Fault management

This *NN10233-911 CICM Fault Management* document provides the fault management strategy and procedures for the Centrex IP Client Manager Series 7.0.

Overview

This section provides the Fault Management strategy and procedures for CICM fault troubleshooting and correction.

The main topics included in this section are:

- Fault management strategy
- User interfaces
- Alarms
- Fault management procedures
  - — General troubleshooting
  - — Fault correction

Refer also to the *Appendix* of this document for a list of error codes.

Fault management strategy

The Centrex IP Client Manager 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 goal of the CICM is to able 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 node is partitioned into two identical independent physical nodes: Node A and Node B. The CICM uses a SAM 16 hardware platform with dual cPCI backplane.

Towards the GWC, the two cards present themselves as a single network entity (one CPU is the master, the other is a warm-standby slave). The terminals are configured with the address of both CPUs. The terminal will failover between them when a failure occurs.

The resulting flexibility allows the CICM to react promptly by adjusting itself to operation in failure conditions, thus ensuring the overall impact on the service provided is kept to a minimum.

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

There are four basic user interfaces used in fault management. These two user interfaces are:

- Web-based Element Manager interface
- Telnet

Web-based Element Manager interface

This interface uses a Web browser to access the Element Manager Web pages. This interface is used in Fault Management to monitor the status of the CICMs and components, and to change configuration as required.

Refer to the *Element Manager Web pages procedures* in the *CICM Security and Administration* document.

Telnet

The Telnet utility is used to copy debug logs from a CICM node to the Element Manager to facilitate troubleshooting by Nortel Networks

Support personnel, to verify the connection of a terminal on the client LAN, and for other troubleshooting activities. Refer also to the Telnet procedures in the *CICM Security and Administration* document.

Alarms

Alarms for CICM 7.0

The alarms of CICM 7.0 behave as those in CICM 6.12. However, the following are the alarms most significant to the dual-node functionality of the 7.0 CICM:

- The 2.5 alarm behavior of the VLCM applies to the 7.0 VGM. A card fault is raised if the VMG is out of service, and the CPU card's alarm light glows red when in this state.
- A chassis alarm is raised as Major if a single VMG/VLMC is out of service, and Critical if the VMGs/VLCMs on both nodes are out of service.
- The loss of a node's critical link hosting the H.248 and Unistim interfaces is raised as a card fault and a major chassis alarm. The loss of both critical adapters results in a critical chassis alarm.

Alarms overview

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 Element Manager 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 E1 system clocking) 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 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 In Service LED**

  No alarms are raised on the CICM.

- **Component Out of Service LED**

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

- **System Out of Service LED**

  One or more critical alarms have been reported.

Fan and chassis alarm monitoring

In Series 7.0, the chassis control software dynamically controls fan speed. Chassis status, including card status, fan speed, and CPU temperature, is shown on the Element Manager CICM 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 Gateway Chassis, refer to the *CPX8216A/IH4 CPX8000 Series CPX8216 and CPX8216T CompactPCI System Installation and Use*.

The following table provides the fan speed settings for different chassis error conditions.

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

Fault management procedures

Procedures for fault management are provided in the following two section: *General Troubleshooting Procedures* and *Fault Correction Procedures.*

Note: Procedures are arranged in alphabetic order for easy reference.

General troubleshooting procedures

This section contains general procedures that are useful in fault troubleshooting and correction. They are arranged in alphabetic order for easy reference.

Backup and restore procedures

The backup and restore procedures included in this section are:

- Backup a registry (manual backup with **reg backup** command)
- View the backup sets and backup logs
- Restore the registries
  Use this procedure to restore the CICM registries from backup files. This restoration process applies to registries backed up manually or by scheduled automatic backup.

Procedure 1 Backup a registry (reg backup command)

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 Backup the registry to a file by typing:

reg backup "hklm\software\nortel networks\centrexip international gateway\7.11" <backupfilename>.mib

then press Enter.

Where **<backupfilename>.mib**
is a name determined by the user for the backup file, for example: backup1.mib

Response: Verification of the backup action is displayed with the backup file name and location.

Note: The backup includes backup of all keys and information underneath that key.

3 This procedure is complete.

Procedure 2 View backup files and logs

On the CICM EM

1 The backup files backed up automatically can be viewed on the Element Manager in the following directory path: **C:\CentrexIP\Backups\<gateway_node>** where **<gatewaynode>** is the name of the CICM node.

Note: The backup files backed up manually can be viewed on the Element Manager in the directory path chosen in the **Backup a registry (reg backup command)** procedure above.

2 Within each CICM node folder the six most recent backups are saved as **backupx.mib,** where **x** is a number from 0 to 5. The files are timestamped to identify the most recent backup.

3 The backup log can be viewed on the Element Manager in the following directory path:
C:\centrexIP\backups\backupx.log

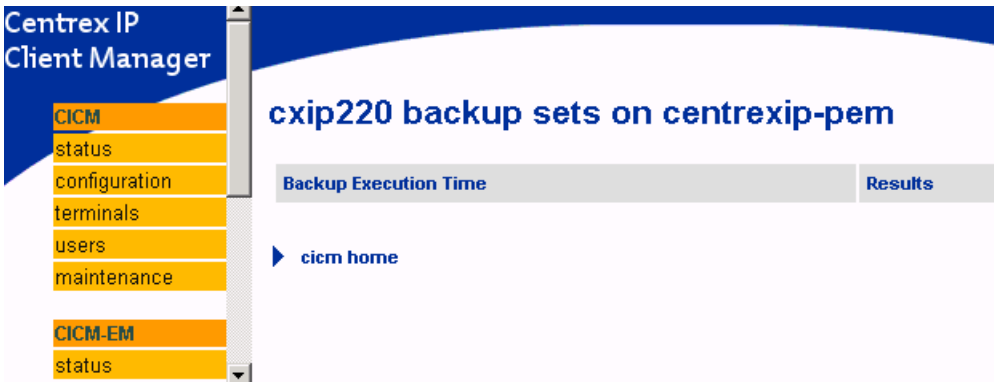
4 To view a list of the execution time of backups and the results of the backups, do:

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.*



5 This procedure is complete.

Procedure 3 Restore the CICM registries

At the CICM home page of the Element Manager web pages

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

2 Disconnect the CICM from the Element Manager.

a On the **CICM home** page on the Element Manager web pages

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

c Click on the **trash can** icon next to the CICM name to delete.

d Click **confirm deletion**.

At a PC on the administration LAN

3 Telnet to each node of the CICM. Refer to the *Telnet to a CICM node* procedure.

Response: Two Telnet windows will now be open, one for each node of the CICM.

Note: The only connection to the CICM should be the Telnet connection to each node. If any other connection exists, this Restore procedure cannot take effect.

At the Telnet command line interface

4 Identify whether the backup will be restored from an automatic backup or manual backup.

If	Do
You are restoring the registries after a manual backup	Locate the backup file and CD to the directory. Skip step 5 and proceed to step 6
You are restoring the registries from an automatic backup	Proceed to the next step.

5 Determine the most recent node backup file by:

Note: Skip this step for manual backup, since the file will already be on the CICM.

a typing in the first Telnet window

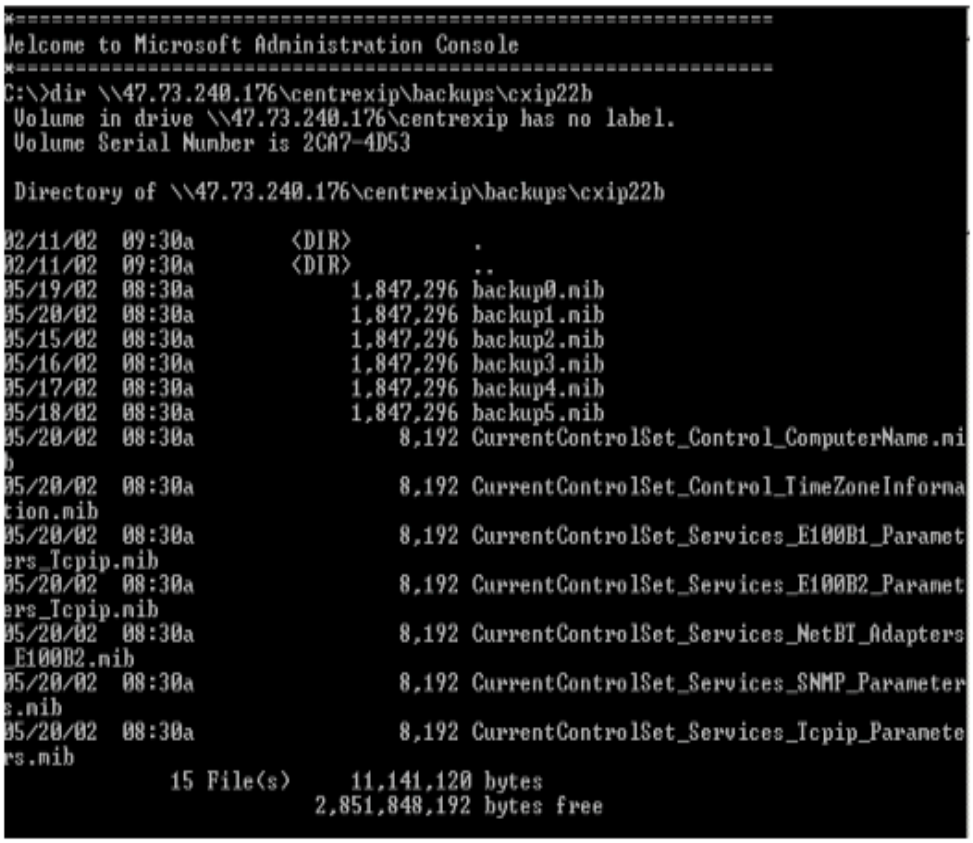
Dir <\\<Element_Manager>\backups\<node_name>>

then press **Enter**.
Where

<Element_Manager>
is the IP address or machine name of the Element Manager, and

<node_name>
is the name of the CICM node with the Telnet connection.

Response: A list of backup files is displayed (backup1.mib, backup2.mib, etc.)



b Check the timestamps on the files to determine the most recent file.

