Upgrading CICM

This document provides the preparation and procedures to upgrade the software of a redundant pair of Centrex IP Client Manager (CICM) element managers (EMs) and its pairs of CICM nodes. The document also includes rolling back from a software upgrade.

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

This document is part of the CICM customer documentation suite. The complete list of documents in the suite is identified in *CICM Basics*, NN0044-111.

The topics in this document include:

What's new for CICM software upgrades

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

- revised the entire document to include a task flow indicating the sequence of all procedures involved in upgrading CICM-EM nodes and the CICM nodes
- added the Task flow of CICM-EM and CICM node upgrades
- added these upgrade procedures:
  - Accessing a CICM-EM through the IEMS
  - Backing up the CICM nodes
  - Backing up the CICM-EMs
  - Copying upgrade files onto the CICM-EMs

  - — Switching activity between CICM nodes
  - — Transferring terminals for an upgrade
  - — Upgrading the CICM-EM with an MR or product release
- updated these upgrades procedures:
  - — Upgrading a CICM node with a product release
  - — Upgrading a CICM node with an MR
  - — Verifying the software version of the CICM-EM and CICM nodes
- added the chapter Rolling back from a CICM upgrade
- added the chapter Upgrading firmware on IP phone sets
- added these procedures to support using IEMS:
  - — Editing and viewing object properties using Java Web Client
  - — Editing and viewing object properties using Web Client
- separated the Prerequisites of each procedure into its own section

Preparing to upgrade CICM software

This *NN10230-461 CICM Upgrades* section provides the software strategy to prepare for upgrading the software of the Centrex IP Client Manager (CICM) element manager (EM) and its pairs of CICM nodes.

Preparing to do a CICM software upgrade includes these sections:

- Understanding CICM software upgrades
- Hardware revision compatibility
- Backing up the CICM-EM and CICM node software configuration
- Software upgrade restrictions and limitations
- Software upgrade strategy

Understanding CICM software upgrades

Prepare for a CICM-EM and CICM nodes software upgrade by understanding the following.

- Software version
- Maintenance release and product release upgrades
- MR upgrade implementation guidelines

Software version

The software to operate CICM nodes and a CICM-EM is applied independently to each. Each pair of CICM nodes must have the same version of software. For example, while the CICM-EMs have version 8.0, each pair of CICM nodes can operate with either version 7.0 or 8.0.

The software version has this format:
<release_number>.<build_number>

Example
8.11.184

The release number is 8.11

The build number is 184

The lower left corner of the top-level screen of the CICM-EM shows the base release of the software version (for example, 8.0). The version that is running on the CICM-EM or on the pair of nodes is located on the *Maintenance* page.

Maintenance release and product release upgrades

The types of upgrades are either a maintenance release (MR) or a product release.

Maintenance release upgrades

A maintenance release (MR) upgrade involves loading an increment of the build number within the same version of the software release. For an MR upgrade to CICM software version 8.0, the MR changes the build number from 8.10.xxx to 8.10.MRy. For CICM version 8.0 or later, the range of build increments for one upgrade to the CICM nodes (excluding the CICM-EM) cannot exceed three increments. Examples of the range are shown with the upgrade procedure in Prerequisites to upgrading a CICM node with an MR.

The generic procedures to upgrade a CICM-EM and a CICM with an MR are in Upgrading CICM software.

MR upgrades are made available on CDs and on the CICM-EM web site as they are released.

Product release upgrade

A product release upgrade involves loading an increment of a different version of software, that is, the software release number increments (for example, from x.y to x+1.y).

The series of procedures to upgrade a CICM-EM and CICM are in Upgrading CICM software.

CICM product releases are made available from the ISO vault. Each release includes its own .cab upgrade file. Releases are available for each of the following:

- the CICM-EM using the CPV5370 cards
- the CICM-EM using the CPN5385 cards
- the CICM nodes using the CPV5370 cards
- the CICM nodes using the CPN5385 cards

MR upgrade implementation guidelines

The guidelines for implementing upgrades are as follows.

- Always read the release notes prior to an upgrade.
- The sequence of upgrading is to upgrade the CICM-EM, then the CICM nodes, then the terminals. If a primary and backup CICM-EM

pair are deployed, both EMs must be upgraded prior to the first CICM node upgrade.

Note: Terminal upgrades are addressed in Upgrading firmware on IP phone sets.

- Each node of the CICM is upgraded individually. However, paired nodes should be upgraded to the same software version. Running paired nodes at different versions for extended periods of time can result in degradation in performance or behavior.
- No network re-configurations are to occur during an upgrade, otherwise rolling back from the upgrade, that is, returning operation to the former software version, is not possible.
- Do the upgrade during the lowest call traffic period to minimize impact on users.
- The upgrade will take one to two hours to complete. Service degradation by call capacity reduction only occurs for portions of the upgrade period.
- For MR upgrades only, Resource utilization (that is, active call count) can be monitored from the CICM-EM.
- To do an upgrade procedure, you must use administrator userids and passwords to login to the CICM-EM.

Hardware revision compatibility

The table Hardware revision compatibility summarizes the hardware to software compatibility for CICM release SN08 and all previous releases.

CICM release 8.0 and later supports two hardware revisions. CICM release 8.0 or later does not support any hardware upgrade paths. If the

telco wants to upgrade from a release prior to CICM release 7.0, an interim upgrade to 7.0 is required.

Hardware revision compatibility

Hardware revision	CICM node	CICM-EM	Supported software releases
6.2	SAM 16 Shelf CPV5370 processor	CXIP1204 Shelf CPV5370 processor	6.12, 7.0, 8.0
7.0	SAM 21 Shelf CPN5385 processor	CXIP1204 Shelf CPV5370 processor	7.0, 8.0

Backing up the CICM-EM and CICM node software configuration

Back up the software of the CICM-EM and CICM nodes prior to an upgrade as a contingency plan to a failed or aborted upgrade. The back-up files are required for the procedures to roll back from an upgrade and restore the former software configuration.

The application that does a CICM node backup resides on the CICM and is controlled by a scheduler through the CICM-EM.

Backing up files can be done at any time either on-demand (manually) or daily (automatically). Backing up on-demand is handled through the CICM-EM while backing up daily is scheduled to run at a user-designated time or the 2:00 am default. The schedule is decided during initial configuration of a CICM node. The procedures to handle an on-demand backup are in Upgrading CICM software.

Backing up files can be done at any time either on-demand (manually) or daily (automatically). Backing up on-demand is handled through the CICM-EM while backing up daily is scheduled to run at a user-designated time or the 2:00 am default. The schedule is decided during initial configuration of a CICM node. The procedures to handle an on-demand backup are in Upgrading CICM software on page 11.

For either backup method, the result is a file with the name *backupconfig_<day_number>_em.xml* for a CICM-EM or *backupconfig_<day_number>.xml* for a CICM. The files are sent to the

CICM-EM through anonymous FTP and stored in this node-specific folder on the D drive of the PC with CICM software:

D:\CentrexIP\support\backups\<cicm_node>

The <day_number> is from the current month. The <cicm_node> is the full name of the CICM so that the backups of Nodes A and B are stored separately. When the first backup is taken, the node-specific folder is automatically created. The craftsperson is responsible for moving or copying the back-up files from the CICM-EM folders to a different and safer storage location before the files are automatically overwritten by the next day with the same date. The CICM-EM has a limited amount of storage space for the back-up files.

What the back-up file stores

The back-up procedure stores all elements of the MIB registry that are static data and that are directly relevant to the configuration of the CICM. The kind of data that is backed up by the procedure includes:

- virtual media gateways
- user configurations, including passwords, locality preferences, and contacts
- terminals, including locality preferences and the auto-login preference
- lines, including their features
- profiles of end-point equipment, including the global profile overrides stored on the CICM

Software upgrade restrictions and limitations

The restrictions and compatibility issues of the software changes are:

- The software upgrade to CICM release 8.0 or later can only be applied from a CICM running a specific MR with version 7.20 or later.
- During the upgrade when nodes temporarily have different versions of software, (for example, one node at release 7.0 and the other at release 8.0) a switch of activity (SWACT) will not result in any terminals being automatically recovered. A manually initiated terminal transfer is still necessary, as in release 7.0.
- During the upgrade when nodes temporarily have different versions of software, initiating a SWACT while the 8.0 or later node is the master will cause the floating UNIStim address to be unbound. Any terminals connected to this node will be lost. Manually transfer the terminals away from the 8.0 or later node before the SWACT.

- During the upgrade to CICM Node A, the CICM selects its existing static UNIStim address as the floating address.
- During the upgrade, the operator must provide an alternative static address to replace node A's old static address (used as the floating address following the upgrade).
- During the upgrade, the CICM does not update the S1 and S2 entries of the terminals connected to the CICM at the time of the upgrade. The operator must make any required configuration changes to the terminals following the upgrade (for example, through DHCP).
- For CICM release 8.0 or later, the Carrier Voice over IP (VoIP) environment and datafill remains consistent with how it was in release 7.0 Plus.

CAUTION
Risk of service prevention
When upgrading from release 7.0, it is critical to upgrade Node A first since the upgrade results in the use of Node A's pre-upgrade (7.0) static UNIStim address as the floating UNIStim address for the post-upgrade (8.0) operation.

Software upgrade strategy

Prerequisites for a CICM software upgrade

Before the software of a CICM node is upgraded, the following must be done.

1. Upgrade the CS2M, Core, and GWC.
2. Copy the CICM-EM upgrade .cab file to the location on the CICM-EM that is used for an upgrade.
3. Copy the CICM node upgrade .cab file to the location on the CICM-EM that is used for an upgrade.
4. Upgrade the CICM-EMs.
5. Upgrade the CICM nodes.

For the sequence of procedures, refer to the task flow in Upgrading CICM software.

CICM software upgrade summary

The CICM software upgrade strategy is summarized as follows.

- The supported software upgrade paths are from these CICM releases:
  - — 6.12 to 7.0
  - — 7.0 to 8.0
- The CICM release 7.0 to 8.0 upgrade must be performed remotely using a process similar to a maintenance release upgrade.
- A CICM release 7.0 to 8.0 upgrade must be performed remotely by telco CICM administrators using a process similar to a maintenance release (MR) upgrade.
- No hardware changes are required for upgrading software from CICM release 7.0 to 8.0.
- For any upgrades prior to 6.12 (such as release 2.4 to 2.5), refer to the *Upgrades* section of the previous versions of *CICM Basics*, NN10044-111 (formerly titled *CICM Product and Technology Fundamentals*).

Follow-up after a CICM software upgrade

After the CICM release 8.0 software upgrade is completed, address or note the following.

- Node B's static UNIStim address is no longer valid for use by terminals in the network. Once the upgrade is complete, it is recommended that the operator take the necessary steps to update all terminals in their network so that they do not attempt to contact the CICM on this (now) invalid address.

  If using dynamic host configuration protocol (DHCP), its configuration should be changed. Refer to DHCP documentation for information on configuration DHCP servers.
- Leaving terminals configured with the old B UNIStim address will not cause harm to the network. However, it may cause individual terminals to take longer to actually locate the CICM following a terminal reboot, since it may use the invalid address for its search.
- If a survivable remote gateway (SRG) is to be deployed, this can safely be done once the CICM has been upgraded. In doing so, the terminal must be reconfigured such that S1 is set to the CICM's floating UNIStim address, and S2 is set to the SRG's address. These must not be reversed. The SRG uses S2.
- For those terminals in the network not serviced by an SRG, it is recommended that both their S1 and S2 entries be set to the CICM's floating UNIStim address.

Conversion from TDM

CICM release 8.0 or later does not support a conversion from TDM to Carrier Voice over IP (VoIP).

Upgrading CICM software

This section of *NN10230-461 CICM Upgrades* provides the task flow and procedures to upgrade the software of a pair of redundant Centrex IP Client Manager (CICM) element managers (CICM-EMs) and their pairs of redundant CICM nodes.

The topics in this section are:

CICM-EM and CICM node software upgrades

The series of procedures to upgrade a pair of Centrex IP Client Manager (CICM) element managers (CICM-EM) and their pairs of CICM nodes are provided in a task flow.

Prerequisites to the task flow of CICM-EM and CICM node upgrades

Before following the task flow, ensure that you have addressed these requirements.

- The task flow and all procedures in it apply to doing these upgrades for either SAM 21 and SAM 16 hardware:
  - an MR from your current release up to three increments apart, for example, 8.0 MRx to 8.0 MRy where x and y are less than or equal to three increments apart or for example

    8.0 MR1 with 8.0 MR2, 8.0 MR3, or 8.0 MR4
  - a product release from your current release to a subsequent release, for example, from 7.0.MRx or later to 8.10

  Refer to the CICM Release Notes for the actual supported versions.
- All Carrier Voice over IP (VoIP) components that are non-gateway-specific (including the CS2000, CMT, and gateway controllers) must already have been successfully upgraded to the target upgrade release and be fully in service.
- IEMS must be configured to enable accessing the CICM-EM, usually as part of an initial installation. Otherwise refer to *Integrated EMS Configuration Management*, NN10330-511.
- CICM must be configured to interwork with IEMS, usually as part of an initial installation. Otherwise refer to *Configuration Management*, NN10240-511.
- The CICM-EM and CICM nodes must be in service without faults.

- Ensure that you have read and understood Preparing to upgrade CICM software.
- You must have Nortel's compact disks (CDs) available with the .cab files. The label on a CD containing CICM software begins *CICM*, for example:
  - on the 3 CDs from order code CICM0080 for CICM nodes:
    - CICM_5385_8.10.204.iso
    - CICM_5370_8.10.204.iso
    - CICM_Upgrade_8.10.204.iso
  - on 1 CD from order code CICE0080 for CICM-EMs:
    - CICMEM_5370_8.10.204.iso
    - CICMEM_5385_8.10.204.iso

  The *_5370_* indicates software for the SAM 16 hardware, while *_5385_* indicates software for the SAM 21.
- Upgrade files for either the CICM-EMs or the CICM nodes must be copied from the Nortel-supplied upgrade CD to a network server (such as an SSPFS) or personal computer (PC) and then transferred to the appropriate directory on the CICM-EM.
- Upgrading with an MR or product release is a manual operation. Start an upgrade during a period of lowest traffic for the CICM-EMs and CICM nodes.
- The pair of CICM-EM nodes must always be upgraded before the pair of CICM nodes.
- Once an upgrade has been started, do not attempt any software configuration changes to any node until each node-pair is confirmed to be upgraded and fully operational.

CAUTION
Risk of service prevention
Before starting the upgrades task, read each procedure to determine what data you will need for entries, especially the preboot and preboot upgrade IP addresses. It is critical to have all the data readily available before starting any procedure in the task flow CICM-EM and CICM node software upgrades.

Task flow of CICM-EM and CICM node upgrades

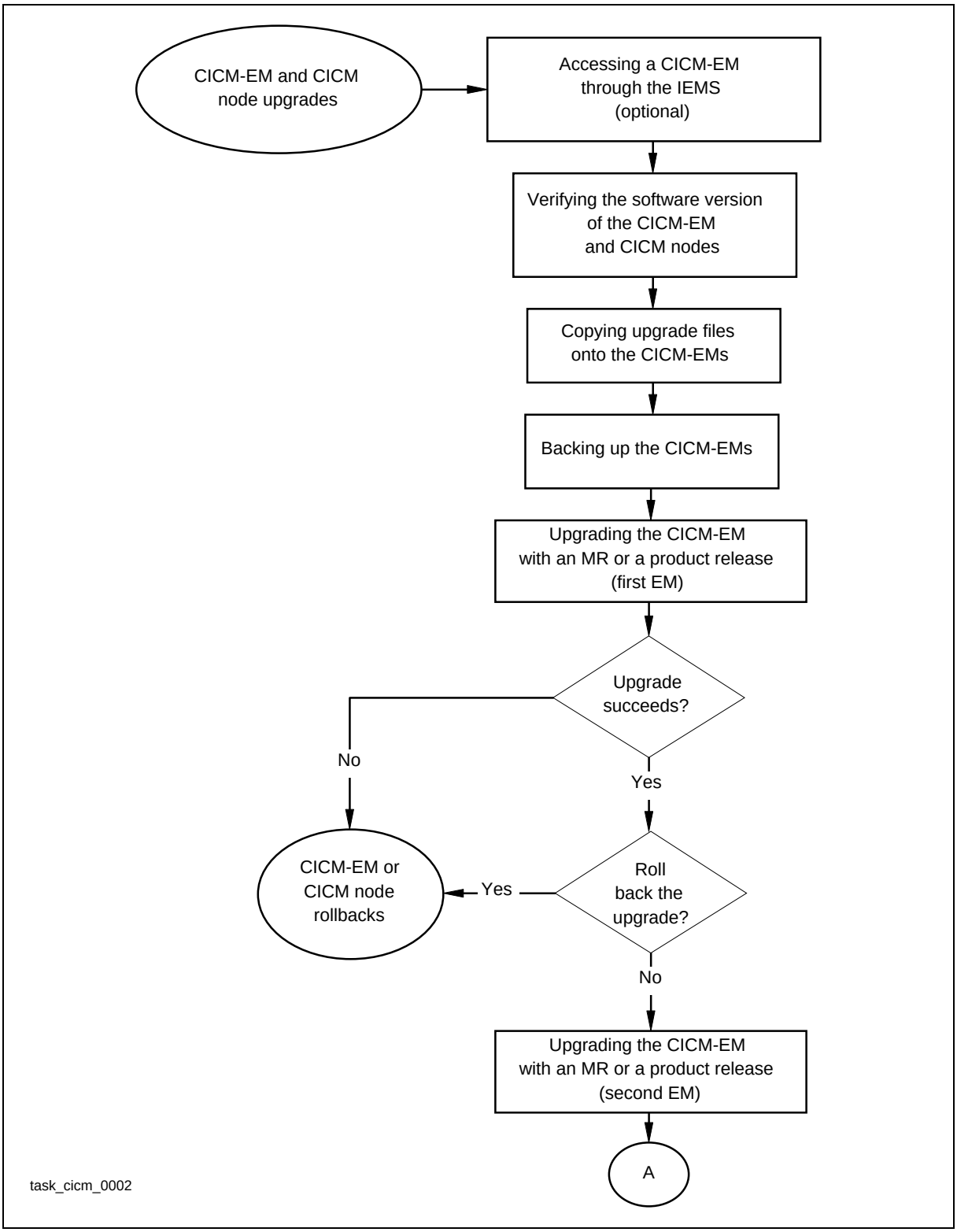
The task flow shows the sequence of procedures to upgrade a pair of redundant CICM-EMs and a pair of CICM nodes. The procedures are shown in the figures

- Task flow of CICM-EM and CICM node upgrades, part 1
- Task flow of CICM-EM and CICM node upgrades, part 2

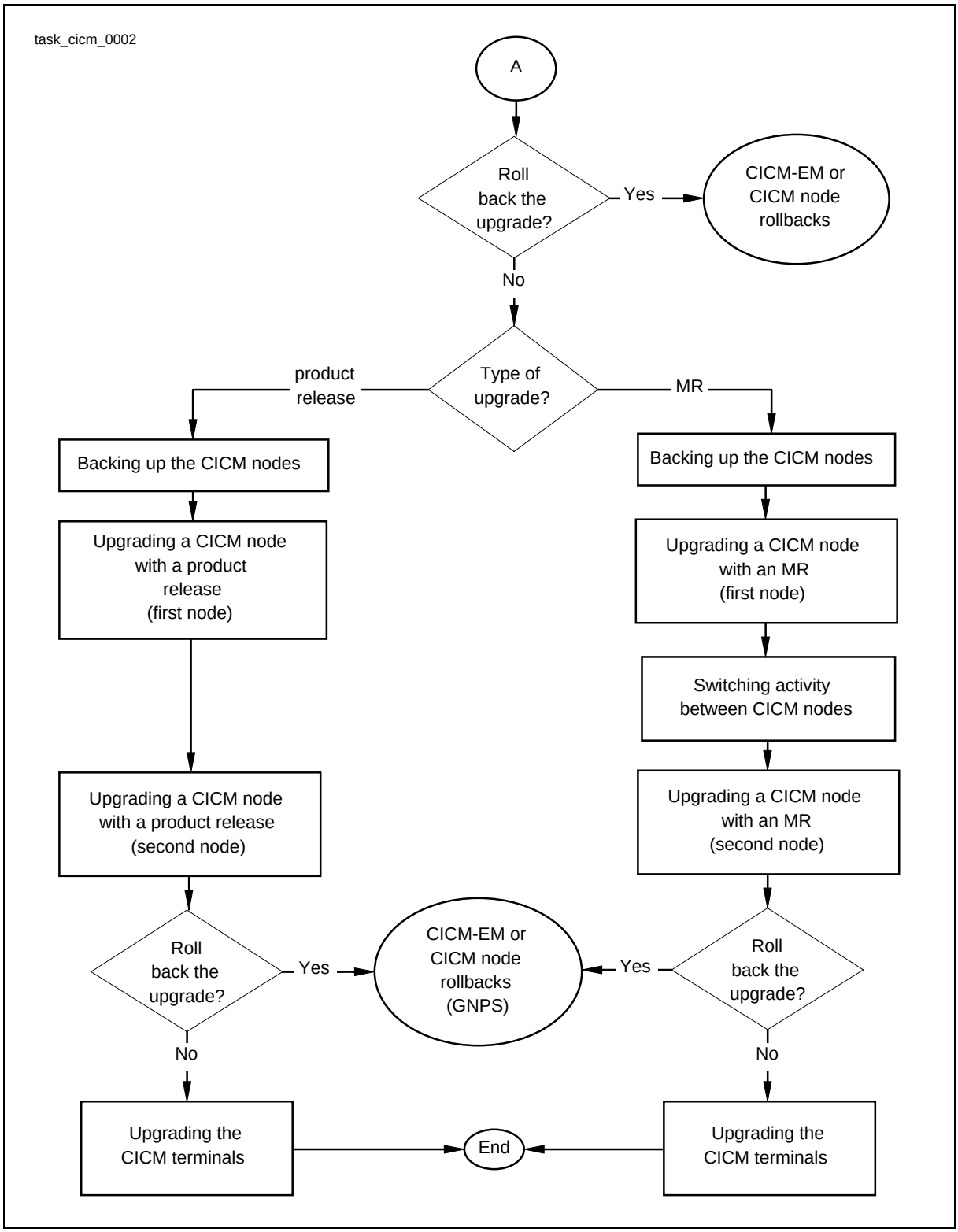
To link any procedure, go to Navigation immediately following the figure.

Note: Some of the rollback decision points do not appear in the task flow because they are included within various procedures.

Task flow of CICM-EM and CICM node upgrades, part 1



Task flow of CICM-EM and CICM node upgrades, part 2



Navigation

The procedures and task flow in the task flow are listed alphabetically.

- Accessing a CICM-EM through the IEMS
- Backing up the CICM nodes
- Backing up the CICM-EMs
- "CICM-EM and CICM node roll backs"
- Copying upgrade files onto the CICM-EMs
- Switching activity between CICM nodes
- Transferring terminals for an upgrade
- Upgrading a CICM node with a product release
- Upgrading a CICM node with an MR
- Upgrading the CICM-EM with an MR or product release
- Upgrading the CICM terminals. See the procedures in *m6350 Softclient Installation Guide*, NN10182-113.
- Verifying the software version of the CICM-EM and CICM nodes

Upgrade procedures for CICM-EM and CICM nodes

The procedures for upgrading the software of a CICM-EM pair and its CICM node pairs are listed alphabetically in this section. The sequence of doing the procedures is identified in CICM-EM and CICM node software upgrades.

Note: You must follow the sequence of procedures identified in the task flow in order to properly complete upgrading.

