CPU node

1 Verify the LAN connectivity to the CICM.

If LAN connectivity is not the cause of the fault, continue.

2 Connect a PC monitor and keyboard to the faulty CPU card. Use either front or rear connectors.

3 If the card has failed to access the hard disk, it is likely that the BIOS has issued an error on the screen. This may require replacement of the CPU card or the hard disk. The node associated with the failure will be out of service until the faulty unit is replaced.

4 If the screen shows a complete blank, the node may be powered down or the CPU card may have suffered a hardware failure.

a First, Telnet to the mate node and attempt a powerup command as described in the procedure Rebooting (hard) a SAM16 with CPV5370 cards.

b If the powerup command does not restart the card, replace the CPU card. Refer to the procedure Card replacement.

5 If the screen is blue and has typical NT crash information displayed, do the procedure Rebooting (hard) a SAM16 with CPV5370 cards to check if the same thing happens on reboot.

6 If the screen is grey with Windows login information displayed, the OS has booted successfully.

a If you have just re-imaged the SAM16 card, verify that the install IP address is not active by pinging 10.28.5.69. If you can ping this address, Telnet to it and complete the software configuration procedures as described in the *Configuration Management* section of this document.

7 This procedure is complete. If this does not resolve the problem with the card, see Card fault and recovery guidelines.

Troubleshooting a CPU card in a SAM21

Troubleshoot the faults of a CPN5385 CPU card in a SAM21 chassis when the CICM-EM cannot indicate the status of itself or its CICM nodes. For example, troubleshoot when:

- a CICM-EM reports an unreachable mate
- a CICM-EM reports the web page cannot be loaded
- the service on a CICM node is unavailable

At CPU node

1 Verify the LAN connectivity to the CICM.

If LAN connectivity is not the cause of the fault, continue.

2 Connect a PC monitor and keyboard to the faulty CPU card. Use either front or rear connectors.

3 If the card has failed to access the hard disk, it is likely that the BIOS has issued an error on the screen. This may require replacement of the CPU card or the hard disk. The node associated with the failure will be out of service until the faulty unit is replaced.

4 If the screen shows a complete blank, reboot the card as described in the procedure Rebooting (hard) a SAM21 with CPN5385 cards and return to this step.

5 If the screen is blue and has typical NT crash information displayed, do the following:

a Do the procedure Rebooting (hard) a SAM21 with CPN5385 cards to check if the same thing happens on reboot.

b If the display is the same blue with Windows crash information, it may be an indication of a corrupt hard disk or a CPU hardware fault.

c Attempt to re-image the node (reinstall the software). If the crash repeats, it is likely that a disk or CPU replacement is required.

6 If the screen is grey with Windows login information displayed, the OS has booted successfully.

a If you have just re-imaged the SAM21 card, telnet to the administration IP address and complete the software configuration procedures as described in the *Configuration Management* section of this document.

b Verify the LAN connectivity to the CICM node by pinging the admin, UNIStim, and H.248 IP addresses as described in the procedure Verifying IP network connectivity. If there is no

response, visually inspect the cabling at the SAM21 and verify the configuration of the switch or router ports connected to the CICM card.

c If there is no response to any of the expected IP addresses, a CPU card hardware failure could be indicated.

7 This procedure is complete. If this does not resolve the problem with the card, see Card fault and recovery guidelines.

Verifying IP network connectivity

Verify the connectivity between a CICM node and a particular IP address or node name in the network.

The commands **ping** and **tracert** are the only ones that are installed on a CICM node.

At a PC on the administration LAN

1 Telnet to the CICM node. Refer to the *Telnet to a CICM node* procedure.

At the command line interface

2 Enter the command:
ping <IP_address or node_name>

where

IP_address
is the IP address of the node to check connectivity to.

Example
ping 47.160.168.173

node_name
is the name of the CICM node to check connectivity to.

Example
ping cxip170b

Response: Verification of ping reply is displayed if connection is active.

3 To see the connection over a longer period of time, add **-t** to the end of the command. This will permanently ping until you enter **Crtl+c** to stop.

Example
ping 47.165.168.173 -t

4 If you know the IP address of the node you want to ping, but need to know the name, add **-a** before the address.

Example
ping -a 47.165.168.173

Response: Verification of ping and reply includes the node name.

5 This procedure is complete.

Viewing the list of back-up files and logs

View the list of back-up files and event logs that have been created manually or automatically for a CICM-EM or CICM node.

Refer to the procedure Copying files to or from a CICM-EM or its CICM nodes move files on or off a CICM-EM.

At the CICM-EM

1 The back-up files that were backed up automatically or manually can be viewed on the CICM-EM in the directory path **D:\CentrexIP\support\backups**

2 The back-up file is called *backupconfig_<day_number>.xml* from the CICM-EM folder called **D:\CentrexIP\support\backups\<cicm_node>**

When a back-up file is created on a subsequent day that is the same number of the month, the backup file automatically overwrites the previous file. For example, when the third day of a month occurs again, that day's backup overwrites the file taken on the previous third of the month.

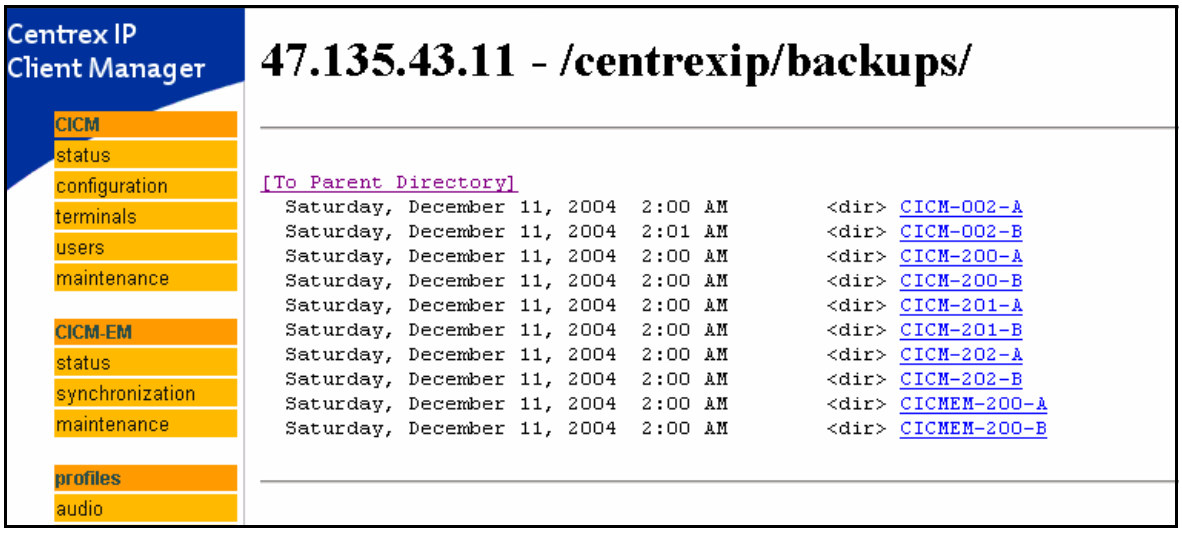
3 To view a list of the execution time of backups and the results of the backups, do:

a From the **CICM-element manager** home page, select **status** from the **CICM** menu to open the **CICM home** page.

b On the **CICM home** (CICM page, select the CICM from the drop-down menu in the **show the backup sets available for** menu option on the right,

c then click on **show the backup sets available for** text

*Response: The **<cicm_name> backup sets on <cicm-em_name>** page opens and displays the backup sets and backup results.*



4 This procedure is complete.

Viewing CS2000 logs

Use this procedure to view CS2000 (CS2K) logs using the command LOGUTIL. Logs associated with the CICM nodes are identical to the logs that the CS2000 normally generates for the DMS peripheral modules (PMs) called remote line concentrating modules (RLCMs) or international RLCMs (IRLCMs).

At the command interface (CI)

1 Enter the command **LOGUTIL**

2 Enter the command **open PM** to view the last Peripheral Module (PM) log generated.

or

enter the command **open PM <log number>** to view a specific PM log.

Response: Logutil output will display the latest log created.

3 To view earlier logs, enter the command **back n**

where

n
is the number of earlier logs to view.

4 This procedure is complete.

Viewing executables running on a node

View a list of tasks, services, or executables running on a CICM node, especially to determine when a service or executable has stopped. Use either procedure:

- Viewing executables running on a node by the command pulist
- Viewing executables running on a node by the command tlist

The command **pulist** also includes the username that the executable runs with.

Viewing executables running on a node by the command pulist

View the list of executables running on a CICM node by using the command **pulist**.

At a PC on the administration LAN

1 Telnet to the CICM node. Refer to the *Telnet to a CICM node* procedure.

At the command line interface

2 List all of the executables and their associated username for the CICM node by entering:

pulist

The list of executables running on the node is displayed with the usernames.

3 List information about one executable by entering:

pulist <exec>.exe

where:

exec
is the file name of the executable.

.exe
is the file extension indicating it is an executable. Not all executable files will have this extension.

The information about the executable running on the node is displayed.

Example
pulist gw.exe

4 This procedure is complete.

Viewing executables running on a node by the command tlist
View the list of executables running on a CICM node by using the command **pulist**.

At a PC on the administration LAN

1 Telnet to the CICM node. Refer to the *Telnet to a CICM node* procedure.

At the command line interface

2 List all executables on a CICM node by entering:

tlist

The list of all executables running on the node is displayed.

3 List information about one executable on a CICM node by entering:

tlist <exec>.exe

where:

exec
is the file name of the executable.

.exe
is the file extension indicating it is an executable. Not all executable files will have this extension.

The information about the executable running on the node is displayed.

Example
tlist gw.exe

4 This procedure is complete.

Viewing the IP configuration of all adapters on a CICM node

View the IP configuration of all adapters on a CICM node. Either procedure will display the two public administration addresses, the private administration address, and the client address:

- Viewing the IP configuration of adapters from the CICM-EM
- Viewing the IP configuration of adapters using command ipconfig

Viewing the IP configuration of adapters from the CICM-EM

View the IP configuration from the CICM-EM interface.

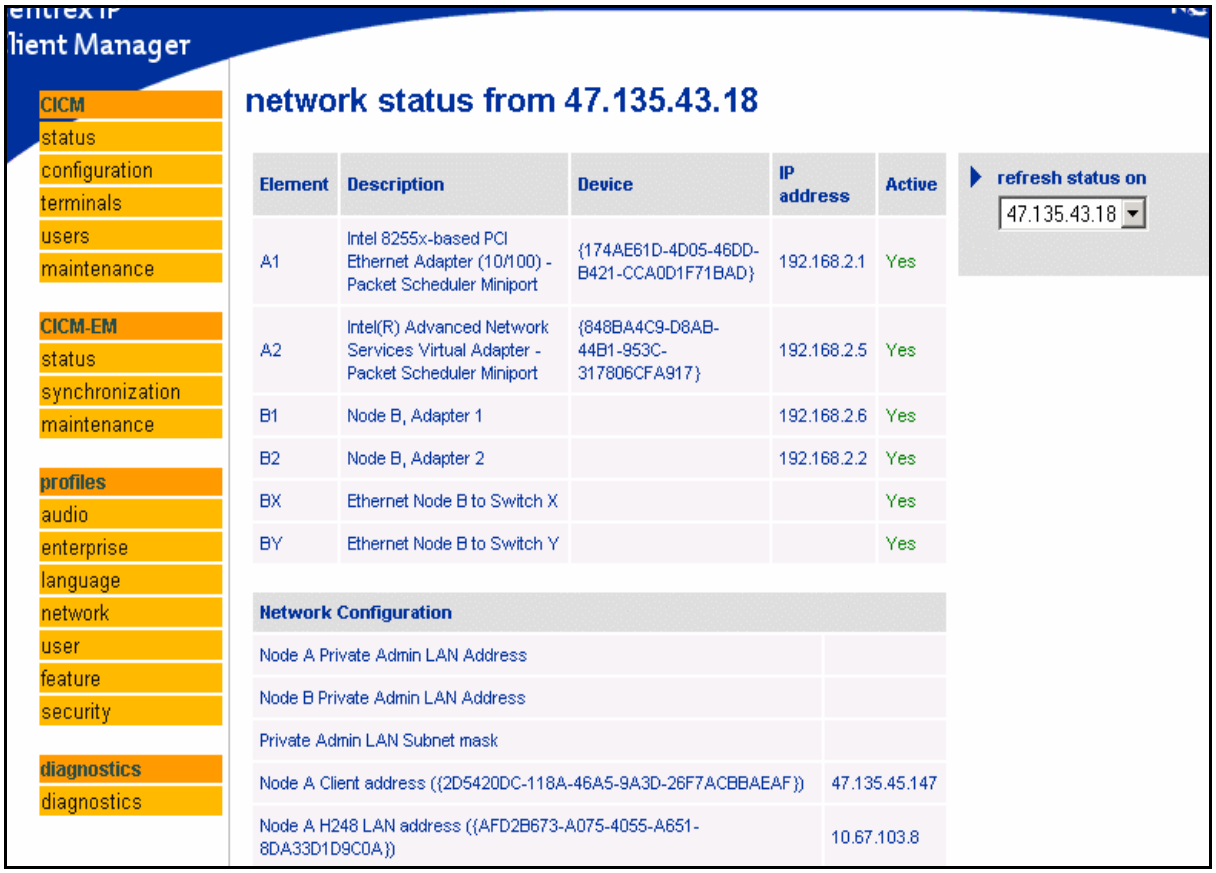
At the CICM Home web page

1 Select **diagnostics** from the left menu.

*Response: The **diagnostics home** page opens.*

2 From **network status check on a CICM** on the right menu, select the CICM from the drop-down menu, then click on **network status check on a CICM**.