6 In the Telnet window, copy the latest backup file from the Element Manager to the CICM node by typing

copy \\<Element_Manager>\backups\<node_name>\backupX.mib
where

backupX.mib
is the most recent backup.

Note: Skip this step for manual backup, since the file will already be on the CICM.

Response: The backup file is now stored on the CICM node, ready to be restored to the node registries.

7 Repeat steps 4, 5, and 6 for the second node.

8

WARNING

This step will delete all current configuration information

In the Telnet window on each node, delete the corrupt CICM configuration registries by typing

reg delete "HKLM\Software\Nortel Networks\CentrexIP International Gateway\7.11"
Where

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

and

6.12
is the (corrupted) CICM version to be deleted.

Response: the corrupt configuration information is deleted.

9 Notify the system that you are going to restore part of the registry by typing in the Telnet window on each node, at the prompt:

reg add "HKLM\Software\Nortel Networks\CentrexIP International Gateway\7.11"

Note: There are spaces in this command line after **reg**, after **add**, after **Nortel**, after **CentrexIP**, and after **International**.

10 In the Telnet window on each node, restore the backed up configuration by typing

reg restore backupX.mib "HKLM\Software\Nortel Networks\CentrexIP International Gateway\6.12"
Where

backupX.mib
is the latest backup file identified above. This backup file must be in 8.3 MS DOS format.

11 Repeat steps 8, 9, and 10 for the second node.

12 Disconnect from the Telnet sessions: in each Telnet Window, select **Connect**, then select **Disconnect**.

At the Element Manager web pages

13 Reconfigure the SNMP parameters for the CICM.

14 Add the CICM to the Element Manager as follows:

- **a** From the **CICMs home** page of the Element Manager web pages
- **b** Click on **Change the list of CICMs stored on the CICM-EM**.
- **c** Click on **Add new CICM**
- **d** Type the name of the CICM, then click **Save new CICM**.

15 Restart the CICM. Refer to the *Start the CICM service* procedure in the *CICM Security and Administration* document.

16 This procedure is complete.

Copy files from one machine to another

Use this procedure to copy files from one machine to another. For example, copy debug logs from the Element Manager to another server that is accessible to the Nortel Networks Support Personnel for troubleshooting purposes.

Series 7.0 CXIP is configured with a folder named **Support** on the root directory of the FTP server on the Element Manager. This is the recommended location for event logs and related information since it is accessible by Nortel Networks Support/GnPS. Other locations are acceptable if they are accessible by Nortel Networks Support/GnPS to upload the files to the GnPS server.

Procedure 4 Copy files from one machine to another

At a PC on the administration LAN

1 Telnet to the CICM node that contains the logs. Refer to the *Telnet to a CICM node* procedure.

At the command line interface

2 Go to the directory where the logs are filed.

Example
D:\debuglog

3 Type
copy *.log \\<destination>\<target file>

then press Enter.

Where

destination
is the IP address of the destination machine, and

target file
is the name of the file to place the copied files in.

Example
copy *.log \\47.160.43.10\support.

Note: The recommended location for event logs and related information (to make them accessible by GnPS/Nortel Support) is the folder named **Support** on the root directory of the FTP server on the Element Manager.

4 This procedure is complete.

Manual shutdown of a node

A node may be shutdown or restarted using the EM's Maintenance page. Three scenarios may exist:

- Both nodes are running; the operator stops the slave
- Both nodes are running; the operator stops the master
- Only the master is running; the operator stops the master

These three scenarios are treated as failures of the respective nodes. No special processing is done to automatically initiate a SWACT, even though such an action may be desirable. It is the responsibility of the operator to ensure that the node is in the correct state before initiating any nodal shutdown.

Initiating the shutdown from the CICM EM (as is recommended) will result in the operator being presented with an appropriate warning message and recommended courses of action in order to minimize any impact on service.

Node failures

In the case where a node is running in standalone mode and it subsequently fails, there is no redundant node to fall back on.

In the case where both master and slave nodes are running, and one or the other node fails (the master or the slave), then there is a redundant node to fall back on.

a node failure may have a number of possible causes. 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 (i.e. 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 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 3; this variable can be configured by the operator). Following the last restart, the boot controller will not start the CICM software load.

Scenario 1: Master fails When the master node experiences an unexpected failure, the slave hot standby component detects it and automatically SWACTs to assume the role of the master. This occurs transparently to the GWC as the new master node binds H.248 address. Some inbound messages from the GWC may be lost during the takeover, but the retransmission algorithm built in to H.248 ensures that they are eventually delivered.

Terminals hosted off of the new master node (previously the slave before the failure) do not lose connectivity to the CICM and these sessions are maintained. However, during the SWACT, only stable calls are guaranteed to survive. Unstable calls may or may not survive.

Terminals hosted off of the node that fails (previously the master) do lose connectivity to the CICM as the south-side operates in a load-sharing mode and does not support hot hand-over in (I)SN07. These terminals eventually reboot and begin searching to connect to the mate node. If the terminal is on a call (stable or unstable), the call is lost.

Scenario 2: Slave fails When the slave node experiences an unexpected failure, the master hot standby component detects it, but does nothing except make note of the failure. No SWACT occurs and so no H.248 messages from the GWC are lost.

Terminals hosted off of the master node will not experience any degree of loss of service. All stable and unstable calls survive the failure on this node.

Terminals hosted off the failed node (previously the slave) again lose connectivity to the CICM. These terminals eventually reboot and begin searching to connect to the master node. If the terminal is on a call (stable or unstable), the call is lost.

Network adapter failures

LAN adapter failures on the CPU cards are treated differently from other types of failures. There are four cases that call for 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, thus maintaining call processing.

  However, the physical adapter hosting the H.248 interface usually also hosts the client LAN interface. As such, this failure scenario results in all terminals hosted on the master lose communication with the node. They then reboot, attempting to connect to the mate.

  Terminals hosted on the new master node (previously slave) remain connected to their node, but unstable calls may experience problems due to the SWACT.

- **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.

  In these cases, terminals hosted on this node lose their connection when the adapters are first lost. Communication to the terminals, and possibly to the GWC (if the node resumes its role as master) can only be re-established if the adapter hosting the client and H.248 interfaces is regained.

- **Slave loses adapter acting as backup H.248 interface**
  Should the slave node lose layer-2 connectivity on the physical adapter that would normally host the H.248 interface were it the master, the slave simply updates its own local state and advises the master node of this change. This is necessary in order to ensure that a SWACT is not inadvertently initiated either manually or autonomously. No SWACT occurs.

  Similarly to the master losing its H.248 adapter, terminals hosted on the slave node will likely lose communication with the node and will reboot, attempting to connect to the mate.

- **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.

  Terminals hosted off this node lose their connection to the node when both adapters are first lost. Communication to the terminals can only be re-established if the adapter hosting the Client LAN interface becomes available.

Powerdown/powerup the node (hard reboot)
Use this procedure to power the mate node up and down. Powerdown/powerup is comparable to turning a PC off then on. Powerdown does not do a graceful shutdown.

Procedure 5 Powerdown/powerup the node (hard reboot)

WARNING
Loss of all service
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 Telnet to the CICM node. Refer to the *Telnet to a CICM node* procedure.

At the command line interface

2 To powerdown, type **powerdown**

then press Enter.

Response:

```
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.

Response:

```
Powerdown completed
```

4 To powerup the mate node, type **powerup**

then press Enter.

Response:

```
This CPU is in domain X
Powering on domain Y processor

Powerup completed.
```

5 This procedure is complete.

Query a registry key
Use this procedure to query a particular key in the registry.

Procedure 6 Query a registry key (reg query command)

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 Type

reg query <registry key><path>

then press Enter.

Example
reg query “hklm\software\nortel networks\centrexip international gateway\7.11”

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

Example
reg query “hklm\software\nortel networks\centrexip international gateway\7.11” /s

Response: Information about the registry key is displayed.

3 This procedure is complete.

Query the state of a service
User this procedure to query the state of a service on the CICM node.

Procedure 7 Query the state of a service (sc query command)

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 Type

sc query <service name>

then press Enter.

Response: The details of the state of the service is displayed.

3 This procedure is complete.

Restart (soft reboot) the node
Use this procedure to reboot the current node. It is a soft reboot comparable to the following PC procedure:
Start > Shutdown > Restart.

Procedure 8 Restart (soft reboot) the 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 Type **shutdown /r /l /t:0 /y**

then press Enter.

Where

r
is reboot,

l
is local machine

t:0
is Time = 0 (to reboot now), and

y
is yes (to confirm)

Response: The node shuts down and automatically restarts.

3 This procedure is complete.

Restore the CICM registries

Refer to the *Backup and Restore* section above for the following procedures:

- Backup a registry (manual backup with the reg backup command)
- Backup the registries (schedule automatic backup)
- View the backup files and logs
- Restore the CICM registries

Start a service running on a node manually

Use either of the following two procedures to manually start a service running on a node. The service can be started by the **net start service** command or the **sc start service** command.

Procedure 9 Start a service running on a node manually (net start service command)

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 Type **net start <service name>**

then press Enter.

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.

Procedure 10 Start a service running on a node manually (sc start service command)

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 Type **sc start <service name>**

then press Enter.

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.

Stop a service running on a node manually

Use either of the following two procedures to manually stop a service running on a node. The service can be stopped by the **net stop service** command or the **sc stop service** command.

Procedure 11 Stop a service running on a node manually (net stop command)

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 Type **net stop <service name>**

then press Enter.

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.

Procedure 12 Stop a service running on a node manually (sc stop command)

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 Type **sc stop <service name>**

then press Enter.

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.

Trace a route

Use this procedure to display the route taken from your machine to the machine you want to connect to. If there are any routers between you and the machine, they will reply as a **hop**.

Procedure 13 Trace a route (traceroute command)

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 Type
tracert <IP address>

then press Enter.

Where

IP address
is the IP address of the machine 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.

Example

```
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.

Use a remote machine
Use this procedure to give the current machine permission to use a remote machine. For example, when you want to copy files into or from a remote machine.