Accessing a CICM-EM through the IEMS

Access a CICM-EM through the integrated element management system (IEMS) to upgrade the CICM-EM or CICM nodes or both with a maintenance release (MR) or a product release.

Prerequisites to accessing a CICM-EM through the IEMS

Address the prerequisites before starting the procedure.

- You must follow the Prerequisites and sequence of procedures identified in CICM-EM and CICM node software upgrades.
- To access IEMS, you must know the IP address of the IEMS server and be able to access it through a web browser.
- You must use an administrator userid and password to log into the CICM-EM from IEMS. Otherwise your access is determined by whatever authentication structure you have configured.

Procedure steps to accessing a CICM-EM through the IEMS

At a web browser

1 Access the IEMS by entering the command:

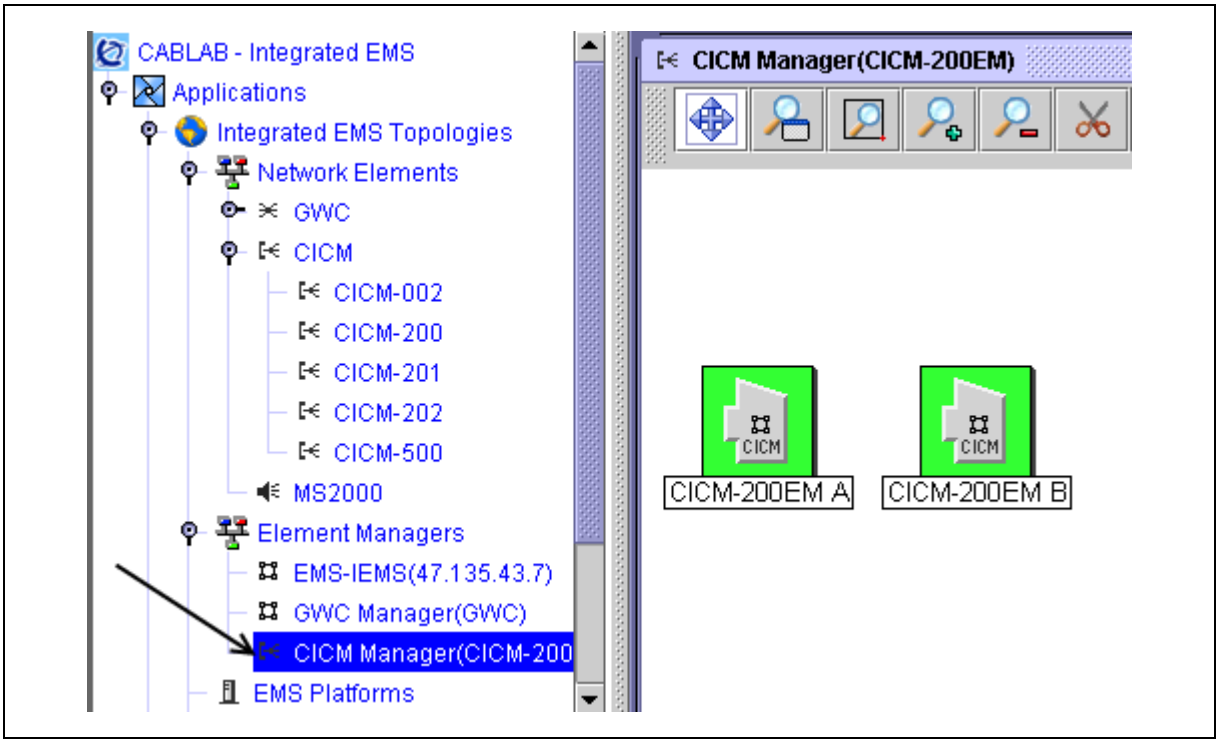
https://<iems_ip_address>:9091/LoginPage.do

2 Once connected, click on option **Web Start Client** (which uses JAVA rather than html).

Unless already installed, you must install the version of JAVA that is provided at the *Web Start Client* link.

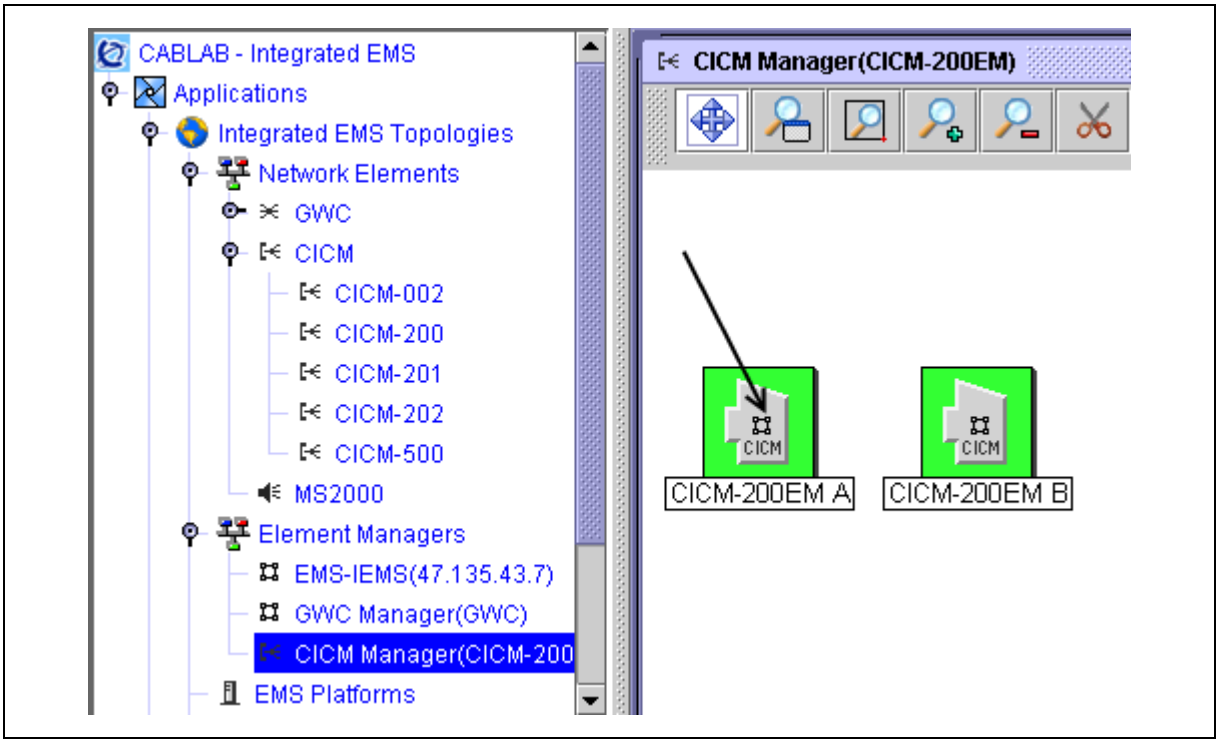
At the IEMS GUI

3 At the IEMS menu of components, locate the item for the CICM-EM to undergo an upgrade. Ensure that the static IP address of the CICM-EM is for the one to be upgraded.



4 Right click the icon of the CICM-EM to undergo an upgrade, and select **Launch CICM Manager**.

A prompt occurs for the userid and password.



5 Enter the CICM-EM administrator userid and password.

The CICM-EM web page opens.

6 Ensure that the node you selected is in-service.

7 To upgrade a pair of CICM-EM or CICM nodes, follow the other procedures in the task flow.

8 This procedure is complete. Return to the task flow Task flow of CICM-EM and CICM node upgrades, part 1.

Backing up the CICM nodes

Back up each node of a redundant CICM pair to prepare for restoring a former software configuration when you want a more recent snap-shot than the scheduled back-up file.

Prerequisites to backing up the CICM nodes

Address the prerequisites before starting the procedure.

- Ensure that you have read and understood Backing up the CICM-EM and CICM node software configuration.
- Back up each node of a CICM pair. The back-up file can only be applied to the node it was taken from.
- Each back-up file name must remain the same as the copied file.
- The back-up files must be used only with the identical software release that they were created from.
- The duration of backing up varies according to the amount of datafill configured on the CICM node. The back-up application runs at a low level of software priority to minimize the impact on the service provided (call processing).
- Backup files for CICM nodes are stored on the CICM-EM in subdirectories at:

  d:\centrexip\support\backups\<cicm-nnn>
- Automated daily backups are stored on alternate CICM-EM nodes.

Procedure steps to backing up the CICM nodes

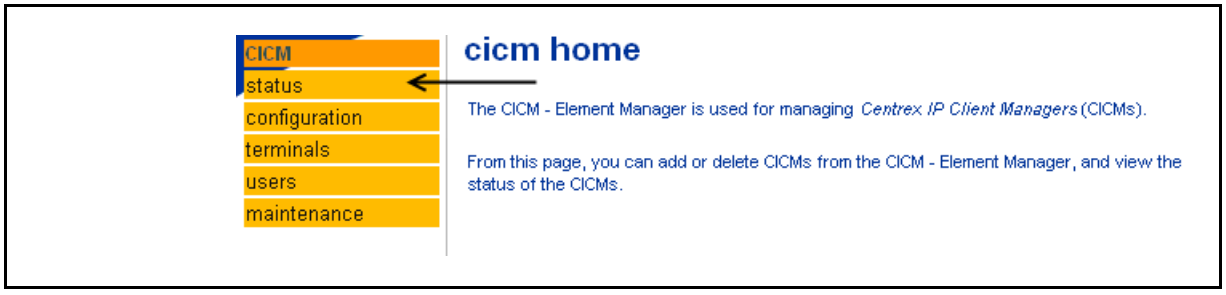
At the PC desktop for remote access to the CICM-EM

1 Access the CICM-EM of the CICM node being backed up from your PC through a web interface by entering:

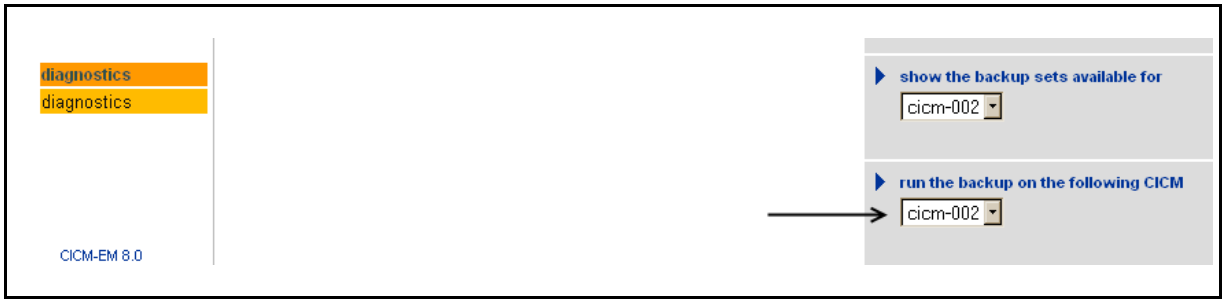
https://<unique_admin_ip_address_of_cicmem>/centrexip

At any CICM-EM web page

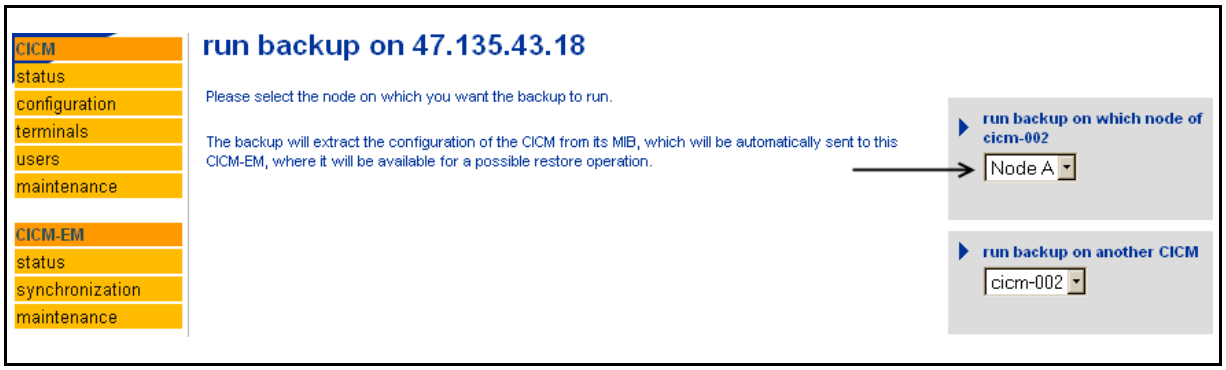
2 In the menu CICM, click on **status**.



3 Select the CICM to be backed up on the drop-down menu and click on **run the backup on the following CICM**.



4 From the pull-down menu, select the CICM *Node A* or *Node B* from which you want to run the backup.



5 Click on **run backup on which node of cicm-nnn**, where nnn echoes the node you selected.

6 Wait for this message which indicates the backup was successful:

```
The backup of the configuration for
<cicm_node_IP_addr> completed successfully.
```

7 Copy the back-up file called *backupconfig_<day_number>.xml* from the CICM-EM folder called *D:\CentrexIP\support\backups\<cicm-nnn>* to your location for storing such files, for example, in the Carrier Voice over IP (VoIP) server platform foundation (SSPS) server. The storage location must be off the CICM-EM. Use a secure FTP session (such as WinSCP) to transfer the file.

Note: Ensure that the copied back-up file ends up with the same name as the original.

8 Repeat the backing up for the mate node starting at step 3.

9 This procedure is complete. Return to the task flow Task flow of CICM-EM and CICM node upgrades, part 1.

Backing up the CICM-EMs

Back up each node of a redundant CICM-EM pair to prepare for restoring a former software configuration when you want a more recent snap-shot than the scheduled back-up file.

Prerequisites to backing up the CICM-EM nodes

Address the prerequisites before starting the procedure.

- Ensure that you have read and understood Backing up the CICM-EM and CICM node software configuration.
- Back up each node of a CICM-EM pair. The back-up file can only be applied to the node it was taken from.
- The back-up file name must remain the same as the copied file. Manual (on-demand) backup files have the form *EMDUMP_CICMEM-<node>_<day_number>.xml*. Scheduled backup files have the form *backupconfig_<day_number>_em.xml*, where <day_number> is the day of the month. In the procedure at step 6 you can use the scheduled back-up file instead of the manual back-up file.
- The duration of backing up varies according to the CICM-EM configuration and your access to the CICM-EM. The back-up application runs at a low level of software priority to minimize the impact on the CICM-EM.
- Backup files for CICN-EMs are stored on the CICM-EM in subdirectories at:

  d:\centrexip\support\backups\<cicmem-nnn>

- Automated daily backups are stored on alternate CICM-EM nodes.

Procedure steps to backing up the CICM-EM nodes

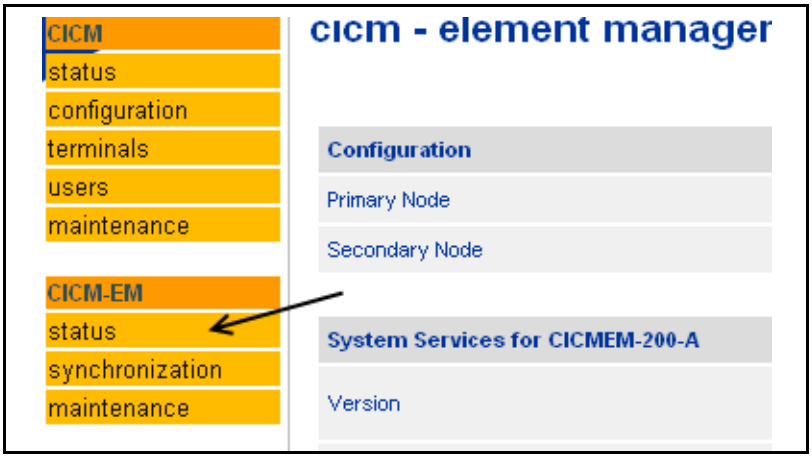
At the PC desktop for remote access to the CICM-EM

1 Access the CICM-EM that iis being backed up from your PC through a web interface by entering:

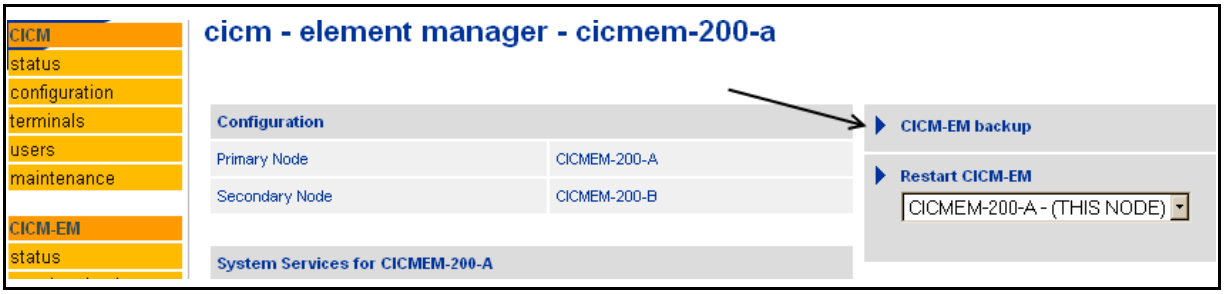
https://<unique_admin_ip_address_of_cicmem>/centrexip

At any CICM-EM web page

2 In the menu CICM-EM, click on **status**.



3 Click on **CICM-EM backup** to start backing up the file.



4 From the response, record the folder path under *Creating file* and the name under *secondary file* (see the example below).

5 Wait for this message indicating a successful backup:

```
Backup of configuration data from CICMEM-<node>
is complete.
```

6 Copy the on-demand back-up file called

EMDUMP_CICMEM-<node_number>_<day_number>.xml

for example,

EMDUMP_CICMEM-200-A_TueFeb151826582005.xml

from the CICM-EM folder called

D:\CentrexIP\support\backups

to your location for storing such files, for example, in the Carrier Voice over IP (VoIP) server platform foundation (SSPS) server. The storage location must be off the CICM-EM. Use a secure FTP session (such as WinSCP) to transfer the file.

Note: Ensure that the copied back-up file ends up with the same name as the original.

7 Access the CICM-EM mate node from your PC through a web interface by entering:

https://<unique_admin_ip_address_of_mate_cicem> /centrexip

8 Repeat this procedure from step 2 to step 6 to back up the mate node.

9 This procedure is complete. Return to the task flow Task flow of CICM-EM and CICM node upgrades, part 1.

Copying upgrade files onto the CICM-EMs

Load the upgrade files onto the SSPFS server and copy them onto each CICM-EM of a redundant pair to make them available for upgrading the CICM-EM and CICM nodes.

Prerequisites to copying upgrade files onto the CICM-EMs

Address the prerequisites before starting the procedure.

- You must follow the Prerequisites and sequence of procedures identified in CICM-EM and CICM node software upgrades.
- You must know the unique Administration IP addresses of each CICM-EM of the pair.
- Both CICM-EMs must be in-service to enable accepting the files.
- Equivalent equipment to the role of the UNIX-based SSPFS server can also be used, in which case, use the procedure as a guide to indicate directories and file names. For example, the SSPFS login steps in the procedure will likely be different for a PC or other equivalent computer.
- You need a working knowledge of UNIX.

Procedure steps to copying upgrade files onto the CICM-EMs

At the UNIX-based SSPFS server or equivalent

1 Load the CD with the upgrade files into the CDROM drive.

The label on a CICM software CD starts with CICM. Examples include:

2 Telnet to the SSPFS or equivalent and log in.

3 Become the root user by entering:

su root

4 Go to the top level directory of the CDROM by entering:

cd /cdrom/cdrom0

The last character of **cdrom0** is a zero.

5 List the files at the directory by entering:

ls -al

Upgrade files for the CICM-EMs have names beginning with *EM_*. Upgrade files for the CICM nodes have names beginning with *GW_*.

6 Go to the directory containing the upgrades files by entering, for example:

cd “Upgrade Files”

7 FTP to the CICM-EM and log into it by entering:

ftp <admin_ip_address_of_cicmem>
<name>
<password>

where <name> is the <userid> of the CICM products, which is administrator, and <password> is the administrator’s passwords.

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

cd /firmware/elementmgr_mrs

9 Set the FTP mode to binary:

bin

10 Copy each EM_ file to the CICM-EM directory */firmware/elementmgr_mrs*:

put EM_...
put EM_...
...
put EM_UPGRADE_...

11 Confirm all EM_ files are present:

ls -al

At this directory, obsolete CICM-EM MR files from previous releases can be removed or archived elsewhere.

12 Go to the directory on the CICM-EM where the CICM node (gateway) upgrade files are to be copied:

cd /firmware/gateway_mrs

13 Copy each GW_ file to the CICM node directory:

put GW_...
put GW_...
...
put GW_UPGRADE_...

14 Confirm all GW_ files are present:

ls -al

At this directory, obsolete gateway .cab files from previous upgrades can be removed or archived elsewhere.

15 Repeat the copying onto the second CICM-EM, starting from step 7. Use the static IP address of the second CICM-EM.

16 Repeat the copying of each additional CD with required files, starting from step 7. Repeat until all the files are copied.

17 Close the FTP session:

quit

18 Release the CD from the server:

cd /
eject cdrom

19 This procedure is complete. Return to the task flow Task flow of CICM-EM and CICM node upgrades, part 1.

Switching activity between CICM nodes

Switch the activity from the master CICM node to the slave node of the redundant pair.

Prerequisites to switching activity between CICM nodes

Address the prerequisites before starting the procedure.

- You must follow the Prerequisites and sequence of procedures identified in CICM-EM and CICM node software upgrades.
- Both nodes must be in-service to enable the switch of activity (SWACT) to occur.
- After the upgrade and before the SWACT, Node A is the slave with status *running* and with no terminals connected to it.
- When upgrading with an MR for SN08 or later, the CICM terminals are automatically transferred during the switch of activity.

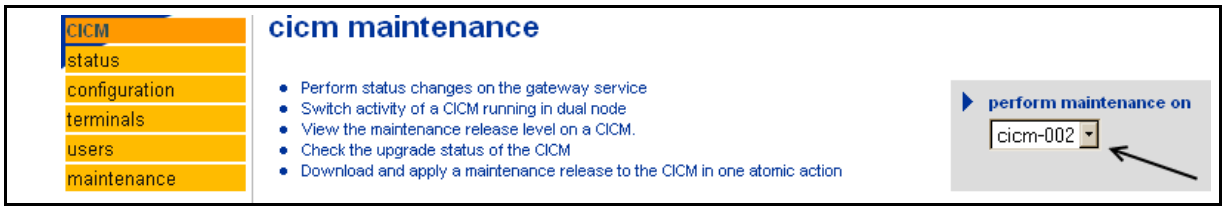
Procedure steps to switching activity between CICM nodes

At any CICM web page

1 In the menu CICM, click on **maintenance**.

At the cicm maintenance page

2 Select the CICM node number from the drop-down menu.



3 Click on **perform maintenance on**.

4 Observe from the *Node Maintenance status* of each node which ones are master and slave.

5 Click on **switch activity**.

The duration of the switchover varies according to the number of users configured on the nodes and the volume of calls being sustained in the node at the time of the SWACT.

When both nodes are not available for a SWACT, the command button is tinted grey and disabled. Ensure that both nodes are in service.

6 Click on **Confirm switch of activity**.

7 Confirm from the *Node Maintenance status* whether the master and slave have switched successfully:

- the *Node status* is *master*
- the *Node Maintenance status* is *system idle*

If not, then contact your next level of support to determine why.

8 This procedure is complete. Return to the task flow Task flow of CICM-EM and CICM node upgrades, part 1 or the step in the procedure Upgrading a CICM node with a product release from where you came:

- step 4 (before applying the .cab upgrade file)
- step 15 (after applying the .cab upgrade file)

Transferring terminals for an upgrade

Transfer the terminals (clients) from one CICM node to another to ensure that service is maintained or can be restored.