*Response: The **network status from <IPaddress>** page opens and displays the IP addresses for the configuration.*



3 This procedure is complete.

Viewing the IP configuration of adapters using command ipconfig

View the IP configuration by using the command **ipconfig** from a personal computer (PC) connected to the CICM-EM through a telnet session.

At a PC on the administration LAN

1 Telnet to the CICM node. Refer to the *Telnet to a CICM node* procedure.

2 At the command line interface (CLI), enter **ipconfig /all**

Response: The IP configuration for all adapters on the node is displayed.

3 This procedure is complete.

Viewing the network configuration

View the network configuration of a user's workstation by using the command **net**.

At a PC on the administration LAN

1 Telnet to the CICM node you want to view. Refer to the *Telnet to a CICM node* procedure.

At the command line interface

2 Enter the command **net config workstation**

Response: The network configuration information for the workstation displays.

3 This procedure is complete.

Fault management guidelines and correction procedures for CICM

This section contains general procedures for troubleshooting. The procedures are arranged in alphabetical order for easy reference.

- Card fault and recovery guidelines
- Card replacement
  - Card replacement in a SAM16 or a SAM21
  - Checking the BIOS of a new CPU card
  - Replacing a hot swap IDE hard disk drive module
  - Replacing a non-hot swap CDROM/DVD drive module
- Correcting a node that is not connected
- Correcting a node that is stopped
- Correcting a VMG out-of-service fault
- Rebooting (hard) a SAM16 with CPV5370 cards
- Rebooting (hard) a SAM21 with CPN5385 cards
- Rebooting (soft) the node
- Restoring the CICM node registries
- Shutting down a CICM node
- Starting a service running on a node
- Stopping a service running on a node

Card fault and recovery guidelines

Use the information in the table Card fault and recovery guidelines to determine your actions when the procedures Troubleshooting a CPU card in a SAM16 or Troubleshooting a CPU card in a SAM21 do not resolve your problem.

Nortel support personnel may ask you to gather the information in the table Card fault and recovery guidelines. This helps to identify the source of a failure. Y

Prior to attempting any fault recovery, use the “Viewing...” procedures in the *CICM Security and Administration*, NN10252-611 document to retrieve the event and debug logs from both nodes of the CICM.

The table Card fault and recovery guidelines lists the effects of a specific card failure and the relevant recovery process to apply.

Card replacement

Replacing a faulty card from the CICM chassis with minimal service interruption applies to these cards:

- for SAM21 (CPN5385):
  - a CPU card
  - a transition module (TM)
- for SAM16 (CPV5370), a hot swap card (HSC)

The product engineering codes (PECs) of the cards that can be replaced are in the table PECs to identify SAM16 cards (blades).

When a CICM service is interrupted due to a hardware failure, the faulty card component of the gateway needs to be replaced.

Note: Testing a faulty card is to be done only by Nortel support.

Before starting to replace a card, the faulty card should already be identified and a replacement card ordered and received. For a SAM21, a TM card must also be ordered and received with each replaced CPU card. Note the slot number of the faulty card and ensure that the replacement has the same product engineering code (PEC) as the card being replaced.

When replacing a card from a SAM21 (CPN5385) hardware platform, refer to *SAM21 Shelf Controller Fault Management*, NN10089-911.

When replacing a card, refer to Card replacement in a SAM16 or a SAM21.

Card replacement in a SAM16 or a SAM21

The table PECs to identify SAM16 cards (blades) identifies the replacement hardware.

For each replaced CPU card, also replace its transition module (TM). The CPU card and TM can be ordered separately.

For additional information about the CPX8216T CompactPCI system installation, components and troubleshooting, refer to the *CPX8000 Series CPX8216 and CPX8216T Compact PCI System Installation and Use* document available on the Motorola website: http://www.motorola.com/

Replacing a CPU, TM, or HSC in a SAM16 or a SAM21

Replace the CPU, TM, or HSC in a SAM16 or SAM21 chassis to return it to service or to upgrade the hardware.

WARNING
Risk of equipment damage or voided warrantee
This procedure only describes how to replace a CICM hardware component. Do not attempt to open or dissemble any CICM hardware. Failure to comply with this requirement may damage the hardware and void the warranty.

WARNING
Risk of equipment damage
Do not attempt to insert any hardware card that is not included in the original design of the CICM. Extra cards may confuse the system and degrade the CICM service, or damage the system.

WARNING
Risk of damage by electrostatic discharge (ESD)
Wear an electrostatic discharge (ESD) grounding wristband connected to the CICM cabinet at all times during this procedure to protect the hardware from damage caused by static electricity.

At the CICM-EM web pages

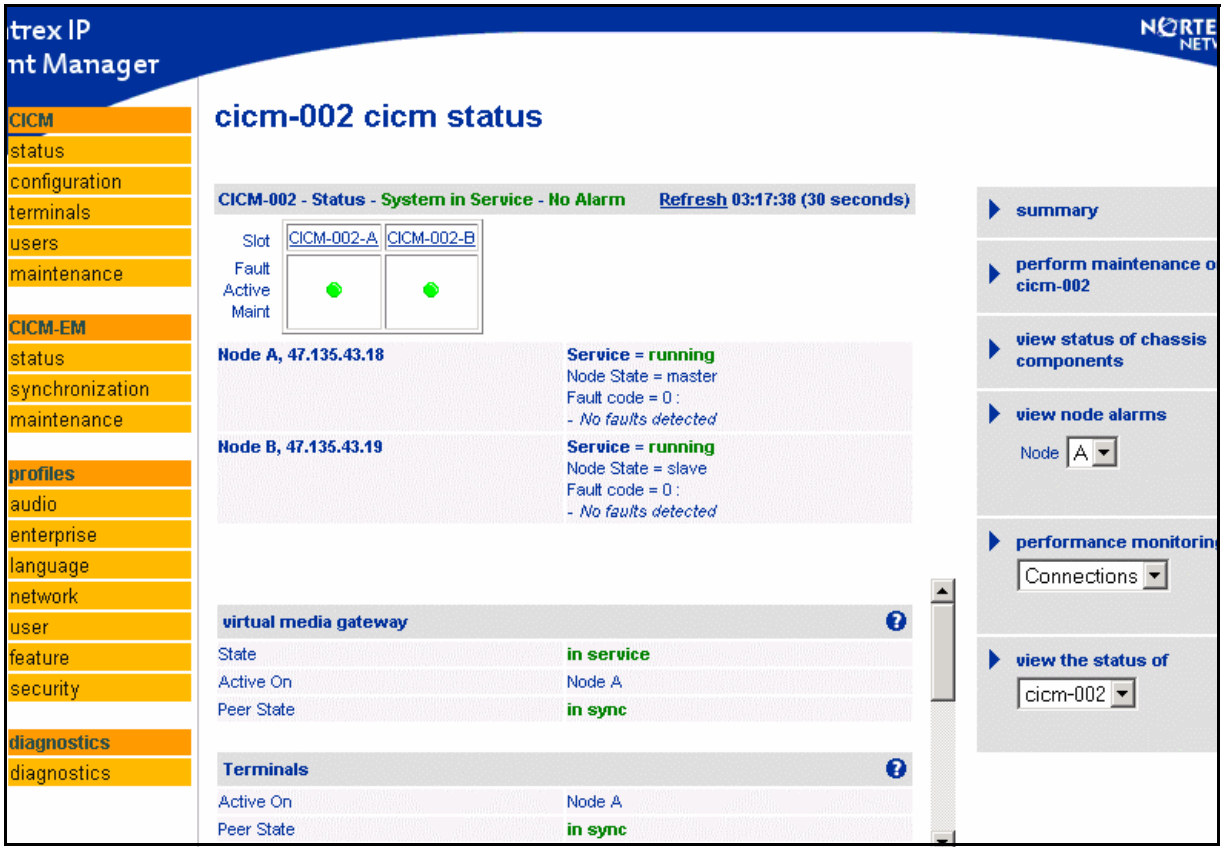
1 When the card to be replaced is the master, do a switch of activity to make it the slave card.

Terminal transfers are automatically handled.

2 Stop the CICM service on the node to be powered down (that is, the node containing the card to be replaced), as follows:

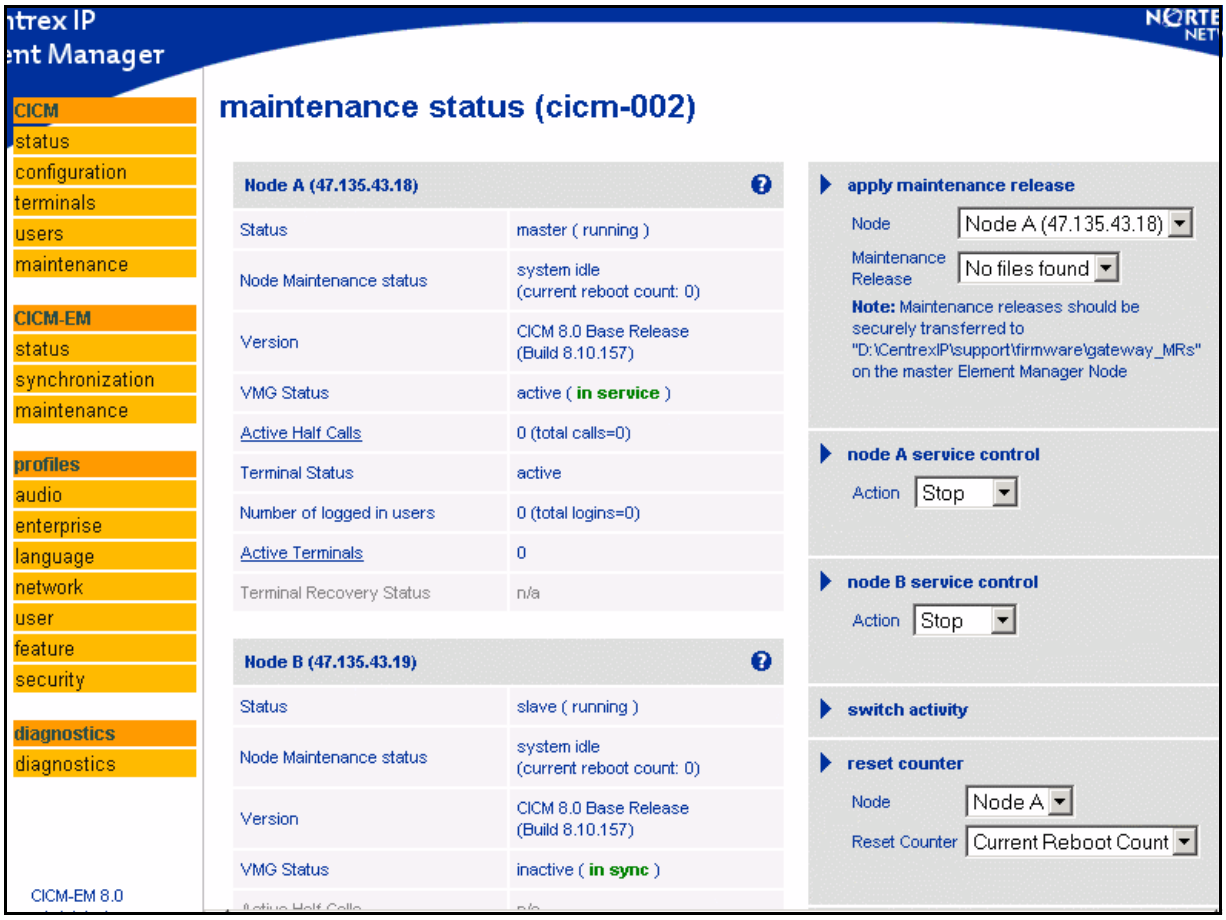
Example
If the faulty card is on node B, you will stop the CICM service on node B.