Procedure 14 Use a remote machine (net use command)

At a PC on the administration LAN

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

At the DOS command prompt

2 Type

net use \\<remote_IP_address> /user:<admin_name> <admin_password>

Or
net use \\<node_name> /user:<admin_name> <admin_password>

then press **Enter**.

Example
net use \\47.165.169.85 /user:administrator centrexpassword

Note: There are spaces after “use”, before “/user:” and after <admin_name>

3 Verify that you receive the response:

```
The command completed successfully.
```

4 This procedure is complete.

Verify connectivity

Use this procedure to verify connectivity with a particular IP address or node name.

Note: **Ping** and **tracert** are the only commands that have any effect on the client LAN. No other commands are installed on the CICM.

Procedure 15 Verify connectivity (ping command)

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 Type
ping <IP address or name>

then press Enter.

Where

IP address
is the IP address of the machine to check connectivity to, and

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

Example
ping 47.160.168.173

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 use **Crtl+c** to stop.

Example
ping 47.165.168.173 -t

4 If you know the IP address of the machine 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.

View details of a service
Use this procedure to view the details about a service on the CICM. This includes information on the dependencies a service has in order for the service to start.

Procedure 16 View details of a service (sc qc command)

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 Type

sc qc <service name>

then press Enter.

Response: The details about the service is displayed, including a list of dependencies.

3 This procedure is complete.

View CS2K logs
Use this procedure to view CS2K logs, using the LOGUTIL command. Logs associated with the CICM are identical to the logs that the CS2K normally generates for RLCMs/IRLCMs.

Procedure 17 View CS2K logs (LOGUTIL)

At the LMM interface

1 Type **LOGUTIL**

then press Enter.

2 Type **open PM**

to view the last Peripheral Module (PM) log generated.

Or type **open PM <log number>**

to view a specific PM log.

Then press Enter.

Response: Logutil output will display the latest log created.

3 To view earlier logs, type **back n**

then press Enter.

Where

n
is the number of earlier logs to view.

4 This procedure is complete.

View error message detail
Use this procedure to view the details of an error message.

Procedure 18 View error message details (net helpmsg command)

At a PC on the administration LAN

1 Open a Telnet session to one of the CICM nodes.

At the command line

2 Type **net helpmsg <error code>**

then press Enter.

Response: The error message definition is displayed.

3 This procedure is complete.

View executables running on a node

Use either of the following two procedures to view a list of executables running on a node. Both commands produce the same list of executables, but the **pulist** command includes the username that the executable runs with.

Procedure 19 View executables running on a node (pulist command)

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 Type

pulist

then press Enter.

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

3 This procedure is complete.

Procedure 20 View executables running on a node (tlist command)

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 Type

tlist

then press Enter.

Response: The list of executables running on the node is displayed.

3 This procedure is complete.

View IP configuration

Use either of the next two procedures to view the IP configuration for all adapters on the node. The procedures will display the two public

administration addresses, the private administration address and the client address.

Use procedure 22 to view IP configuration using the EM web interface, or use procedure 23 to view IP configuration by using a Telnet session.

Procedure 21 View IP configuration (EM web interface)

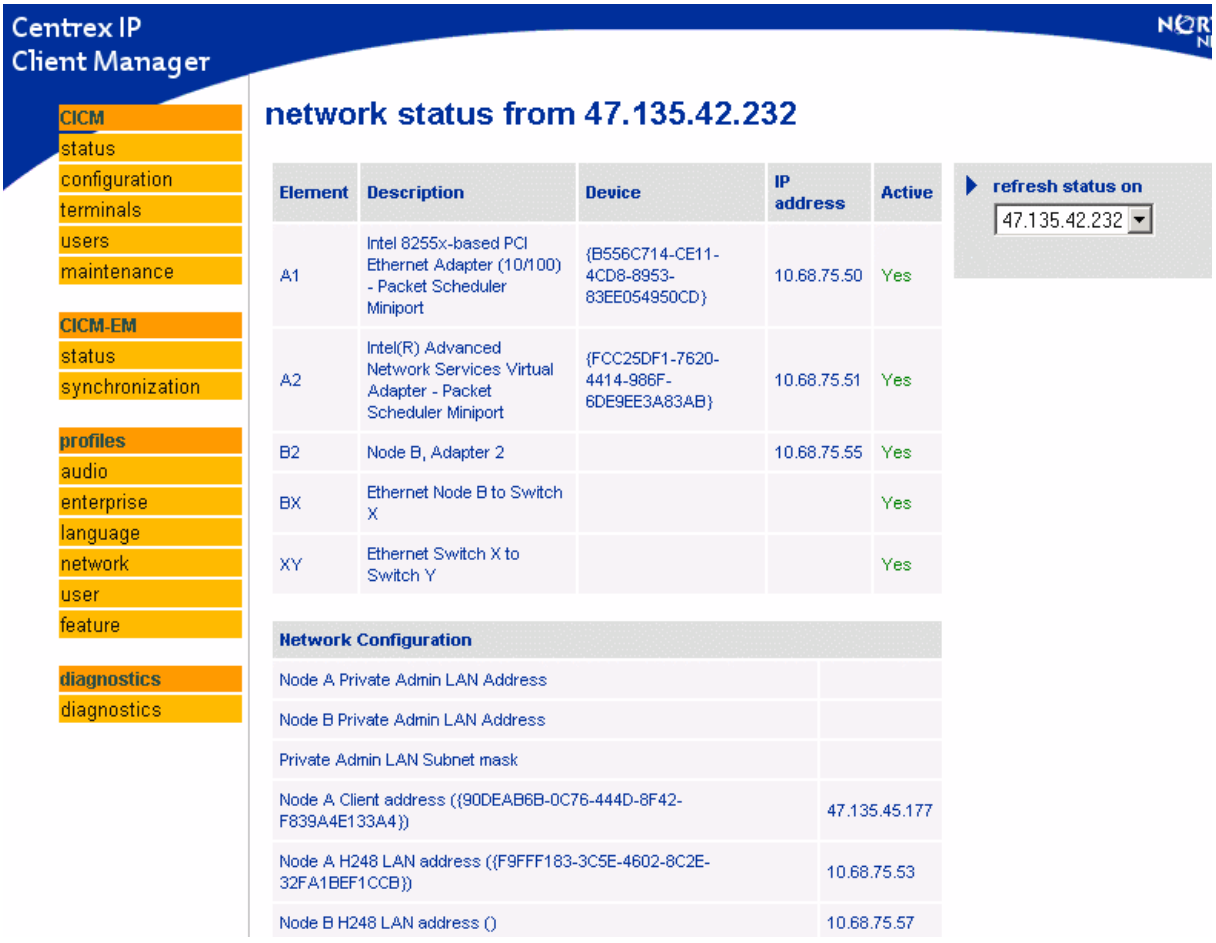
At the CICM Home Web page

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

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

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

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



3 This procedure is complete.

Procedure 22 View IP configuration (ipconfig /all command)

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, type **ipconfig /all**

then press Enter.

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

3 This procedure is complete.

View members of a group
Use this command to view the list of members of a particular group.

Procedure 23 View members of a group (net localgroup command)

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 Type **net localgroup <group name>**

then press Enter.

Where

<group name>
is the name of the group you want to view.

Example
net localgroup administrators

Response: The list of members of the group is displayed.

3 This procedure is complete.

View network configuration
Use the **net config workstation** command to view the network configuration of a user's workstation.

Procedure 24 View network configuration (net config workstation

command)

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 Type **net config workstation**

then press Enter.

Response: The network configuration information for the workstation displays.

3 This procedure is complete.

View servers in a network
Use this command to view a list of servers in a network.

Procedure 25 View servers in a network (net view command)

At a PC on the administration LAN

1 Telnet to the CICM node.

At the command line interface

2 Type **net view**, then press **Enter**.

Response: A list of servers on the network is displayed.

3 This procedure is complete.

View services running on a node
Use this procedure to view the services running on a node. This is a good indicator of the health of the node.

Procedure 26 View services running on a node (net start command)

At a PC on the administration LAN

1 Telnet to the CICM node.

At the command line interface

2 Type **net start ,** then press **Enter** .

Response: Displays a list of the services running on the node.

3 This procedure is complete.

Fault correction procedures

Card fault and recovery guidelines

Prior to attempting any fault recovery, use the *Event Viewer procedures* in the *Security and Administration* document to retrieve the event and debug logs from both nodes of the CICM. This helps Nortel Support personnel to identify the source of a failure.

Following is a table listing the effects of a specific card failure and the relevant recovery process to apply.

Table 1 Card fault and recovery guidelines

Fault Type	Effect	Recovery
Loss of CPU LAN connection to Client/Port A	• Clients connected to the affected node will reboot and connect to the mate node. • All active calls using this node will be dropped. • A failure alarm will be triggered.	Recover the LAN connection. Resolution of the LAN failure will allow the client to reconnect with this node.
Loss of CPU LAN connection to OSS/Port B	• Connectivity to the EM for this node will be lost, preventing status updates being relayed to the EM. • A failure alarm will be triggered.	Recover the LAN connection. Resolution of the LAN failure will allow connectivity to be restored to the EM.

Table 1 Card fault and recovery guidelines

Fault Type	Effect	Recovery
Loss of both CPU LAN connections on one node.	• Clients connected to the affected node will reboot and connect to the mate node. • All active calls using this node are dropped. • Connectivity to the EM for this node is lost, preventing status updates being relayed to the EM. • A failure alarm is triggered.	Recover the LAN connection. After the resolution of the LAN failure, the affected node will determine that it is out of sync with its mate node and reboot.
Loss of CPU card	• Clients connected to the affected node will reboot and connect to the mate node. • Connectivity to the EM for this node is lost, preventing status updates from being relayed to the EM. • The CS2K indicates that VMGs with units on this node are OOS. Calls for this CICM will be routed via the mate node. • All active calls using this node are dropped. • A failure alarm is triggered. • On a node with multiple CPU cards, when one CPU card is out of service, the CICM continues to function, but with a reduced call capacity. This is due to the reduced capability for load sharing.	• Telnet to the CPU card and issue the **shutdown** command. Refer to the *Start a service running on a node manually (net start service command)* procedure in this *Fault Management* document. • If the shutdown cannot be achieved, Telnet to the mate node and perform the *Powerdown/powerup the node (hard reboot)* procedure in this *Fault Management* document. • If the node reboots successfully, the VMGs will be brought into service, allowing calls to be made over the node. If the node does not come into service, additional troubleshooting will be required to determine whether the CPU card has failed or the associated hard disk is faulty.