Prerequisites to transferring terminals for an upgrade

Address the prerequisites before starting the procedure.

- You must follow the Prerequisites and sequence of procedures identified in CICM-EM and CICM node software upgrades.
- When upgrading from SN07, a transfer of terminals must be done manually, as indicated in the procedure. A transfer process:
  - transfers terminals that are not in-call (handling a call)
  - notifies the users of in-call terminals that a maintenance activity is pending and asks them to terminate their session as soon as possible
  - after a telco-defined timeout period, forces the in-call terminals to transfer (thereby dropping all calls in progress)
- Have a working CICM terminal (for example, an m6350 or IP Phone 200x) available to test the operation of an upgraded node.
- The section “Terminal transfers” and the procedure “Perform a terminal transfer” in *CICM Security and Administration*, NN10252-611.

Procedure steps to transferring terminals for an upgrade

At the CICM maintenance status (cicm-nnn) page

1 On the right menu, ensure that **start auto refresh** is showing, but do not click on it.

If **stop auto refresh** is shown, click on it to show **start auto refresh**.

2 When upgrading the first CICM node, which is always node A, transfer its terminals to the mate by clicking on **from node A to node B** at the Node drop-down menu.

When upgrading the second CICM node, which is always node B, transfer its terminals to the mate by clicking on **from node B to node A.**

3 Select the minutes from the *Terminal Shutdown Timeout* drop-down menu. The minutes are to allow CICM clients time to log off themselves before they are automatically dropped by the transfer.

4 Click on **transfer terminals**.

5 When the confirmation screen appears, click on **confirm terminal transfer**.

```
The terminal transfer will commence immediately
upon confirmation, and will terminate when the
selected timeout interval has expired.
```

6 Click on **start auto refresh** of the *maintenance status (cicm-nnn)* page.

The button **stop auto refresh** appears.

During a transfer when Node A has SN08 and Node B has SN07, the statuses shown for *Terminal service* (SN07) and *Terminal status* (SN08) indicate temporary transitional hybrid combinations. Since terminal transfers are handled differently between SN07 and SN08, ignore the transitional terminal statuses.

7

CAUTION
Risk of service interruption
Wait until the terminal transfer has completed before proceeding. If the transfer does not complete, discontinue the procedure and contact your next level of technical support to determine your next actions.

When the terminals have transferred, all should be hosted on CICM Node A. Completion of the transfer is indicated by *stopped* or *inactive* appearing for *Terminal service* (SN07) or *Terminal status* (SN08).

8 This procedure is complete. Return to the step in the procedure Upgrading a CICM node with a product release from where you came:

- step 5 (before applying the .cab upgrade file)
- step 17 (after applying the .cab upgrade file)

Upgrading a CICM node with a product release

Upgrade the CICM slave node with a product release as part of upgrading all CICM components in a network.

Prerequisites to upgrading a CICM node with a product release

Address the prerequisites before starting the procedure.

- You must follow the Prerequisites and sequence of procedures identified in CICM-EM and CICM node software upgrades.
- You must determine the new unique static UNIStim IP address for Node A.
- You must use an administrator userid and password to log into the CICM-EM from a remote PC for this upgrade.
- A CICM node fails an upgrade when it does not return to service and the version of the upgrade does not appear beside the *Version* status. When an upgrade fails, you must re-attempt the upgrade or roll back from the upgrade.
- Always upgrade node A first. A node must be the slave before it can be upgraded. When Node A is the master, it must be made the slave as indicated in the procedure.

CAUTION
Risk of service outage
It is critical to upgrade Node A first since the upgrade results in the use of Node A's pre-upgrade (SN07) static UNIStim address as the floating UNIStim address for the post-upgrade (SN08) operation.

Procedure steps to upgrading a CICM node with a product release

At the CICM-EM home page through the web interface

1 When upgrading the second CICM node of a redundant pair, start this procedure from step 19. Do not repeat the procedure a third time for the same upgrade to the same pair of nodes.

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

2 Access the CICM-EM of the CICM node from your PC through a web interface by entering:

https://<unique_admin_ip_address_of_cicmem>/centrexip

At the cicm maintenance page

3 In the menu CICM, click on **maintenance**.

4 From the display *Node Maintenance status*, determine the statuses of Nodes A and B.

When upgrading Node A, Node B must be the master. When Node A is the master, do the procedure Switching activity between CICM nodes and return to this step.

When upgrading Node B, Node A must be the master. When Node B is the master, do the procedure Switching activity between CICM nodes and return to this step.

At the cicm maintenance status (cicm-nnn) page

5 When upgrading the first or second CICM node of a redundant pair, transfer all terminals from the node being upgraded to its mate using the procedure Transferring terminals for an upgrade.

6 On the right menu, ensure that **start auto refresh** is showing, but do not click on it.

If **stop auto refresh** is shown, click on it to show **start auto refresh**.

7 Apply the upgrade .cab file to Node A (or B) as follows.

a From the **Maintenance Release** drop-down menu, select the appropriate upgrade .cab file. The .cab files for a CICM node start with GW in the file name.

b From the **Node** drop-down menu, select Node A (or B).

c Click on **apply maintenance release**.

8 Confirm applying the upgrade by clicking on the prompt **confirm maintenance release application**.

The prompt applies to either an MR or a product release upgrade.

9 Track the progress of the upgrade to the slave CICM node by clicking on **start auto refresh**.

10 Monitor Node A (or B) as it goes through a series of restarts as part of the upgrade process. When *Node Maintenance status* of

Node A displays the status *awaiting external step*, then proceed to the next step.

At the PC desktop for remote access to the CICM node

11

CAUTION
Risk of service prevention
Take extreme care when entering preboot data. Errors may result in unexpected and undesirable behavior when the node later attempts to return to service.

Telnet to the admin IP address of the node being upgraded to enter the following commands.

Note: Preboot will collect a new static UNIStim IP address for one on Node A. This step will modify the routing tables to match the required new configuration.

a At the CLI prompt (shown as*C:\temp>*), enter the preboot command, for example: **preboot /upgrade**

b Enter the floating UNIStim IP address for this CICM, for example: **47.165.76.180**.

Note: The floating UNIStim address must be identical to the existing static UNIStim address of Node A. You must use the existing 7.xx Node A static UNIStim IP address as the new 8.xx floating UNIStim IP address.

c Enter the new static UNIStim IP address for Node A, for example: **47.165.76.181**

d Enter the existing static UNIStim IP address for Node B, for example: **47.165.76.185**

e Enter the existing network mask for the UNIStim IP network, for example: **255.255.255.0**

f Enter the existing default route for the UNIStim IP network, for example: **47.165.76.1**

or for no route (for the clients to communicate only within the same subnet instead of to the gateway), enter: **0.0.0.0**

Enter a no route only if you do not have a default and you understand the consequences of not having one.

```
[SC] ChangeServiceConfig SUCCESS
The DHCP Client service is starting.
```

```
The DHCP Client service was started
successfully.

Applying IP Address and Subnet Mask: The
ReturnValue is 96 (4 byte int)
The DHCP Client service is stopping.
The DHCP Client service was stopped
successfully.

[SC] ChangeServiceConfig SUCCESS

Correcting H248 routing...
Deleting old defunct routes...
Marking the upgrade step as run...
Preboot /upgrade completed successfully.
```

12 At the last step to the preboot, you will receive a prompt to restart the node to complete the upgrade. Enter **Y** to confirm.

13 Wait for the reboot to occur. The duration depends upon the number of configured users for the CICM node.

After the reboot, the final changes will be applied to the node, then the node will be brought into service as a CICM slave running the new release.

At the maintenance status (cicm-nnn) page

14 Monitor the status of Node A until it is running as slave before proceeding.

> ***Note:*** While Node A is the slave, it is bound to its new static UNIStim IP address but not the floating UNIStim IP address. The floating address is always bound to the master node for SN08 or later. At this point in an upgrade, terminals cannot be connected to Node A while it is a slave.

At this point you can choose to roll back the upgrade as described in “CICM-EM or CICM node rollbacks” with no SWACT and no terminal transfers.

15 Do the procedure Switching activity between CICM nodes.

Following the switch of activity (SWACT), as the master, Node A becomes the master and is bound to the UNIStim floating address. Node B continues to be running version 7.xx, so it continues to be bound to its static UNIStim address.

16 Verify that Node A is working properly, which means:

- the *Node status* is *master*
- the *Node Maintenance* status is *system idle*
- the *Version* is w.xx.yyy of the target upgrade version, for example, 8.10.183

If Node A is not working properly, you must discontinue this procedure and follow the rollback path indicated in the task flow "CICM-EM or CICM node rollbacks".

At this point you can choose to roll back the upgrade as described in "CICM-EM or CICM node rollbacks" with a SWACT and no terminal transfers.

17 Prior to upgrading the second CICM node of a redundant pair, transfer all terminals from the node being upgraded to its mate using the procedure Transferring terminals for an upgrade.

18

CAUTION
Risk of service prevention
This is the last chance to roll back a node. Once an upgrade to the second node is attempted, a rollback then becomes a re-installation of the base software and upgrades for each node. Nortel's GNPS must be requested to do the re-installation.

At this point you can choose to roll back the upgrade as described in the task flow "CICM-EM or CICM node rollbacks" with a SWACT and terminal transfers.

19 With Node B in slave mode and hosting no terminals, begin the upgrade of Node B by repeating step 7 to step 13.

Note: While Node B is starting, you can monitor its status. On start-up of the slave node, there is a delay before the load achieves a state of synchronization with the master. Only when this data synchronization is achieved is it possible to initiate a switch of activity.

20 Verify that Node B is working properly, which means:

- the *Node status* is *master*
- the *Node Maintenance* status is *system idle*
- the *Version* is w.xx.yyy of the target upgrade version, for example, 8.10.183

If Node B is not working properly, you must contact your next higher level of technical support to determine what to do next.

The command button for terminal transfer is no longer present.

At the IEMS interface

21 Edit the object properties in the IEMS for the CICM network elements you just upgraded to reflect the new software version. Refer to either of the procedures that follow to update the software version in the field *Device Version*:

- Editing and viewing object properties using Java Web Client
- Editing and viewing object properties using Web Client

22 This procedure is complete. Return to the task flow Task flow of CICM-EM and CICM node upgrades, part 1.

Also address After an upgrade from CICM SN07 to SN08. These are to be done as part of the upgrade, but independently from the task flow.

After an upgrade from CICM SN07 to SN08

After the CICM release SN08 upgrade has been completed, address the following.

- Node B's static UNIStim address is no longer valid for use by terminals in the network. Once the upgrade is complete, it is recommended that the operator take the necessary steps to update all terminals in their network so that they do not attempt to contact the CICM on this (now) invalid address.

  If using DHCP, its configuration should be changed. Refer to DHCP documentation for information on configuration DHCP servers.

- Leaving terminals configured with the old B UNIStim address will not cause harm to the network. However, it may cause individual terminals to take longer to locate the CICM following a terminal reboot, since it may use the invalid address for its search.

- If a survivable remote gateway (SRG) is to be deployed, this can safely be done once the CICM has been upgraded. In doing so, the terminal must be reconfigured such that S1 is set to the CICM's floating UNIStim address, and S2 is set to the SRG's address. These must not be reversed. The SRG uses S2.

- For those terminals in the network not serviced by an SRG, it is recommended that both their S1 and S2 entries be set to the CICM's floating UNIStim address.

Upgrading a CICM node with an MR

Upgrade a CICM node with a maintenance release (MR) upgrade to CICM nodes already running the same software release (for example, both have release 8.10 MR1).

Prerequisites to upgrading a CICM node with an MR

Address the prerequisites before starting the procedure.

- You must follow the Prerequisites and sequence of procedures identified in CICM-EM and CICM node software upgrades.
- Both nodes of a CICM pair must operate with the same version of software prior to and after the upgrade. Operating within three MRs applies only during the transition of upgrading two nodes one at a time. The nodes are updated one at a time using the same procedure as indicated by the task flow.
- Always upgrade the slave node first and one node at a time.
- Both nodes of the CICM must be in service for an upgrade to complete successfully.
- You must use the administrator userid and password to log into the CICM-EM for this upgrade.
- Terminals connected to the node being upgraded will maintain service while they locate the mate node.
- Active calls using resources on the node being upgraded are maintained.
- When the system detects an invalid software release or corrupt file for an upgrade, the CICM node does not apply the upgrade and will resume activity at its current software release.
- A CICM node fails an upgrade when it does not return to service and the version of the upgrade does not appear beside the Version status. When an upgrade fails, you must re-attempt the upgrade or roll back from the upgrade.

Procedure steps to upgrading a CICM node with an MR

At the CICM-EM home page through the web interface

1 When upgrading the second CICM node of a redundant pair, start this procedure from step 4. Do not repeat the procedure a third time for the same upgrade to the same pair of nodes.

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

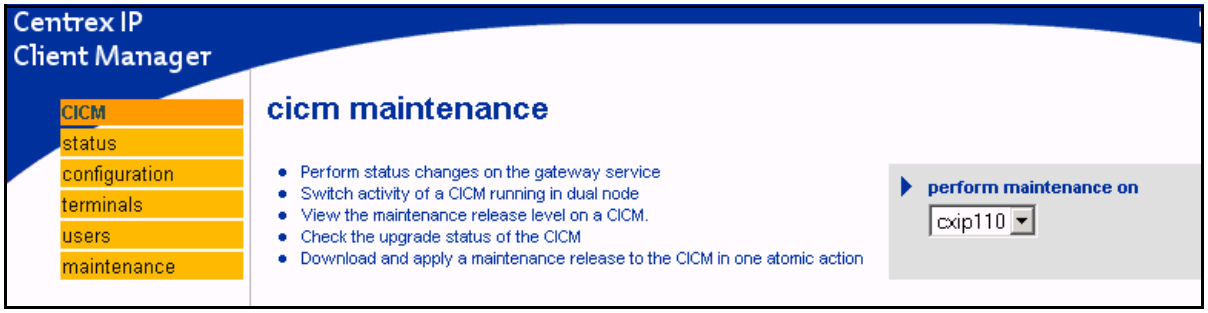
2 Access the CICM-EM from your PC through a web interface by entering:

https://<unique_admin_ip_address_of_cicmem>/centrexip

At any CICM-EM web page through the web interface

3 In the menu CICM, click on **maintenance**.

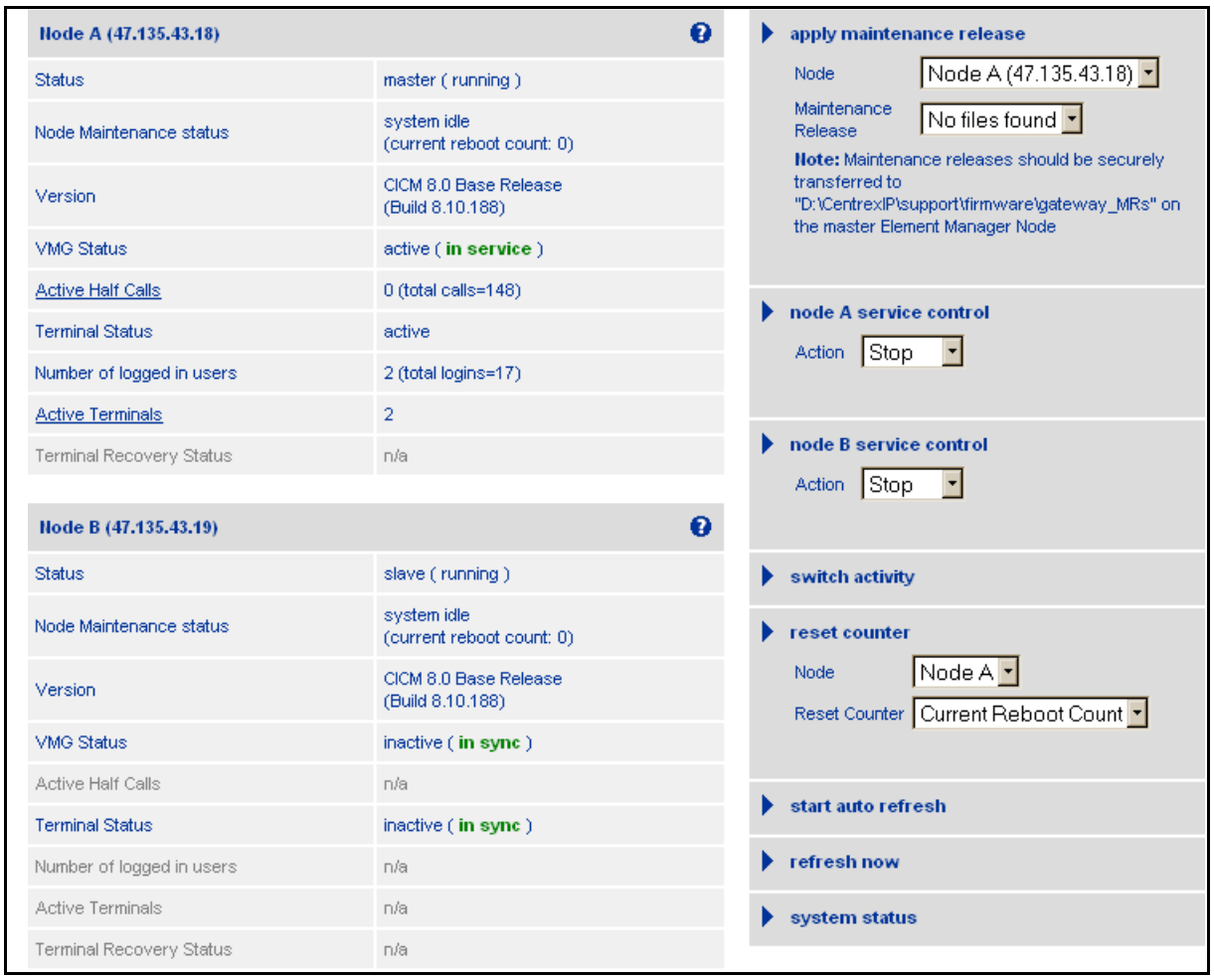
The page *cicm - maintenance* opens.



4 Select the CICM to upgrade from the drop-down menu below **perform maintenance on**.

The page *maintenance status (cicm-nnn)* opens. The current software version for each node is displayed.

The display **Node maintenance status** indicates the actions that are being performed on that node (for example, *system idle*, *stopping the cxipboot service*, and *starting the cxipboot service*). When the node is in service, it displays *system idle* or *system running*.



At the maintenance status (cicm-nnn) page

5 Ensure that **start auto refresh** is showing. If **stop auto refresh** is displayed, click on it. Stopping the auto refresh will stabilize the drop-down menus used.

6 Apply the maintenance release as follows from the right menu bar:

a Select the node to upgrade from the *Node* drop-down menu.

b Select the CICM MR upgrade file to apply from the *Maintenance Release* drop-down menu.

The name of a .cab file for a CICM node starts with GW. (The name of a .cab file for a CICM-EM starts with EM.)

Note: In the figure of maintenance status in step 4, the display *Maintenance Release* indicates the available maintenance releases, or it displays *No files found* when

there are no upgrade files of the appropriate names found in the designated directory.

c Click on **apply maintenance release**.

d Verify the proper node and file have been selected, then click on **confirm maintenance release application**.

The page *maintenance status (cicm-nnn)* updates to show the status of the upgrade.

7 To aid in monitoring the progress of the update, click on **start auto refresh** for a periodic automatic refresh of the status pages.

To stop automatic refresh when monitoring is complete, click on **stop auto refresh**.

The **auto refresh** option toggles between **start** and **stop**.

8 To monitor the progress of the upgrade, click on **system status**.

The page *<cicm-nnn> cicm status* opens and displays the status details of the CICM.

At the <cicm-nnn> cicm status page

9 Monitor the *<cicm-nnn>* status until *Service* shows *running*.

A manual restart of the node is not required.

10 Upon successful completion of the upgrade, click on **perform maintenance on <cicm-nnn>** to return to the maintenance status.

At the maintenance status (cicm-nnn) page

11 Check the new CICM node version as displayed beside *Version* of the *Node A and B* status.

12 Perform test calls on the upgraded node to verify that the upgraded node is working.

If calls cannot occur on the first upgraded node, you must roll back the upgrade as described in the task flow “CICM-EM or CICM node rollbacks”.

13

CAUTION
Risk of service prevention
After upgrading the first CICM node, this is the last chance to roll back the upgrade. Once an upgrade to the second node is attempted, a rollback then becomes a re-installation of the base software and upgrades for each node. Nortel's GNPS must be requested to do the re-installation.

If the tests pass for the first upgraded node, you can choose to roll back the upgrade as described in the task flow "CICM-EM or CICM node rollbacks".

At the IEMS interface

14 Edit the object properties in the IEMS for the CICM network elements you just upgraded to reflect the new software version. Refer to either of the procedures that follow to update the software version in the field *Device Version*:

- Editing and viewing object properties using Java Web Client
- Editing and viewing object properties using Web Client

15 This procedure is complete. Return to the task flow Task flow of CICM-EM and CICM node upgrades, part 2.

Upgrading the CICM-EM with an MR or product release

Upgrade a CICM element manager (CICM-EM) of a redundant pair with a maintenance release (MR) or a product release.

Prerequisites to upgrading the CICM-EM with an MR or a product release

Prerequisites to upgrading the CICM-EM with an MR or a product release include the following.

- You must follow the Prerequisites and sequence of procedures identified in CICM-EM and CICM node software upgrades. The first occurrence of a procedure is for the slave CICM-EM, and the second occurrence is for the master after it becomes the slave.
- The CICM-EM node-pair can support CICM node-pairs running either the same version or one previous version (for example, the EMs running 9.0 while a pair of nodes run 7.0 or 8.0).
- You need a PC or equivalent to remotely access the CICM-EM web pages. Upgrading is not done locally to a CICM-EM.
- When upgrading the master CICM-EM, it will automatically become the slave node as part of the upgrade process. You may have a brief disconnect from the CICM-EM maintenance page during this phase.
- You must use an administrator userid and password to log into the CICM-EM for this upgrade.
- A failed CICM-EM upgrade is indicated by one of the following.
  - The upgrade aborts and the system stays at the pre-upgrade release.
  - The upgraded CICM-EM hangs and remains out of service.

CAUTION
Risk of service prevention
Before upgrading the first CICM-EM of a redundant pair to a different version of software, both must be running the same software version, including the same MR incremental version. For example, version 8.10.001 is the same release as 8.10.200 but not the same version.

Procedure steps to upgrading the CICM-EM with an MR or a product release

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

1 Access the CICM-EM from your PC through a web interface by entering:

https://<floating_http_ip_address_of_cicmem>/centrexip

At the maintenance page of the CICM-EM

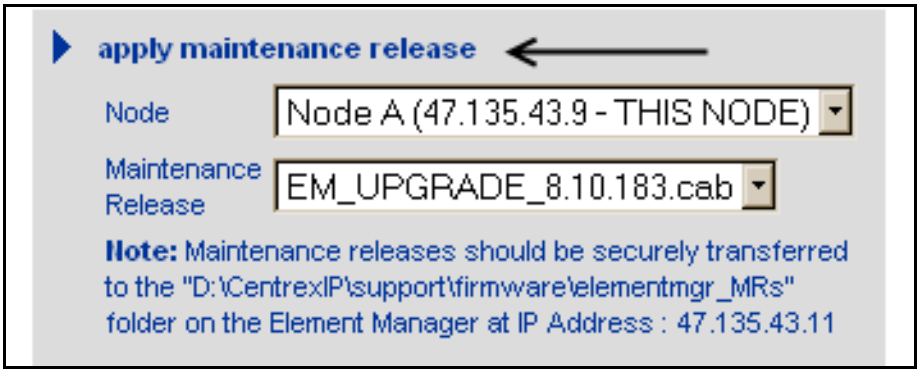
2 Identify from the display *Node status* whether Node A or B is the slave CICM-EM.