a After the terminal handover is complete, from the **<cicm_name> cicm status** page of the CICM-EM web pages:



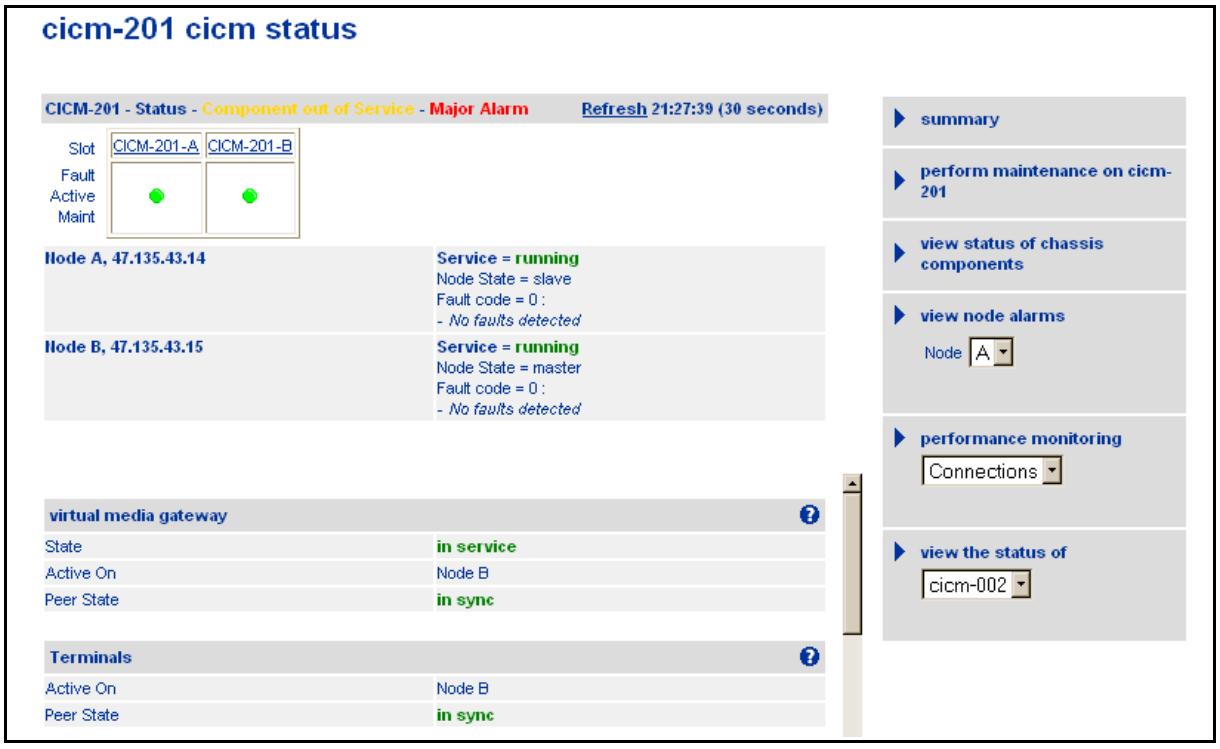
b Click on **perform maintenance on cicm_name** on the right menu.

*Response: The **maintenance status (cicm_name)** page opens.*



c For the node with the faulty card, select **stop** from the **node A service control** or **node B service control** drop-down menu on the right, then click on the **node A/B service control** text.

*Response: The stop action is performed and the status of the node changes to **stop pending**, then changes to **stop**.*



3 Shut down the node where the faulty card is seated, as follows:

a Open a Telnet session to the CICM node *(in our example, node B)*, and enter the following on the command line:

shutdown -s -t 00

where:

s
is for shut down.

t
is for time and 00 (two zeros) means immediately.

Response: A request for confirmation is displayed.

b Confirm the shutdown of the node by entering:

y

Response: A confirmation of the shutdown completion is displayed.

4 For a SAM21, lock the card from the element mangager GUI of the CS2000 SAM21.

For a SAM16, power down the node where the faulty card is seated, as follows:

Note: **CAUTION**
It is critical to power down only the node of the CICM with the faulty card. The mate node of the CICM will take over the workload in order to maintain services to all customers hosted on the CICM.
If both nodes are powered down, it will result in total loss of CICM power and service.

a Open a Telnet session to the CICM mate node, and enter the following on the command line:

C:\>**powerdown**

Example
If the faulty card is on node B, you will Telnet to node A.

Response:
```
This CPU is in domain A
Continuing will power off domain B processor
resulting in the loss of all CentrexIP
service on that node.

Press ENTER to continue, Ctrl-C to abort.
```

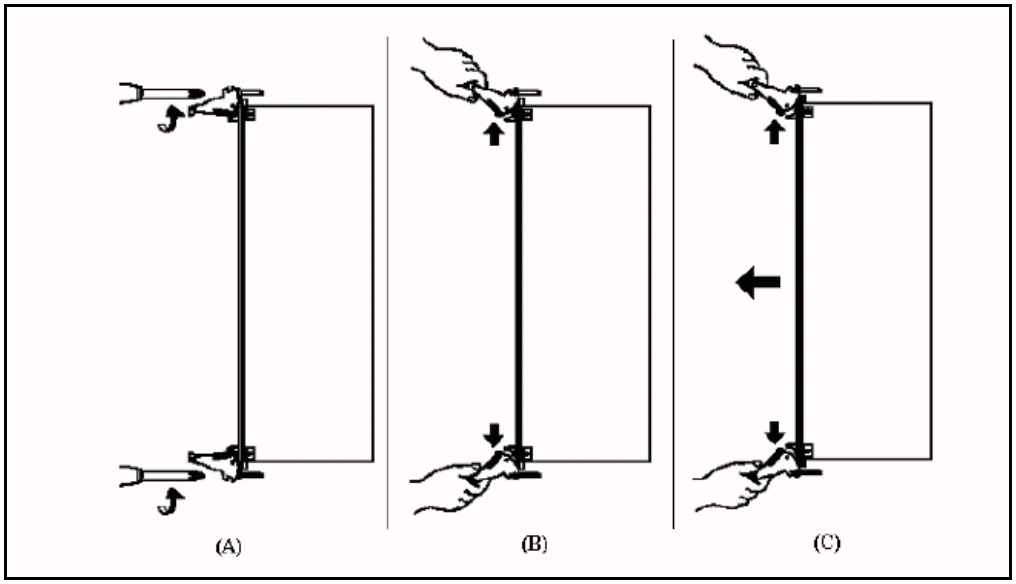
b Continue to power down the node by pressing Enter.

Response:
```
Powering down domain B processor
Powerdown complete.
```

5 Disconnect all cables from the faulty card. Make a note on which port the cables are connected to.

6 Remove the faulty card from the chassis as shown in the following figure.

Note: For each CPU card removed, remove the CPU card first, and then its associated TM.



a Loosen the holding screws of the card with a screwdriver.

b Press the two ejector levers outwards. This action will unseat the card from the back plane connectors.

c After the card is unseated, pull the card out of the chassis.

d Repeat this step for all cards that need to be replaced. For each CPU card, remove the associated Transition Module from the back of the chassis as well.

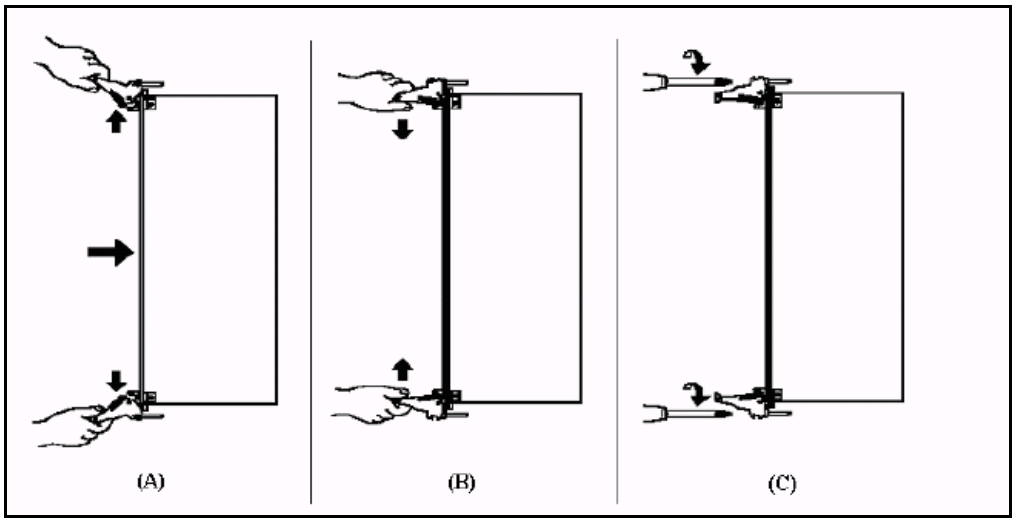
7 If a CPU card is being replaced, connect a suitable PC monitor and keyboard to the card or TM prior to inserting.

IF	THEN
If a CPU card is being replaced and the powerdown command in step 5 did not succeed	The CPU card will boot as soon as it is inserted into the chassis in this step. Be prepared to enter the BIOS settings before the CPU card is allowed to boot fully. Refer to the procedure Checking the BIOS of a new CPU card.
If the powerdown command in step 5 did succeed	Proceed with this procedure through step 13, then check the BIOS settings as directed.

8 Insert the new card into the CICM chassis, as illustrated in the following figure.

Note 1: For each CPM card, insert the TM first, and then the main card.

Note 2: Each HSC is paired with a CPU card and does not have an associated TM. The CPU card in slot 7 is paired with the HSC in slot 10, and the CPU card in slot 9 is paired with the HSC in slot 8.



a Holding the ejector levers outwards, carefully insert the new card into the designated slot of the CICM.

b After the card is inserted, push the ejector lever towards each other. The card will be seated onto the back plane connectors by performing this action.

c Tighten the screws to secure the card to the designated slot.

d Repeat this step for all cards that need to be replaced. For each CPU card, replace the associated Transition Module into the back of the chassis as well.

9 Reconnect all the cables for the replaced card to the same ports that they were previously connected to.

10 For a SAM21, unlock the card from the element mangager GUI of the CS2000 SAM21.

For a SAM16, power up the node from the mate node as follows.

a Establish a Telnet session to the CICM mate node.

Example
If the faulty and replaced card was on node B, Telnet to node A.

b On the command line of the mate node, enter the following:

C:\>**powerup**

Response:

```
Powerup: Power up the other domain processor.

This CPU is in domain A
Powering up on domain B processor
Powerup completed.
```

The service of the node will be recovered in a few minutes.

11 Depending which card was replaced, follow the appropriate step.

IF	DO
An HSC was replaced	Continue to the next step.
A CPU card was replaced	Skip the remainder of this procedure and immediately check the BIOS settings as indicated in the procedure Checking the BIOS of a new CPU card.

12 Verify that the service has started correctly.
On the **<cicm_name> cicm status** page of the CICM-EM web pages, scroll down the **node modification on <cicm_name>** section to the **Service State** field, and verify that it is in the **running** state.

