Carrier VoIP

CICM Fault Management

NN10233-911

Document status: Standard
Document version: 06.04
Document date: 20 October 2006

Contents

New in this release

The following sections detail what's new in CICM Fault Management (NN10233-911) for (I)SN09U.

Features

Release (I)SN09U contains no feature updates.

Other changes

See the following sections for information about changes that are not feature-related:

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-EM). 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).

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

Centrex IP Client Manager (CICM) nodes can be run on a SAM16 or SAM21 hardware platform. CICM Element Manager (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 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 restart and connect to the SRG. The SRG acts as a basic call server to route calls between terminals on the local network.

Refer to "Alarms for CICM" (page 9) for a description of the alarm light-emitting diode (LED) behavior for SAM16 cards.

Software resilience

Only the core components of the operating system for which reliability has been tested and proved definitively, are used. No graphical user interface is provided. This reduces the number and complexity of the components running on the system, which reduces 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 Centrex IP Client Manager (CICM) software.

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

Backup and restore capabilities

Centrex IP Client Manager (CICM) products can have their software configuration restored from backup files rather than manually re-configuring an entire node. See "Restoring CICM-EM or CICM node configuration" (page 71) for a description of the restoration capabilities.

User interfaces for CICM

The basic user interfaces for Centrex IP Client Management (CICM) fault management are:

- a Web-based CICM Element Manager (CICM-EM) interface
- a Web-based interface through the integrated element manager system (IEMS)
- a secure Telnet (SSH) session for CICM-EM
- a secure session for CICM nodes through the **`cicmconnect`** command

Interfacing through the Web-based CICM-EM

This interface uses a Web browser to access the Centrex IP Client Management Element Manager (CICM-EM) Web pages. Through the Web pages you can:

- 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 Administration and Security* (NN10252-611).

Interfacing through the IEMS

The integrate element management system (IEMS) provides access to the Centrex IP Client Management Element Manager (CICM-EM) and CICM node Web pages. IEMS also collects and stores CICM traps and system logs where they can be monitored. IEMS is the main interface to voice over IP (VoIP) networks.

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 secure Telnet (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 power 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 technical support personnel
- perform other troubleshooting activities

Alarms for CICM

Centrex IP Client Management (CICM) alarms indicate operating faults with the hardware or software of the CICM nodes or the CICM Element Managers (CICM-EM) on the SAM16 or SAM21 hardware platforms. The status of hardware is indicated by light emitting diodes on the chassis. 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:

- add an entry to the CICM debug log
- add an entry to the CICM event log
- send an SNMP trap
- raise an alarm with a severity of critical, major, or minor

All of the current active alarm states are viewable from the CICM-EM Web pages. CICM 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 the CICM-EM is hosted in a SAM21, light-emitting diodes (LED) are controlled by the SAM21 Shelf Controller and the behavior is different.

- "Alarms overview of CICM hardware" (page 10)
- "Domain control" (page 11)
- "Telco alarm LEDs" (page 11)
- "System status LEDs" (page 11)
- "Fan and chassis alarm monitoring" (page 12)

With the SAM16 platform, the A and B nodes are installed in different chassis. For example, CICM-001A and CICM-002B are in one chassis while CICM-001B and CICM-002A 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 Centrex IP Client Management (CICM) chassis through a series of light-emitting diodes (LED) on the CICM front panel. This physical alarm panel is reproduced on the CICM-EM Web page 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 that occur in the physical hardware state, for example the loss of a mate node, is reported as a fault alarm above the corresponding CompactPCI card.

This alarm panel displays three status conditions: Active, Maintenance, and Fault. After 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 light emitting diodes (LED). 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 assumes failure. In this case, the Component out of Service LED, and a Major alarm LED, is illuminated.

Because Domain A controls the alarm panel, if Domain A is down, there are no alarms available on the chassis. However, the Centrex IP Client Management Element Manager (CICM-EM) virtual alarm panel is still correctly updated.

The Fault, Active, and Maintenance LED 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 light-emitting diodes (LED) signal faults on Centrex IP Client Management (CICM) cards and components. Minor, major, and critical alarms are consistent with Call Server 2000 alarms, and are defined as:

- **Minor**

  A minor chassis alarm is raised when one domain is reporting a minor alarm.

- **Major**

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

- **Critical**

  A critical chassis alarm is raised 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 light-emitting diodes (LED) signify:

- **System Out of Service**

  One or more critical alarms have been reported.

- **Component Out of Service**

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

- **System In Service**

  No alarms are raised on the Centrex IP Client Management (CICM) node.

Fan and chassis alarm monitoring

Beginning with release SN08, the chassis control software dynamically controls fan speed. Chassis status, including card status, fan speed, and CPU temperature, is shown on the Centrex IP Client Management Element Manager (CICM-EM) Status Web pages.

For fan replacement in the CICM chassis, refer to the Motorola documentation and procedures at 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*.

"Fan speed settings" (page 12) lists the chassis error conditions.

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

CICM-EM and CICM node fault management troubleshooting procedures

Follow these procedures to troubleshoot the Centrex IP Client Management Element Manager (CICM-EM) or CICM nodes.

Navigation

- "Accessing a CICM-EM or CICM node" (page 17)
- "Querying a registry key" (page 19)
- "Querying the state of a service" (page 21)
- "Restoring the CICM node registries" (page 73)
- "Retrieving logs from a CICM-EM or a CICM node" (page 23)

- "Tracing a route" (page 25)
- "Troubleshooting a CPU card" (page 27)
- "Verifying IP network connectivity" (page 31)
- "Viewing CS2000 logs" (page 33)
- "View executables running on a node" (page 35)
- "View adapter configuration" (page 41)
- "Viewing the network configuration" (page 43)

Hardware fault management guidelines and correction procedures

Use the information in "Card fault and recovery guidelines" (page 13) to determine your actions if the procedures in "Troubleshooting a CPU card" (page 27) do not resolve the problem.

Nortel technical support personnel may ask you to gather the information in listed in the table, to help to identify the source of a failure.

Before you attempt any fault recovery, use the *Viewing...* procedures in *CICM Administration and Security* (NN10252-611) to retrieve the event and debug logs from both CICM nodes.

Card fault and recovery guidelines

Fault type	Effect	Recovery
Loss of CPU LAN connection to Client/Port A	• A failure alarm is triggered. • If this is the master node, an automatic switch activity (SWACT) occurs to make the slave node the master while it becomes the slave. • Active calls stay in service. • The CICM node is running without redundancy (backup).	Recover the LAN connection. The new slave is fully available. CICM node redundancy is restored.
Loss of CPU LAN connection to OSS/Port B	• Connectivity to the CICM-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 CICM-EM.