CPU card troubleshooting

Use this procedure for troubleshooting CPU card faults. See also the *Card Fault and Recovery Guidelines*.

Procedure 27 CPU card troubleshooting

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 Procedure 6, *Powerdown/powerup a node (hard reboot)*, above.

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

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

a Perform the *Powerdown/powerup a node (hard reboot)* procedure to check if the same thing happens on reboot

b If the display is the same blue with NT 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 blue with NT boot information displayed, the OS has booted successfully.

a If you have just re-imaged the node, 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.

b If you have not just re-imaged the node, it is possible that the wrong ethernet ports have been enabled on the CPU card. If the ethernet cables are connected to the front, try moving the cables to the TM card at the back. If they are connected to the back TM card, try moving them to the front.

c If there is no response to any of the expected IP addresses, a CPU card hardware failure could be indicated. Before replacing the CPU card or hard disk, busy the VMG from the CS2K console to ensure that the VMGs are taken out of service correctly. Refer to the *Card Replacement* procedure in this document.

7 This procedure is complete.

Card replacement

Use this procedure to replace the faulty card from the CICM chassis with minimal service interruption. It applies to the replacement of CPU, Hot Swap Cards (HSC), and transition modules (TMs).

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

Note: Testing of faulty card shall be performed by Nortel Networks Support only.

Before using this procedure, the faulty card should already be identified and a replacement card and its TM ordered and received. Before replacing the faulty component, make note of the correct slot and make sure the replacement card has the same PEC code as the faulty card being replaced, as indicated in the following table.

Nortel PEC	Name
NTRX51VB	5370 CPU
NTRX51VC	5370 Transition Module
NTAR02JY	HSC Card
NTRX51VY	DSP TP610
NTRX51VZ	DSP TP610 Transition Module
NTRX51VP	E1/T1 NS300
NTRX51WP	E1/T1 NS301

It is recommended to replace the Transition Module for each CPU card that is replaced. The CPUs card and TMs 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/

Procedure 28 Card Replacement (CPU, TM or HSC)

STOP
CICM Gateway Hardware Warranty
This procedure only describes how to replace a CICM hardware component. Do not attempt to open or disassemble any CICM hardware modules. Failure to comply with this requirement may damage the hardware and void the hardware warranty.

CAUTION
System Damage
Do not attempt to insert any hardware module that is not included in the original design of the CICM. Extra modules may confuse the system and degrade the CICM service, or damage the system.

WARNING
Static Electricity Damage
An electrostatic discharge (ESD) grounding wristband must be worn and connected to the CICM cabinet at all times during this procedure. This protects the hardware against damage caused by static electricity.

At the LMM interface

1 *(OPTIONAL)*

Note: This step is not essential, because the VMGs/VLCMs will come into service automatically. However, it may speed up the process of bringing the VMGs/VLCMs into service after the card replacement.

Busy the VMG/VLCM units on the CS2K, using standard CS2K procedures.

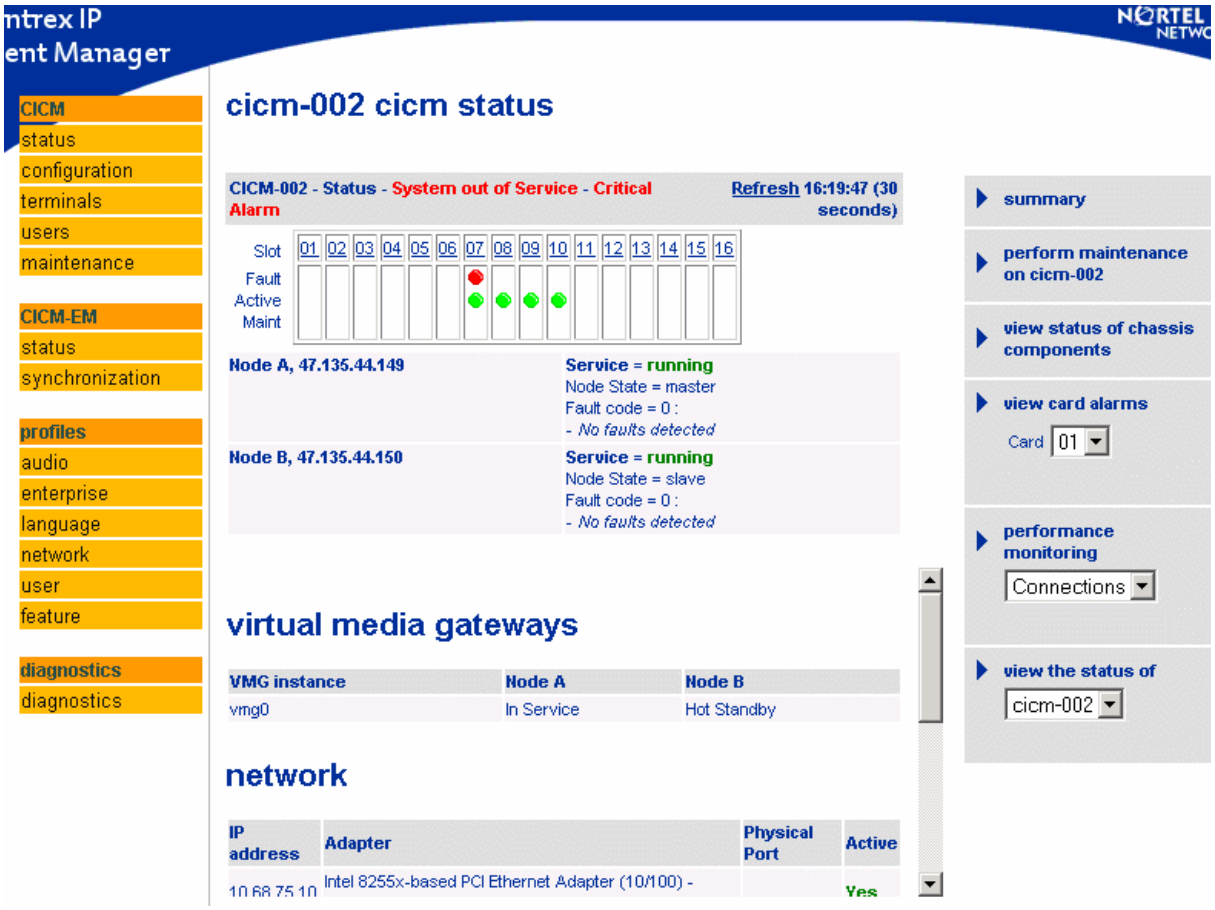
At the CICM EM web pages

2 **Perform a terminal handover** to transfer service from the node containing the card to be replaced. Do the *Perform Terminal Handover* procedure in this document through step 6, *Verify the terminal service has stopped*.

3 Stop the CICM service on the node to be powered down (i.e. the node containing the card to be replaced), as follows:

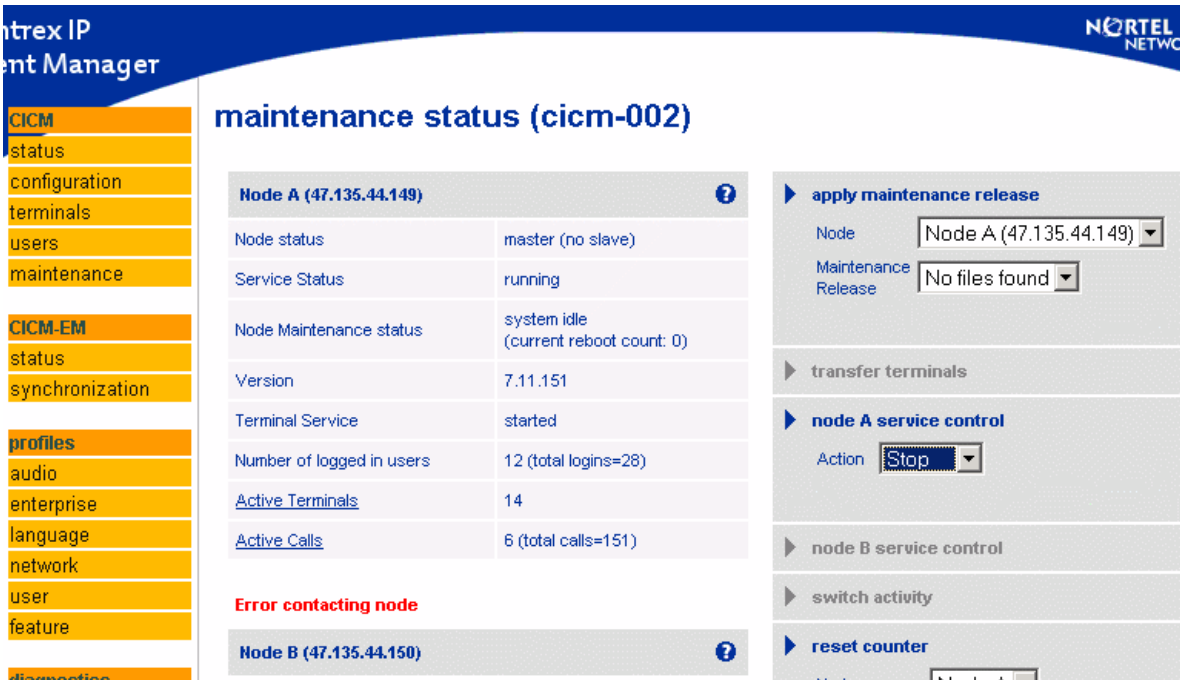
Example
If the faulty card is on node B, you will stop the CICM service on node B.