3 Select the slave Node from the drop-down menu of the Node window.

4 Select the MR or product release .cab file from the drop-down menu of *Maintenance Release*. The name of the files are:

- EM_<release>.cab for an MR
- EM_UPGRADE_<release>.cab for a product release

5 Apply an MR or product release upgrade by clicking on **apply maintenance release**.

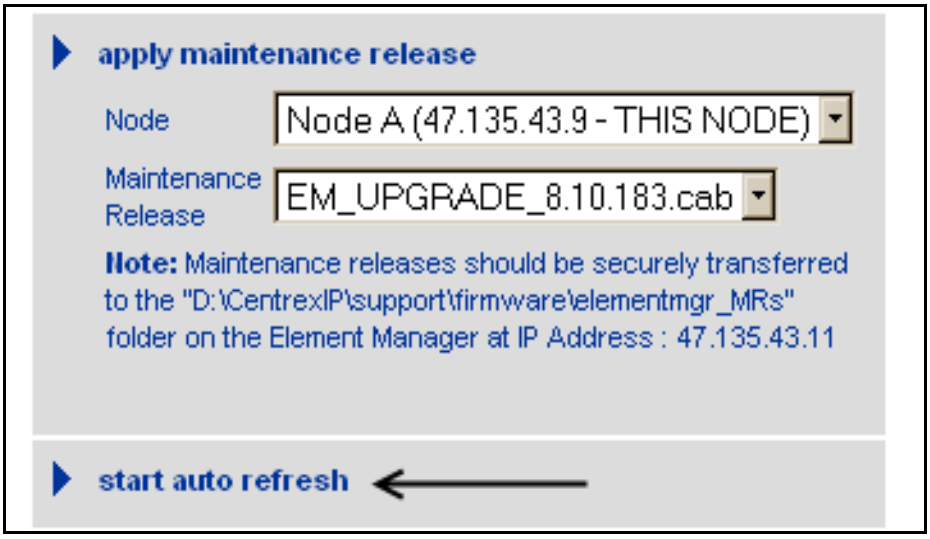


6 Confirm applying the upgrade by clicking on the prompt **confirm maintenance release application**.

The prompt applies to either an MR or a product release upgrade.

At the status page of the CICM-EM

7 Track the progress of the upgrade to the slave EM by clicking on **start auto refresh**.



The refresh button toggles to show **stop auto refresh**.

8 Wait until the CICM-EM being upgraded shows the following combination:

- the *Node status* is *slave*
- the *Node Maintenance status* is *system idle*
- the *Version* is w.xx.yyy of the target upgrade version, for example, 8.10.183

If the EM is not in service and idle within 30 minutes, abort the upgrade. Refer to the task flow in Task flow of CICM-EM and CICM node upgrades for the procedures to roll back from an upgrade.

At the maintenance page of the CICM-EM

9

CAUTION
Risk of service prevention
Do not repeat step 3 when both CICM-EMs have been upgraded.

Upgrade the master CICM-EM by repeating the procedure from step 7. Do not repeat this step when both EMs have been upgraded.

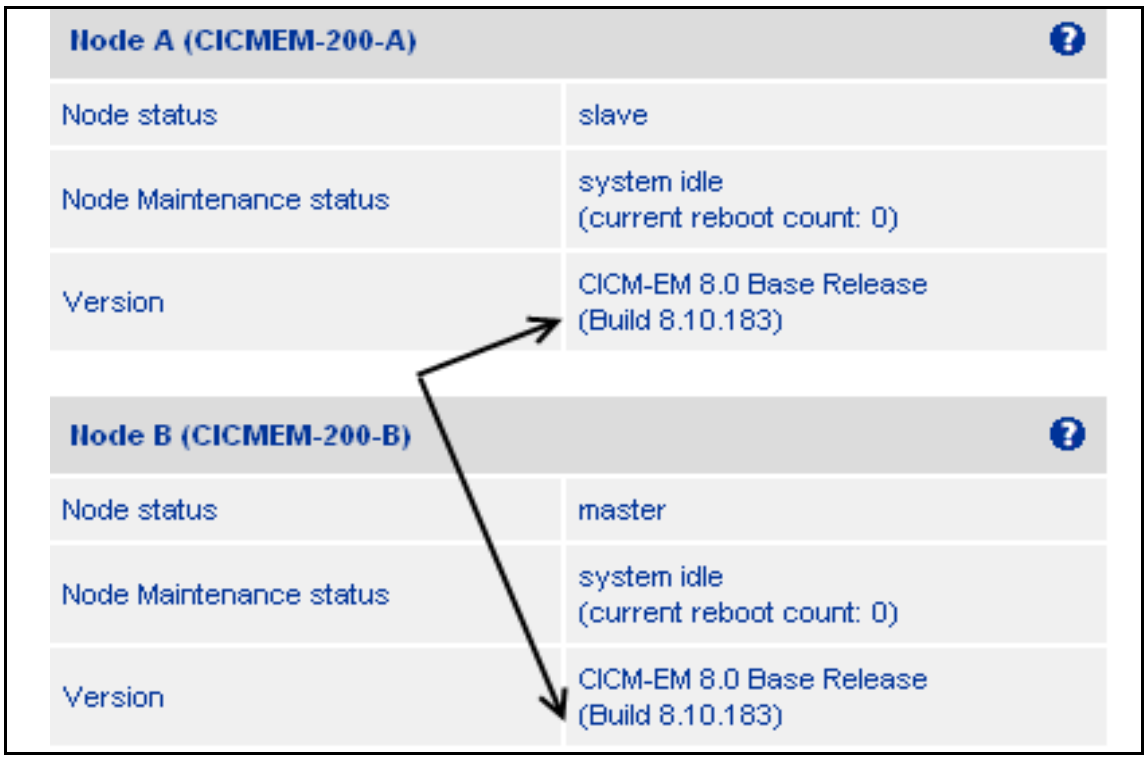
Upgrading the master causes it to automatically switch activity with the slave following a brief transitional period. In effect, only a slave CICM-EM is ever upgraded.

If the EMs do not switch activity, then the upgrading failed. Contact you next level of technical support to determine your next actions.

10 Wait until the second CICM-EM of the redundant pair being upgraded shows it is in service (*system idle* or *system running*).

If the second EM fails the upgrade, refer to the rollback task flow in Task flow of CICM-EM and CICM node upgrades.

11 When both EMs of a redundant pair are in service and running with identical versions of software (for example, 8.10.183), the upgrade is complete.



At the IEMS interface

12 Edit the object properties in the IEMS for the CICM network elements you just upgraded to reflect the new software version. Refer to either of the procedures that follow to update the software version in the field *Device Version*:

- Editing and viewing object properties using Java Web Client
- Editing and viewing object properties using Web Client

13 The procedure is complete. Return to the task flow Task flow of CICM-EM and CICM node upgrades, part 1.

Verifying the software version of the CICM-EM and CICM nodes

Verify the software version of a CICM-EM and its CICM nodes.

Prerequisites to verifying the software version of the CICM-EM and CICM nodes

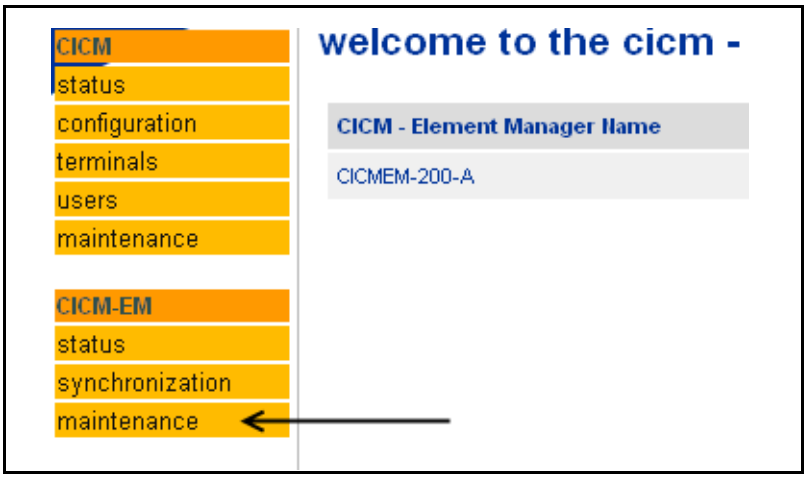
Address the prerequisites before starting the procedure.

- You must follow the Prerequisites and sequence of procedures identified in CICM-EM and CICM node software upgrades.
- You must use administrator userids and passwords to login to the CICM-EM.

Procedure steps to verifying the software version of the CICM-EM and CICM nodes

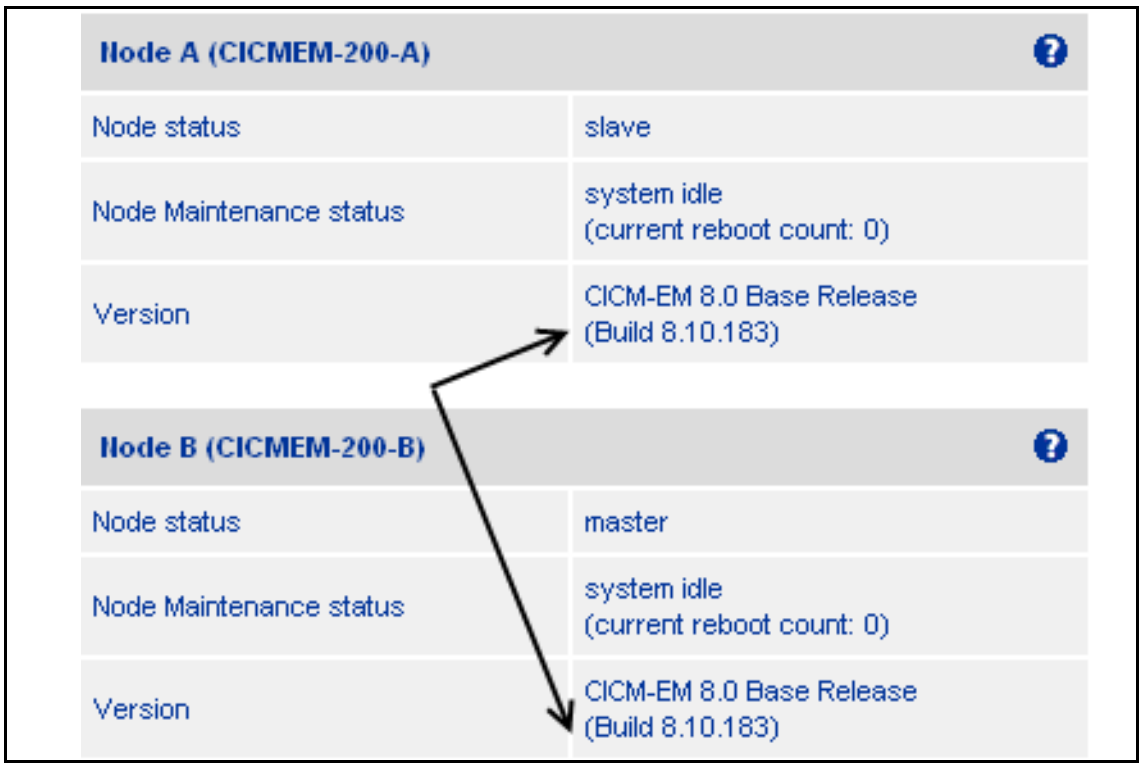
At any CICM-EM web page

1 Click on **maintenance** in the CICM-EM menu.



At the maintenance page of the CICM-EM

2 View the versions of each CICM-EM beside *Version* under the status of each Node.

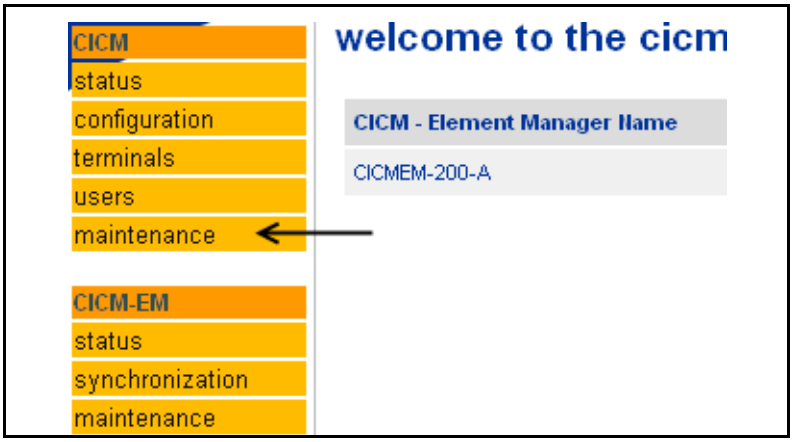


If the versions are identical, proceed with the upgrade.

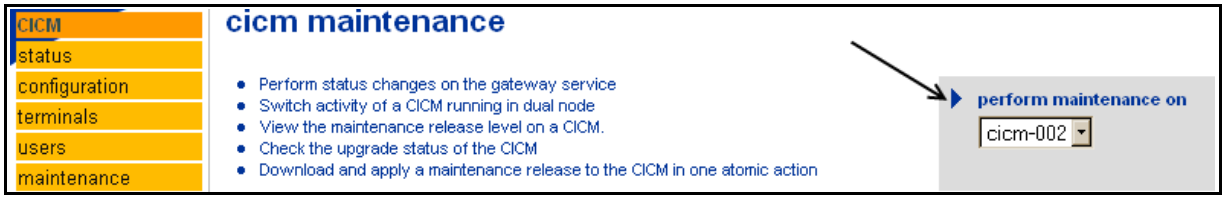
If the last 3 loadbuild numbers are different by at least one number, then you must upgrade the older version (lower number) with an MR before you can upgrade with a product release.

If the first 3 release numbers are different by at least one number, you must upgrade the Node with the older version (lower number) to have the same version as its mate.

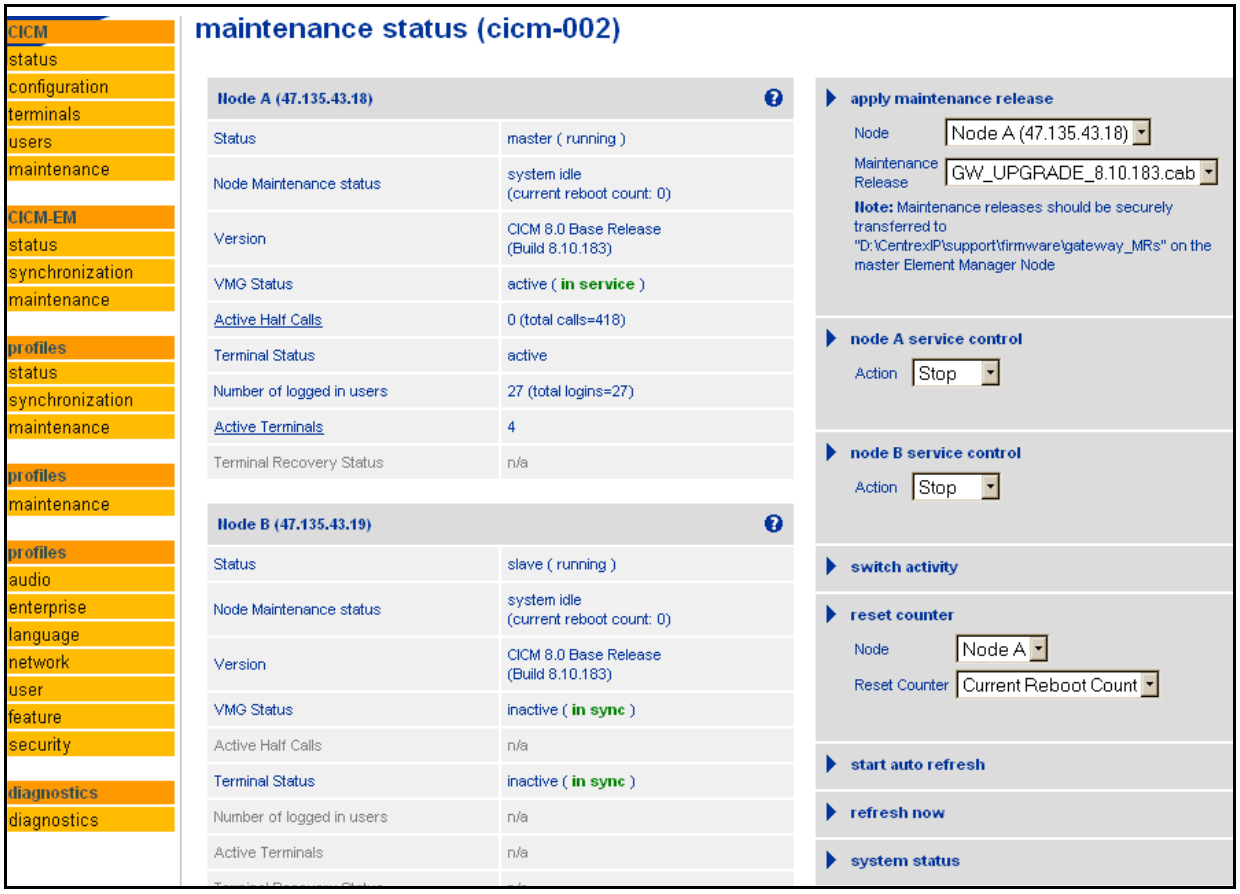
3 Compare the CICM nodes versions by clicking on **maintenance** in the CICM menu.



4 Select the CICM to view from the drop-down menu below **perform maintenance on**.



The page *maintenance status (cicm-nnn)* opens.



5 The software version for each CICM node is shown beside *Version* of the *Node A and B* status windows. In the figure above, Node A and Node B are both at version 8.10.183.

Note: The software of the CICM-EM and CICM nodes should all be the same version for optimal performance.

6 This procedure is complete. Return to the task flow Task flow of CICM-EM and CICM node upgrades, part 1.

Rolling back from a CICM upgrade

This section of *NN10230-461 CICM Upgrades* provides the procedures to roll back from upgrading the software of a single Centrex IP Client Manager (CICM) element manager (CICM-EM) or a single CICM node. Rolling back from an upgrade means restoring the previous version of software.

The topics in this section are:

CICM-EM and CICM node rollbacks

The series of procedures to roll back Centrex IP Client Manager (CICM) element managers (CICM-EMs) or CICM nodes are provided in a task flow.

Prerequisites to the task flow of CICM-EM and CICM rollbacks

Before following the task flow, ensure that you have addressed these requirements.

CAUTION
Risk of service prevention
When you wish to roll back from upgrading both CICM-EMs or both CICM nodes of a redundant pair, the software must be re-imaged as if doing an initial installation. Contact Nortel's GNPS to assist with re-imaging a pair of CICM-EMs or CICM nodes.

CAUTION
Risk of service prevention
Before starting the rolling back task, read each procedure to determine what data you will need for your re-imaging, especially the preboot IP addresses. It is critical to have all the data readily available before starting any procedure in the task flow CICM-EM and CICM node rollbacks.

CAUTION
Risk of service interruption
When rolling back from a software upgrade of release 7.0 to 8.0, do it immediately.

Before following the task flow, ensure that you have addressed these requirements.

- Only one CICM-EM of the redundant pair can have been upgraded, or one CICM node of a redundant pair.
- Be very familiar with the configuration and setup choices that were made when the CICM-EM or CICM node was initially installed. Rolling back requires a partial re-configuration through the command **preboot**.
- The task flow applies to doing a rollback to release 7.0 MRx from either:
  - — a maintenance release (MR) 8.10.MRx or earlier
  - — a product release from 8.10 or earlier
- Ensure that you have all of the necessary CDs to re-install your previous base CICM software, upgrade, and MRs into the node being rolled back. Refer to Prerequisites to the task flow of CICM-EM and CICM node upgrades for examples of CD labels.

  Also for a CPN5385, at the EM of the SAM 21 in the provisioning tab of the node's card view, verify that the image and load files can be located in the directory */data/swd/cicm* on the CMT server (also known as the SSPFS server).
- Rolling back a CICM-EM node or a CICM node is basically reloading the base software onto the node, configuring software using command **preboot**, and waiting for data synchronization to occur. Details in the procedures may vary for the CICM-EM and a CICM node, but the rollback approach is essentially the same for either type of node.
- The task flow supports rolling back a node only on-site with the hardware (that is, it does not support doing a remote rollback). You need a console serial port available on each CPU card of the SAM 16 shelf (with CPV5370 cards) or SAM 21 shelf (with CPN5385 cards). The serial port is the access portal to the command prompt associated with each of the processors. If you are connecting your external personal computer (PC) to a CICM-EM card, then you will be accessing the command prompt for the CICM-EM through its serial port. If you are connecting your external personal computer (PC) to a CICM node card (using a null modem

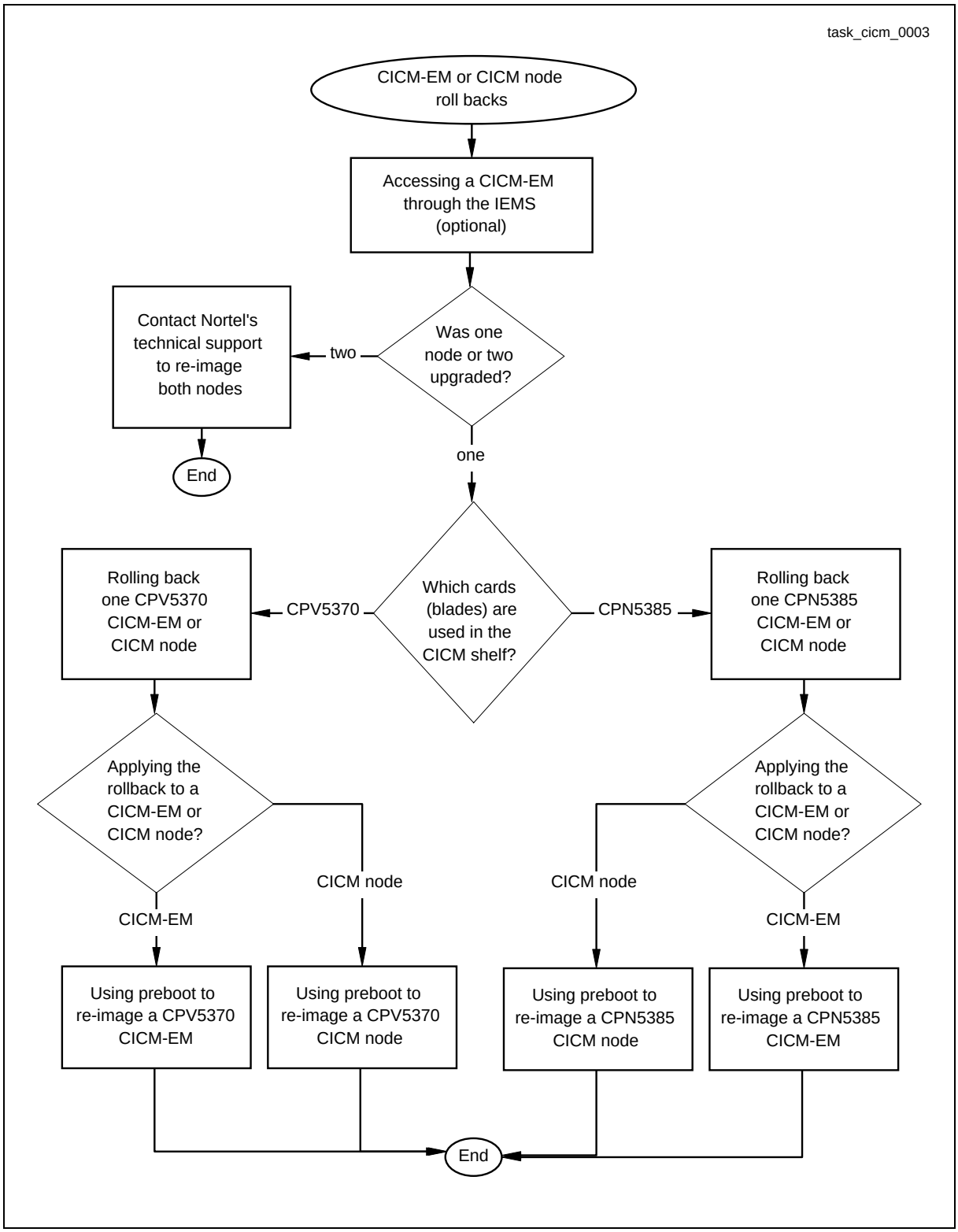
cable), then you will be accessing the command prompt for the CICM node through its serial port. The PC must have a hyperterminal software application.