Fault type	Effect	Recovery
Loss of both CPU LAN connections on one node	• A failure alarm is triggered. • If this is the master node, an automatic SWACT occurs to make the slave node the master while it becomes the slave. • Active calls stay in service. • The CICM node is running without redundancy (backup). • Connectivity to the CICM-EM for this node is lost, preventing status updates being relayed to the EM.	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	• A failure alarm is triggered. • If this is the master node, an automatic SWACT occurs to make the slave node the master while it becomes the slave. • Active calls stay in service. • The CICM node is running without redundancy (backup). • Connectivity to the CICM-EM for this node is lost, preventing status updates being relayed to the EM.	Follow one of these procedures: • Troubleshooting a CPU card in a SAM16 • Troubleshooting a CPU card in a SAM21

Correction procedures

Follow the procedures listed here, to troubleshoot Centrex IP Client Management (CICM) hardware.

Navigation

- "Card replacement" (page 45)
- "Card replacement in a SAM16 or a SAM21" (page 45)
- "Checking the BIOS of a new CPU card" (page 52)
- "Copying files to or from a CICM-EM or its CICM nodes" (page 57)
- "Correcting a node that is not connected" (page 59)
- "Correcting a node that stopped" (page 55)
- "Correcting a VMG out-of-service fault" (page 61)
- "Booting (hard) a SAM16 with CPV5370 cards" (page 63)

Accessing a CICM-EM or CICM node

Follow this procedure to open a Telnet session with a Centrex IP Client Management Element Manager (CICM-EM) or CICM node.

Node access allows you to

- monitor or maintain CICM-EM and CICM node operation
- transfer files from node to node, for example, product releases, maintenance releases (MRs), upgrades, and backup files

Access the master or slave CICM-EM through a Telnet session, or access a CICM node through a **`cicmconnect`** session from a computer that has network connectivity to the public administration network.

Use any GUI Telnet of SSH program, such as such as PuTTY, to connect to the CICM-EM

Step	Action

At a PC on the administration LAN

1 Perform one of these actions:

- To open a normal Telnet session enter

  `telnet <EM_IP_address>`

- To open a secure (SSH) session enter

  `ssh<username>@<EM_IP_address>`

2 Open a Telnet session to the CICM-EM IP address using a normal or secure Telnet session by entering this command:

`telnet <admin_ip_address>`

At the command line interface

3 Log on to the node by entering the administrator user ID and password for the node.

4 To connect to the CICM nodes hosted on this CICM-EM, type one of these **cicmconnect** commands on CICM-EM in this directory: D:\CentrexIP\tools.

- **cicmConnect /disp** —to display a list of nodes hosted on the CICM-EM
- **cicmConnect <cicm_node_name> <a or b>**—you specify which node to connect with, node A (a) or node B (b)

SSL connectivity is the default. If the CICM nodes do not support SSL, use the **/telnet** option

- **/telnet**—use the default Telnet port
- **/telnet:<port>**—you specify which Telnet port to use

Example

```
cicmconnect cicm-001 a

cicmconnect cicm-001 a /telnet
```

—End—

Querying a registry key

Follow this procedure to query a particular key in the Windows registry for Centrex IP Client Management (CICM) static data.

Step	Action

At a PC on the administration LAN

1 Open a Telnet session with the node, follow procedure "Accessing a CICM-EM or CICM node" (page 17).

At the command line interface

2 Enter **`reg query <registry><path>`**

Example

```
reg query hklm\software\nortel networks\cen-
trexip international gateway\8.10
```

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

Example

```
reg query hklm\software\nortel networks\cen-
trexip international gateway\8.10 /s
```

Information about the registry key is displayed.

—End—

Querying the state of a service

Follow this procedure to query the state of a service on a Centrex IP Client Management (CICM) node. Query the state of a node to determine the dependencies a service needs to start, or to confirm that a CICM node is running when the CICM-EMs are unavailable.

Step	Action

At a PC on the administration LAN

1 Open a Telnet session with the disconnected node, follow procedure "Accessing a CICM-EM or CICM node" (page 17).

At the command line interface

2 Enter **`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 are displayed.

When the Status is Stopped, there is no service running on that CICM-EM or CICM node. When Status is Running, there is a service operating on the CICM node.

—End—

Retrieving logs from a CICM-EM or a CICM node

Follow this procedure to retrieve Centrex IP Client Management (CICM) logs from a Centrex IP Client Management Element Manager (CICM-EM) or a CICM node, to help troubleshoot faults.

Step	Action
	At the home page of the CICM-EM
1	From the menu, click **diagnostics**. *The logs page opens.*
2	Select the CICM node identifier from the **inspect logs on** pick-list.
3	Select the CICM node A or B from the **logs on which node of** pick-list. *The logs for the selected node appear.* *A clock indicates the time that elapsed from the time the request was made and the time the logs appeared.*
4	Click the check box to select the type of logs you want collected.
5	To update the contents of logs that are already collected, click and select **overwrite files on fetch**.
6	Click **fetch logs from node A/B cicm-nnn**. *A clock indicates the time that elapsed from the time the request was made and the time the logs appeared.*

—End—

Tracing a route

Follow this procedure to 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 reply as a hop.

Step	Action

At a PC on the administration LAN

1 Open a Telnet session with the node, follow procedure "Accessing a CICM-EM or CICM node" (page 17).

At the command line interface

2 Enter **`tracert <IP_address>`**

where

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

Example
`tracert 47.160.168.173`

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.
```

—End—

Troubleshooting a CPU card

Troubleshooting a CPU card in a SAM16

Follow this procedure to troubleshoot the faults of a CPV5370 CPU card in a SAM16 chassis. Perform this procedure if the Centrex IP Client Management Element Manager (CICM-EM) cannot determine its own status, or that of 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

Step	Action
	At CPU node
1	Verify the LAN connectivity to the CICM. If LAN connectivity is not the cause of the fault, continue this procedure.
2	Connect a PC monitor and keyboard to the faulty CPU card. Use the front or rear connectors on the card.
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 remains blank, the node may be powered down or the CPU card may have suffered a hardware failure. Perform these steps: a. Open a Telnet session with the mate node, see "Accessing a CICM-EM or CICM node" (page 17) and attempt to start the card as described in "Booting (hard) a SAM16 with CPV5370 cards" (page 63). b. If the boot fails, replace the CPU card. Refer to "Card replacement" (page 45).

5 If the screen is blue, with typical NT crash information displayed, perform this procedure "Booting (hard) a SAM16 with CPV5370 cards" (page 63), to determine if the same thing happens on reboot.

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

7 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, open a Telnet session with it and complete the software configuration procedures as described in *CICM Configuration Management* (NN10240-511).

8 If this does not resolve the problem with the card, see "Card fault and recovery guidelines" (page 13).

—End—

Troubleshooting a CPU card in a SAM21

Follow this procedure to troubleshoot the faults of a CPN5385 CPU card in a SAM21 chassis. Perform this procedure if the Centrex IP Client Management Element Manager (CICM-EM) cannot determine its own status, or the status of 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

Step	Action

At CPU node

1 Verify the LAN connectivity to the node.

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

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

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 remains blank, start the card as described in the procedure "Booting (hard) a SAM21 with CPN5385 cards" (page 65) and return to this step.

5 If the screen is blue and shows the typical NT crash information perform these steps:

a. Perform the procedure "Booting (hard) a SAM21 with CPN5385 cards" (page 65) to determine if the same thing happens on reboot.

b. If the display shows the same blue screen and 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 booted successfully. Perform these steps:

a. If you have just re-imaged the SAM21 card, open a Telnet session with the administration IP address and complete the software configuration procedures as described in *CICM Configuration Management* (NN10240-511).

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" (page 31). 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 If this does not resolve the problem with the card, see "Card fault and recovery guidelines" (page 13).

—End—

Verifying IP network connectivity

Follow this procedure to verify the connectivity between a Centrex IP Client Management (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.

Step	Action

At a PC on the administration LAN

1 Open a Telnet session with the node, follow procedure "Accessing a CICM-EM or CICM node" (page 17).

At the command line interface

2 Enter this command:

```
ping <IP_address or node_name>
```

where

IP_address
is the IP address of the node to ping, for example
ping 47.160.168.173
or
node_name
is the name of the CICM node to check, for example
ping cxip170b

If the connection is active, the reply is displayed.

3 To continuously ping the connection, add **-t** to the end of the command. Press **Crtl+C** to stop pinging the node.

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
```

The ping reply includes the node name.

—End—

Viewing CS2000 logs

Follow this procedure to view Call Server 2000 (CS2000) logs for Centrex IP Client Management (CICM) nodes 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 (PM) called remote line concentrating modules (RLCM) or international RLCMs (IRLCM).

Step	Action

At the command interface (CI)

1 Enter this command:

```
LOGUTIL.
```

2 Perform one of these steps:

- To view the last Peripheral Module (PM) log generated, enter this command:

  ```
  open PM
  ```

- To view a specific PM log, enter this command:

  ```
  open PM <log number>
  ```

Logutil output will display the latest log created.

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

where

`n` is the quantity of earlier logs to view.

—End—

View executables running on a node

Follow these procedures to view a list of tasks, services, or executables running on a CICM node. Perform either procedure to determine when a service or executable has stopped running.

Navigation

- "Viewing executables using the pulist command" (page 35)
- "Viewing executables using the tlist command" (page 35) "Viewing executables using the tlist command" (page 36)

The output from the **pulist** command includes the user name the executable runs with.

Viewing executables using the pulist command

Follow this procedure to view the list of executable files running on a Centrex IP Client Management (CICM) node by using the **pulist** command.

Step	Action

At a PC on the administration LAN

1 Open a Telnet session with the node, follow procedure "Accessing a CICM-EM or CICM node" (page 17).

At the command line interface

2 To view a list of all of the CICM node executable files, with their associated user name, enter:

```
pulist
```

The list of executable files running on the node is displayed with the user names.

3 To view a specific executable, enter

```
pulist <exec>.exe
```

where

exec is the file name of the file.

.exe is the file extension of the file. Not all executable files use have this extension.

The information is displayed.

The data returned is a list of process names, process IDs, and if it can be determined, the user name under which the tasks were run.

Example

```
pulist gw.exe
cxipmibsync.exe   1040
cxipnodemgmt.exe  1724
UftpSrv.exe       1840
gw.exe            1912
mgm.exe           1944
Sessions.exe      1968
MegacoMG.exe      392
cxiptaskserver.exe 796
explorer.exe      1100 CICM-001-A\Administrator
PRONoMgr.exe      104  CICM-001-A\Administrator
cmd.exe           1220 CICM-001-A\Administrator
```

—End—

Viewing executables using the tlist command

Follow this procedure to view the list of executable files running on a Centrex IP Client Management (CICM) node by using the **tlist** command.

Step	Action

At a PC on the administration LAN

1 Open a Telnet session with he node, follow procedure "Accessing a CICM-EM or CICM node" (page 17).

At the command line interface

2 List all executable files on a CICM node by entering:

tlist

or

tlist 1912 (useful if more than one process with the same name is running)

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 of the file. Not all executable files use this extension.

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

Example

```
1912 gw.exe
9.20.0.104 shp  0x00400000  gw.exe
1912 gw.exe
CWD:     C:\WINDOWS\system32\
CmdLine: D:\CentrexIP\gw.exe
VirtualSize:    22812 KB   PeakVirtualSize:
23840 KB
WorkingSetSize:  3380 KB   PeakWorkingSetSize:
3384 KB
NumberOfThreads: 7
0 Win32StartAddr:0x00000000 LastErr:0x00000000
State:Initialized
5Win32StartAddr:0x00000000 LastErr:0x00000000
State:Initialized
5 Win32StartAddr:0x00000000 LastErr:0x00000000
State:Initialized
5 Win32StartAddr:0x00000000 LastErr:0x00000000
State:Initialized
5 Win32StartAddr:0x00000000 LastErr:0x00000000
State:Initialized
5 Win32StartAddr:0x00000000 LastErr:0x00000000
State:Initialized
5 Win32StartAddr:0x00000000 LastErr:0x00000000
State:Initialized
9.20.0.104 shp  0x00400000  gw.exe
5.1.2600.1217 shp  0x77f50000  ntdll.dll
5.1.2600.1560 shp  0x77e60000  kernel32.dll
5.1.2600.1634 shp  0x77d40000  USER32.dll
5.1.2600.1561 shp  0x7f000000  GDI32.dll
5.1.2600.1106 shp  0x77dd0000  ADVAPI32.dll
5.1.2600.1361 shp  0x78000000  RPCRT4.dll
5.1.2600.1619 shp  0x4fec0000  ole32.dll
3.50.5016.0 shp  0x77120000  OLEAUT32.dll
7.0.2600.1106 shp  0x77c10000  MSVCRT.DLL
6.0.2800.1612 shp  0x70a70000  SHLWAPI.dll
2001.12.4414.53 sh  0x7c890000  CLBCATQ.DLL
```

```
2001.12.4414.42 sh  0x77050000  COMRes.dll
5.1.2600.0 shp  0x77c00000  VERSION.dll
9.20.0.104 shp  0x10000000  centrexipproxy.dll
5.1.2600.1106 shp  0x76f90000  Secur32.dll
```

—End—

Viewing QoS reports for a CICM node

To view the Centrex IP Client Management (CICM) node quality of service (QoS) reports that are generated for each call, see this procedure *Viewing QoS statistics for CICM nodes* in *CICM Performance* (NN10252-611).

View adapter configuration

Viewing the IP configuration of adapters from the CICM-EM

Follow this procedure to view the IP configuration from the CICM-EM interface.