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



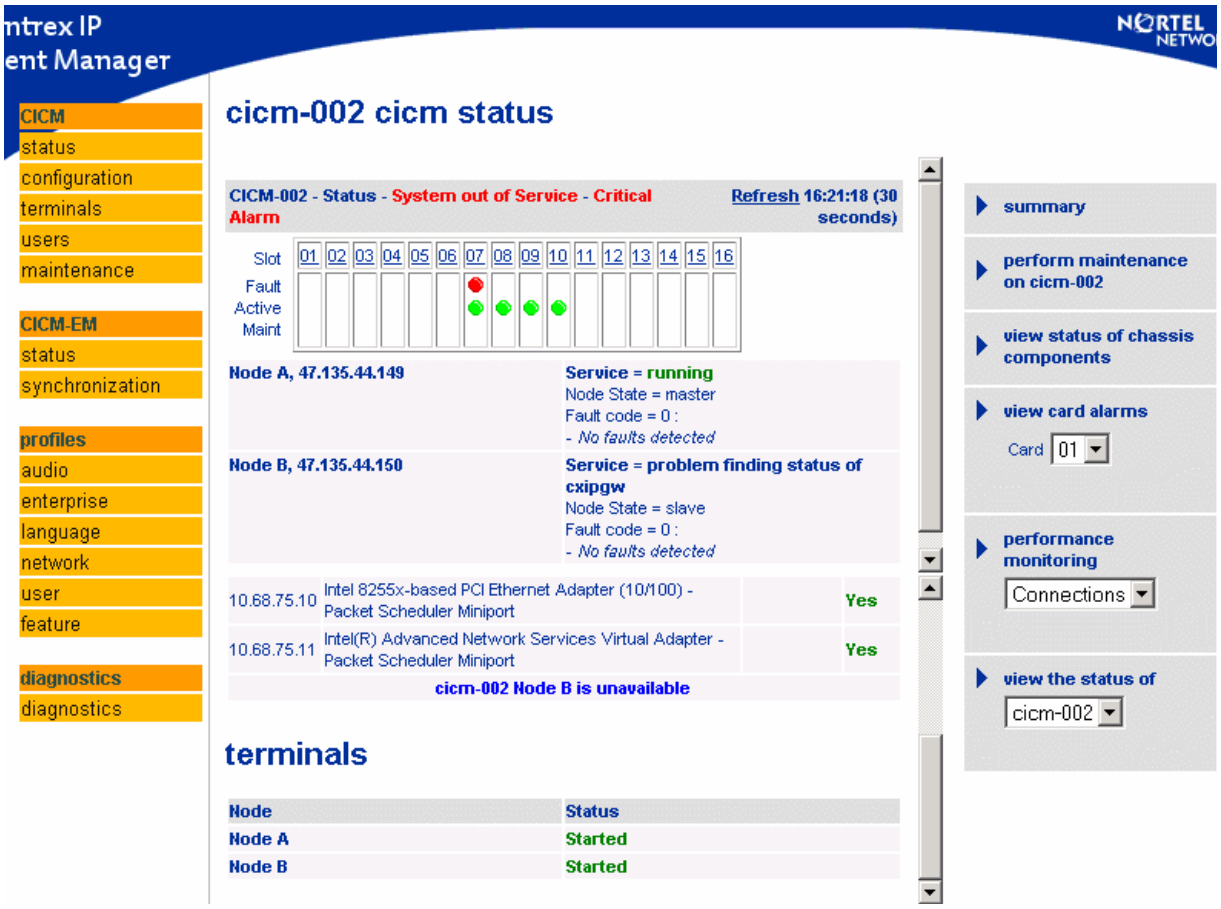
b Click on the **perform maintenance on cicm_name** option on the right menu.

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**.*



4 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 type the following on the command line:

C:\>**shutdown /l /t:0**

Then press **Enter**

Response: A request for confirmation is displayed.

b To confirm the shutdown of the node, type

y

then press **Enter**

Response: A confirmation of the shutdown completion is displayed.

5 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 type the following on the command line:

C:\>**powerdown**

Then press **Enter**

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 To continue to powerdown the node, press **Enter**

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

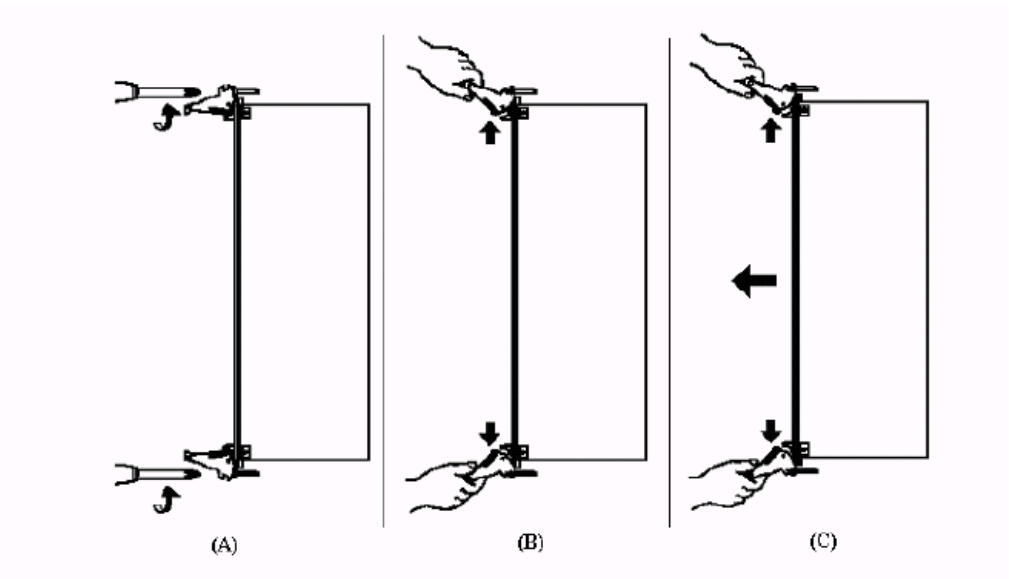
6 Verify that the faulty node is powered down by checking on the LED indicator panel (on the physical device) that all LEDs on the CPU card are off, including the PWR LED.

Example
If the faulty card is on node B, check the physical LED panel for node B.

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

8 Remove the faulty card from the chassis as illustrated in the following figure.

Note: For each CPU card removed, remove the main 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.

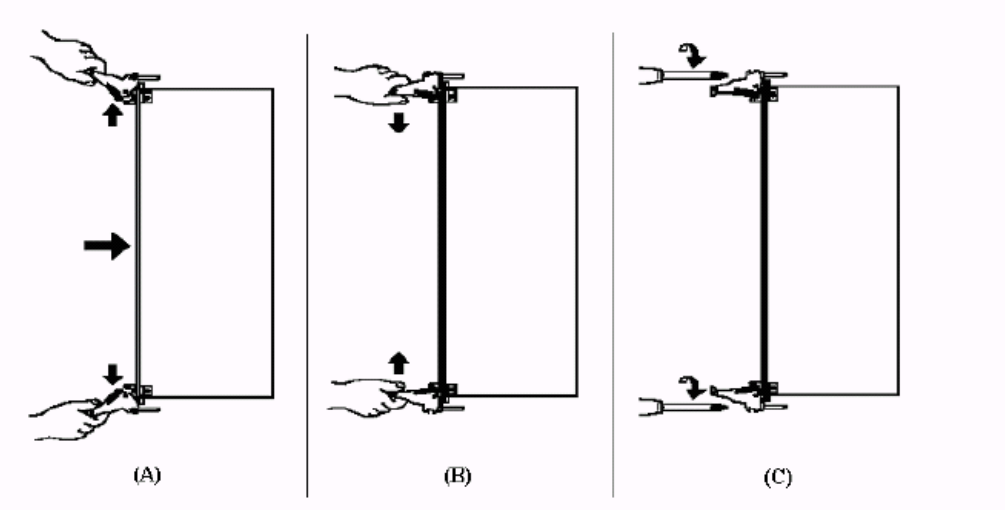
9 If a CPU card is being replaced, connect a suitable PC monitor and keyboard to the card or TM prior to inserting.

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 *Check the BIOS of a new CPU card* procedure below.
If the powerdown command in step 5 did succeed	Proceed with this procedure through step 13, then check the BIOS settings as directed.

10 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.

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

12 If the node was successfully powered down from the mate node in step 5, issue the powerup command from the mate node now 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, type the following:

C:\>**powerup**

Then press **Enter**

Response:

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

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

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

13

IF	DO
An HSC was replaced	Continue with the next step and complete this procedure.
A CPU card was replaced	Skip the remainder of this procedure and immediately check the BIOS settings. Refer to the following procedure, *Check the BIOS of a CPU card*.

14 *(REQUIRED ONLY IF STEP 1 WAS COMPLETED)*

If the VMG unit was busied in step 1, return the VMG unit to service as soon as the **<cicm_name> cicm status** page shows the service is running on the upgraded node.

15 Verify that the service has started correctly.
On the **<cicm_name> cicm status** page of the Element Manager 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.

16 This procedure is complete.

Check the BIOS of a new CPU card

Perform this procedure as soon as a CPU card has been replaced (from step 13 of the *Card Replacement* procedure above).

Procedure 29 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 NT 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, type the following:

C:\>**powerdown**

Then press **Enter**

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, type the following:

C:\>**powerup**

Then press **Enter**

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

Note: *The service of the node will be recovered in 15-20 minutes.*

5 (REQUIRED ONLY IF THE VMG UNIT WAS BUSIED.)

If the VMG unit was busied, return the VMG unit to service as soon as the **<cicm_name> cicm status** page shows the service is running on the node that was out of service.

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

7 This procedure is complete.

Node is stopped fault correction

Procedure 30 Node is stopped fault correction

CAUTION
Loss of service

Under no circumstances should the **Restart** button be used without Nortel Support direction.
This procedure shall only be performed under Nortel Support direction.