- A CICM node must always be rolled back before either of its CICM-EMs.
- Since rolling back from an upgrade is a manual operation, start it during a period of lowest traffic for the CICM-EMs and CICM nodes.
- Once a rollback has been started, do not attempt any software configuration changes until each node-pair is confirmed to be fully in service according to the node's *status* and *maintenance* menus.
- When entering values for the command **preboot**, if you enter a typo you can exit the preboot sequence with keys *Ctrl* plus *c*, then re-enter the command **preboot** and scroll using the space bar to the last step of entry. Correct the typo and continue. Otherwise a captured error means you must re-do the **preboot** procedure.

Task flow of CICM-EM and CICM node rollbacks

The task flow shows the sequence of procedures to roll back an upgraded CICM-EM or CICM node. The procedures are shown in the figure Task flow of CICM-EM and CICM node rollbacks. To link any procedure, go to Navigation immediately following the figure.

Task flow of CICM-EM and CICM node rollbacks



Navigation

The procedures in the task flow are listed alphabetically.

- "Accessing the CICM through the IEMS"
- Rolling back one CPN5385 CICM-EM or CICM node
- Rolling back one CPV5370 CICM-EM or CICM node
- Switching activity between CICM nodes for a rollback
- Transferring terminals for a rollback
- Using preboot to re-image a CPN5385 CICM node
- Using preboot to re-image a CPN5385 CICM-EM
- Using preboot to re-image a CPV5370 CICM node
- Using preboot to re-image a CPV5370 CICM-EM

Rollback procedures for CICM-EM and CICM nodes

The procedures for rolling back the software of a CICM-EM pair and its CICM node pairs are listed alphabetically in this section. The sequence of doing the procedures is identified in CICM-EM and CICM node rollbacks.

Note: You must follow the sequence of procedures identified in the task flow in order to properly complete rolling back.

Rolling back one CPN5385 CICM-EM or CICM node

Roll back to the previous software of one CICM-EM or CICM node with CPN5385 CPU blades (cards) that was upgraded with an MR or product release.

Prerequisites to rolling back one CPN5385 CICM-EM or CICM node

Address the prerequisites before starting the procedure.

- You must follow the sequence of procedures identified in Task flow of CICM-EM and CICM node rollbacks.
- Since upgrading a CICM node from SN08 or later always starts with Node A, the rolling back applies to Node A. From the upgrade, Node A should already be the slave and not running terminal service.
- The CICM-EM can be either the master or the slave.

Procedure steps to rolling back one CPN5385 CICM-EM or CICM node

At an address window of the Internet

1 Access the master or slave CICM-EM by entering:

http://<https_IP_address>/centrexip

At the CICM maintenance status page

2 When rolling back a CICM node that has had a successful upgrade, followed by a successful SWACT and terminal transfer but has terminals that will not operate, transfer its terminals to its mate by using the procedure Transferring terminals for a rollback. Do not transfer terminals for any other rollback.

This step does not apply to a CICM-EM.

At the maintenance status page of the CICM-EM or CICM node

3 Observe from the *Node Maintenance status* which nodes are master and slave.

When rolling back a CICM node that has had a successful upgrade followed by a successful SWACT or that has had a successful upgrade followed by a successful SWACT and terminal transfer, but in either scenario has terminals that will not operate, ensure that Node A is the slave. If not, do the procedure Switching activity between CICM nodes for a rollback and return to this step.

When rolling back a CICM-EM, it can be either master or slave.

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

4 Locally access the node being rolled back by:

- connecting the serial port of your PC to the serial port of the CICM-EM or CICM blade (card)
- starting the program *hyperterminal* on your PC
- using *hyperterminal* to connect to the blade's console session

The Windows command prompt appears:

login:

5 Enter the userid of the node.

6 Enter the password of the node.

When access is successful, the command prompt is:

C:\temp>

7 Reset the node's bootflag by entering:

cxippreboot /bootflag /clear

When complete, the response is:

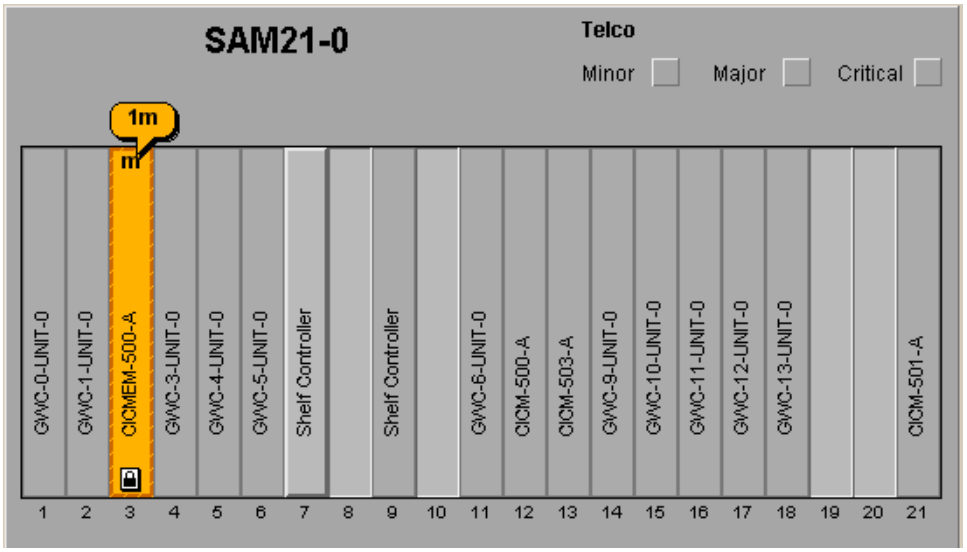
```
Active Boot Flag was Cleared Successfully.
```

At the element manager for the SAM 21 shelf with CPN5385s

8 Lock and unlock the node being rolled back by placing the cursor on the card, right clicking, and selecting **Lock**, then **Unlock**.

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

The locked card turns orange and shows a padlock symbol.

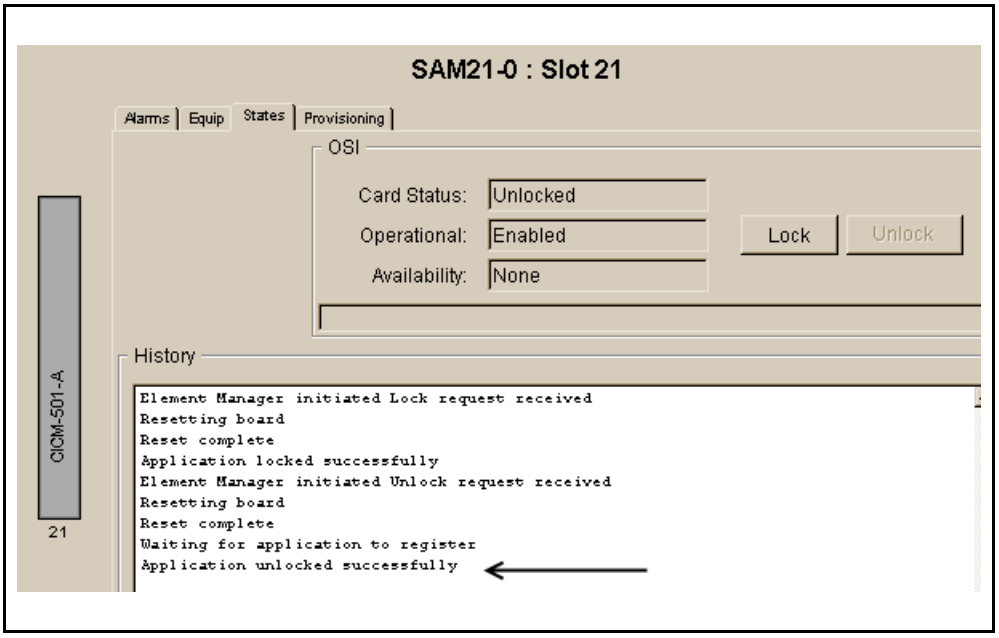


10

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

Wait for the node to fully unlock.

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



11 This procedure is complete. Return to the task flow Task flow of CICM-EM and CICM node rollbacks.

Rolling back one CPV5370 CICM-EM or CICM node

Roll back to the previous software of one CICM-EM or CICM node with CPV5370 CPU blades (cards) that was upgraded with an MR or product release.

Prerequisites to rolling back one CPV5370 CICM-EM or CICM node

Address the prerequisites before starting the procedure.

- You must follow the sequence of procedures identified in Task flow of CICM-EM and CICM node rollbacks.
- Since upgrading a CICM node from SN08 or later always starts with Node A, the rolling back applies to Node A. From the upgrade, Node A should already be the slave and not running terminal service.
- The CICM-EM can be either the master or the slave.
- You must have Nortel's CD available with the .cab files for the same software release that the mate has (for example, 7.0 MR5). Refer to Prerequisites to the task flow of CICM-EM and CICM node upgrades for examples of CD labels.

Procedure steps to rolling back one CPV5370 CICM-EM or CICM node

At an address window of the Internet

1 Access the master or slave CICM-EM by entering:

http://<https_IP_address>/centrexip

At the CICM maintenance status page

2 When rolling back a CICM node, transfer its terminals to its mate by using the procedure Transferring terminals for a rollback. (This does not apply to a CICM-EM.)

At the maintenance status page of the CICM-EM or the CICM node

3 Observe from the *Node Maintenance status* which nodes are master and slave.

When rolling back a CICM node, ensure that Node A is the slave. If not, do the procedure Switching activity between CICM nodes for a rollback and return to this step.

When rolling back a CICM-EM it can be either master or slave.

At the SAM 16 shelf containing CPV5370 cards

4 Open the drawer of the CD-ROM drive for Node A of the CICM-EM or CICM node being rolled back.

5 Place the CD of CICM-EM or CICM node software into the drawer. Avoid getting finger prints on the flat surfaces of the disk.

6 Close the drawer.

7 On node A's CPV5370 CPU card, press the small *Reset* button using a non-metallic stick (such as a tooth pick with a flat end).

The LED next the CD-ROM drawer flashes amber to indicate loading (reboot) is in progress.

8 Wait for the CD-ROM drawer to automatically open when loading is complete.

9 Remove the disk and close the drawer again.

10 With the disk removed, press the *Reset* button again.

11 This procedure is complete. Return to the task flow Task flow of CICM-EM and CICM node rollbacks.

Switching activity between CICM nodes for a rollback

Switch the activity from the master CICM node to the slave node of the redundant pair.

Prerequisites to switching activity between CICM nodes

Address the prerequisites before starting the procedure.

- You must follow the sequence of procedures identified in Task flow of CICM-EM and CICM node rollbacks or use this procedure only when invoked from another procedure.
- Both nodes must be in-service to enable the switch of activity (SWACT) to occur.
- When an upgrade to the first node of a redundant pair does not succeed, do not use this procedure as part of the rollback. Use this procedure for all other rollbacks.

CAUTION
Risk of service interruption
When node A has SN08 software and node B has SN07, all terminals must have been transferred from node A to node B through a terminal transfer before switching activity from A to B.

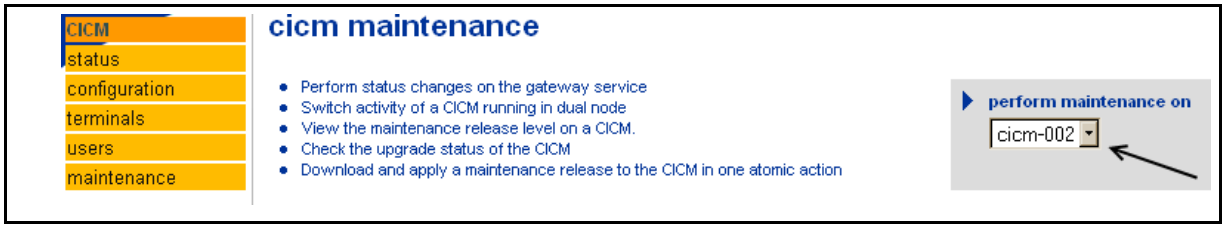
Procedure steps to switching activity between CICM nodes

At the home page of CICM

1 In the menu CICM, click on **maintenance**.

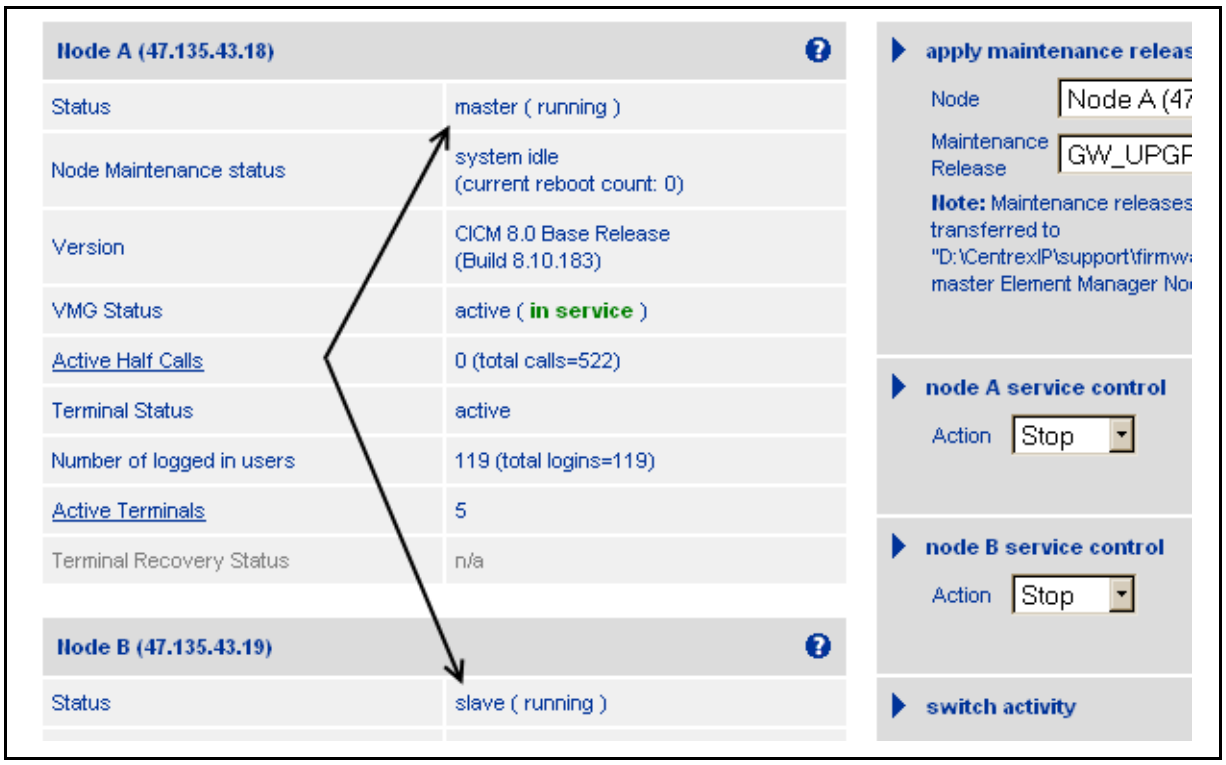
At the cicm maintenance page

2 Select the CICM node number from the drop-down menu.



3 Click on **perform maintenance on**.

4 Observe from the *Node Maintenance status* of each node which ones are master and slave.



5 Click on **switch activity**.

The duration of the switchover varies according to the number of users configured on the nodes and the volume of calls being sustained in the node at the time of the SWACT.

When both nodes are not available for a SWACT, the command button is tinted grey and disabled. Ensure that both nodes are in service.

6 Click on **Confirm switch of activity**.

7 Confirm from the *Node Maintenance status* that CICM Node A is the slave and they have switched successfully.

If not, then contact your next level of support to determine why.

8 This procedure is complete. Return to the step in the procedure from where you came:

- step 3 in Rolling back one CPN5385 CICM-EM or CICM node
- step 3 in Rolling back one CPV5370 CICM-EM or CICM node

Transferring terminals for a rollback

Transfer the terminals (clients) from one node to another to ensure that service can be restored.

Prerequisites to transferring terminals for a rollback

Address the prerequisites before starting the procedure.

- You must follow the sequence of procedures identified in Task flow of CICM-EM and CICM node rollbacks or use this procedure only when invoked from another procedure.
- Have a working CICM terminal (for example, an m6350 or IP Phone 200x) available to test the operation of a rolled back node.
- Do not use this procedure as part of the rollback:
  - when an upgrade to the first node of a redundant pair fails
  - when operational tests fail after the SWACT that follows a successful upgrade
  - The section “Terminal transfers” and the procedure “Perform a terminal transfer” in *CICM Security and Administration*, NN10252-611.

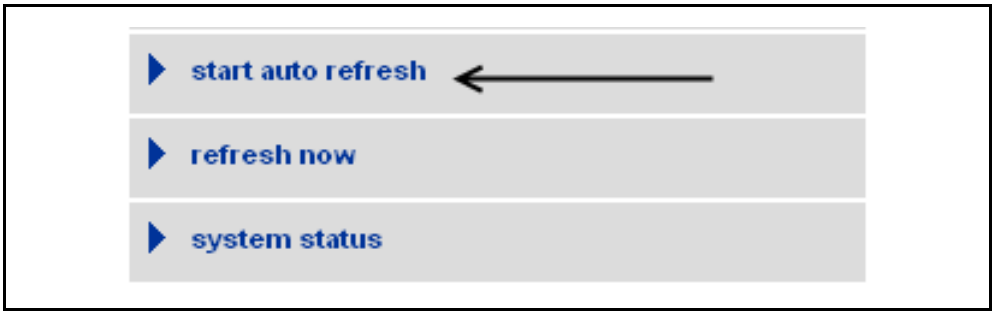
CAUTION
Risk of service loss
Do not attempt to abort a terminal transfer during a rollback. Aborting may cause the terminals to hang without a connection.

Procedure steps to transferring terminals for a rollback

At the CICM maintenance status <cicm_id> page

1 On the right menu, ensure that **start auto refresh** is showing, but do not click on it.

If **stop auto refresh** is shown, click on it to show **start auto refresh**.



2 When rolling back a CICM node, which is always node A, transfer its terminals to the mate by clicking on **from node A to node B** at the Node drop-down menu.

3 Select the minutes from the *Terminal Shutdown Timeout* drop-down menu. The minutes are to allow CICM clients time to log off themselves before they are automatically dropped by the transfer.

4 Click on **transfer terminals**.

5 When the confirmation screen appears, click on **confirm terminal transfer**.

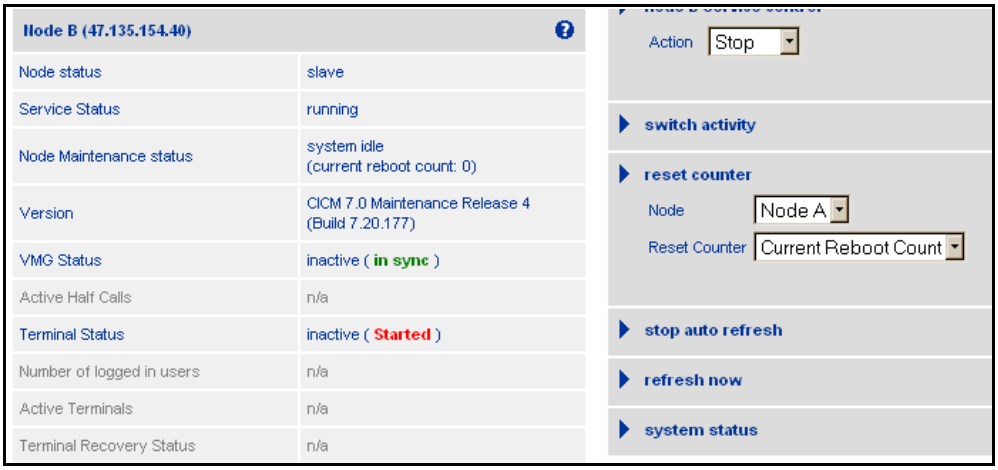
```
The terminal transfer will commence immediately
upon confirmation, and will terminate when the
selected timeout interval has expired.
```

6 Click on **start auto refresh** of the *maintenance status <cicm_id>* page.

The button **stop auto refresh** appears.

Note: In *CICM Security and Administration*, NN10252-611 the section “Terminal handover” and the procedure “Perform a terminal handover” provide details on terminal handovers.

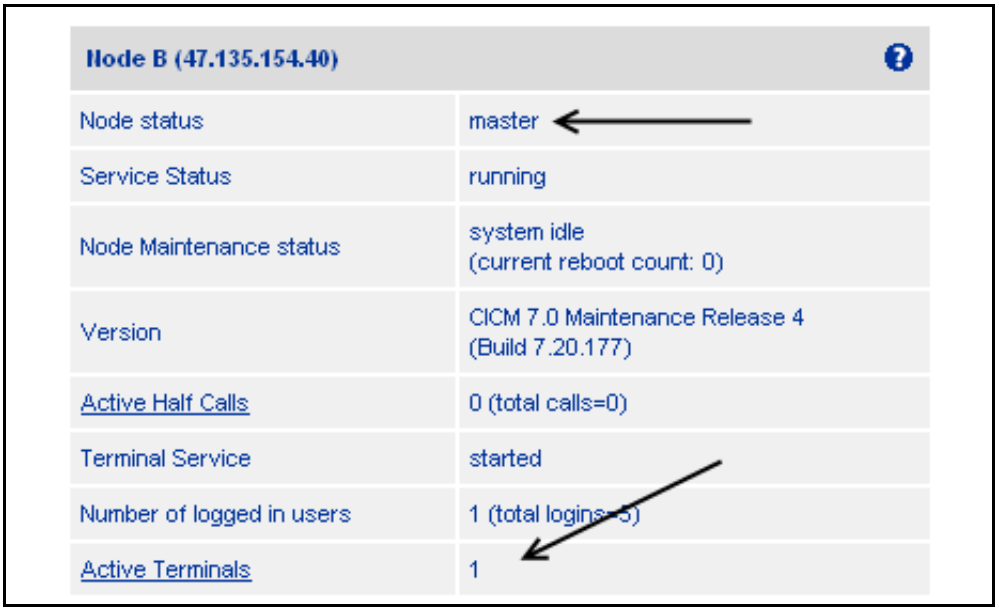
Observe that portions of the terminal statuses for Nodes A and B are greyed out during the transfer. Since SN07 handles a terminal transfer manually and SN08 handles it automatically, the status displays cannot be the same during the transition. This is normal.



7

CAUTION
Risk of service interruption
Wait until the terminal transfer has completed before proceeding. If the transfer does not complete, discontinue the procedure and contact your next level of technical support to determine your next actions.

When the terminals have transferred, all should be hosted on CICM Node B. Completion of the transfer is indicated by *stopped* or *inactive* appearing for *Terminal service* (SN07) or *Terminal status* (SN08).