Step	Action
	At the CICM Home Web page
1	From the menu, click **diagnostics**. *The diagnostics home page opens.*
2	From **network status check on a CICM** pick-list, select the CICM and then click **network status check on a CICM**. *The network status from page opens and displays the IP addresses for the configuration.*
	—End—

Viewing adapter IP configuration using the ipconfig command

Follow this procedure to view the IP configuration by using the command **`ipconfig`**. Issue the command from a personal computer (PC) connected to the CICM-EM through a Telnet session.

Step	Action
	At a PC on the administration LAN
1	Open a Telnet session with the node, follow procedure "Accessing a CICM-EM or CICM node" (page 17).
2	At the command line interface (CLI), enter **`ipconfig /all`** *The IP configuration for all adapters on the node is displayed.*
	—End—

Viewing the network configuration

Follow this procedure to view the network configuration of a user workstation by using the **net** command.

Step	Action

At a PC on the administration LAN

1 Open a Telnet session with the node, see procedure "Accessing a CICM-EM or CICM node" (page 17).

At the command line interface

2 Enter this command:

```
net config workstation
```

The network configuration information for the workstation appears.

—End—

Card replacement

Replacing a faulty card from the Centrex IP Client Management (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)

"Product Engineering Codes for SAM16 and SAM 21 cards (blades)" (page 46) lists the product engineering codes (PECs) for the cards that can be replaced.

When a Centrex IP Client Management (CICM) service is interrupted due to a hardware failure, the faulty card component of the gateway needs to be replaced.

ATTENTION

Testing faulty cards must be done by Nortel technical support only.

Before replacing 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. Make a note of 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, refer to this procedure,"Card replacement in a SAM16 or a SAM21" (page 45).

Card replacement in a SAM16 or a SAM21

"Product Engineering Codes for SAM16 and SAM 21 cards (blades)" (page 46) lists the replacement hardware.

For each CPU card that you replace, you must 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/

Product Engineering Codes for SAM16 and SAM 21 cards (blades)

Code	Name
SAM 16	
NTRX51VB	CPV5370 CPU
NTRX51VC	CPV5370 Transition Module (TM)
NTAR02JY	HSC Card
SAM21	
NTRX51HJ	CPN5385 CPU
NTRX51HK	CPTM85 Transition Module (TM)

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

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

WARNING
This procedure describes only 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
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
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.

Step	Action
	At the CICM-EM Web pages

1 When the card you are replacing is the master, perform one of these actions:

- To replace a CICM card, switch activity away from the master card to make it the slave card.

  Terminal transfers are automatically handled.

- To replace a CICM-EM card, restart the card and make it the slave card.

2 Perform one of these actions:

- To replace a CICM card, go to the next step.
- To replace a CICM-EM card, go to step 6.

3 At the **cicm status** page, click **perform maintenance on cicm_name**.

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

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

5 For the node with the faulty card, select **stop** from the **node A service control** or **node B service control** pick-list, then click **node A/B service control**.

The action is performed. The status of the node changes from stop pending, to stop.

6 Perform these steps to shut down the node where the faulty card is seated.

a. Open a Telnet session with the node, follow "Accessing a CICM-EM or CICM node" (page 17) (node B in this example), and enter this command:

```
shutdown -s -t 00
```

where

`s` is for shut down.
`t 00` is for time and 00 (two zeros) means immediately.

You are prompted to confirm the action.

b. Type **Y** to confirm the node shutdown.

The shutdown is confirmed.

CAUTION
Risk of loss of service
It is critical to power down only the CICM node 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.

A total loss of CICM power and service results if both nodes are powered down.

7 For a SAM21, lock the card from the element manager GUI of the CS2000 SAM21 and go to step 8.

For a SAM16, perform these steps to power down the node where the faulty card is seated.

a. Follow the "Accessing a CICM-EM or CICM node" (page 17) procedure to access the CICM mate node, and enter the command:

```
C:\>powerdown
```

Example
If the faulty card is on node B, open a Telnet session with node A.

This response appears:

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. Press **Enter** to continue.

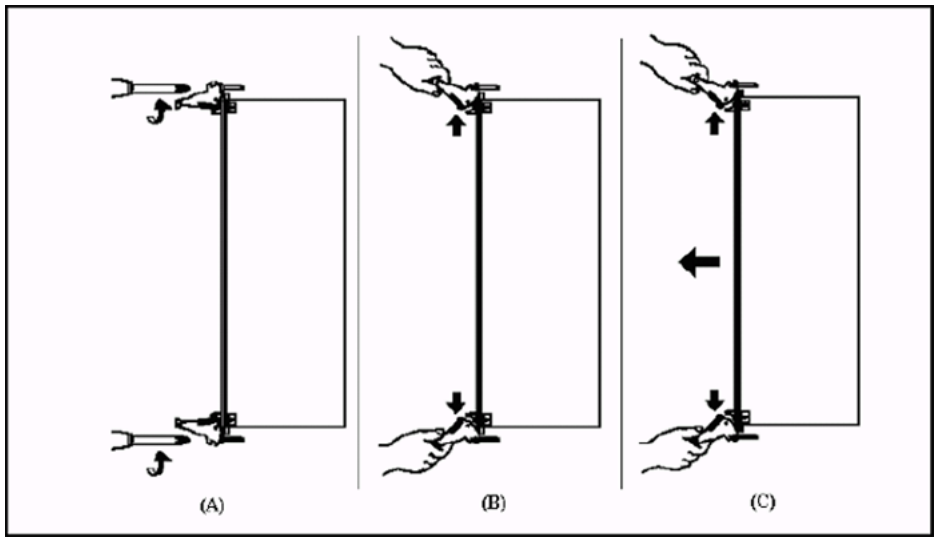
This response appears:

Powering down domain B processor. Powerdown complete.

8 Make a note of all the cable connections to the ports on the faulty card, then disconnect all the cables from the card.

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

ATTENTION
If the faulty card is a TM card, remove the CPU card first. Always remove the CPU card before you remove its associated TM card.



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.

10 If you are replacing a CPU card, connect a suitable PC monitor and keyboard to the card or TM before you insert the new card.

For a SAM16, perform one of these actions:

- If you are replacing a CPU card and the **`powerdown`** command in step 7 was not successful, the CPU card boots as soon as you insert it into the chassis (step 12).

  Be prepared to enter the BIOS settings before the CPU card is allowed to fully boot. See procedure "Checking the BIOS of a new CPU card" (page 52).

  Return to this procedure and this step when you complete that procedure.