On a PC connected to the Administration LAN

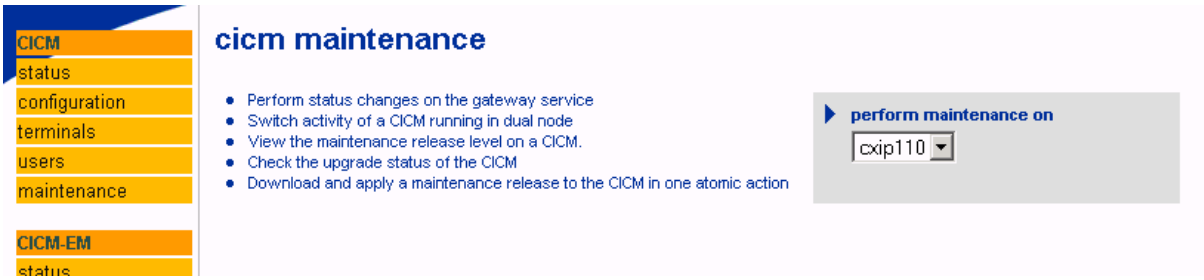
1 Open a Telnet session and attempt to connect to the stopped node.

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

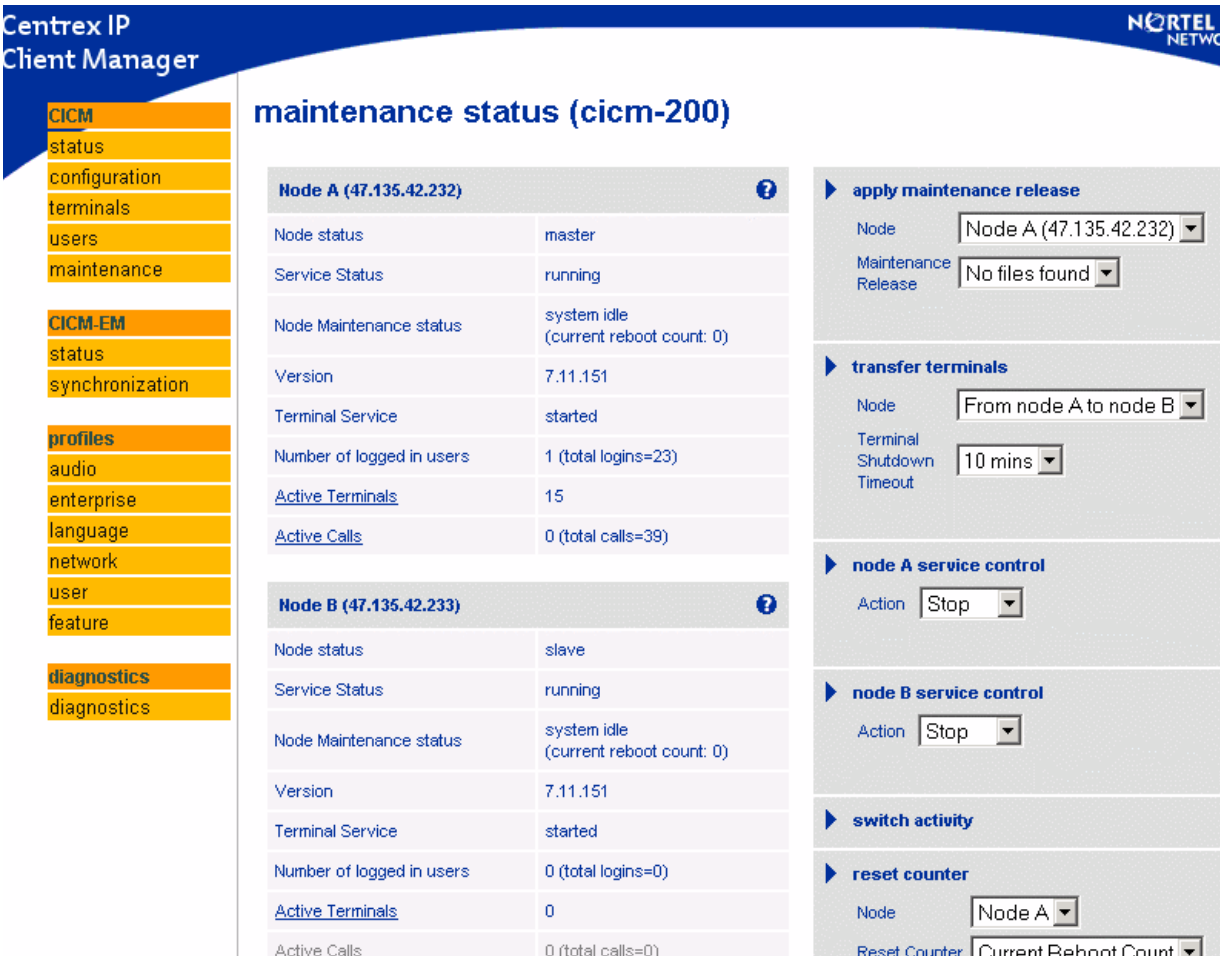
2 From the **CICM home** page, select **maintenance** from the left menu.

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



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

*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** menu option on the right menu (whichever node is applicable) ***Note:*** Perform this step only under Nortel Networks 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.

Node not connected fault correction

Procedure 31 Node not connected fault correction

CAUTION
Loss of service

Under no circumstances should the **Restart** button be used without Nortel Support direction.
This procedure shall only be performed under Nortel Support direction.

On a PC connected to the Administration LAN

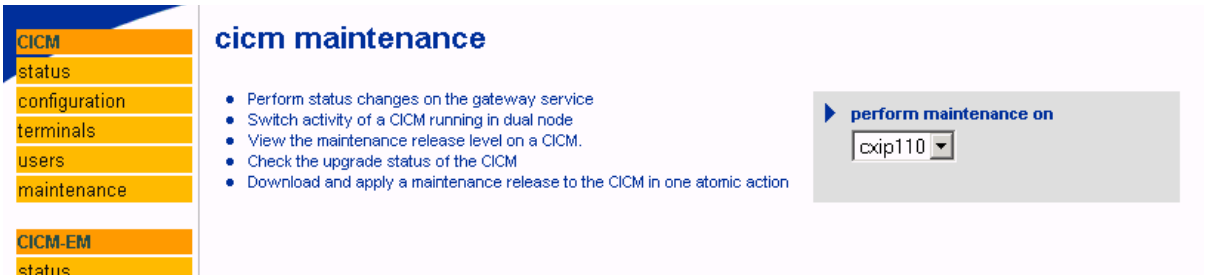
1 Open a Telnet session and attempt to connect to the disconnected node.

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

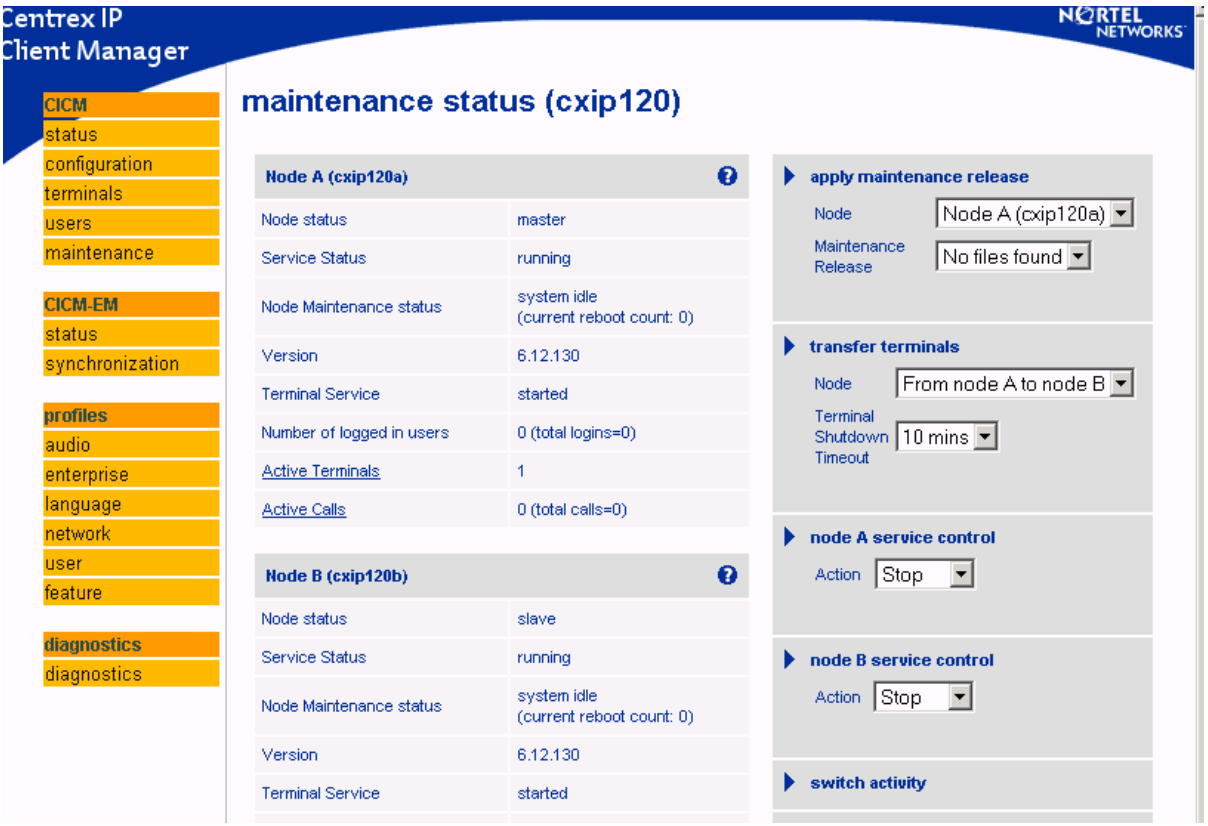
2 From the **CICM home** page, select **maintenance** from the left menu.

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



3 Select the CICM from the drop-down menu in the **perform maintenance on** option 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** menu option on the right menu (whichever node is applicable) ***Note:*** Perform this step only under Nortel Networks 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.

VMG faults

Use the following procedure to view if a VMG service state is **out of service**, and restart the service.