13 This procedure is complete.

Checking the BIOS of a new CPU card

Perform this procedure as soon as a CPU card has been replaced in a SAM16 shelf as described in the procedure Card replacement.

Procedure 1 Check the BIOS of a new CPU card

At the node of the replaced CPU card

1 If the BIOS boot screen is not shown on the monitor connected to the new CPU card (for example, if the blue Windows XP OS boot screen is shown instead), perform a hardware reset on the new CPU card by pressing the **Reset** button on the front of the card, using a suitable non-conductive implement.

Note: A PC keyboard and monitor were connected to the new CPU card prior to inserting it into the chassis, for the purpose of checking the BIOS in this procedure.

2 Change the BIOS configuration as follows:

a Press the **F2** key on the keyboard to enter the BIOS **Setup** main menu.

b In the **Setup** main menu, select and open the **Advanced** menu.

c Using the arrow keys on the keyboard, move the curser to highlight **PCI configurations**, then press the **Enter** key to enter this sub-menu.

d In the **PCI configurations** menu, scroll down the menu with the arrow keys on the keyboard to locate **Domain A** and **Domain B**.

e Verify the PCI configuration as follows:

If	Then
The new CPU is in Domain A	Ensure PCI for Domain A is set to **Enabled** and Domain B is set to **Disabled**.
The new CPU is in Domain B	Ensure PCI for Domain B is set to **Enabled** and Domain A is set to **Disabled**.

f Verify the Ethernet ports configuration by checking that both Ethernet ports are configured to use the **Front** option, or both configured to use the **Rear** option, whichever is preferred.

g Save the BIOS configuration by pressing the **F10** key on the keyboard. This will exit the **Setup** menu.

3 Power down the node as follows:

a Establish a Telnet session to the CICM mate node.

b On the command line of the mate node, enter:

C:\>**powerdown**

4 Power up the node as follows:

a In the Telnet session to the CICM mate node,

b On the command line of the mate node, enter:

C:\>**powerup**

A powerup status window is displayed and the powerup completion confirmed.

The service of the node will be recovered in 15 to 20 minutes.

5 Verify that the CICM is booted up. If the CICM is not able to boot up, contact the Nortel Support Team for assistance.

6 This procedure is complete.

Replacing a hot swap IDE hard disk drive module

Replace a hot swap IDE hard disk drive module from a Motorola SAM16 chassis for the CICM by doing these procedures:

- At the CICM home page of the CICM-EM web site on page 42
- At the CICMs home page of the CICM-EM web site on page 45

Removing the hot swap IDE hard disk drive module

Remove the hot swap IDE hard disk drive module as part of a replacement or upgrade.

CAUTION
Loss of service
This step will cause active calls hosted on this node to drop, and will cause a loss of redundancy. Terminals hosted on this node will also reboot.

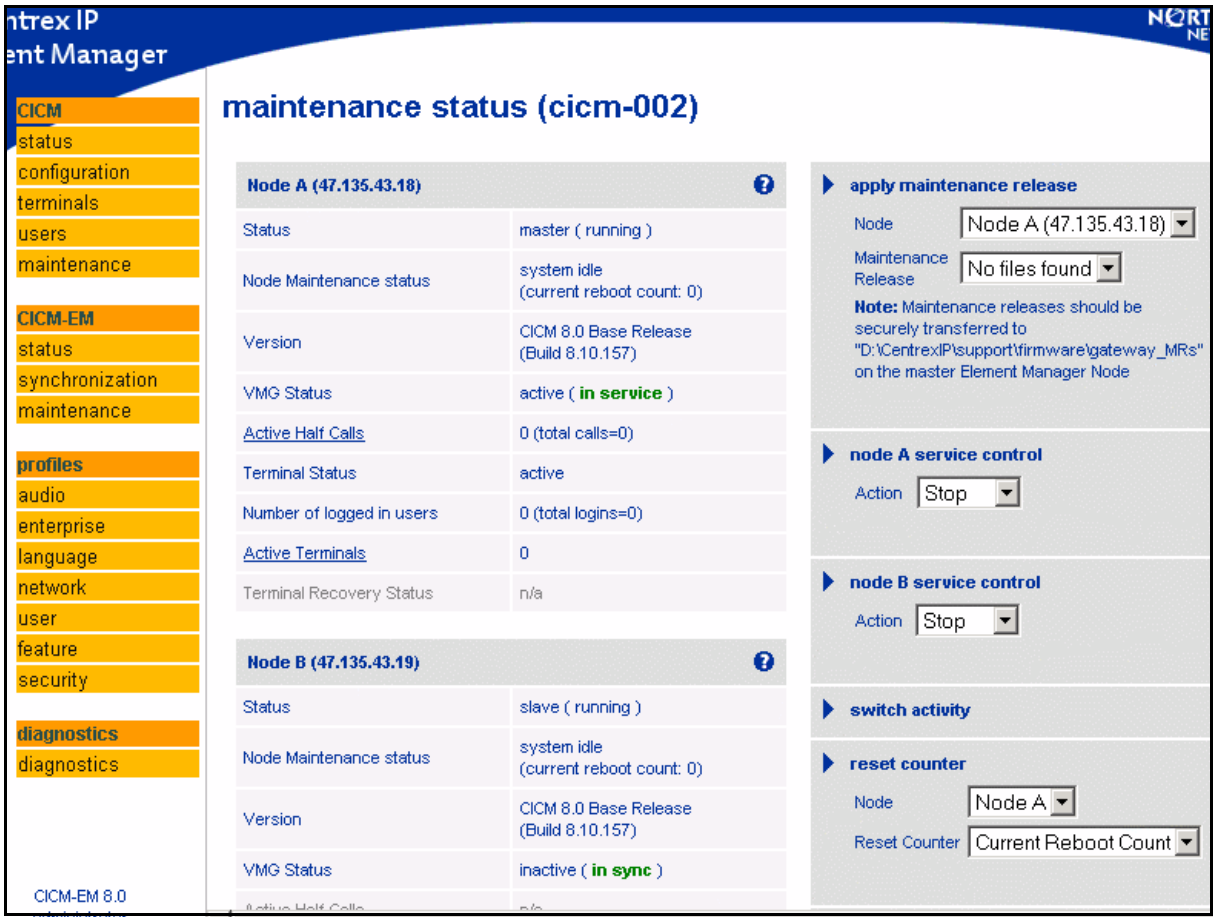
At the CICM home page of the CICM-EM web site

1 At the CICM home page, select the CICM from the drop-down menu, then click on **view the status**.

*Response: The **<cicm_name> cicm status** page opens.*

2 Click on **perform maintenance on <cicm_name>** on the right menu.

Response: The maintenance status (cicm_name) page opens.



3 In the **node A/B service control** on the right menu, select **Stop** from the drop-down menu for the node containing the disk to be taken out of service.

4 When presented with a confirmation window, select **Yes** to confirm.

5 Back up the contents of the hard disk using the Backup and Restore Tool. Use the procedure *Disk Backup of CICM Node* in the *Method of Procedure (MOP) for Disk Backup and Restoration,* which can be found on the *Backup and Restore Tool* CD. Use this procedure to take an image of the hard disk that is to be replaced.

Note 1: Do not reboot the CICM node at step 13 in the *Disk Backup of CICM Node* procedure.

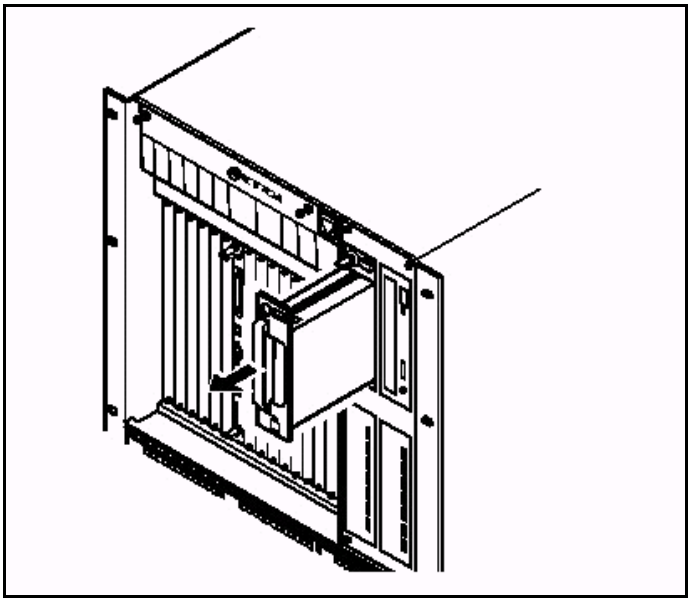
Note 2: If the hard disk is too damaged, it may not be possible to back up the disk.

6 Unlock the drive by pushing the keyswitch in, and turning it ¼ turn anti-clockwise. This lets the system know that the drive module is about to be removed from the chassis.

7

WARNING
Risk of equipment damage
Do not remove the drive module while the green LED is illuminated. When the module is ready to be removed, the green LED will go out and the yellow LED will light up. However, since the LEDs are controlled by the system software, the yellow LED may not light.

After the yellow LED is illuminated, remove the drive module from the frame by sliding the drive module out of its bay, as shown in the figure below.



8 Remove hard disk from the drive module by pulling off the top and bottom covers from the drive module. Remove the mounting screws that hold the hard disk in place. Push the hard disk up through the drive module and disconnect all the power and data cables.

9 This procedure is complete.

Installing the hot swap IDE hard disk drive module
Install the hot swap IDE hard disk drive module as part of a replacement or upgrade.

At the CICMs home page of the CICM-EM web site

1 Configure the replacement hard disk.

The hard disk must be replaced with another hard disk of the same type (IDE). The new disk must also be set up in the same way as the disk removed (master or slave), using the DIP switches on the rear of the drive module.

2 Re-cable the hard disk to the drive module by connecting the six-conductor, red, yellow, and green pair cable to the hard disks jumper header as shown in the table below. Each jumper is connected with the DIP switches noted in the table set to the **On** position, as described in the following substeps.

Wire color	Configuration	DIP Switch
Red	Slave	4
Yellow	Cable Select	3
Green	Master	2

a With DIP switch 2 in the **On** position and the others in the **Off** position, the drive is set to **Master**

b With DIP switch 4 in the **On** position and the others in the **Off** position, the drive is set to **Slave**

c With DIP switch 3 in the **On** position and the others in the **Off** position, the drive is set to **Cable Select**

3 Reconnect the IDE cable and power cable.

4 Secure the hard disk back in the drive module with the screws that were removed in Procedure 34, then reattach the top and bottom drive module covers.

5 Insert the drive module into the frame.
Align the drive module connector with the chassis connector, then push the drive module into its bay and secure firmly.

6 Push the keyswitch in, then turn it ¼ turn clockwise.

7 Restore the contents of the hard disk using the Backup and Restore Tool. Follow the procedure *Disk Image Restoration of CICM Node*, in the *Method of Procedure for Disk Backup and Restoration*, which is on the Backup and Restore Tool CD. Using

this procedure, restore the node image to the new hard disk, using the last known good image. Once the node has rebooted, it will be synchronized with the other node.

Note: If no backup image is available, the node will have to be re-imaged, upgraded to the relevant MR, and then synchronized with the other node. If this is the case, contact Nortel Support for assistance.

8 This procedure is complete.

Replacing a non-hot swap CDROM/DVD drive module

Replace the non-hot swap CDROM/DVD drive module from a Motorola SAM16 chassis by doing these procedures:

- Replacing a non-hot swap CDROM/DVD drive module
- Installing a non-hot swap CDROM/DVD drive module

Removing a non-hot swap CDROM/DVD drive module

Remove a non-hot swap CDROM/DVD drive module as part of a replacement or upgrade.

CAUTION
Service outage
The following step causes a complete outage of the CICM node. No call processing will be possible on this CICM.

At the CICMs home page of the CICM-EM web site

1 From the **cicm home** page on the CICM-EM, select the correct CICM from the drop-down menu, then click on **View the Status of the Following CICM**.

*Response: The **Perform maintenance <cicm_name>** page opens.*

2 On **node A service control** on the right menu, select **Stop** from the drop-down menu, then click on **node A service control**.

Response: A confirmation dialog box opens.