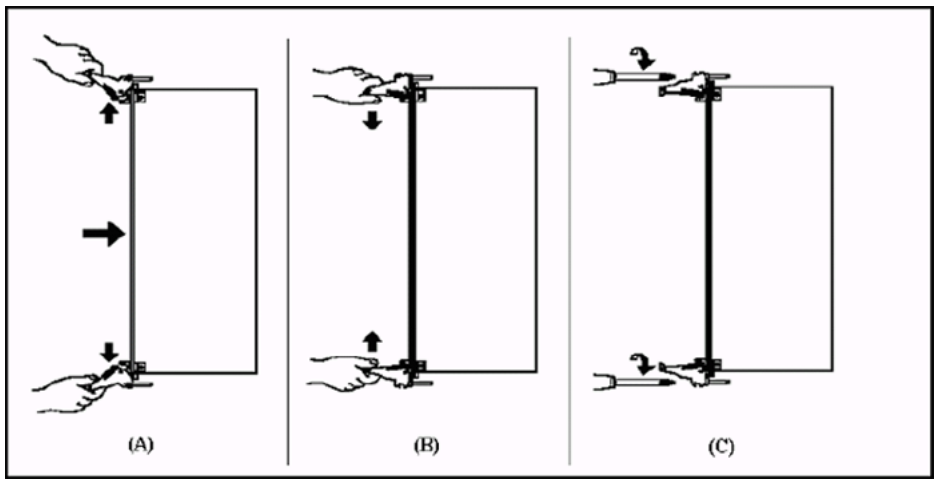
- If the powerdown command in step 7 was successful, continue this procedure through step 13, then check the BIOS settings as directed.

11 For a SAM21, update the MAC address on SAM21 element manager with the MAC address of the new CPU card.

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

ATTENTION
For each CPU card, insert the TM card first, and then the main card.

For a SAM16, 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, 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 is seated into the back plane connectors.

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.

13 Refer to the notes you made in step 8, and reconnect all the cables to the same ports that they were previously connected to.

14 For a SAM21, unlock the CPU card using the SAM21 Element Manager.

15 For a SAM21, go to step 16.

For a SAM16, perform these steps to power up the node from the mate node.

a. Open a Telnet session with the mate node, follow procedure "Accessing a CICM-EM or CICM node" (page 17)

Example
If the card replaced was on node B, open a Telnet session with node A.

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

```
C:\>powerup
```

You see this reply:

Powerup: Power up the other domain processor.

This CPU is in domain A

Powering up on domain B processor

Powerup completed.

The service recovers in a few minutes.

16 Perform one of these actions:

- If you replaced an HSC card, go to step 19.
- If you replaced a CPU card, go immediately to "Checking the BIOS of a new CPU card" (page 52) and perform that procedure. Then return to this step.

  Wait until the process to restart the card is complete before you proceed with this procedure.

17 If a CPU card was replaced you must perform the preboot procedures before you continue with this procedure. Go to either CICM-EM preboot procedures or CICM preboot procedures.

Do not perform preboot procedures if you replaced an HSC card.

18 Go to "Restoring CICM-EM or CICM node configuration" (page 71) to restore the configuration to the new CPU card. Return to this procedure and this step when you complete that procedure.

19 Verify that the service has started correctly and then perform one of these actions:

- If you replaced a CICM card, on the **cicm status** page, scroll through the **node modification on** section, view the Service State field and verify that the state is Running.
- If you replaced a CICM-EM card, on the **cicm—element manager status** page, verify that the state of all the services is Running.

20 Make sure that there are no alarms raised that relate to the new CPU card.

—End—

Checking the BIOS of a new CPU card

Perform this procedure as soon as you replace a CPU card in a SAM16 or SAM21 shelf as described in the procedure "Card replacement in a SAM16 or a SAM21" (page 45).

Prerequisites

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

Step	Action

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.

To change the BIOS configuration on a SAM16, go to the next step.

To change the BIOS configuration on a SAM21, go to step 3.

2 Perform these steps to change the BIOS configuration on a SAM16:

a. On the keyboard, press **F2** to open the BIOS **Setup** main menu.

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

c. Using the keyboard arrow keys, move the curser to highlight **PCI configurations** and press **Enter** to open this submenu.

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

e. Perform one of these actions to verify the PCI configuration.

- The new CPU is in Domain A, make sure that the PCI for Domain A is set to **Enabled**, and the PCI for Domain B is set to **Disabled**.
- The new CPU is in Domain B, make sure that the PCI for Domain B is set to **Enabled** , and that the PCI for Domain A is set to **Disabled**.

f. Verify the Ethernet ports configuration. Both ports should be configured to use the same option, either **Front** or **Rear** option, whichever is preferred.

g. Press the keyboard **F10** key to save the BIOS configuration.

You exit the Setup menu.

h. Go to step 4.

3 Perform these steps to change the BIOS configuration on a SAM21:

a. On the keyboard, press **F2** to open the BIOS Setup main menu.

b. Select the **Advanced** menu.

c. If necessary, enable the 100base-T Ethernet Adapter's **ROM** option. This option enables the adapter Intel PXE ROM, which facilitates the network boot.

d. Select the **Boot** menu.

e. If necessary enable the **Boot Retry** option. This ensures that, in the case of a PXE failure the system retries to start each device in turn, indefinitely.

f. Use the keyboard arrow keys to navigate to the **Boot Device Priority** and open the submenu.

g. If necessary, set the **internal PMC hard disk** to be the first device the system boots.

h. Set the **On-Card 10/100 Ethernet** option as the second device the system boots.

i. Disable the other boot devices (use "!").

j. On the keyboard, press the **F10** to save the BIOS configuration.

k. Go to step 6.

4 Perform these steps to power down the SAM16 node:

a. Open a Telnet session with the mate node, follow procedure "Accessing a CICM-EM or CICM node" (page 17).

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

C:\>**powerdown**

5 Perform these steps to power up the SAM16 node:

a. Open a Telnet session with the mate node, follow procedure "Accessing a CICM-EM or CICM node" (page 17).

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 recover in 15 to 20 minutes.

6 Verify that the CICM node booted up. If the node does not restart, contact the Nortel technical support for assistance.

—End—

Correcting a node that stopped

Follow this procedure to correct a stopped Centrex IP Client Management Element Manager (CICM-EM), or CICM node to restore service.

CAUTION
This procedure must be performed only under direction from Nortel technical support.

Under no circumstances should the Restart button be pressed without specific instructions from Nortel technical support.

Step	Action

On a PC connected to the Administration LAN

1 Follow the "Accessing a CICM-EM or CICM node" (page 17) procedure to attempt to connect to the stopped node. Perform one of these actions:

- If you can access the node, the node is functioning. This procedure is complete.
- If you cannot access the node, go to the next step to check if the node is running.

At the CICM home page

2 From the menu, click **maintenance**.

The cicm maintenance page opens.

3 Select the CICM node from the **perform maintenance on** pick-list, then click **perform maintenance on**.

The maintenance status page opens.

4 View the **Service Status** field for the node and verify that the node is running.

- If the Service State is running, this procedure is complete.

- If the Service State is stopped, contact Nortel technical support.