Node B (47.135.154.40)	
Node status	master
Service Status	running
Node Maintenance status	system idle (current reboot count: 0)
Version	CICM 7.0 Maintenance Release 4 (Build 7.20.177)
Active Half Calls	0 (total calls=0)
Terminal Service	started
Number of logged in users	1 (total logins=5)
Active Terminals	1

8 Have the telco test the operation of each CICM terminal on the node that is supposed to have them connected. Ensure that all terminals are registered on the node. A registered terminal means the S1 and S2 addresses point to the floating UNIStim IP address.

If the tests fail, contact your next level of support to determine your next actions.

9 This procedure is complete. Return to the step in the procedure from where you came:

- step 2 in Rolling back one CPN5385 CICM-EM or CICM node
- step 2 in Rolling back one CPV5370 CICM-EM or CICM node

Using preboot to re-image a CPN5385 CICM node

Use preboot to re-image a CICM node with CPN5385 CPU blades (cards) to a base CICM software release.

Prerequisites to using preboot to re-image a CPN5385 CICM node

Address the prerequisites before starting the procedure.

- You must follow the sequence of procedures identified in Task flow of CICM-EM and CICM node rollbacks.
- When the CICM node's software has been restored, its data is automatically synchronized with the mate CICM node.
- Output from the progression of preboot is shown by `this font`. Command entries are shown by **this font**.
- When *more* appears on the screen, press the keyboard spacebar to advance the screen.

CAUTION
Risk of service prevention
Using preboot means re-entering specific configuration data that would normally be handled by an initial installation. While configuring, extreme care must be taken to ensure accurate entries especially with IP addresses.

Procedure steps to using preboot to re-image a CPN5385 CICM node

At the PC desktop for remote access to the CICM node

1 Locally access CICM Node A through the console serial port.

2 Pressing enter in the terminal window will eventually get the login prompt.

```
login:
```

3 For the userid enter *Administrator* and for the password enter *Administrator*.

The screen prompt becomes:

C:\Documents and Settings\Administrator>

4 At the command line interface (CLI) of a Windows XP session, enter:

`preboot`

5
```
Press CTRL-C at any prompt to abort preboot.
Press ENTER now to start preboot configuration.
```

```
This CICM-EM is Node A.
```

Press enter to start *preboot*.

6 `STEP 1: Configure BOOTP options (CPV5370 ONLY)`

```
Skipping option bootp (skip configured in mib)
```

No user input is required. The output indicates CPV5370 even though this is a CPN5385 procedure.

7 `STEP 2: Configure IPSec`

```
This step configures IPSec. You will be prompted
for the IPSec pre-shared key. This is the key
that is used to connect to the IPSec protected
ports on the CICM[EM]. A hash of this pre-shared
key will be used for the software account
(comuser) password. It is important to remember
the pre-shared key entered, as this key MUST be
the same on both the CICM and the CICM EM. The
IPSec step can only be run once.
To re-key IPSec use the following command:
preboot ipsec /rekey

Enter the IPSec Pre-Shared Key:
```

<customer_configuration_password>

Record the pre-shared key (password) for your records.

```
Re-enter to confirm:
```

<customer_configuration_password>

```
Secure the telnet port? [Y|N, default=Y]:
```

N

At this point in the configuration, Nortel recommends not securing the telnet port. It can be configured later after the rollback is completed.

8 `STEP 3: Configure the gateway type`

```
This Gateway is automatically set up in a H248
configuration. Gateway configured to support
H248.
```

No user input is required.

9 `STEP 4: Configure the workgroup and computer name`

```
The CICM/CICM-EM can operate in either a single
or dual node configuration. In a dual node
configuration, the CICM/CICM-EM has two nodes,
```

```
A and B. The two nodes belong to a unique
workgroup. The node(s) will be named as the
workgroup name with an '-A' (or '-B' appended).
In a single node configuration, only node A can
be installed. It's name will be the workgroup
name with an '-A' appended.
```

No user input is required.

10 `STEP 5: Configure the administration accounts`

```
The CICM and the CICMEM both have a
Administration Account. The preboot section is
used to configure this account.

Enter the local Administrator account password:
```

<customer_configuration_password>

The password (up to 8 alphanumerical characters) can be different than the one you specified earlier for the pre-shared key. Record the password for your records.

```
Re-enter to confirm:
```

<customer_configuration_password>

11 `STEP 6: Configure the software user account`

```
The CICM/CICM-EM use a single security [aka
COMUSER] account under which all software is
executed. This account should be configured with
the same username and password on each system
(CICM-EMs and CICMs).
NOTE: this account should *NOT* be used for
interactive logins.
The /display option will display the comuser
password [only do this over a secure
connection]. Note that this will display the
auto-generated password based on the IPSec
pre-shared key (which you must re-enter). If you
enter the wrong key then an incorrect software
account password will be displayed.

Enter a username under the software will run
(hit ENTER to accept "COMUSER"):
```

<customer_userid>

Nortel recommends you press enter to accept the default value of *COMUSER* as the userid for the COMUSER account. Note that the CICM-EM and all subtending CICM nodes must have the same COMUSER userid. Record the userid for your records.

```
Software account successfully configured.
```

12 `STEP 7: Configure the Static adapter settings`

```
This section creates and configures the 'Static'
LAN Adapters. There are two static adapters per
node - A1/A2 and B1/B2. Each has a single IP
address. Heartbeat messages are sent between the
addresses on A and the addresses on B. These
addresses are restricted to the CICM and they
must be in a distinct subnet from any other
addresses used on the CICM or in the network in
general.

Enter Admin VLAN id [1...4094, default=2]:
```

<customer_admin_vlan_value>

```
Enter H248 VLAN id [1...4094, default=4]:
```

<customer_h248_vlan_value>

```
The static addresses have been autogenerated
based on the system ID of <specified in
provisioning tab for CICM node at SAM 21 Element
Manager>.
The base address is <auto generated IP address>
and will be used to create a subnet range with
mask 255.255.255.248.

Do you wish to use the base address? [Y|N,
default=Y]
```

<customer_static_address>

Nortel recommends entering Y (yes) to accept it provided the auto-generated address does not conflict with an existing IP address in the network. Entering N (no) means you must provide the valid static address values.

13 `STEP 8: Configure the Unistim LAN settings`

```
This section configures the CICM's Unistim LAN
adapter. The Unistim LAN is used for call
signalling between CICM and its clients
(terminals). The LAN's port filter only permits
those UDP ports used to communicate with
clients. [OAMP functions are blocked on the
Unistim LAN.]

Enter Unistim VLAN id [1...4094, default=3]:
```

<unistim_vlan_id>

Enter the Unistim IP address for this node:

<unistim_static_ip_address_for_the_node>

Enter the network mask for the Unistim IP network:

<network_mask_for_unistim_ip_network>

Enter the default route for the Unistim IP network (Enter 0.0.0.0 for no route):

<default_route_for_unistim_ip_network>

Enter a no route only if you do not have a default and you understand the consequences of not having one.

14 STEP 9: Configure the H248 LAN settings

This section configures the H248 floating adapter. The floating H248 IP address will be bound to the A4/B4 adapter on whichever CICM node is Master. Therefore, datafill the same address on each node. This address will be used for all communication with the Gateway Controller and should match the Media Gateway IP Address provisioned for the CICM on the Gateway Controller EM.

Enter the Floating H248 IP address for this CICM:

<floating_h248_ip_address_for_cicm>

Enter the Static H248 IP address for Node A:

<static_h248_ip_address_for_node_A>

Enter the Static H248 IP address for Node B:

<static_h248_ip_address_for_node_B>

Enter the network mask for the H248 IP network:

<network_mask_for_h248_ip_network>

Enter the default route for the H248 IP network (Enter 0.0.0.0 for no route):

<default_route_for_h248_ip_network>

Enter a no route only if you do not have a default and you understand the consequences of not having one.

15 STEP 10: Configure the VMG settings

This step configures the Virtual Media Gateway. The CICM can support up to 3069 lines (up to 1023

```
on the 5370 hardware) [for Nortel testing
purposes *ONLY*, a lower value may be entered.]
WARNING - in a dual node configuration, the
number of lines must be datafilled the same on
both nodes of the CICM.
To re-size the VMG to the maximum number of
lines use the following command:
preboot vmg /resize

Enter the number of lines for the gateway
[1...3069, default=3069]:
```

Nortel recommends you accept the default number of lines.

<number_of_lines_for_the_gateway>

```
Enter the Media Gateway Controller IP address:
```

<media_gateway_controller_ip_address>

```
Enter the Media Gateway Controller UDP port
[0...65535, default=2944]:
```

<media_gateway_controller_udp_port>

16 `STEP 11: Configure the Floating Admin adapter settings`

```
This section configures the Floating Admin
adapter information. The floating Admin IP
address will be bound to the most available
interface on the Gateway node.

Enter the Node A Admin address:
```

<node_A_admin_address>

```
Enter the Node B Admin address:
```

<node_B_admin_address>

```
Enter the network mask for the Admin IP network:
```

<network_mask_for_admin_ip_network>

```
Enter the default router for the Admin IP
network:
```

<default_router_for_admin_ip_network>

17 `STEP 12: Configure the SNMP settings`

<customer_snmp_configuration>

Configure the *SNMP settings* by entering your configuration values or if not using SNMP, press enter to accept all the default values. The progression of information is not shown in this step.

```
... ---Finished
```

18 `STEP 13: Configure the time settings for the gateway`

```
You can use this utility to set the time and time
zone on the CICM. It will inform any running
software of the time change.
Current time zone is n.n hours from GMT (GMT
Standard Time).
Daylight time zone is n.n hours from GMT (GMT
Daylight Time)

Do you want to change it [Y|N, default=N]:
```

Entering **Y** presents a choice of time zones. Select the time zone by entering the number associated with it or press enter to accept the default.

Y

```
Current local date is <value>.

Do you want to change it [Y|N, default=N]:
```

Enter **N** to accept the local date or enter **Y** to change it. After **Y**, answer the prompts to specify the day, month, and year.

Y

```
Current local time is <value>.

Do you want to change it [Y|N, default=N]:
```

Enter **N** to accept the local time or enter **Y** to change it. After **Y**, answer the prompts to specify the hours and minutes.

Y

```
Current time for scheduled backups is 02:00.

Do you want to change it [Y|N, default=N]:
```

Accept the default or configure a different time to schedule the automatic backup of the software image by entering **Y** (yes), then a 24-hour time as **<hh:mm>**.

N

19 `STEP 14: Configure the Hard disk`

No user input is required.

```
The CICM and CICM-EM have two disk partitions,
C: and D:. These must be converted to the NTFS
file system.
```

```
Setting system to convert C: and D: to NTFS file
system on next boot.
```

20 STEP 15: Apply the CICM software load

```
Apply the default software image to the Gateway.
```

Wait while preboot configures the software. The progression of information is not shown in this step.

```
... Registry Flush Complete.

A reboot must now be performed to complete
installation. Do you want to restart now? [Y|N,
default=N]:
```

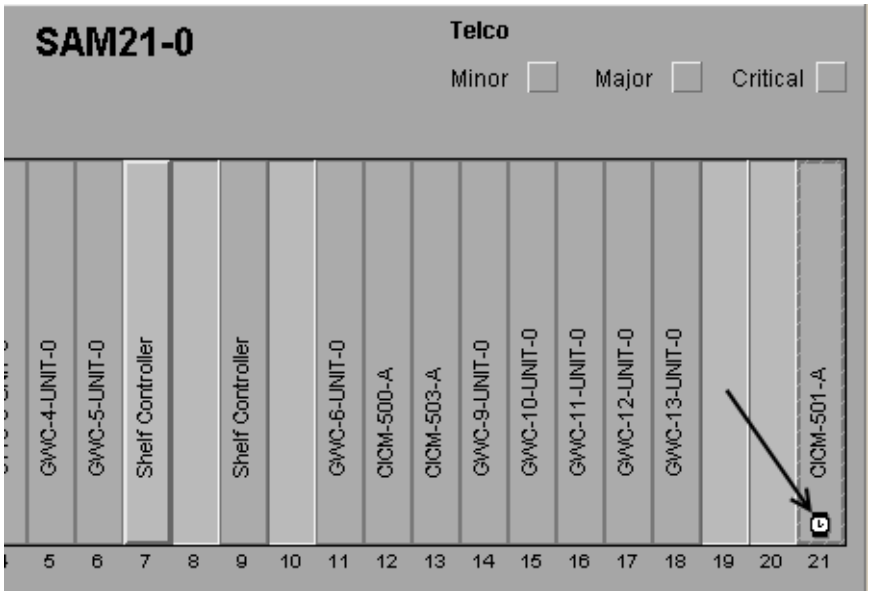
Y

```
The computer is shutting down .............
Console disconnected.
```

At the element manager for the SAM 21 shelf with CPN5385s

21 At the GUI of the SAM 21 EM, place the cursor on the card, right click, and select **Card View.**

The rebooting card shows a watch symbol which appears three times.



Rebooting is complete when the watch symbol disappears and the card *State History* (right click) indicates

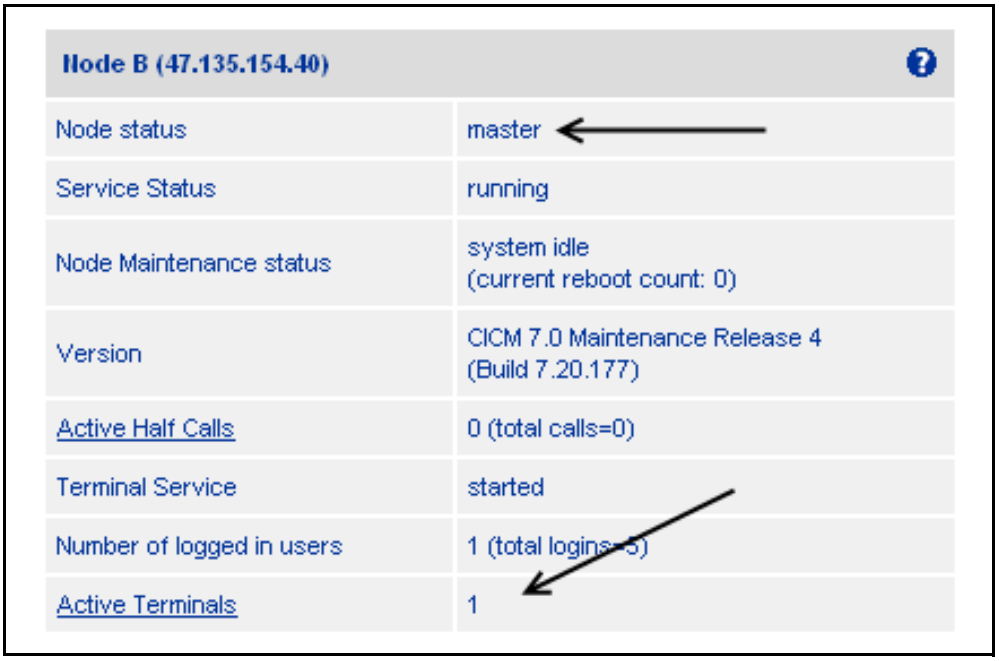
```
Application initiated reset completed
successfully.
```

At the CICM maintenance page

22 Wait for the node to synchronize data with its mate node. While waiting, click on **refresh now**.

When synchronized, the node is fully in service as shown by the status *system idle* or *system running*.

Node B shows active terminals if they were active before Node A was reloaded.



23 Apply additional MRs as needed to restore the node to the same MR level as its mate node. Refer to the procedure “Perform a CICM 7.0.xxx MR upgrade” in *CICM Upgrading*, NN10230-461, the version for SN07.

At the CICM status page

24 Verify the CICM node pair is fully in service.

25 Leave the CICM terminals on Node B, the active master. Although an initial SN07 configuration typically splits the terminal connections between Nodes A and B, there is no need to split them after the rollback.

At the PC desktop for remote access to the CICM node

26 Locally access CICM Node A through the console serial port.

27 At the prompt, log in.

```
login:
```

For the userid enter *Administrator* and for the password enter *Administrator*.

The screen prompt becomes:

```
C:\Documents and Settings\Administrator>
```

28 At the CLI of a Windows session, you apply your SNMP data to enable a connection with IEMS by entering:

```
preboot snmp /interactive
```

29 This procedure is complete. Return to the task flow Task flow of CICM-EM and CICM node rollbacks.

Using preboot to re-image a CPN5385 CICM-EM

Use preboot to re-image a CICM-EM with CPN5385 CPU cards (blades) to a base CICM-EM software release.

Prerequisites to using preboot to re-image a CPN5385 CICM-EM

Address the prerequisites before starting the procedure.

- You must follow the sequence of procedures identified in Task flow of CICM-EM and CICM node rollbacks.
- When the CICM-EM's software has been restored, its data is automatically synchronized with the mate EM.
- Output from the progression of preboot is shown by `this font`. Command entries are shown by **this font**.
- When *more* appears on the screen, press the keyboard spacebar to advance the screen.

CAUTION
Risk of service prevention
Using preboot means re-entering specific configuration data that would normally be handled by an initial installation. While configuring, extreme care must be taken to ensure accurate entries especially with IP addresses.

Procedure steps to using preboot to re-image a CPN5385 CICM-EM

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

1. Locally access Node A through the console serial port.
2. Pressing enter in the terminal window will eventually get the login prompt.

   ```
   login:
   ```

3. For the userid enter *Administrator* and for the password enter *Administrator*.
4. At the command line interface (CLI) of a Windows 2000 session, enter **preboot**.
5. ```
   Press CTRL-C at any prompt to abort preboot.
   Press ENTER now to start preboot configuration.

   This CICM-EM is Node A.
   ```

   Press enter to start *preboot*.
6. Wait while preboot starts.
   ```

```
STEP 1: Configure BOOTP options (CPV5370 ONLY)

Skipping option bootp (skip configured in mib).
```

7

```
STEP 2: Configure SSH

Access to the CICM EM may be achieved either by
using a secured SSH connection or via the EM's
serial port. SSH keys are generated during this
step (which takes some time). On completion the
SSH fingerprint will be displayed. Use this
fingerprint for server validation when
connecting to the CICM EM. Do not trust any
other fingerprint.
To display the SSH fingerprint after the SSH
step use the following:
preboot ssh /fingerprint
Generating SSH keys ...
...
The CICM EM SSH Fingerprint is:
<fingerprint_code>

Press ENTER to continue.
SSH Configuration Complete.
```

Complete configuring the *SSH* by pressing enter.

8

```
Flushing Registry Data...
Registry Flush Complete.

A reboot must now be performed to complete
installation. Do you want to restart now? [Y|N,
default=N]:
```

Y

```
Rebooting now...
```

The following prompt appears and then lockout occurs.

C:\>

9 Pressing enter in the terminal window will eventually get the login prompt.

```
login:
```

10 For the userid enter *Administrator* and for the password enter *Administrator*.

The screen prompt becomes:

C:\Documents and Settings\Administrator>

11 At the command line interface (CLI) of a Windows XP session, enter:

preboot

12
```
Press CTRL-C at any prompt to abort preboot.
Press ENTER now to start preboot configuration.
This CICM-EM is node A.
```

Press enter to start *preboot*.

13
```
STEP 1: Configure BOOTP options (CPV5370 ONLY)

Skipping option bootp (skip configured in mib).

STEP 3: Configure SSH

Skipping option ssh (already complete).
```

14
```
STEP 3: Configure IPSec

This step configures IPSec. You will be prompted
for the IPSec pre-shared key. This is the key
that is used to connect to the IPSec protected
ports on the CICM[EM]. A hash of this pre-shared
key will be used for the software account
(comuser) password.
It is important to remember the pre-shared key
entered, as this key MUST be the same on both
the CICM and the CICM EM. The IPSec step can only
be run once.
To re-key IPSec use the following command:
preboot ipsec /rekey
...
NB: <cicmname> must be identical to the name
specified in the /permitcicm.

Enter the IPSec Pre-Shared Key:
```

<customer_configuration_password>

Record the pre-shared key (password) for your records.

```
Re-enter to confirm:
```

<customer_configuration_password>

```
Secure the telnet port? [Y|N, default=Y]:
```

N

At this point in the configuration, Nortel recommends not securing the telnet port. It can be configured later after the rollback is completed.

15 STEP 4: Configure the workgroup and computer name

No user input is required.

```
The CICM/CICM-EM can operate in either a single
or dual node configuration. In a dual node
configuration, the CICM/CICM-EM has two nodes,
A and B. The two nodes belong to a unique
workgroup. The node(s) will be named as the
workgroup name with an '-A' (or '-B' appended).
In a single node configuration, only node A can
be installed. It's name will be the workgroup
name with an '-A' appended.

Setting machine name to CICMEM-nnn-A.
Configuring node A [CICMEM-nnn-A].
Configuring node B [CICMEM-nnn-B].
Setting workgroup name to CICMEM-nnn.
```

16 STEP 5: Configure the administration accounts

```
The CICM and the CICMEM both have an
Administration Account. The preboot section is
used to configure this account.

Enter the local Administrator account password:
```

<customer_configuration_password>

The password (up to 8 alphanumerical characters) can be different than the one you specified earlier for the pre-shared key. Record the password for your records.

```
Re-enter to confirm:
```

<customer_configuration_password>

```
Successfully set administrator password.
```

17 STEP 6: Configure the software user account

```
The CICM/CICM-EM use a single security [aka
COMUSER] account under which all software is
executed. This account should be configured with
the same username and password on each system
(CICM-EMs and CICMs).
NOTE: this account should *NOT* be used for
interactive logins.
The /display option will display the comuser
password [only do this over a secure
connection]. Note that this will display the
auto-generated password based on the IPSec
pre-shared key (which you must re-enter). If you
```

```
enter the wrong key then an incorrect software
account password will be displayed.

Enter a username under which the software will
run (hit ENTER to accept "COMUSER"):
```

<customer_userid>

Nortel recommends you press enter to accept the default value of *COMUSER* as the userid for the COMUSER account. Note that the CICM-EM and all subtending CICM nodes must have the same COMUSER userid. Record the userid for your records.

```
Using default account name "comuser".
Creating user account.
Configuring user group.
Setting user account expiry to UNLIMITED.
Setting failed login attempts to UNLIMITED.
Configuring access permissions.
Configuring launch permissions.
Configuring logon rights.
Configuring applications.....................
Installing cxippreboot.
Reinstalling cxippreboot.
Software account successfully configured.
```

18 `STEP 7: Configure the element manager environment`

No user input is required.

```
The Element Manager has additional data that
needs to be set [EM domain/machine names, DCOM
protocols preferences etc].
Setting up Element Manager environment.
Setting up DCOM protocols.
WARNING: An important change was made to DCOM
protocols preferences. You MUST reboot after
install has finished to make the changes take
effect.
Element Manager environment successfully
configured.
```

19 `STEP 8: Configure the Static adapter settings`

```
This section creates and configures the 'Static'
LAN Adapters. There are two static adapters per
node - A1/A2 and B1/B2. Each has a single IP
address. Heartbeat messages are sent between the
addresses on A and the addresses on B. These
addresses are restricted to the CICM-EM and they
must be in a distinct subnet from any other
```

```
addresses used on the CICM-EM or in the network
in general.
The static addresses have been autogenerated
based on the system ID of nnn.
The base address is <auto_generated_IP_address>
and will be used to create a subnet range with
mask 255.255.255.248.

Do you wish to use the base address? [Y|N,
default=Y]
```

<customer_static_address>

Nortel recommends entering **Y** (yes) to accept it provided the auto-generated address does not conflict with an existing IP address in the network. Entering **N** (no) means you must provide the valid static address values.

```
Configuring A1
Configuring A2
Configuring B1
Configuring B2
Configuring RPC...
[SC] ChangeServiceConfig SUCCESS.
```

20 STEP 9: Configure the Floating Admin adapter settings

```
This section configures the Floating Admin
adapter information. The floating Admin IP
address will be bound to the most available
interface on the Element Manager node.

Enter the Node A Admin address:
```

<node_A_admin_address>

```
Enter the Node B Admin address:
```

<node_B_admin_address>

```
Enter the network mask for the Admin IP network:
```

<network_mask_for_admin_ip_network>

```
Enter the default router for the Admin IP
network:
```

<default_router_for_admin_ip_network>

```
Configuring PA
Configuring PB
Configuring route for A1
Configuring route for A2
```

21 STEP 10: Configure the Floating Http adapter settings

This section configures the HTTP floating adapter information. The floating HTTP address will be bound to the most available adapter on whichever node of the CICM-EM is the Master. Therefore the same address should be datafilled on each CICM-EM node. The address will be used for all Web Browser communication.