3 Choose **Yes** to confirm.

4 Repeat step 2 for node B.

5 Back up the contents of the hard disk using the Backup and Restore Tool. Use the procedure *Disk Backup of CICM Node* in the *Method of Procedure (MOP) for Disk Backup and*

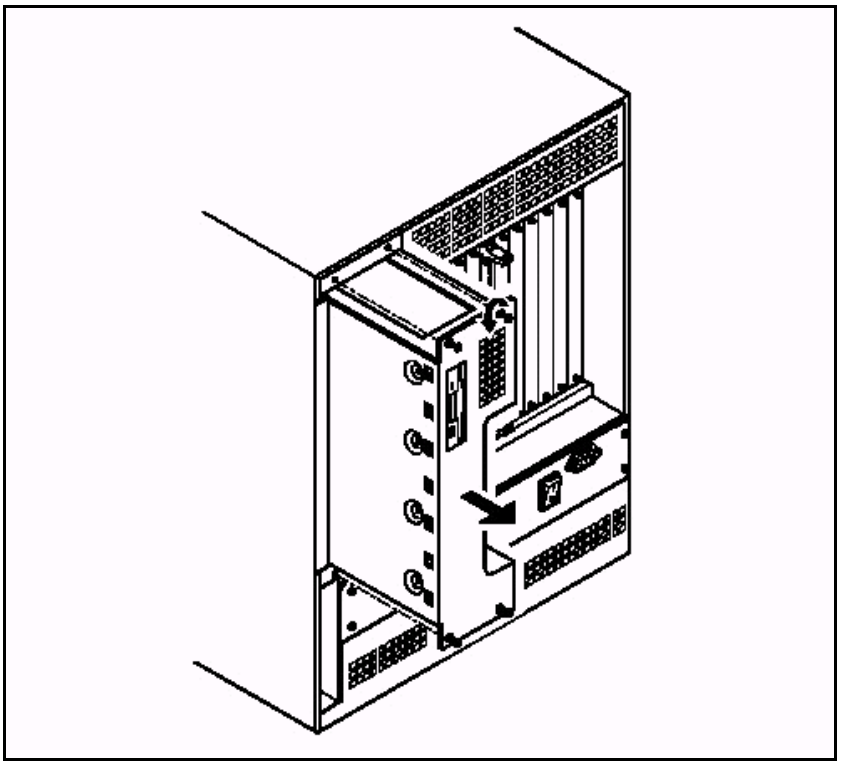
Restoration, which can be found on the *Backup and Restore Tool* CD. Use this procedure to take an image of the hard disks on both nodes..

Note 1: Do not reboot the CICM node at step 13 in the *Disk Backup of CICM Node* procedure.

Note 2: If the hard disk is too damaged, it may not be possible to back up the disk.

6 Shutdown the system and power off.
Power off the chassis using the switch at the back, then remove the power feed.

7 Remove floppy drive housing.
Loosen the four screws holding the floppy drive housing and pull it carefully out of the chassis, as illustrated in the following figure. Then detach the cables from the floppy drive housing, making a note of where they connect, and put the housing to one side.

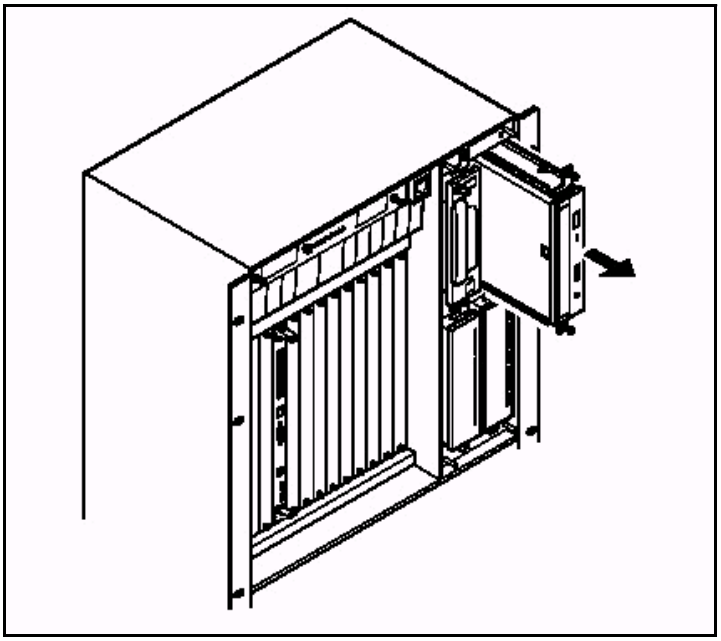


8 Detach the power and data cables from the drive being removed from the system.

9 Remove the front drive bay bezel from the front of the chassis.

10 Remove the drive from the bay.
Loosen the captive screws that are holding the drive in the bay

and pull the drive straight out, as illustrated in the following figure. Then remove the mounting rails from the side of the drive.



11 This procedure is complete.

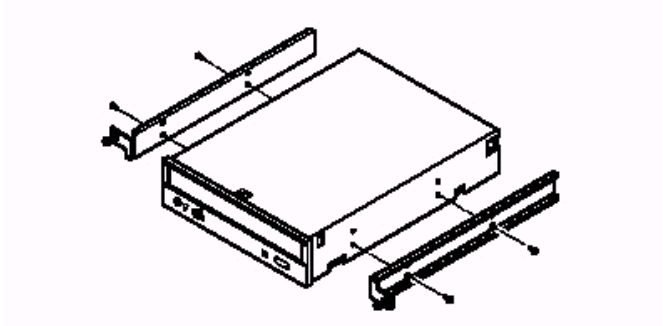
Installing a non-hot swap CDROM/DVD drive module

Install a non-hot swap CDROM/DVD drive module as part of a replacement or upgrade.

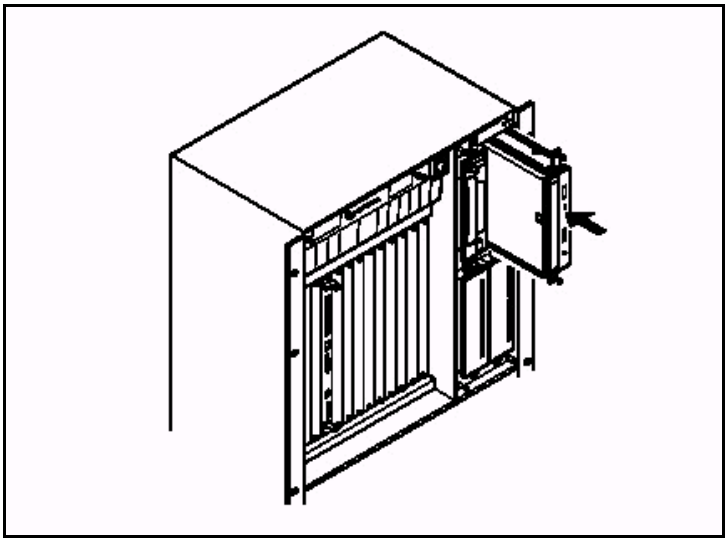
At the CICM chassis

1 Configure the new drive to have the same settings as the drive that has been removed with the jumpers on its back.

2 Attach the mounting rails (which were removed from the old drive in procedure 36 above) to the new drive.



3 Insert the drive into the empty bay in the chassis and secure it with the captive screws. The top of the drive should face left.



4 Replace the front drive bay bezel.

5 Reattach the data and power cables to the drive.

6 Reattach the cables to the floppy drive housing. Slide the floppy drive housing back into the chassis and secure it with the four captive screws.

7 Insert the power cable and turn the system back on. Once the system has booted up, check from the CICM-EM that everything is OK.

8 This procedure is complete.

Correcting a node that is stopped

Correct a stopped CICM-EM or CICM node to enable restoring service.

CAUTION
Loss of service
Under no circumstances should the **Restart** button be used without Nortel Support direction.
This procedure must be performed only under direction from Nortel **Support.**

On a PC connected to the Administration LAN

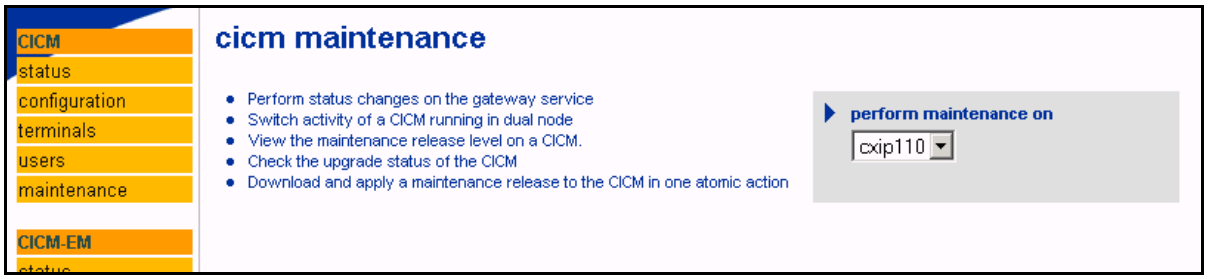
1 Open a Telnet session and attempt to connect to the stopped node.

IF	THEN
You are able to access the node	You have confirmed that the node is functioning. This procedure is complete.
You are not able to access the node	Proceed to the next step to check if the node is powered on.

At the CICM home page

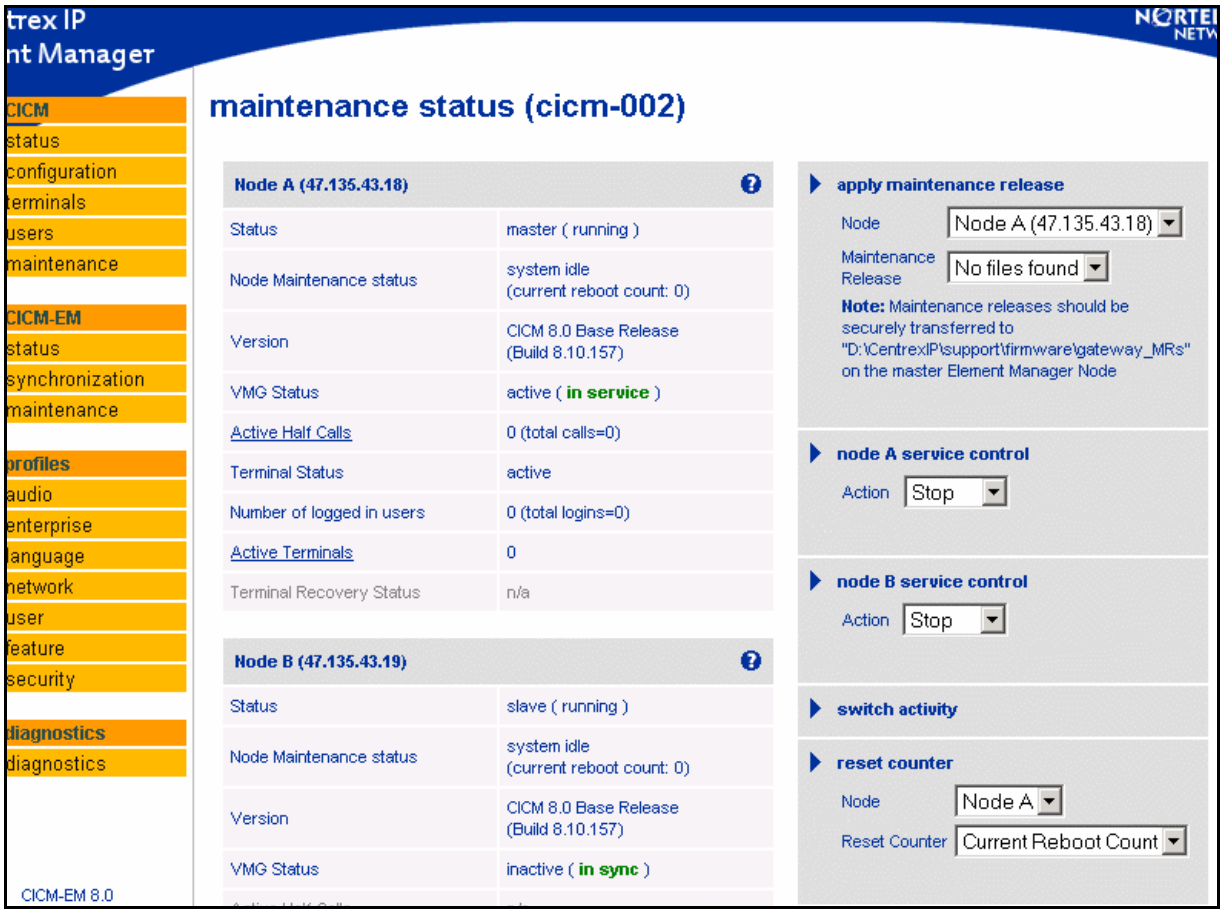
2 Click on **maintenance** in the left menu.