—End—

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

To copy files to a Centrex IP Client Management Element Manager (CICM-EM) from:

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

see these procedures in *Upgrading CICM* (NN10230-461):

- *Copying upgrade or patch files to and from an SPFS server*
- *Copying upgrade or patch files to and from your PC*

You copy backup files to preserve a copy before the system overwrites it.

Correcting a node that is not connected

Follow this procedure to correct a Centrex IP Client Management Element Manager (CICM-EM) or CICM node that is not connected, to restore service.

CAUTION
Under no circumstances should the Restart button be pressed without specific instructions from Nortel technical support. This procedure must be performed only under direction from Nortel technical support.

Step	Action

On a PC connected to the Administration LAN

1 Open a Telnet session with the disconnected node, follow "Accessing a CICM-EM or CICM node" (page 17). Perform one of these actions:

- If you can access the node, the node is functioning. This procedure is complete.
- If you cannot access the node, proceed to the next step.

At the CICM home page

2 From the **CICM home** page, select **maintenance**.

The cicm maintenance page opens.

3 Select the node from the **perform maintenance on** pick-list.

The maintenance status page opens.

4 View the **Service Status** field for the node and verify that the node is running. Perform one of these actions:

- If the Service state is running, this procedure is complete.
- If the Service state is stopped, contact Nortel Support.

—End—

Correcting a VMG out-of-service fault

Follow this procedure to restart Virtual Media gateway (VMG) service when its state is out of service while it is connected to the SAM16 platform.

If the CICM Status page shows the status of the VMG is stopped, the most likely cause is that a node has stopped. See "Correcting a node that stopped" (page 55).

Step	Action
	At the CICM home Web page
1	View the **service state** of the VMG by selecting the node to view from the **view the status of** pick-list. *The cicm status page opens.*
2	If the **cicm status** page shows that the VMG has stopped, the cause is likely due to a stopped node. To restart the node, click **maintenance** in the CICM menu. *The cicm maintenance page opens.*
3	Select the node from the **perform maintenance on** pick-list. *The maintenance status page opens.*
4	View the **Service Status** field for the node and verify that the node is running. Perform one of these actions: • If the Service state is running, this procedure is complete. • If the Service state is stopped, contact Nortel Support.

—End—

Booting (hard) a SAM16 with CPV5370 cards

Hard boot a SAM16 node with CPV5370 CPU cards by powering it down and powering it up. Perform this procedure after replacing a card.

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

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

Step	Action

At a PC on the administration LAN

1 Open a Telnet session with the node, follow procedure "Accessing a CICM-EM or CICM node" (page 17).

At the command line interface

2 To power down, enter **powerdown**.

```
You are prompted to confirm the action.
This CPU is in domain X.
Continuing will power off domain Y processor
resulting in the loss of all CICM service on that node.
Press ENTER to continue, Ctrl-C to abort.
```

3 To continue, press **Enter**.

The system displays a message when the power down is finished.

```
Powerdown completed.
```

4 To power up the mate node, enter:

powerup

The system displays a message when the power up is finished.

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

—End—

Booting (hard) a SAM21 with CPN5385 cards

Hard boot a SAM21 node with CPN5385 CPU cards by locking and unlocking the card from the Centrex IP Client Management Element Manager Element Manager (CICM-EM) of the SAM21.

Apply this procedure to the slave node only. 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 card in the chassis.

CAUTION
Completing this procedure shuts down the CICM node, causing a loss of service.

Step	Action

At a PC on the administration LAN

1 Through IEMS, double-click the 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 the shelf view of the SAM21 chassis to open it.

3 With the cursor on the card of the node to reboot, right-click and select **lock**

4 To observe the state changes, right-click and selecting **Card View**.

The locked card turns orange and a padlock symbol appears at the bottom of the card. See "Example: A locked card" (page 66).

CAUTION
Wait until the unlocking process is complete. Do not affect the state of the card (blade). If unlocking takes longer than 30 minutes, contact Nortel technical support.

5 Wait for the node to fully unlock.

Unlocking is complete after the **Card View... State History** is displayed and when the *Card View...* indicates that the card is fully in service.

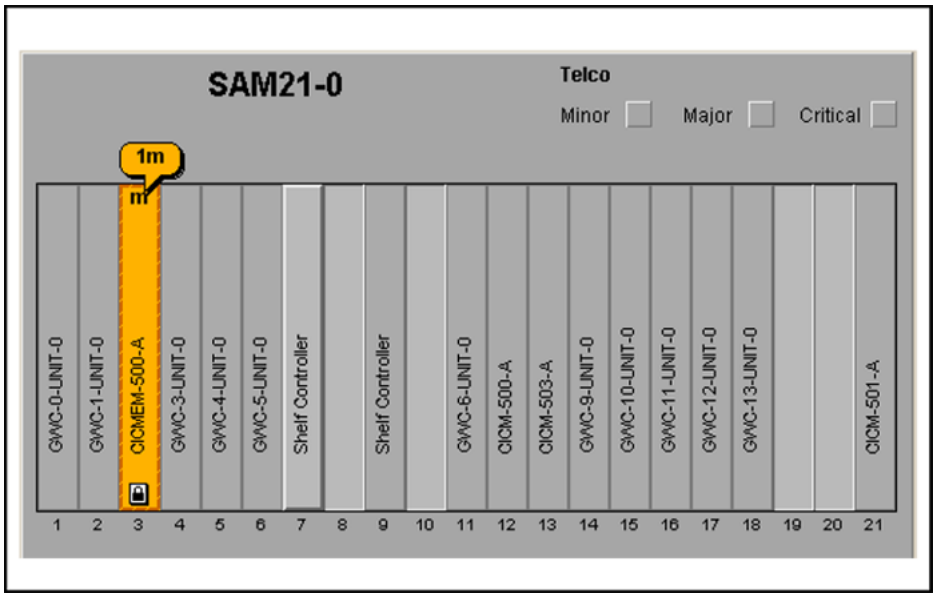
6 When the locking is complete, return to the **Card View**, and on the same card right-click and select **unlock**.

Completion of the reboot is shown on the **History** tab of the **Card View**. See "Example: Card history" (page 67).