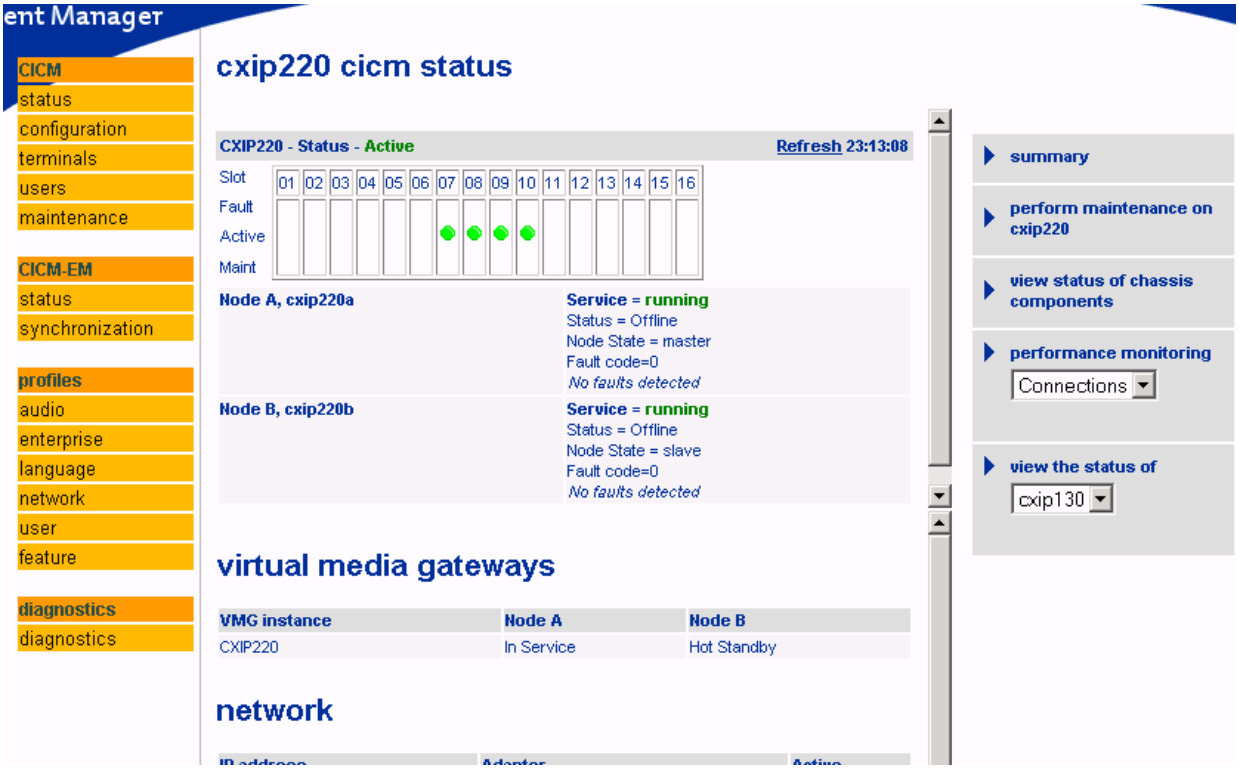
If the **<cicm_name> CICM Status** page indicates that the VMG is **stopped**, it is likely due to a node being stopped. Go to the *Node is stopped fault correction* procedure to correct the fault.

Procedure 32 VMG out of service fault correction

At the CICM home web page

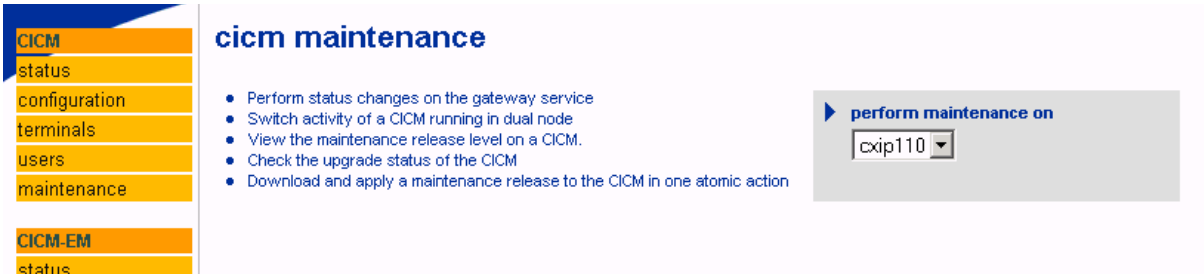
1 View the **service state** of the VMG.
From the **cicm home** page, select the CICM to view from the drop-down menu in the **view the status on the following CICM** option on the right menu.

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



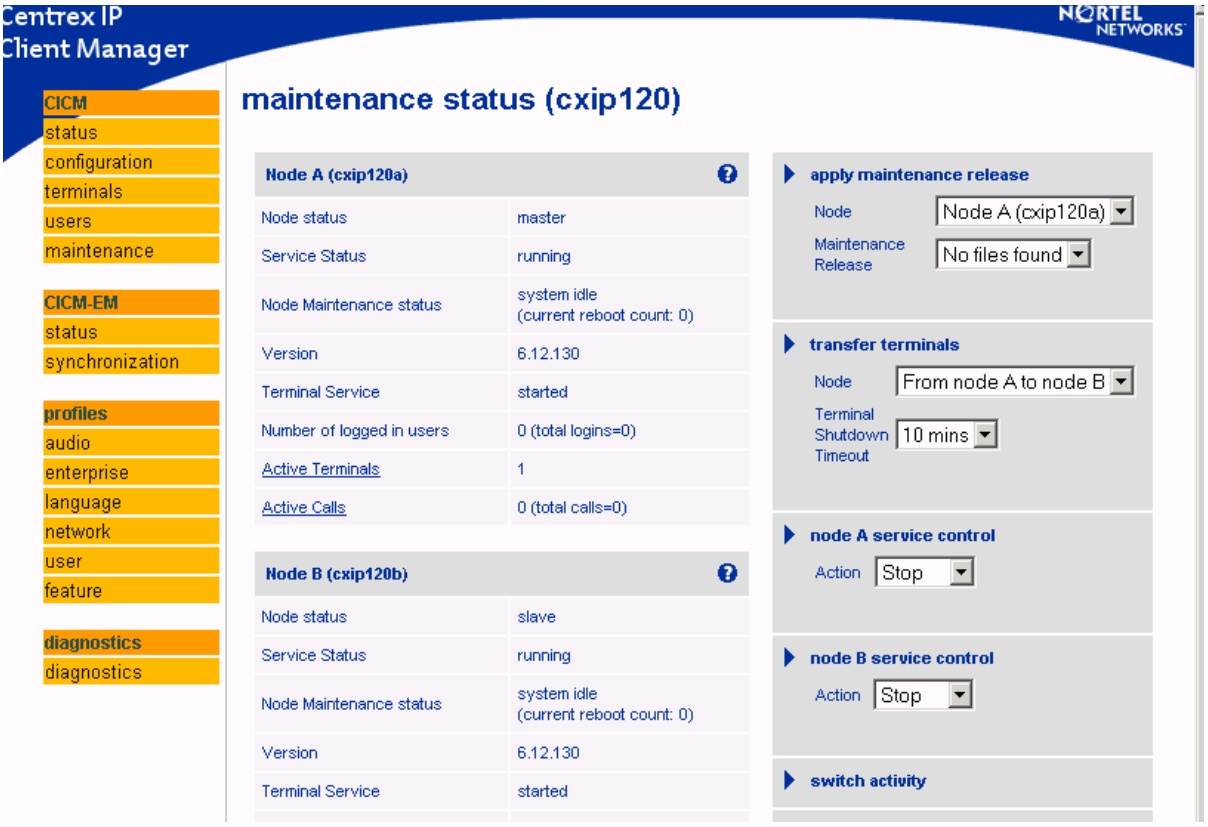
2 If the **<cicm_name> cicm status** page indicates that the VMG is **stopped**, it is likely due to a node being stopped.
To restart the node:
Select **maintenance** from the left menu.

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



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

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



4 View the **Service 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 Networks 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.

Replace Hot Swap IDE Hard Disk Drive Module

Use Procedure 34 to remove the Hot Swap IDE Hard Disk Drive Module from a Motorola SAM16 chassis for the CICM, then use Procedure 35 to install the replacement module.

Procedure 33 Remove the Hot Swap IDE Hard Disk Drive Module

WARNING
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.

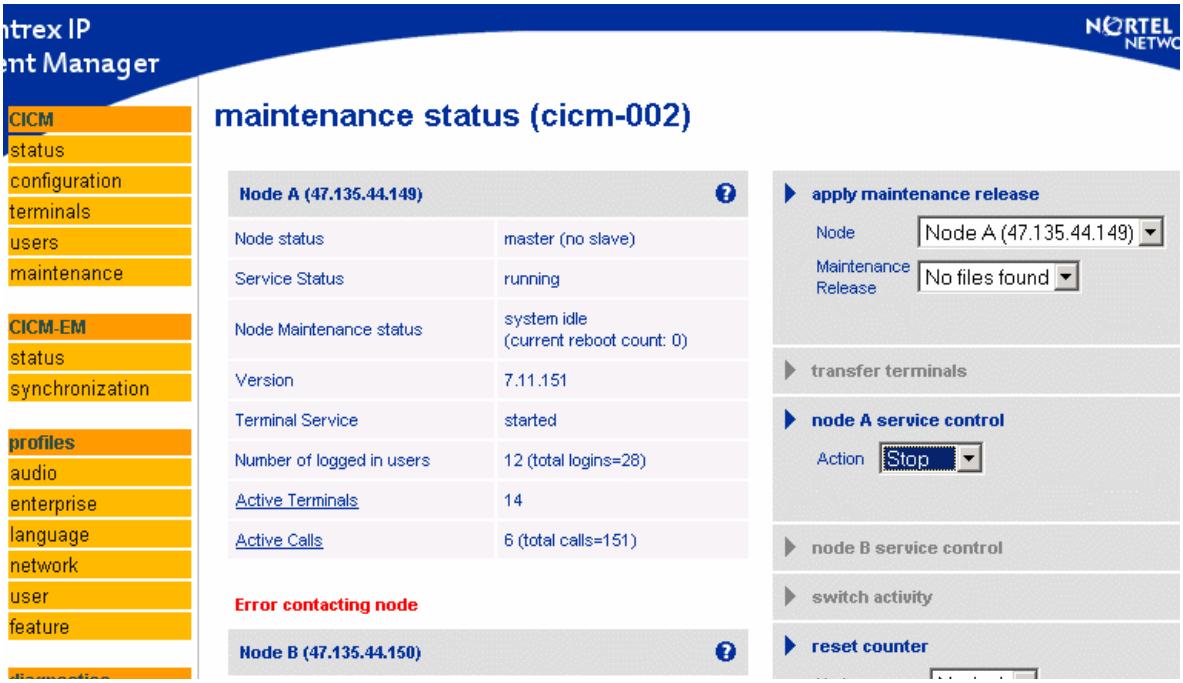
At the CICMs home page of the CICM-EM web site