*Response: The **cicm maintenance** page opens.*



3 Select the CICM from the drop-down menu in **perform maintenance on** in the right menu, then click on **perform maintenance on**.

*Response: The **maintenance status <cicm_name>** page opens.*



4 View the **Service Status** field for the node and check that the node is powered on.

IF	DO
Service state is **running**	This procedure is complete.
Service state is **stopped**	Select **Restart** from the drop-down menu in the **node A service control** or **node B service control** on the right menu (whichever node is applicable). ***Note:*** Perform this step only under Nortel Support supervision.

5 If the **Restart** option was chosen, check that the **Service State** field has changed to the **running** state on the **maintenance status <cicm_name>** page.

6 This procedure is complete.

Correcting a node that is not connected

Correct a CICM-EM or CICM node that is not connected to enable restoring service.

CAUTION
Loss of service
Under no circumstances should the **Restart** button be used without explicit instruction from Nortel support personnel.
This procedure must be performed only under direction from Nortel **support.**

On a PC connected to the Administration LAN

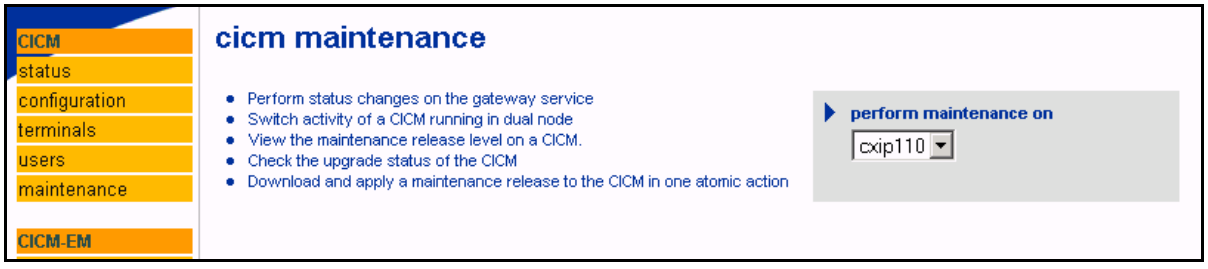
1 Open a Telnet session and attempt to connect to the disconnected node.

IF	THEN
You are able to access the node	You have confirmed that the node is functioning. This procedure is complete.
You are not able to access the node	Proceed to the next step to check if the node is powered on.

At the CICM home page

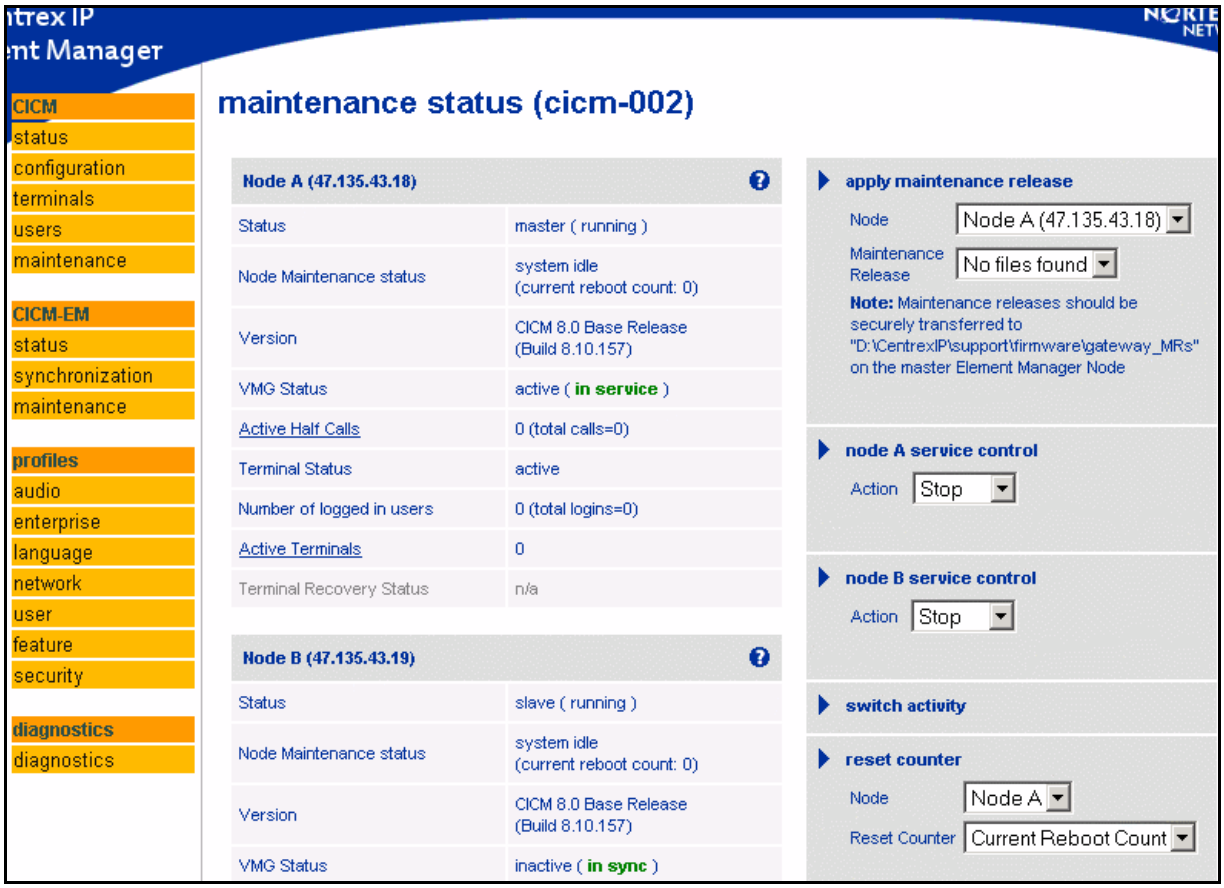
2 From the **CICM home** page, select **maintenance** from the left menu.

*Response: The **cicm maintenance** page opens.*



3 Select the CICM from the drop-down menu in **perform maintenance on** in the right menu.

*Response: The **maintenance status <cicm_name>** page opens.*



4 View the **Service Status** field for the node and check that the node is powered on.

IF	DO
Service state is **running**	This procedure is complete.
Service state is **stopped**	Select **Restart** from the drop-down menu in the **node A service control** or **node B service control** on the right menu (whichever node is applicable). ***Note:*** Perform this step only under Nortel Support supervision.

5 If **Restart** was chosen, check that the **Service State** field has changed to the **running** state on the **maintenance status <cicm_name>** page.

6 This procedure is complete.

Correcting a VMG out-of-service fault

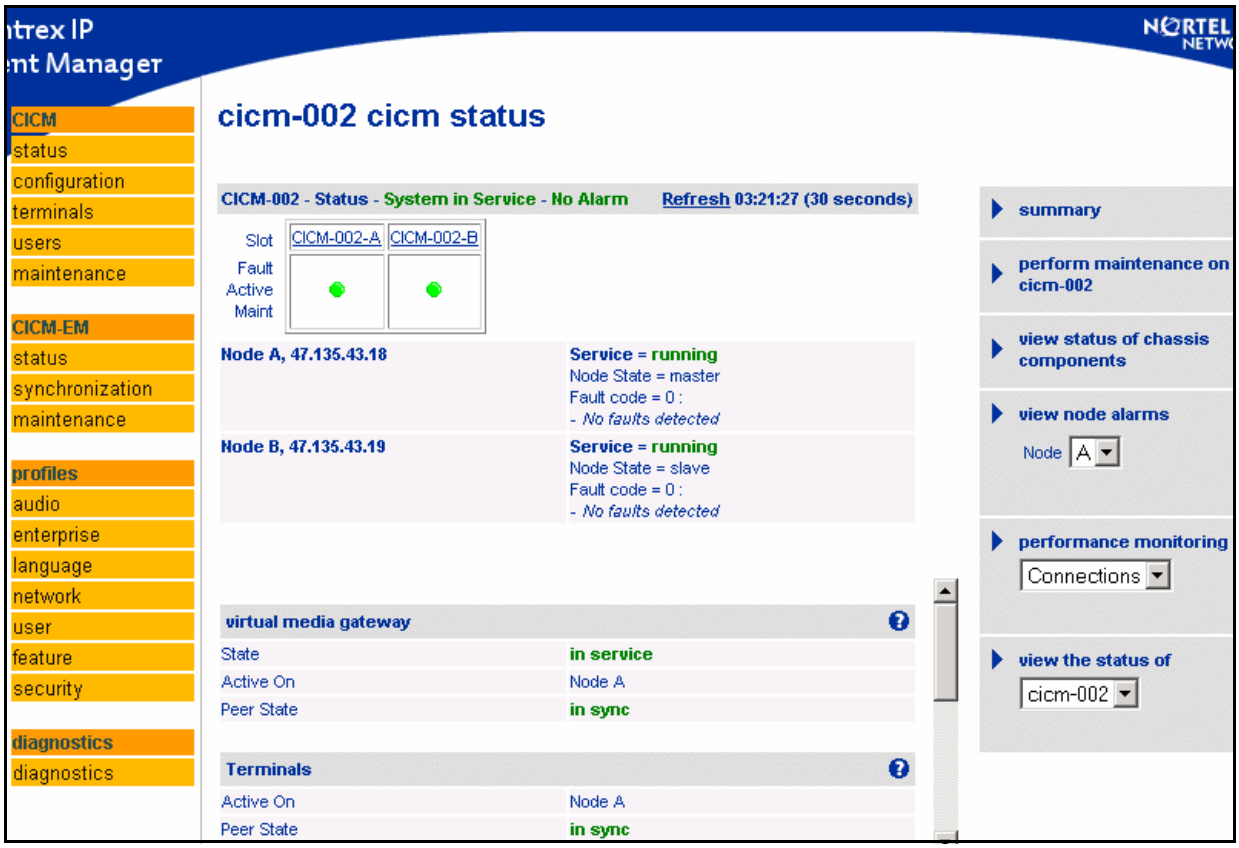
Restart VMG service when it has the state **out of service** while connected to the a SAM16 platform.

When the **<cicm_name> CICM Status** page indicates that the VMG is **stopped**, it is likely due to a node being stopped. Do the procedure On a PC connected to the Administration LAN.

At the CICM home web page

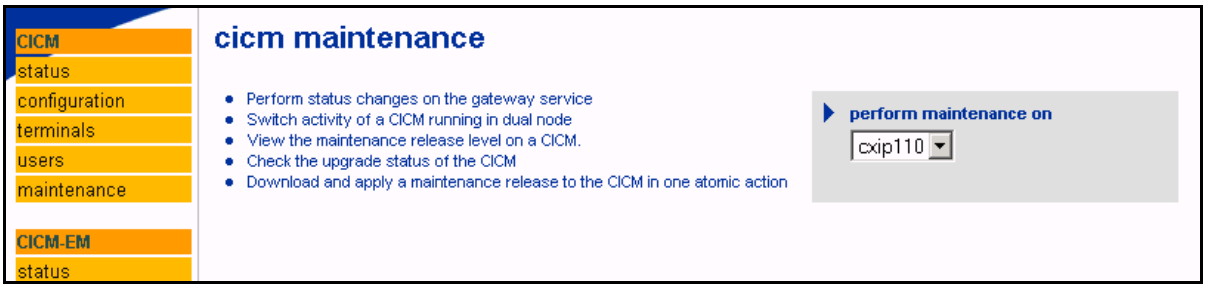
1 View the **service state** of the VMG by selecting the CICM to view from the drop-down menu of **view the status on the following CICM** on the right menu.