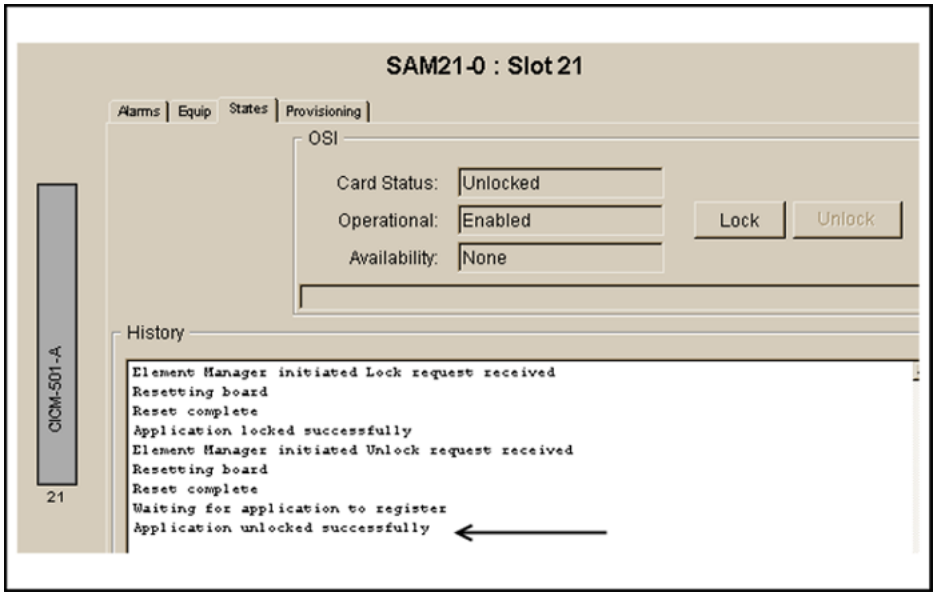
—End—

Procedure job aid

Example: A locked card



Example: Card history



Booting (soft) the node

Follow this procedure to restore service to the Centrex IP Client Management Element Manager (CICM-EM) or CICM node in a SAM16 or SAM21 chassis,

ATTENTION

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

Step	Action

At a PC on the administration LAN

1 Open a Telnet session with the node, follow procedure "Accessing a CICM-EM or CICM node" (page 17).

At the command line interface

2 Execute a soft reboot by entering this command:

```
shutdown /l /r /t:0
```

where

l is for the local machine
r is for reboot
t:0 is for time and 0 (zero) means immediately.

—End—

Restoring CICM-EM or CICM node configuration

Follow this procedure to restore the software configuration to a pair of Centrex IP Client Management Element Managers (CICM-EM) or CICM nodes when:

- An unexpected system failure of one or both nodes occurs. This condition can be verified through logs and alarms, and if it occurs it is necessary to re-image the node or pair with a fresh software load.
- The accidental loss or deletion of a portion of the MIB occurs on a pair of fully configured nodes.

Restore the node by loading a backup file of the software configuration onto one or both nodes of a CICM or CICM-EM pair. If no configuration backup file exists, you have to manually reconfigure the node. Refer to *CICM Administration and Security* (NN10252-611), for the process and procedures for creating the backup configuration files for a CICM-EM or a CICM node.

Each node backup file is unique. When you apply a backup file, it must be for the same version of software that was running on the node. Do not use this procedure under these conditions:

- across software upgrades within the same product release, for example, 8.11 to 8.12
- across software upgrades across two different product releases, for example, 7.20 to release 8.12

The system prevents you from accidentally installing an inappropriate backup file.

To prepare for applying the backup file, you must do the following:

By using the **`/restart`** option, the main CICM services are stopped prior to re-applying the actual data, and restarted when the restoration is complete.

The **`/norestart`** option has no impact on the services running at the time the restore is done.

These procedures are associated with restoring a software configuration:

- "Copying files to or from a CICM-EM or its CICM nodes" (page 57) to copy the backup file to the CICM-EM
- "Restoring the CICM node registries" (page 73) to restore registries from the backup file
- "Viewing the backup files and log" (page 85) to select a backup file

Step	Action
1	You must make a direct connection to both the CICM-EM and the CICM node because the CICM-EM does not include a restore interface.
2	Locate the applicable .xml file on the CICM-EM (or wherever you have it stored) and copy it to the node, or FTP it to the CICM node.
3	Open a Telnet session with the node, follow procedure "Accessing a CICM-EM or CICM node" (page 17).
4	On the command line, enter one of these commands: **`cxiprestore <xml_backup_file> /norestart <xml_backup_file>`** or **`cxiprestore <xml_backup_file> /restart <xml_backup_file>`** where **`<xml_backup_file>`** is the configuration file, **`/norestart`** is specified to restore on fully configured CICM nodes **`/restart`** is used for freshly re-imaged CICM nodes after completing a preboot

—End—

Restoring the CICM node registries

Follow this procedure to restore Centrex IP Client Management (CICM) node registries using a backup file from the CICM-EM.

The **CXIPRestore** command uses the **/norestart** or **/restart** options depending upon the scenario in which the data is restored. The **/norestart** option is used to restore registries on fully configured CICM nodes. The **/restart** option is used to restore registries on freshly re-imaged CICM nodes (following completion of preboot).

In a case where the **/restart** option is chosen, the main CICM services are stopped prior to reapplying the actual data. The services are restarted upon completion of the restore operation. The services do not need to be manually stopped. Conversely, the **/norestart** option has no impact on the services running at the time the restore is performed.

In order for the restore procedure to succeed on freshly re-imaged CICM nodes (**/restart** is used), the node being restored must be the only one currently running. So it must be the master node of the pair, with no slave presently connected to the network or switched on. This is essential to ensure that the newly restored MIB content is not accidentally deleted by a premature synchronization with the mate node. The data will be properly replicated to the slave node following the re-imaging of the Slave at a later stage.

For the same reason, for the restore procedure to succeed on running CICM nodes (**/norestart** is used), the node being restored must be the master of the pair, to ensure that the newly restored MIB content is synchronized across to the slave node.

When using the **/restart** option, restarting the main CICM services means that all network adapters for the node are reinitialised. As a result the Telnet connection is dropped.

ATTENTION

Do not use other command options that are available for the **cxiprestore** tool.

Prerequisites

Perform the following procedure before restoring a registry.

- Refer to "Restoring CICM-EM or CICM node configuration" (page 71) for an explanation of the restoration process and a list of the associated procedures.

Step	Action

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

1 Open a Telnet session with the node, follow procedure "Accessing a CICM-EM or CICM node" (page 17).

2 Verify that the backup registry file is present at the FTP home directory by issuing this command: **`D:\\CentrexIP\support`**.

The backup files follow this naming convention:

- *backupconfig <day_number>.xml*, for a CICM node
- *backupconfig <day_number_em>.xml*, for a CICM-EM

3 Retrieve the latest backup file from the CICM node you are restoring.

4 Repeat step 2 for the mate node for the mate node.

5 In the Telnet window to the same CICM node, restore the back up file by issuing this command:

```
cxiprestore backup_file_name.xml /norestart
```

where

`backup_file_name.xml` is the latest backup file

6 Repeat step 4 for the mate node.

7 Disconnect the Telnet sessions from the CICM nodes.

At the CICM home page

8 Perform these steps to add the CICM node to the CICM-EM:

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

b. Click **add new CICM.**

c. Enter the name of the CICM.

d. Click **save new CICM**.