Enter the Http IP address for this CICM-EM:

<http_ip_address_for_cicmem>

22 STEP 10: Configure PAM authentication

Will this CICM-EM use PAM to authenticate users? [Y|N, default=N]:

Enter **Y** (yes) to enable PAM authentication or **N** (no). With **Y** you must answer the prompts to configure PAM data (for example, the proxy server). With N the response is:

The Element Manager will use local NT authentication.

23 STEP 12: Configure the SNMP settings

The Element Manager can be managed remotely by an SNMP management station. Most of the data accessible via SNMP is derived directly from the CentrexIP internal MIB but certain data must be entered during initial configuration. This data includes ...

<customer_snmp_configuration>

Configure the *SNMP settings* by entering your configuration values or if not using SNMP, press enter to accept all the default values. The progression of information is not shown in this step.

Are you satisfied with the above responses [Y|N, default=Y]:

Enter **Y** (yes) to accept or **N** (no) to make changes.

```
--- Starting
--- Looking up system description from host OS
--- ...
--- Finished
```

24 STEP 13: Configure the time settings for the EM

```
You can use this utility to set the time and time
zone on the EM.
Current time zone is n.n hours from GMT (GMT
Daylight Time).
Standard zone is n.n hours from GMT (GMT
Standard Time)

Do you want to change it [Y|N, default=N]:
```

Entering **Y** presents a choice of time zones. Select the time zone by entering the number associated with it or press enter to accept the default.

Y

```
Current local date is <value>.

Do you want to change it [Y|N, default=N]:
```

Enter **N** to accept the local date or enter **Y** to change it. After **Y**, answer the prompts to specify the day, month, and year.

Y

```
Current local time is <value>.

Do you want to change it [Y|N, default=N]:
```

Enter **N** to accept the local time or enter **Y** to change it. After **Y**, answer the prompts to specify the hours and minutes.

Y

```
Current time for scheduled backups is 02:00.

Do you want to change it [Y|N, default=N]:
```

Configure a different time to schedule the automatic backup of the software image by entering **Y** (yes), then a 24-hour time as **<hh:mm>**.

N

```
Found NTP Server Configuration: -
Primary NTP Server Address = <ip_address>
Backup NTP Server Address = <ip_address>
Configuring W32Time Service with NTP Server
parameters...
Successfully configured NTP Server Parameters
```

25 `STEP 14: Configure the Hard disk`

No user input is required.

```
The CICM and CICM-EM have two disk partitions,
C: and D:. These must be converted to the NTFS
file system.
```

```
Setting system to convert C: and D: to NTFS file
system on next boot.
```

26 `STEP 15: Apply the EM software load`

```
Apply the default software image to the Element
Manager.
Registering {...
```

Wait while preboot configures the software. The progression of information is not shown in this step.

```
... Registry Flush Complete.

A reboot must now be performed to complete
installation. Do you want to restart now? [Y|N,
default=N]:
```

`Y`

```
Rebooting now...
```

Temporary lockout occurs at the command prompt.

At the CICM-EM maintenance page

27 Wait for the node to synchronize data with its mate node.

When synchronized, the node is fully in service as shown by the status *system idle* or *system running*.

28 Apply additional MRs as needed to restore the node to the same MR level as its mate node. Refer to the procedure “Perform a CICM 7.0.xxx MR upgrade” in *CICM Upgrades*, NN10230-461, the version for SN07.

29 Verify the CICM-EM pair is fully in service.

At the PC desktop for remote access to the CICM node

30 Locally access CICM Node A through the console serial port.

31 At the prompt, log in.

```
login:
```

For the userid enter *Administrator* and for the password enter *Administrator*.

The screen prompt becomes:

```
C:\Documents and Settings\Administrator>
```

32 At the CLI of a Windows session, you apply your SNMP data to enable a connection with IEMS by entering:

`preboot snmp /interactive`

33 This procedure is complete. Return to the task flow Task flow of CICM-EM and CICM node rollbacks.

Using preboot to re-image a CPV5370 CICM node

Use preboot to re-image a CICM node with CPV5370 CPU cards (blades) to a base CICM software release.

Prerequisites to using preboot to re-image a CPV5370 CICM node

Address the prerequisites before starting the procedure.

- You must follow the sequence of procedures identified in Task flow of CICM-EM and CICM node rollbacks.
- When the CICM node's software has been restored, its data is automatically synchronized with the mate EM.
- Output from the progression of preboot is shown by `this font`. Command entries are shown by **this font**.
- When *more* appears on the screen, press the keyboard spacebar to advance the screen.

CAUTION
Risk of service prevention
Using preboot means re-entering specific configuration data that would normally be handled by an initial installation. While configuring, extreme care must be taken to ensure accurate entries especially with IP addresses.

Procedure steps to using preboot to re-image a CPV5370 CICM node

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

1 Locally access Node A through the console serial port.

2 Pressing enter in the terminal window will eventually get the login prompt.

```
login:
```

3 For the userid enter *Administrator* and for the password enter *Administrator*.

4 At the command line interface (CLI) of a Windows XP session, enter:

```
preboot
```

5
```
Press CTRL-C at any prompt to abort preboot.
Press ENTER now to start preboot configuration.
```

Press enter to start *preboot*.

6
```
Is this node A of the CICM? [Y|N, default=Y]:
```

Ensure that you are prebooting node A and enter **Y** (yes).

7 STEP 1: Configure BOOTP options (CPV5370 ONLY)

BOOTP Settings must be entered by the craftsperson for CPV5370 CPUs since network BOOTP is only possible on hardware installed in a SAM 21 chassis i.e. CPN5385 slave CPUs. This is a CICM Node. The identifier (name) for this node has the format CICM-000-X where 000 is the numeric system identifier for this node and its mate node and X is the node identifier and can be either 'A' or 'B'.

Enter the 3 digit system identifier for this chassis [range 000-511]:

<3_digit_system_identifier>

Node name recorded as CICM-nnn-A.

Enter the Public Admin Network IP Address for this node:

<public_admin_network_ip_address_for_cicm>

Enter the Public Admin Network Subnet mask for this node:

<public_admin_network_subnet_mask_for_cicm>

Enter the default route for the Public Admin Network (Enter 0.0.0.0 for no route):

<default_route_for_public_admin_network>

Enter a no route only if you do not have a default and you understand the consequences of not having one.

Enter the Primary NTP Server IP Address:

<primary_ntp_server_ip_address>

Enter the Secondary NTP Server IP Address:

<secondary_ntp_server_ip_address>

Enter the Primary EM IP Address:

<primary_em_ip_address>

Enter the Backup EM IP Address for the public admin network. (Enter 0.0.0.0 for no Backup EM):

<backup_em_ip_address_for_public_admin_net>

Flushing Registry Data...
Registry Flush Complete.

8 `A reboot must now be performed to complete installation. Do you want to restart now? [Y|N, default=N]:`

Y

`Rebooting now...`

9 Pressing enter in the terminal window will eventually get the login prompt.

`login:`

10 For the userid enter *Administrator* and for the password enter *Administrator*.

The screen prompt becomes:

C:\Documents and Settings\Administrator>

11 At the command line interface (CLI) of a Windows XP session, enter:

preboot

12 `Press CTRL-C at any prompt to abort preboot.`
`Press ENTER now to start preboot configuration.`

Press enter to start *preboot*.

`This CICM is node A.`

13 `STEP 1: Configure BOOTP options (CPV5370 ONLY)`

`Skipping option bootp (already complete).`

No user input is required.

14 `STEP 2: Configure IPSec`

```
This step configures IPSec. You will be prompted
for the IPSec pre-shared key. This is the key
that is used to connect to the IPSec protected
ports on the CICM[EM]. A hash of this pre-shared
key will be used for the software account
(comuser) password. It is important to remember
the pre-shared key entered, as this key MUST be
the same on both the CICM and the CICM EM. The
IPSec step can only be run once.
To re-key IPSec use the following command:
preboot ipsec /rekey
To toggle the security setting of telnet use the
following command
preboot ipsec /telnet
To deactivate the ipsec policy:
preboot ipsec /deactivate
```

```
To re activate the ipsec policy:
preboot ipsec /activate

Enter the IPSec Pre-Shared Key:
```

<customer_configuration_password>

Record the pre-shared key (password) for your records.

```
Re-enter to confirm:
```

<customer_configuration_password>

```
Secure the telnet port? [Y|N, default=Y]:
```

N

At this point in the configuration, Nortel recommends not securing the telnet port. It can be configured later after the rollback is completed.

15 `STEP 3: Configure the gateway type`

```
This Gateway is automatically set up in a H248
configuration. Gateway configured to support
H248.
```

No user input is required.

16 `STEP 4: Configure the workgroup and computer name`

```
The CICM/CICM-EM can operate in either a single
or dual node configuration. In a dual node
configuration, the CICM/CICM-EM has two nodes,
A and B. The two nodes belong to a unique
workgroup. The node(s) will be named as the
workgroup name with an '-A' (or '-B' appended).
In a single node configuration, only node A can
be installed. It's name will be the workgroup
name with an '-A' appended.
```

No user input is required.

```
Setting machine name to CICM-nnn-A.
Configuring node A [CICM-nnn-A].
Configuring node B [CICM-nnn-B].
Setting workgroup name to CICM-nnn.
```

17 `STEP 5: Configure the administration accounts`

```
The CICM and the CICMEM both have an
Administration Account. The preboot section is
used to configure this account.
```

```
Enter the local Administrator account password:
```

<customer_configuration_password>

The password (up to 8 alphanumerical characters) can be different than the one you specified earlier for the pre-shared key. Record the password for your records.

```
Re-enter to confirm:
```

<customer_configuration_password>

```
Successfully set administrator password.
Creating Nortel Networks TAS account.
Successfully created Nortel TAS account.
```

18 `STEP 6: Configure the software user account`

```
The CICM/CICM-EM use a single security [aka
COMUSER] account under which all software is
executed. This account should be configured with
the same username and password on each system
(CICM-EMs and CICMs).
NOTE: this account should *NOT* be used for
interactive logins.
The /display option will display the comuser
password [only do this over a secure
connection]. Note that this will display the
auto-generated password based on the IPSec
pre-shared key (which you must re-enter). If you
enter the wrong key then an incorrect software
account password will be displayed.

Enter a username under which the software will
run (hit ENTER to accept "COMUSER"):
```

<customer_userid>

Nortel recommends you press enter to accept the default value of *COMUSER* as the userid for the COMUSER account. Note that the CICM-EM and all subtending CICM nodes must have the same COMUSER userid. Record the userid for your records.

```
Using default account name "comuser".
Creating user account.
Configuring user group.
Setting user account expiry to UNLIMITED.
Setting failed login attempts to UNLIMITED.
Configuring access permissions.
Configuring launch permissions.
Configuring logon rights.
Configuring applications.....................
Installing cxippreboot.
```

```
Reinstalling cxippreboot.
Software account successfully configured.
```

19 STEP 7: Configure the Static adapter settings

This section creates and configures the 'Static' LAN Adapters. There are two static adapters per node - A1/A2 and B1/B2. Each has a single IP address. Heartbeat messages are sent between the addresses on A and the addresses on B. These addresses are restricted to the CICM and they must be in a distinct subnet from any other addresses used on the CICM or in the network in general.

Enter Admin VLAN id [1...4094, default=2]:

<customer_admin_vlan_value>

Enter H248 VLAN id [1...4094, default=4]:

<customer_h248_vlan_value>

The static addresses have been autogenerated based on the system ID of nnn.
The base address is <auto generated IP address> and will be used to create a subnet range with mask 255.255.255.248.

Do you wish to use the base address? [Y|N, default=Y]

Nortel recommends entering Y (yes) to accept it provided the auto-generated address does not conflict with an existing IP address in the network. Entering N (no) means you must provide the valid static address values.

```
Configuring adapter A1 - this may take a few
minutes...
…
Configuring adapter A2 - this may take a few
minutes...
…
Configuring adapter A4 - this may take a few
minutes...
…
[SC] ChangeServiceConfig SUCCESS.
```

20 STEP 8: Configure the Unistim LAN settings

This section configures the CICM's Unistim LAN adapter. The Unistim LAN is used for call signalling between CICM and its clients

(terminals). The LAN's port filter only permits those UDP ports used to communicate with clients. [OAMP functions are blocked on the Unistim LAN.]

Enter Unistim VLAN id [1...4094, default=3]:

<unistim_vlan_id>

Enter the Unistim IP address for this node:

<unistim_static_ip_address_for_the_node>

Enter the network mask for the Unistim IP network:

<network_mask_for_unistim_ip_network>

Enter the default route for the Unistim IP network (Enter 0.0.0.0 for no route):

<default_route_for_unistim_ip_network>

Enter a no route only if you do not have a default and you understand the consequences of not having one.

Configuring Unistim Adapter - this may take a few minutes...
...
Applying Default Gateway: The ReturnValue is nn (4 byte int)

21 STEP 9: Configure the H248 LAN settings

This section configures the H248 floating adapter. The floating H248 IP address will be bound to the A4/B4 adapter on whichever CICM node is Master. Therefore, datafill the same address on each node. This address will be used for all communication with the Gateway Controller and should match the Media Gateway IP Address provisioned for the CICM on the Gateway Controller EM. The H248 LAN's port filter permits only the UDP traffic used to communicate with the Gateway Controller. [OAMP functions are blocked on the H248 LAN.] You must also enter two static addresses for the H248 LAN. One is for Node A and the other is for Node B.

Enter the Floating H248 IP address for this CICM:

<floating_h248_ip_address_for_cicm>

```
Enter the Static H248 IP address for Node A:
```

<static_h248_ip_address_for_node_A>

```
Enter the Static H248 IP address for Node B:
```

<static_h248_ip_address_for_node_B>

```
Enter the network mask for the H248 IP network:
```

<network_mask_for_h248_ip_network>

```
Enter the default route for the H248 IP network
(Enter 0.0.0.0 for no route):
```

<default_route_for_h248_ip_network>

Enter a no route only if you do not have a default and you understand the consequences of not having one.

```
Applying IP Address and Subnet Mask
```

22 `STEP 10: Configure the VMG settings`

```
This step configures the Virtual Media Gateway.
The CICM can support up to 3069 lines (up to 1023
on the 5370 hardware) [for Nortel testing
purposes *ONLY*, a lower value may be entered.]
WARNING - in a dual node configuration, the
number of lines must be datafilled the same on
both nodes of the CICM.
To re-size the VMG to the maximum number of
lines use the following command:
preboot vmg /resize

Enter the number of lines for the gateway
[1...1023, default=1023]:
```

Nortel recommends you accept the default number of lines.

<number_of_lines_for_the_gateway>

```
Enter the Media Gateway Controller IP address:
```

<media_gateway_controller_ip_address>

```
Enter the Media Gateway Controller UDP port
[0...65535, default=2944]:
```

<media_gateway_controller_udp_port>

23 `STEP 11: Configure the Floating Admin adapter settings`

```
This section configures the Floating Admin
adapter information. The floating Admin IP
```

```
address will be bound to the most available
interface on the Gateway node.

Enter the Node A Admin address:
```

<node_A_admin_address>

```
Enter the Node B Admin address:
```

<node_B_admin_address>

```
Enter the network mask for the Admin IP network:
```

<network_mask_for_admin_ip_network>

```
Enter the default router for the Admin IP
network:
```

<default_router_for_admin_ip_network>

```
Configuring PA
Configuring PB
Configuring route for A1
Configuring route for A2
```

24 `STEP 12: Configure the SNMP settings`

```
The Gateway can be managed remotely by an SNMP
management station. Most of the data accessible
via SNMP is derived directly from the CentrexIP
internal MIB but certain data must be entered
during initial configuration. This data
includes ...
```

<customer_snmp_configuration>

Configure the *SNMP settings* by entering your configuration values or if not using SNMP, press enter to accept all the default values. The progression of information is not shown in this step.

```
... ---Finished

Are you satisfied with the above responses [Y|N,
default=Y]:
```

Enter **Y** (yes) to accept or **N** (no) to make changes.

```
--- Starting
--- Looking up system description from host OS
--- ...
--- Finished
```

25 `STEP 13: Configure the time settings for the gateway`

```
You can use this utility to set the time and time
zone on the CICM. It will inform any running
```

```
software of the time change.
Current time zone is n.n hours from GMT (GMT
Daylight Time).
Standard zone is n.n hours from GMT (GMT
Standard Time)

Do you want to change it [Y|N, default=N]:
```

Entering **Y** presents a choice of time zones. Select the time zone by entering the number associated with it or press enter to accept the default.

Y

```
Current local date is <value>.

Do you want to change it [Y|N, default=N]:
```

Enter **N** to accept the local date or enter **Y** to change it. After **Y**, answer the prompts to specify the day, month, and year.

Y

```
Current local time is <value>.

Do you want to change it [Y|N, default=N]:
```

Enter **N** to accept the local time or enter **Y** to change it. After **Y**, answer the prompts to specify the hours and minutes.

Y

```
Current time for scheduled backups is 02:00.

Do you want to change it [Y|N, default=N]:
```

Configure a different time to schedule the automatic backup of the software image by entering **Y** (yes), then a 24-hour time as **<hh:mm>**.

N

26 `STEP 14: Configure the Hard disk`

No user input is required.

```
The CICM and CICM-EM have two disk partitions,
C: and D:. These must be converted to the NTFS
file system.
Setting system to convert C: and D: to NTFS file
system on next boot.
```

27 `STEP 15: Apply the CICM software load`

```
Apply the default software image to the Gateway.
```

Wait while preboot configures the software. The progression of information is not shown in this step.

```
Registering ...
... Registry Flush Complete.

A reboot must now be performed to complete
installation. Do you want to restart now? [Y|N,
default=N]:
```

Y

```
Rebooting now...
```

Temporary lockout occurs at the command prompt.

At the CICM maintenance page

28 Wait for the node to synchronize data with its mate node.

When synchronized, the node is fully in service as shown by the status *system idle* or *system running*, and the *VMG Status* is also synchronized (shown with the Node status).

29 Apply additional MRs as needed to restore the node to the same MR level as its mate node. Refer to the procedure “Perform a CICM 7.0.xxx MR upgrade” in *CICM Upgrades*, NN10230-461, the version for SN07.

At the CICM status page

30 Verify the CICM node pair fully in service.

31 Leave the CICM terminals on Node B, the active master. Although an initial SN07 configuration typically splits the terminal connections between Nodes A and B, there is no need to split them after the rollback.

At the PC desktop for remote access to the CICM node

32 Locally access CICM Node A through the console serial port.

33 At the prompt, log in.

```
login:
```

For the userid enter *Administrator* and for the password enter *Administrator*.

The screen prompt becomes:

```
C:\Documents and Settings\Administrator>
```

34 At the CLI of a Windows session, you apply your SNMP data to enable a connection with IEMS by entering:

```
preboot snmp /interactive
```

35 This procedure is complete. Return to the task flow Task flow of CICM-EM and CICM node rollbacks.

Using preboot to re-image a CPV5370 CICM-EM

Use preboot to re-image a CICM-EM with CPV5370 CPU cards (blades) to a base CICM-EM software release.

Prerequisites to using preboot to re-image a CPV5370 CICM-EM

Address the prerequisites before starting the procedure.

- You must follow the sequence of procedures identified in Task flow of CICM-EM and CICM node rollbacks.
- When the CICM-EM's software has been restored, its data is automatically synchronized with the mate EM.
- Output from the progression of preboot is shown by `this font`. Command entries are shown by **this font**.
- When *more* appears on the screen, press the keyboard spacebar to advance the screen.

CAUTION
Risk of service prevention
Using preboot means re-entering specific configuration data that would normally be handled by an initial installation. While configuring, extreme care must be taken to ensure accurate entries especially with IP addresses.

Procedure steps to using preboot to re-image a CPV5370 CICM-EM

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

1 Locally access Node A through the console serial port.

2 Pressing enter in the terminal window will eventually get the login prompt.

```
login:
```

3 For the userid enter *Administrator* and for the password enter *Administrator*.

4 At the command line interface (CLI) of a Windows 2000 session, enter **preboot**.

5
```
Press CTRL-C at any prompt to abort preboot.
Press ENTER now to start preboot configuration.
```

Press enter to start *preboot*.

6
```
Is this node A of the CICM? [Y|N, default=Y]:
```

Ensure that you are prebooting node A and enter **Y** (yes).

This CICM-EM is Node A.

7 STEP 1: Configure BOOTP options (CPV5370 ONLY)

BOOTP Settings must be entered by the craftsperson for CPV5370 CPUs since network BOOTP is only possible on hardware installed in a SAM 21 chassis i.e. CPN5385 slave CPUs. This is a CICM-EM Node. The identifier (name) for this node has the format CICMEM-000-X where 000 is the numeric system identifier for this node and its mate node and X is the node identifier and can be either 'A' or 'B'.

Enter the 3 digit system identifier for this chassis [range 000-511]:

<3_digit_system_identifier>

Node name recorded as CICM-nnn-A.

Enter the Public Admin Network IP Address for this node:

<public_admin_network_ip_address_for_cicm>

Enter the Public Admin Network Subnet mask for this node:

<public_admin_network_subnet_mask_for_cicm>

Enter the default route for the Public Admin Network (Enter 0.0.0.0 for no route):

<default_route_for_public_admin_network>

Enter a no route only if you do not have a default and you understand the consequences of not having one.

Enter the Primary NTP Server IP Address:

<primary_ntp_server_ip_address>

Enter the Secondary NTP Server IP Address:

<secondary_ntp_server_ip_address>

8 STEP 2: Configure SSH

Access to the CICM EM may be achieved either by using a secured SSH connection or via the EM's serial port. SSH keys are generated during this step (which takes some time). On completion the SSH fingerprint will be displayed. Use this fingerprint for server validation when connecting to the CICM EM. Do not trust any

```
other fingerprint.
To display the SSH fingerprint after the SSH
step use the following:
preboot ssh /fingerprint
Generating SSH keys ...
...
The CICM EM SSH Fingerprint is:
<fingerprint_code>
```

No user input is required.

```
Press ENTER to continue.
SSH Configuration Complete.
```

9 Messages: `Flushing Registry Data...`
`Registry Flush Complete.`

```
A reboot must now be performed to complete
installation. Do you want to restart now? [Y|N,
default=N]:
```

Y

```
Rebooting now...
```

10 Pressing enter in the terminal window will eventually get the login prompt.

```
login:
```

11 For the userid enter *Administrator* and for the password enter *Administrator*.

The screen prompt becomes:

C:\Documents and Settings\Administrator>

12 At the command line interface (CLI) of a Windows XP session, enter:

preboot

13
```
Press CTRL-C at any prompt to abort preboot.
Press ENTER now to start preboot configuration.
```

Press enter to start *preboot*.

```
This CICM-EM is node A.
```

14
```
STEP 1: Configure BOOTP options (CPV5370 ONLY)
Skipping option bootp (already complete).
```

No user input is required.