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

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

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

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



3 In the **node A/B service control** option 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.

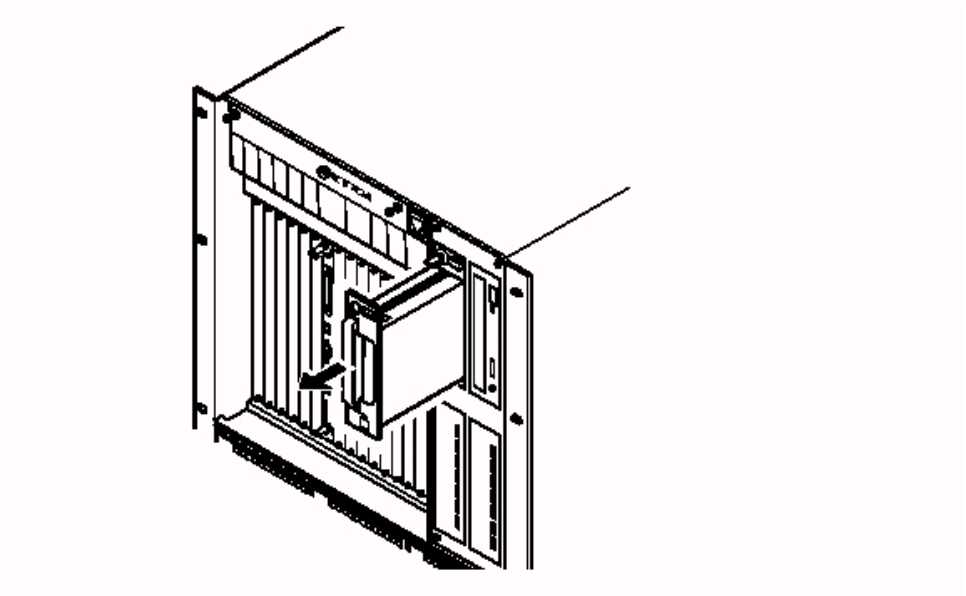
Note 1: Do not reboot the CICM node at step 13 in the *Disk Backup of CICM Node* procedure.

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

WARNING: 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.



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 End of Procedure.

Procedure 34 Install the Hot Swap IDE Hard Disk Drive Module

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.
Connect 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

Wire color	Configuration	DIP Switch
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 Networks Support for assistance.

8 End of Procedure.

Replace Non-Hot Swap CDROM/DVD Drive Module

Use Procedure 36 to remove the Non-Hot Swap CDROM/DVD Drive Module, then use Procedure 37 to install the replacement module in a Motorola SAM16 chassis for the CICM.

Procedure 35 Remove the Non-Hot Swap CDROM/DVD Drive

Module

WARNING

This step causes a complete outage of the CICM. 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 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 the **node A service control** option 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.

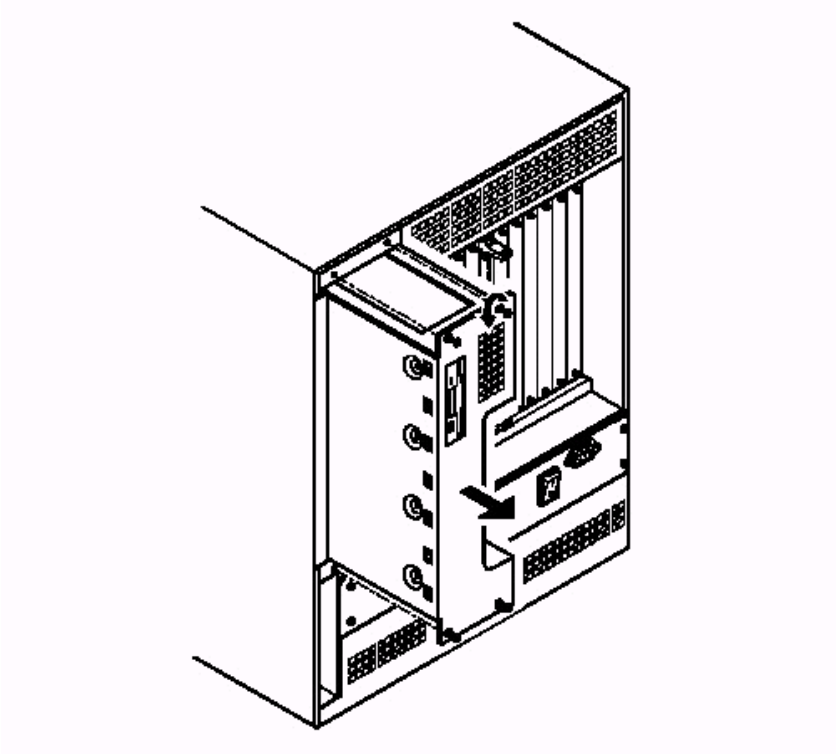
5 Back up the contents of the hard disk using the Backup and Restore Tool. Use the procedure *Disk Backup of CICM Node* in the *Method of Procedure (MOP) for Disk Backup and Restoration,* which can be found on the *Backup and Restore Tool* CD. Use this procedure to take an image of the hard disks on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

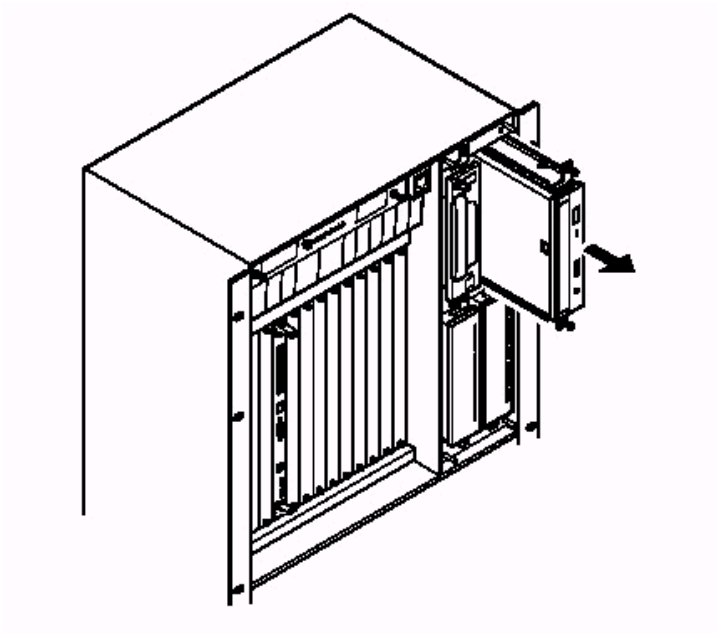
7 Remove floppy drive housing.
Loosen the four screws holding the floppy drive housing and pull it carefully out of the chassis, as illustrated in the following figure. Then detach the cables from the floppy drive housing, making a note of where they connect, and put the housing to one side.



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.



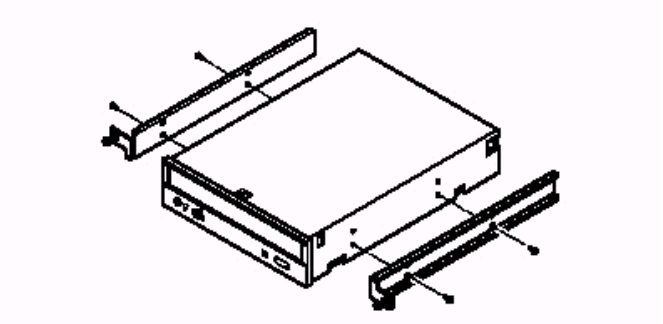
11 End of Procedure.

Procedure 36 Install the Non-Hot Swap CDROM/DVD Drive Module

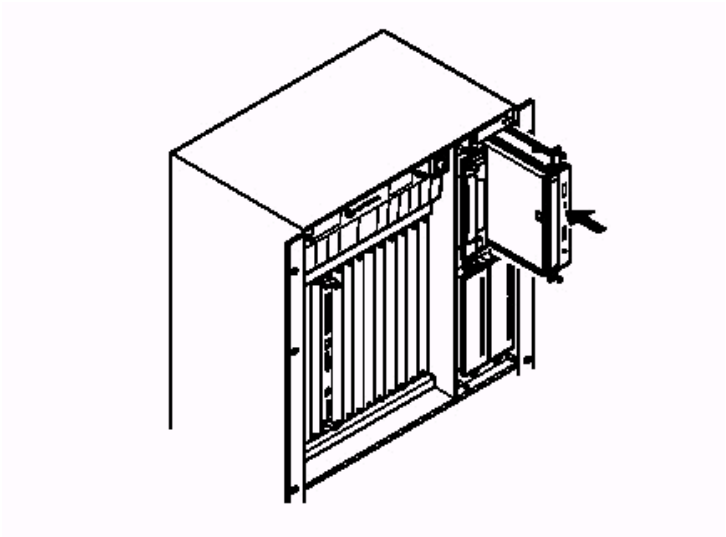
At the CICM chassis

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 EM that everything is OK.

8 End of Procedure.

Glossary

Acronym	Definition
CICM	Centrex IP Client Manager
DIP	Dual Inline Pole
EM	Element Manager
IDE	Integrated Drive Electronics
LED	Light Emitting Diode