9 To restart one CICM node, go to "Booting (soft) the node" (page 69) and return to this step.

10 Log on to the restored CICM node to confirm that the back-up was successfully loaded.

If you can log on, the back-up was successful.

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

11 To restart the second CICM node, go to "Booting (soft) the node" (page 69) and return to this step.

12 Log on to the restored CICM node to confirm that the backup file was successfully loaded.

If you can log on, the back-up was successful.

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

—End—

Shutting down a CICM node

Follow this procedure to manually shut down a Centrex IP Client Manager (CICM) node to resolve a hardware or software problem.

Refer to "CICM node failures" (page 77) to understand what happens in a failure.

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

CICM node failures

When both master and slave nodes are synchronized and running, there is a redundant node that continues to provide service if one node fails.

The term node failure applies to hardware failures of the physical CPU card running the Centrex IP Client Manager (CICM) load, and to a critical software error for which no recovery action is possible. Some possible node failures include:

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

From the perspective of the remaining node, these two cases are identical, because the mate node stops sending a signal. The remaining node takes appropriate action, as described in the scenarios 1 and 2.

All but LAN adapter failures, which are described in "Network adapter failures" (page 78), are treated equally by the dual-node redundancy functionality. When physically possible, any critical failure results in the node automatically attempting to restart. By default, the node makes three attempts. Following the last failed restart, the boot controller will not start the CICM software load.

Node failure scenarios

Scenario 1: Master node failure

If the master node has an unexpected failure, the hot standby slave node detects it and automatically switches activity (SWACT) 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 during the SWACT of the nodes. Unstable calls may or may not survive.

Scenario 2: Slave node failure

If 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.

Because all the terminals are always hosted by 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 situations require special consideration.

- **Master loses adapter hosting H.248 interface**

  When the master node detects a loss of layer-2 connectivity on the physical adapter hosting the H.248 interface, the master initiates an automatic switch of activity (SWACT). This is done to conserve connectivity to the gateway controller card (GWC) and to the VoIP client, thereby maintaining call processing and client connectivity.

- **Master loses both adapters**

  If the master node detects a layer-2 loss of connectivity on both its physical adapters, it determines that has a fault and demotes itself to the slave state. When the slave determines that the master has failed, it takes over and becomes the master.

  If either of the physical adapters on the failed node 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 a physical adapter the node does not find a mate, it again promotes itself to the master state. Regular software monitoring ensures that only one node is ever the master at any given time.

- **Slave loses adapter acting as backup H.248 and client interface**

  If the slave node loses layer-2 connectivity on the physical adapter that normally hosts the back-up H.248 and the client interface, the slave updates its own local state and informs the master node of the 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, the actions are virtually the same as those described in *Master looses both adapters*. The only difference is that the node does not need to demote itself because it is already the slave.

Step	Action

At the maintenance page of the CICM-EM

1 Select the identifier of the CICM node from the **view of the following CICM** pick-list.

Example
CICM-002

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

3 Check the **Status** of the selected node to verify that the node to shut down is the slave.

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

5 For the slave node A or B, select **Stop** from the pick-list under **node A/B service control**.

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

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

—End—

Start a service running on a node

Follow this procedure to manually start a service running on a Centrex IP Client Manager (CICM) node.

ATTENTION
Do not perform this procedure unless you are instructed to do so by Nortel technical support.

Navigation

- "Starting a service manually using the net command" (page 81)
- "Starting a service manually using the sc command" (page 82)

Starting a service manually using the net command

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

Use the **net start** command to view of list of services and find the service name. See the procedure, "View executables running on a node" (page 35).

Step	Action
	At a PC on the administration LAN
1	Open a Telnet session with the node, follow procedure "Accessing a CICM-EM or CICM node" (page 17).
	At the command line interface
2	Enter **net start <service_name>** where **service_name** is the name of the service to start. *A status message appears confirming that the service started successfully.*

—End—

Starting a service manually using the sc command

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

Use the **net start** command to view of list of services and find the service name. See the procedure, "View executables running on a node" (page 35).

Step	Action
	At a PC on the administration LAN
1	Open a Telnet session with the node, follow procedure "Accessing a CICM-EM or CICM node" (page 17).
	At the command line interface
2	Enter **sc start <service_name>** where **service_name** is the name of the service to start. *A status message appears confirming that the service was started successfully.*

—End—

Stop a service running on a node

Follow one of these procedures to manually stop a service running on a Centrex IP Client Manager (CICM) node.

The service can be stopped using either procedure:

- "Stopping a service manually using the net command " (page 83)
- "Stopping a service manually using the sc command" (page 83)

Use the **net start** command to view of list of services and find the service name. See the procedure, "View executables running on a node" (page 35).

Stopping a service manually using the net command

Follow this procedure to manually stop a service using the **net** command .

Step	Action

At a PC on the administration LAN

1 Open a Telnet session with the node, follow procedure "Accessing a CICM-EM or CICM node" (page 17).

At the command line interface

2 Enter this command:

```
net stop <service_name>
```

where

service_name is the name of the service to start.

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

—End—

Stopping a service manually using the sc command

Follow this procedure to manually stop a service using the **sc** command.

Use the **net start** command to view of list of services and find the service name. See the procedure, "View executables running on a node" (page 35).

Step	Action

At a PC on the administration LAN

1 Open a Telnet session with the node, follow procedure "Accessing a CICM-EM or CICM node" (page 17).

At the command line interface

2 Enter this command:

```
sc stop <service_name>
```

where

service_name is the name of the service to start.

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

—End—

Viewing the backup files and log

Follow this procedure to view the list of backup files and event logs. Centrex IP Client Manager Element Manager (CICM-EM) or CICM node logs are created manually or automatically.

When a backup file is created on a day that is the same number of the day of the month of the previous back up, the backup file automatically overwrites the older file. For example, when the third day of a month occurs again, that backup file for that day overwrites the file saved on the third day of the previous month.

Refer to the procedure "Copying files to or from a CICM-EM or its CICM nodes" (page 57).

Step	Action
	At the PC to access the CICM-EM
1	Open a Telnet session with the slave or the master node to view the backup files. Follow "Accessing a CICM-EM or CICM node" (page 17).
	At the CICM-EM
2	Go to the directory *D:\CentrexIP\support\backups*.
3	Locate and identify the back-up files. Each file name follows this naming convention: *backupconfig_<day_number>.xml*
4	View the time when the backup was executed, and the results of the backup by following these steps: a. From the **CICM-element manager** home page, select **Status** from the **CICM** menu to open the **CICM home** page. *The CICM home page opens.* b. On the **CICM home**, select the CICM from the **show the backup sets available for** pick-list on the right, c. Click **show the backup sets available for** text.

The cicm backup sets on page opens and displays the backup sets and backup results.

—End—

Carrier VoIP

CICM Fault Management

Publication: NN10233-911
Document status: Standard
Document version: 06.04
Document date: 20 October 2006

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback.

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.