*Response: The **<cicm_name> cicm status** page opens.*



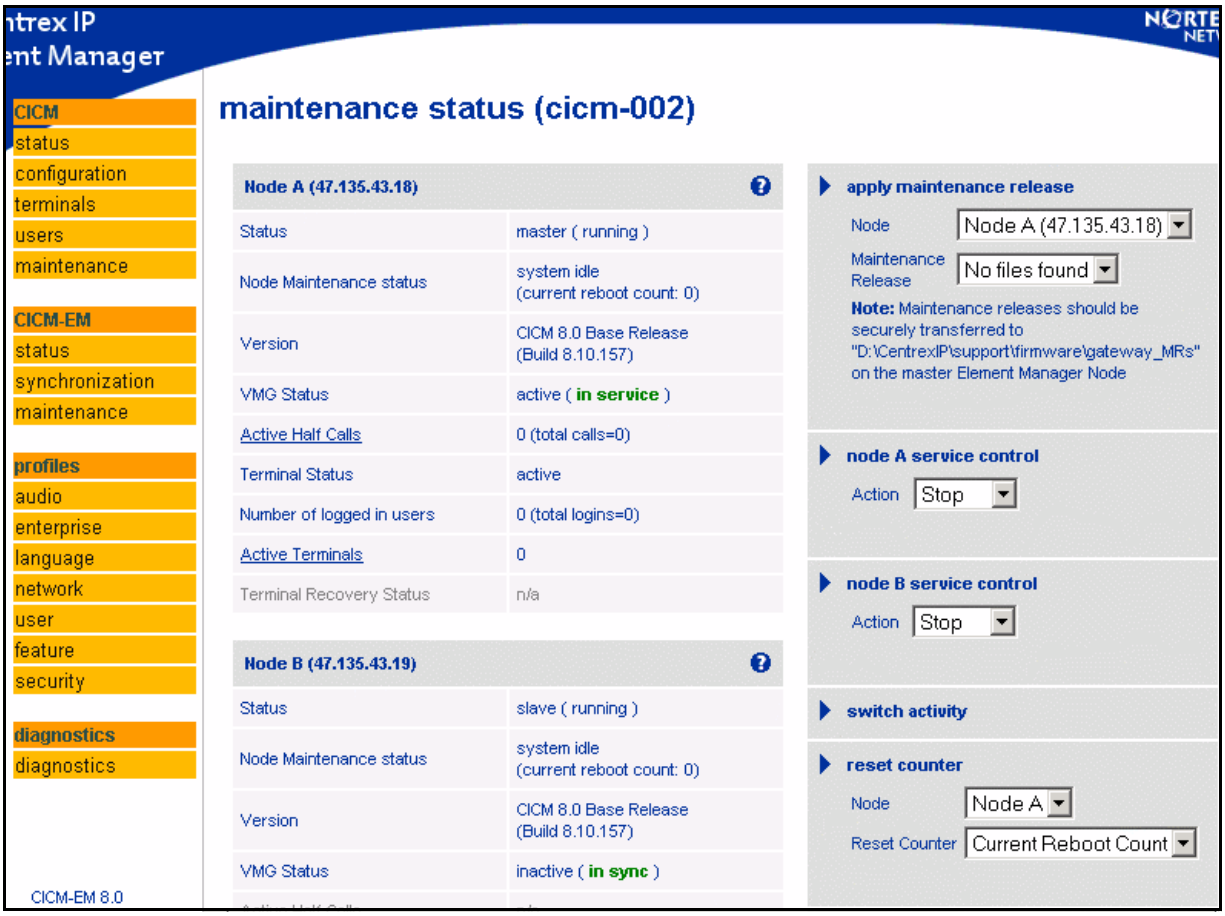
2 If the **<cicm_name> cicm status** page indicates that the VMG is **stopped**, it is likely due to a node being stopped.
To restart the node, click on **maintenance** from the CICM menu.

*Response: The **cicm maintenance** page opens.*



3 Select the CICM from the drop-down menu in **perform maintenance on** in the right menu.

*Response: The **maintenance status <cicm_name>** page opens.*



4 View the **Status** field for the nodes and check that the nodes are powered on.

IF	DO
Service state is **running** for both nodes	This procedure is complete.
Service state is **stopped**	Select **Restart** from the drop-down menu in the **node A service control** or **node B service control** menu option on the right menu (whichever node is applicable). ***Note:*** Perform this step only under Nortel Support supervision.

5 If the **Restart** option was chosen, check that the **Service State** field has changed to the **running** state on the **maintenance status <cicm_name>** page for each node and the VMG.

6 This procedure is complete.

Rebooting (hard) a SAM16 with CPV5370 cards

Hard reboot a SAM16 node with CPV5370 CPU cards by powering it up and down, especially after replacing hardware.

Apply this procedure only to the slave node. Rebooting a master CICM-EM or CICM node can cause an interruption in service.

CAUTION
Risk of service loss
Completing this procedure powers off both nodes of a redundant pair and results in loss of all Centrex IP service on nodes A and B.

At a PC on the administration LAN

1 Telnet to the CICM node. Refer to the *Telnet to a CICM node* procedure.

At the command line interface

2 To powerdown, enter:

powerdown

```
The CPU is in domain X
Continuing will power off domain Y processor
resulting in loss of all CentrexIP service on
that node.
Press ENTER to continue, Ctrl-C to abort
```

3 To continue, press **Enter**.

```
Powerdown completed.
```

4 To powerup the mate node, enter:

powerup

```
This CPU is in domain X
Powering on domain Y processor
Powerup completed.
```

5 This procedure is complete.

Rebooting (hard) a SAM21 with CPN5385 cards

Hard reboot a SAM21 node with CPN5385 CPU cards by locking and unlocking the card from the element manager GUI of the SAM21.

Apply this procedure only to the slave node. Rebooting a master CICM-EM or CICM node can cause an interruption in service.

You need to know which SAM 21 chassis contains the CPN5385 card of the CICM-EM or CICM node you want to reboot, and also the slot number of the crad in the chassis.

CAUTION
Risk of service loss
Completing this procedure will power off the node and result in loss of all CentrexIP service on that node.

At a PC on the administration LAN

1 Through IEMS, double-click on the element manager (EM) of the SAM21 chassis that contains the card for the CICM-EM or CICM node that you want to reboot.

At the EM of the SAM21

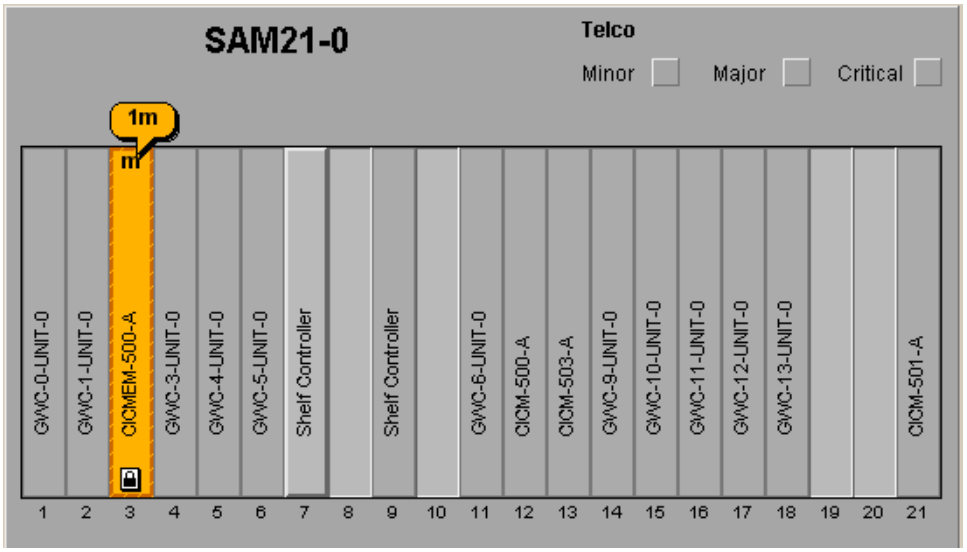
2 Double-click on the shelf view of the SAM21 chassis to open it.

3 With the cursor on the card of the node to be rebooted, right click to select:

lock

4 Observe the change of states by right clicking and selecting *Card View.*

The locked card turns orange and shows a padlock symbol.

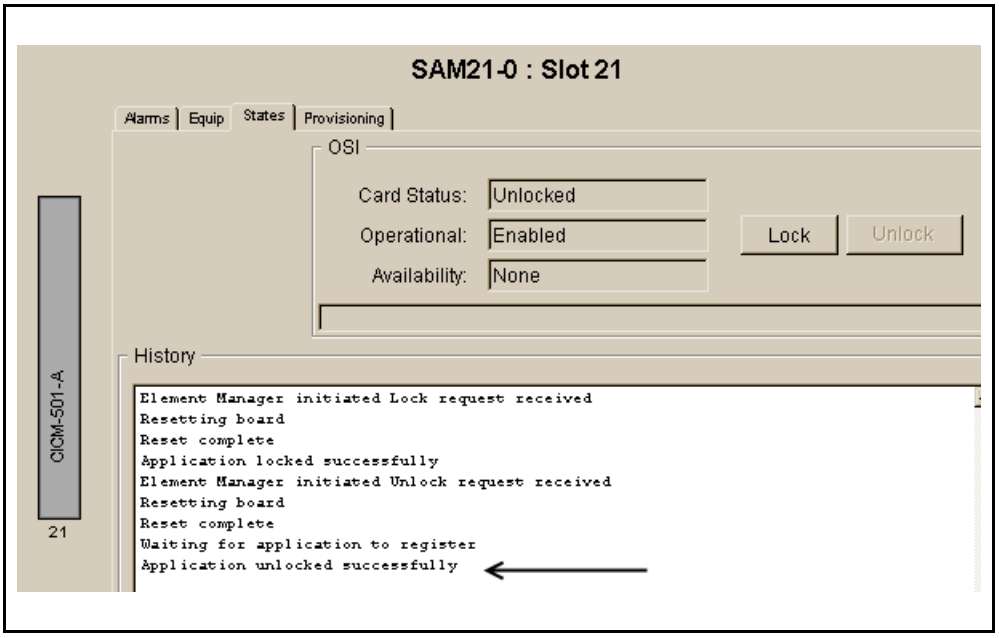


5

CAUTION
Risk of service interruption
Wait until the unlocking has completed. Do not affect the state of the card (blade). If unlocking takes longer than 30 minutes, contact GNPS for help.

Wait for the node to fully unlock.

Unlocking is complete after the following *Card View... State History* is displayed and when the *Card View...* above changes to indicate that the card is fully in service.



6 When the locking is complete, return to the *Card View* and on the same card right click to select:

unlock

Completion of the reboot is indicated under the *History* tab of the *Card View*.

7 This procedure is complete.

Rebooting (soft) the node

Reboot (restart) the CICM-EM or CICM node in a SAM16 or SAM21 to restore service.

Apply this procedure only to the slave node. Rebooting a master CICM-EM or CICM node can cause an interruption in service.

At a PC on the administration LAN

1 Telnet to the CICM node. Refer to the *Telnet to a CICM node* procedure.

At the command line interface

2 Softly reboot the node by entering:

shutdown /l /r /t:0

r
is for reboot.

t
is for time and 0 (zero) means immediately.

The node shuts down and automatically restarts.

3 This procedure is complete.

Restoring the CICM node registries

Restore the CICM node registries using a back-up file from the CICM-EM. Refer to the section Backup and restore procedures for associated procedures.

At the CICM home page of the CICM-EM web pages

1 Stop the CICM node as described in the procedure *Stop the CICM service* in the NN10252-611 *CICM Security and Administration* document.

At the CICM status page

2 Disconnect the CICM from the CICM-EM.

   a Click on **change the list of CICMs stored on the element manager** on the right menu.

3 Click on the trash can icon next to the CICM node to delete.

4 Click on **confirm deletion**.

At the PC desktop for remote access to the CICM-EM

5 Telnet to the CICM-EM of the CICM node and ensure that the registry back-up file is present at the FTP home directory:

   D:\\CentrexIP\support

   The back-up files have file name backupconfig_<day_number>.xml for a CICM node or backupconfig_<day_number>_em.xml for a CICM-EM.

6 Telnet to the CICM node being restored.

7 From the CICM node being restored, FTP to its CICM-EM and retrieve the latest backup file.

8 Repeat step 1 to step 7 for the mate node.

9

CAUTION
Risk of service loss
This step deletes all current configuration information.

Confirm the prompt.

10 In a telnet window to one of the CICM nodes, delete the corrupt CICM configuration registry by entering:

```
reg delete "HKLM\Software\Nortel
Networks\CentrexIP International Gateway\8.10"
```

where

HKLM
refers to **HKEY local machine** and is part of the registry where the CICM configuration files are stored

8.10
is the name of the corrupted CICM software version to be deleted

Note: The command string includes spaces.

11 In a telnet window to the same CICM node, notify the system that you are going to restore part of the CICM configuration registry by entering:

```
reg add "HKLM\Software\Nortel
Networks\CentrexIP International Gateway\8.10"
```

where

HKLM
refers to **HKEY local machine** and is part of the registry where the CICM configuration files are stored

8.10
is the name of the CICM software version to be added

Note: The command string includes spaces.

12 In the telnet window to the same CICM node, restore the backed up configuration by entering:

```
cxiprestore /norestart <backup_file_name>.xml
```

where

<backup_file_name>.xml
is the latest CICM node backup file

13 Repeat step 9 to step 12 for the mate node.

14 Disconnect the telnet sessions from the CICM nodes.

At the CICM home page

15 Add the CICM node to the CICM-EM as follows:

a click on **change the list of CICMs stored on the CICM-EM**

b click on **add new CICM**

c enter the name of the CICM, then click on **save new CICM**

16 Restart one CICM node according to the procedure Rebooting (soft) the node and return to this step.

17 Confirm the back-up has been loaded successfully by logging into the restored CICM node.

If you log in, the back-up was successful.

If you cannot log in, contact your next level of technical support.

18 Restart the second CICM node according to the procedure Rebooting (soft) the node and return to this step.

19 Confirm the back-up has been loaded successfully by logging into the restored CICM node.

If you log in, the back-up was successful.

If you cannot log in, contact your next level of technical support.

20 This procedure is complete.

Shutting down a CICM node

Manually shut down a CICM node to enable addressing a problem with its hardware or software.

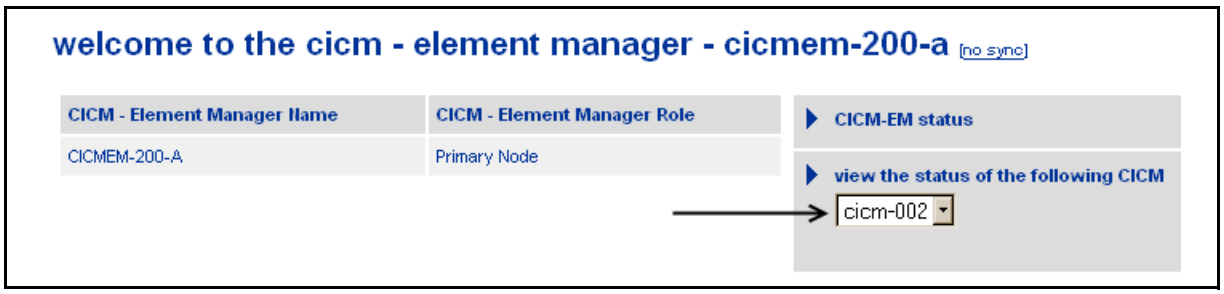
Refer to CICM node failures to understand what happens for a failure.

Only a slave CICM node of a redundant pair can be shut down or restarted. With SN08, all terminals (clients) are active only through the master CICM node.

At the maintenance page of the CICM-EM

1 Select the identifier of the CICM node from the drop-down menu under **view of the following CICM**.

Example
CICM-002

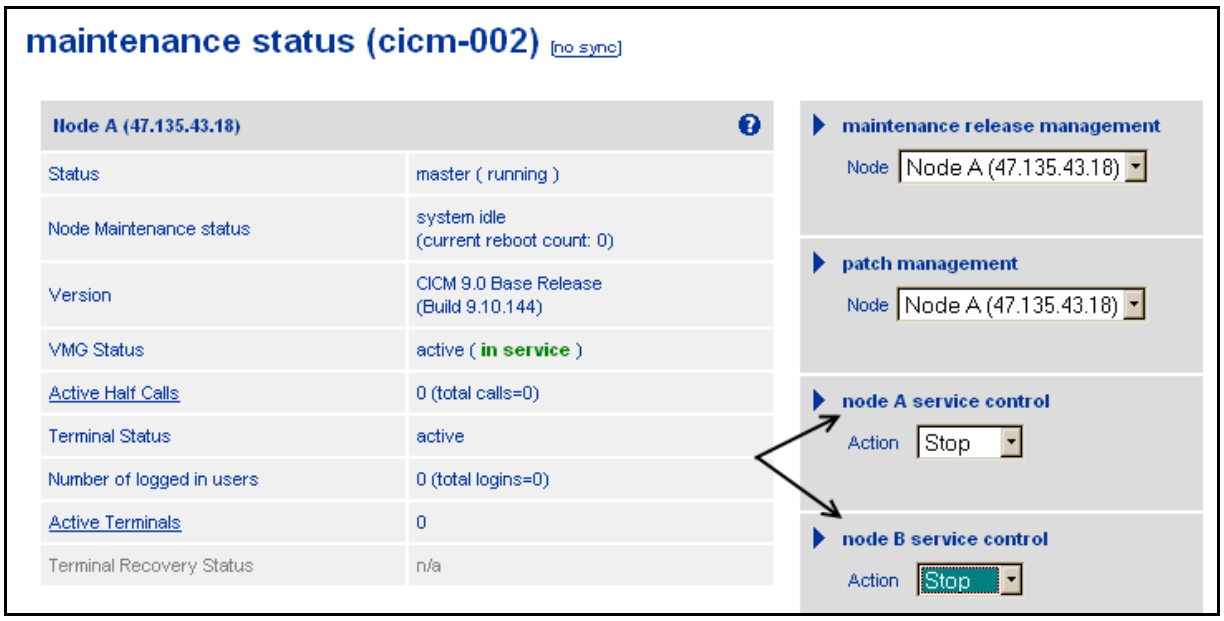


2 Click on **view of the following CICM**.

3 Ensure from the status that the CICM node to be shut down is the slave.

4 Click on **perform maintenance on cicm-nnn**.

5 For the slave node A or B, select **Stop** as the action from the drop-down menu under **node A/B service control**.



6 Click on **node A/B service control** for the slave node.

7 Click on **confirm service state change** to shut down the node or **cancel** to leave it as is.

8 This procedure is complete.

CICM node failures

When both master and slave nodes are running synchronized, and either CICM node fails, then there is a redundant node to continue service.

The term *node failure* applies to both hardware failures of the physical CPU card running the CICM load, or to a critical software error for which no recovery action is possible. Some possible node failures include:

- when any of the software components that make up the CICM load experiences a software exception (a trap), then the monitoring software automatically initiates an immediate restart of the node
- a general failure of the CPU card

From the remaining node perspective, these two cases are identical in that its mate suddenly stops providing heartbeats. The remaining node takes appropriate action, as described in the scenarios below.

All but LAN adapter failures (described in Network adapter failures) are treated equally by the dual-node redundancy functionality. When physically possible, any critical failure will result in the node automatically restarting a preset number of times (the default is three;

this variable can be configured by the telco administrator). Following the last restart, the boot controller will not start the CICM software load.

Scenario 1: the master node fails

When the master node has an unexpected failure, the slave node on hot standby detects it and automatically switches activity (SWACTs) to take over from the master. This occurs transparently to the gateway controller (GWC) as the new master node binds to the H.248 and client (terminal) addresses. Some inbound messages from the GWC may be lost during the takeover, but the retransmission algorithm built into H.248 ensures that they are eventually delivered. Inbound messages from the clients may be lost, but the retransmission algorithm built into UNIStim ensures that they are eventually delivered.

The connectivity of clients (terminals) is maintained for stable calls as connections are switched over during the SWACT of the nodes. Unstable calls may or may not survive.

Scenario 2: the slave node fails

When the slave node has an unexpected failure, the master node detects it and continues service. No SWACT occurs, so H.248 or UNIStim messages from the GWC are maintained.

Since all terminals are always hosted off of the master node, full service to the clients is maintained. All stable and unstable calls survive the failure on this node.

Network adapter failures

LAN adapter failures on the CPU cards are treated differently from other types of failures. The following cases require special consideration.

- **Master looses adapter hosting H.248 interface**
  When the master node detects that it has lost layer-2 connectivity (typically representing a physical loss of a network adapter) on the physical adapter hosting the H.248 interface, the master initiates an automatic SWACT. This is done to conserve connectivity to the GWC and to the VoIP client, thereby maintaining call processing and client connectivity.
- **Master looses both adapters**
  If the master node detects layer-2 loss of connectivity on both its physical adapters, it determines that it is at fault, and demotes itself to the slave state. The original slave determines that the master has failed, and promotes itself to master.

  When either of the isolated node's adapters becomes available, the node looks for its mate. If found, the node restarts itself in order to

refresh itself as the slave and ensure that all its MIB data is synchronized with the master node.

If, upon regaining either physical adapter, the node does not find a mate, it re-promotes itself to the master state. Appropriate monitoring software ensures that only one node is ever master at any given time.

- **Slave loses adapter acting as backup H.248 and client interface**
When the slave node loses layer-2 connectivity on the physical adapter that would normally host the back-up H.248 and the client interface, the slave updates its own local state and advises the master node of this change. This is necessary to ensure that a SWACT is not inadvertently initiated either manually or automatically. No SWACT occurs.
- **Slave loses both adapters**
If the slave detects layer-2 loss of connectivity on both its physical adapters, it acts almost exactly as in the above-described scenario: *Master looses both adapters*. The only difference is that the node does not need to demote itself. It is already the slave.

Starting a service running on a node

Manually start a service to run on a CICM node. The service can be started by using either procedure:

- Starting a service manually on a node using the command net
- Starting a service manually on a node using the command sc

This procedure is typically done only when requested by Nortel's GNPS team.

Starting a service manually on a node using the command net

Start a service on a CICM node using the command **net**.

At a PC on the administration LAN

1 Telnet to the CICM node. Refer to the *Telnet to a CICM node* procedure.

At the command line interface

2 Enter **net start <service_name>**

where

service_name
is the name of the service to start.

Response: A status message appears confirming that the service was started successfully.

Note: To find the service name, use the **net start** command. A list of services will display. See the *View the services running on a node* procedure.

3 This procedure is complete.

Starting a service manually on a node using the command sc

Start a service on a CICM node using the command **sc**.

At a PC on the administration LAN

1 Telnet to the CICM node. Refer to the *Telnet to a CICM node* procedure.

At the command line interface

2 Enter **sc start <service_name>**

where

service_name
is the name of the service to start.

Response: A status message appears confirming that the service was started successfully.

Note: To find the service name, use the **net start** command. A list of services will display. See the *View the services running on a node* procedure.

3 This procedure is complete.

Stopping a service running on a node

Manually stop a service running on a CICM node. The service can be stopped using either procedure:

- Stopping a service manually on a node by using the command net
- Stopping a service manually on a node by using the command sc

Stopping a service manually on a node by using the command net

Stop a service on a CICM node using the command **net**.

At a PC on the administration LAN

1 Telnet to the CICM node. Refer to the *Telnet to a CICM node* procedure.

At the command line interface

2 Enter **net stop <service_name>**

where

service_name
is the name of the service to start.

Response: A status message appears confirming that the service was stopped successfully.

Note: To find the service name, use the **net start** command. See the *View the services running on a node* procedure.

3 This procedure is complete.

Stopping a service manually on a node by using the command sc

Stop a service on a CICM node using the command **sc**.

At a PC on the administration LAN

1 Telnet to the CICM node. Refer to the *Telnet to a CICM node* procedure.

At the command line interface

2 Enter the command:
sc stop <service_name>

where

service_name
is the name of the service to start.

Response: A status message appears confirming that the service was stopped successfully.

Note: To find the service name, use the **net start** command. See the *View the services running on a node* procedure.

3 This procedure is complete.