15
```
STEP 2: Configure SSH
Skipping option ssh (already complete).
```

No user input is required.

16 This step configures IPSec. You will be prompted for the IPSec pre-shared key. This is the key that is used to connect to the IPSec protected ports on the CICM[EM]. A hash of this pre-shared key will be used for the software account (comuser) password. It is important to remember the pre-shared key entered, as this key MUST be the same on both the CICM and the CICM EM. The IPSec step can only be run once.
To re-key IPSec use the following command:
preboot ipsec /rekey
preboot ipsec /telnet
To deactivate the ipsec policy:
preboot ipsec /deactivate
To re activate the ipsec policy:
preboot ipsec /activate
NB: <cicmname> must be identical to the name specified in the /permitcicm.

Enter the IPSec Pre-Shared Key:

<customer_configuration_password>

Record the pre-shared key (password) for your records.

Re-enter to confirm:

<customer_configuration_password>

Secure the telnet port? [Y|N, default=Y]:

N

At this point in the configuration, Nortel recommends not securing the telnet port. It can be configured later after the rollback is completed.

17 STEP 4: Configure the workgroup and computer name

No user input is required.

The CICM/CICM-EM can operate in either a single or dual node configuration. In a dual node configuration, the CICM/CICM-EM has two nodes, A and B. The two nodes belong to a unique workgroup. The node(s) will be named as the workgroup name with an '-A' (or '-B' appended). In a single node configuration, only node A can be installed. It's name will be the workgroup name with an '-A' appended.

```
Setting machine name to CICMEM-nnn-A.
Configuring node A [CICMEM-nnn-A].
Configuring node B [CICMEM-nnn-B].
Setting workgroup name to CICMEM-nnn.
```

18 `STEP 5: Configure the administration accounts`

```
The CICM and the CICMEM both have an
Administration Account. The preboot section is
used to configure this account.

Enter the local Administrator account password:
```

<customer_configuration_password>

The password (up to 8 alphanumerical characters) can be different than the one you specified earlier for the pre-shared key. Record the password for your records.

```
Re-enter to confirm:
```

<customer_configuration_password>

```
Successfully set administrator password.
```

19 `STEP 6: Configure the software user account`

```
The CICM/CICM-EM use a single security [aka
COMUSER] account under which all software is
executed. This account should be configured with
the same username and password on each system
(CICM-EMs and CICMs).
NOTE: this account should *NOT* be used for
interactive logins.
The /display option will display the comuser
password [only do this over a secure
connection]. Note that this will display the
auto-generated password based on the IPSec
pre-shared key (which you must re-enter). If you
enter the wrong key then an incorrect software
account password will be displayed.

Enter a username under which the software will
run (hit ENTER to accept "COMUSER"):
```

<customer_userid>

Nortel recommends you press enter to accept the default value of *COMUSER* as the userid for the COMUSER account. Note that the CICM-EM and all subtending CICM nodes must have the same COMUSER userid. Record the userid for your records.

```
Using default account name "comuser".
Creating user account.
```

```
Configuring user group.
Setting user account expiry to UNLIMITED.
Setting failed login attempts to UNLIMITED.
Configuring access permissions.
Configuring launch permissions.
Configuring logon rights.
Configuring applications.....................
Installing cxippreboot.
Reinstalling cxippreboot.
Software account successfully configured.
```

20 STEP 7: Configure the element manager environment

No user input is required.

```
The Element Manager has additional data that
needs to be set [EM domain/machine names, DCOM
protocols preferences etc].
Setting up Element Manager environment.
Setting up DCOM protocols.
WARNING: An important change was made to DCOM
protocols preferences. You MUST reboot after
install has finished to make the changes take
effect.
Element Manager environment successfully
configured.
```

21 STEP 8: Configure the Static adapter settings

```
This section creates and configures the 'Static'
LAN Adapters. There are two static adapters per
node - A1/A2 and B1/B2. Each has a single IP
address. Heartbeat messages are sent between the
addresses on A and the addresses on B. These
addresses are restricted to the CICM-EM and they
must be in a distinct subnet from any other
addresses used on the CICM-EM or in the network
in general.
The static addresses have been autogenerated
based on the system ID of nnn.
The base address is <auto generated IP address>
and will be used to create a subnet range with
mask 255.255.255.248.

Do you wish to use the base address? [Y|N,
default=Y]
```

<customer_static_address>

Nortel recommends entering **Y** (yes) to accept it provided the auto-generated address does not conflict with an existing IP address in the network. Entering **N** (no) means you must provide the valid static address values.

```
Configuring A1
Configuring A2
Configuring B1
Configuring B2
Configuring RPC...
[SC] ChangeServiceConfig SUCCESS.
```

22 `This section configures the Floating Admin adapter information. The floating Admin IP address will be bound to the most available interface on the Element Manager node.`

Configure the *Floating Admin Adapter settings* by entering:

<node_A_admin_address>

<node_B_admin_address>

<network_mask_for_admin_ip_network>

<default_router_for_admin_ip_network>

```
Configuring PA
Configuring PB
Configuring route for A1
Configuring route for A2
```

23 `STEP 9: Configure the Floating Admin adapter settings`

`This section configures the HTTP floating adapter information. The floating HTTP address will be bound to the most available adapter on whichever node of the CICM-EM is the Master. Therefore the same address should be datafilled on each CICM-EM node. The address will be used for all Web Browser communication.`

`Enter the Node A Admin address:`

<node_A_admin_address>

`Enter the Node B Admin address:`

<node_B_admin_address>

`Enter the network mask for the Admin IP network:`

<network_mask_for_admin_ip_network>

```
Enter the default router for the Admin IP
network:
```

<default_router_for_admin_ip_network>

```
Configuring PA
Configuring PB
Configuring route for A1
Configuring route for A2
```

24 `STEP 10: Configure PAM authentication`

```
Will this CICM-EM use PAM to authenticate users?
[Y|N, default=N]:
```

Enter **Y** (yes) to enable PAM authentication or **N** (no). With **Y** you must answer the prompts to configure PAM data (for example, the proxy server). With N the response is:

```
The Element Manager will use local NT
authentication.
```

25 `STEP 12: Configure the SNMP settings`

```
The Element Manager can be managed remotely by
an SNMP management station. Most of the data
accessible via SNMP is derived directly from the
CentrexIP internal MIB but certain data must be
entered during initial configuration. This data
includes ...
```

<customer_snmp_configuration>

Configure the *SNMP settings* by entering your configuration values or if not using SNMP, press enter to accept all the default values. The progression of information is not shown in this step.

```
Are you satisfied with the above responses [Y|N,
default=Y]:
```

Enter **Y** (yes) to accept or **N** (no) to make changes.

```
--- Starting
--- Looking up system description from host OS
--- ...
--- Finished
```

26 `STEP 13: Configure the time settings for the EM`

```
You can use this utility to set the time and time
zone on the EM.
Current time zone is n.n hours from GMT (GMT
Daylight Time).
Standard zone is n.n hours from GMT (GMT
Standard Time)
```

```
Do you want to change it [Y|N, default=N]:
```

Entering **Y** presents a choice of time zones. Select the time zone by entering the number associated with it or press enter to accept the default.

Y

```
Current local date is <value>.
Do you want to change it [Y|N, default=N]:
```

Enter **N** to accept the local date or enter **Y** to change it. After **Y**, answer the prompts to specify the day, month, and year.

Y

```
Current local time is <value>.
Do you want to change it [Y|N, default=N]:
```

Enter **N** to accept the local time or enter **Y** to change it. After **Y**, answer the prompts to specify the hours and minutes.

Y

```
Current time for scheduled backups is 02:00.
Do you want to change it [Y|N, default=N]:
```

Accept the default or configure a different time to schedule the automatic backup of the software image by entering **Y** (yes), then a 24-hour time as **<hh:mm>**.

27 `STEP 14: Configure the Hard disk`

No user input is required.

```
The CICM and CICM-EM have two disk partitions,
C: and D:. These must be converted to the NTFS
file system.
Setting system to convert C: and D: to NTFS file
system on next boot.
```

28 `STEP 15: Apply the EM software load`

```
Apply the default software image to the Element
Manager.
Registering {...
```

Wait while preboot configures the software. The progression of information is not shown in this step.

```
... Registry Flush Complete.
```

```
A reboot must now be performed to complete
installation. Do you want to restart now? [Y|N,
default=N]:
```

Y

```
Rebooting now...
```

Temporary lockout occurs at the command prompt.

At the CICM-EM maintenance page

29 Wait for the node to synchronize data with its mate node.

When synchronized, the node is fully in service as shown by the status *system idle* or *system running*, and the *VMG Status* is also synchronized (shown with the Node status).

30 Apply additional MRs as needed to restore the node to the same MR level as its mate node. Refer to the procedure “Perform a CICM 7.0.xxx MR upgrade” in *CICM Upgrades*, NN10230-461, the version for SN07.

31 Verify the CICM-EM pair is fully in service.

At the PC desktop for remote access to the CICM node

32 Locally access CICM Node A through the console serial port.

33 At the prompt, log in.

```
login:
```

For the userid enter *Administrator* and for the password enter *Administrator*.

The screen prompt becomes:

```
C:\Documents and Settings\Administrator>
```

34 At the CLI of a Windows session, you apply your SNMP data to enable a connection with IEMS by entering:

`preboot snmp /interactive`

35 This procedure is complete. Return to the task flow Task flow of CICM-EM and CICM node rollbacks.

Upgrading firmware on IP phone sets

This section of *NN10230-461 CICM Upgrades* provides the task flow and procedure to upgrade the firmware of the IP phone sets that connect to a Centrex IP Client Manager (CICM) node.

The topics in this section are:

- CICM IP phone firmware upgrades
- Upgrading the firmware on an IP phone set

CICM IP phone firmware upgrades

This section includes the task flow to upgrade the firmware of the types of IP phones that can connect to the CICM nodes. The topics are:

- Prerequisites to the task flow of CICM IP phone firmware upgrades
- Task flow of CICM IP phone firmware upgrades

Prerequisites to the task flow of CICM IP phone firmware upgrades

Before following the task flow, ensure that you have addressed these requirements.

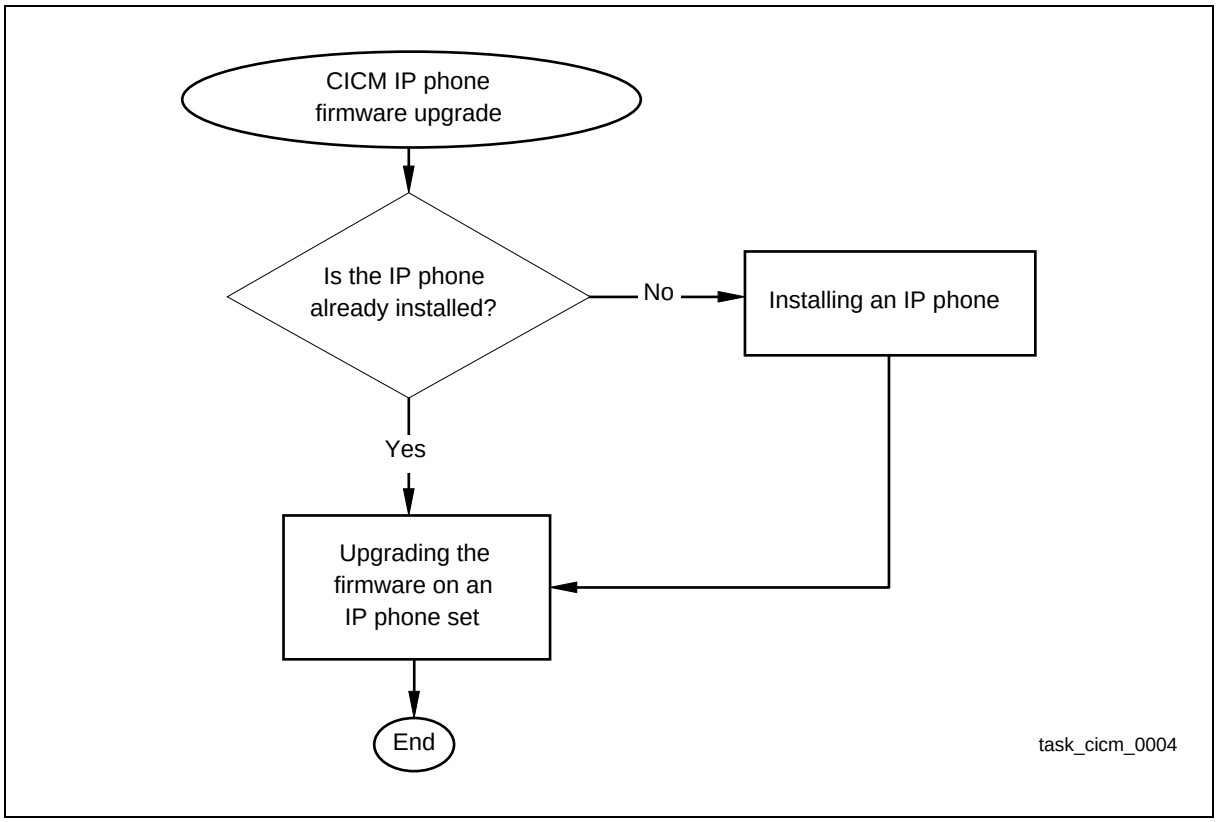
- The IP phone must already be installed as described in *m6350 Softclient Installation Guide*, NN10182-113.
- The IP phones supported with CICM are:
  - IP Phone 2001
  - IP Phone 2002
  - IP Phone 2004
  - IP Conference Phone 2033
- You must be familiar with the user guide of the Nortel IP phone you are upgrading. The user guides are:
  - *CS 2100 IP Phone 2001 User Guide*, NN10300-005
  - *CS 2100 IP Phone 2002 User Guide*, NN10300-007
  - *CS 2100 IP Phone 2004 User Guide*, NN10300-009
  - *CS 2100 IP Phone Key Expansion Module User Guide*, NN10300-011

Task flow of CICM IP phone firmware upgrades

The task flow shows the sequence of procedures to upgrade the firmware of a CICM IP phone, as shown in the figure Task flow of a CICM IP phone firmware upgrade.

To link any procedure, go to Navigation immediately following the figure.

Task flow of a CICM IP phone firmware upgrade



Navigation

The procedures and task flow in the task flow are listed alphabetically.

- “Installing an IP phone”. See the procedure in *m6350 Softclient Installation Guide*, NN10183-113.
- Upgrading the firmware on an IP phone set

Upgrading the firmware on an IP phone set

Upgrade the firmware of an IP phone set to ensure optimum operation of the phone and the CICM services supported by that model.

Prerequisites to upgrading the firmware on an IP phone set

Address the prerequisites before starting the procedure.

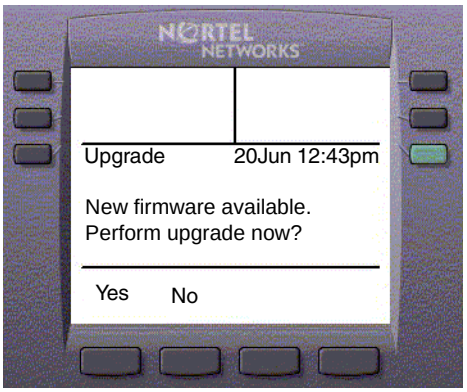
- You must follow the Prerequisites and sequence of procedures identified in CICM IP phone firmware upgrades.
- The indication that a firmware upgrade is available for the IP phone is either:
  - an upgrade button is displayed at the login screen when the user is not logged in
  - an upgrade option is displayed in the options menu when the user is logged in

Procedure steps to upgrading the firmware on an IP phone set

At the IP phone set

1 When the firmware upgrade icon is shown on the login screen, log in as described by the user guide for that model of IP phone.

2 When the firmware upgrade is indicated on the options menu, press the key **Upgrade**.



3 Press the key next to *Yes* to begin the upgrade.

During the upgrade, the softkey icons flash and the screen remains blank for about two minutes.

4 The appearance of a normal screen indicates the upgrade is completed.

Confirm the operation of the phone by logging in again and trying some of your capabilities.

5 This procedure is complete. Return to the task flow Task flow of a CICM IP phone firmware upgrade.

Editing and viewing object properties using Java Web Client

Application

Use this procedure to edit or view the properties of objects that are displayed in the IEMS topology using Java Web Client.

Prerequisites

None

Action

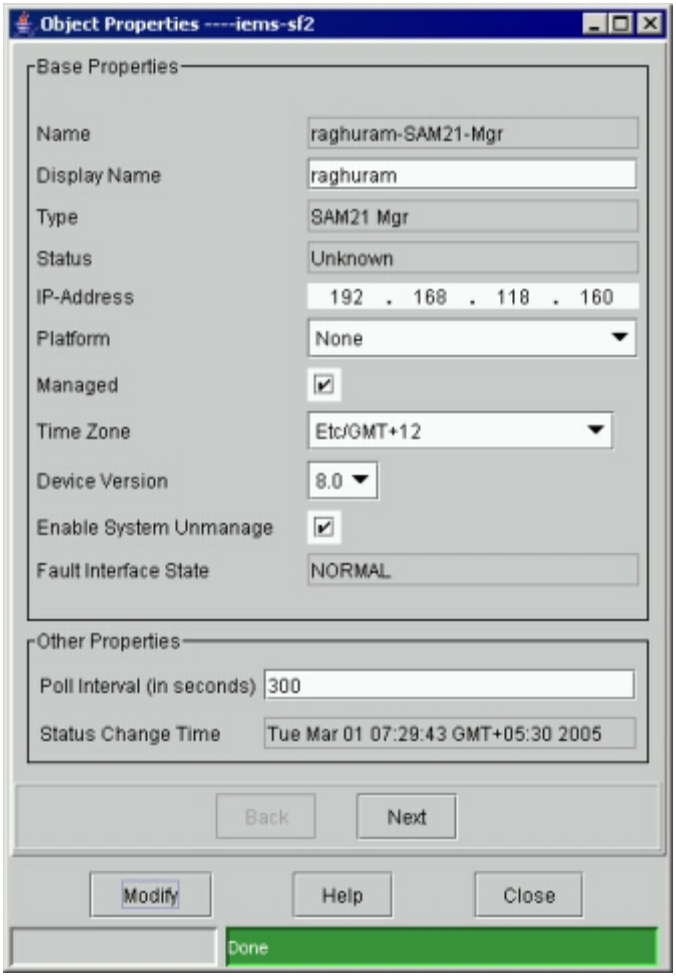
At the IEMS workstation

1. Launch the IEMS Java Web Start Client. Refer to Launching IEMS Java Web Start Client in *Integrated EMS Basics*, NN10329-111.
2. Select the required object in the Integrated EMS Topologies tree under Applications.

   Note: The properties of an object from the Inventory panel of Integrated EMS tree can also be viewed. To view the Inventory object properties, select the object in the Integrated Topologies tree under Applications to open the Inventory view. Double-click the required row in the Inventory view.
3. Right-click the map symbol and select the **Managed Object Properties** menu item or double-click the map symbol to open the Object Properties window.

   Note: The object properties displayed can differ for each component.

   A window similar to the following figure opens.



4 Modify the object properties listed in the table below if required.

Managed object properties in Java Web Client

Field	Description
Name	Displays a unique name for the object
Display Name	Edit the name displayed in the topology for the object
Type	Displays the type of object (element manager, EMS, EMS platform or NE)
Status	Displays the status of the object
IP-Address	Edit the IP address of the object

Managed object properties in Java Web Client

Field	Description
Platform	Select the platform where the object resides from the drop-down list
Managed	Indicates whether the object is managed or unmanaged
Time Zone	Select the time zone of the geographical location where the object exists from the drop-down list
Device Version	Select the device version of the managed object from the drop-down list
Enable System Unmanage	Enable or disable the System_Unmanaged state. Refer to the System_Unmanaged state section of Configuring the Message Overload Controller parameters in *Integrated EMS Fault Management*, NN10334-911.
Poll Interval	Edit the Poll Interval for status updates
Status Change Time	Displays the last status change time of the object
Note: For the following objects, only the Display Name and the Managed field can be modified. • SDM platform, APS EMS application, CS 2000 Core, Call Agent Core, IMX/CSE MX, Media Proxy, Media Gateway 7480/15000, MSS 15000	

5 Select your next step.

If	Do
you do not want to modify any other properties	go to step 6
you want to view or modify the fault interface or performance interface properties	go to step 8

6 Click the **Modify** button to update the changes.

7 Go to step 16.

8 Click the **Next** button to proceed to the Fault Interface window.

A window similar to the following figure opens.

9 Edit or view the fault interface properties of the object as required.

Note: The Details panel dynamically changes according to the fault interface of the EMS/NE.

10 Select your next step.

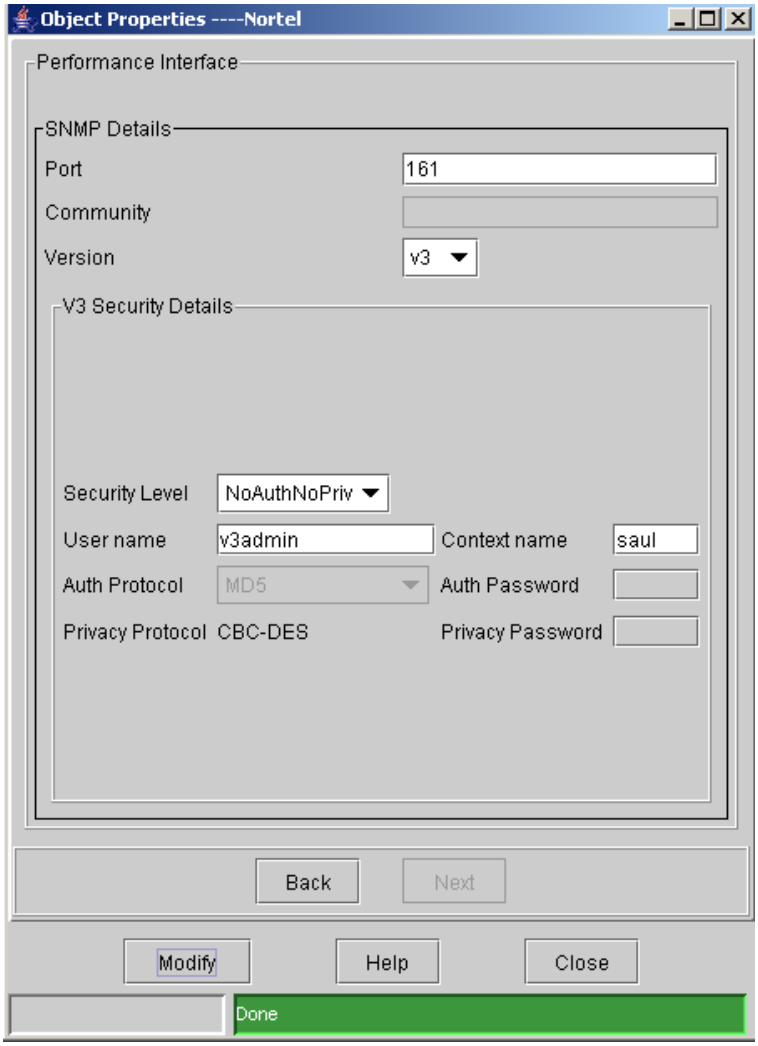
If	Do
you do not want to modify any other properties	step 11
you want to view or modify the performance interface properties	step 13

11 Click the **Modify** button to update the changes.

12 Go to step 16.

13 Click the **Next** button to proceed to the Performance Interface window.

A window similar to the following figure opens.



14 Edit or view the performance interface properties of the object as required.

15 Click the **Modify** button to update the changes.

16 You have completed this procedure.

Editing and viewing object properties using Web Client

Application

Use this procedure to modify or view the properties of an object in the IEMS topology using Web Client.

Prerequisites

None

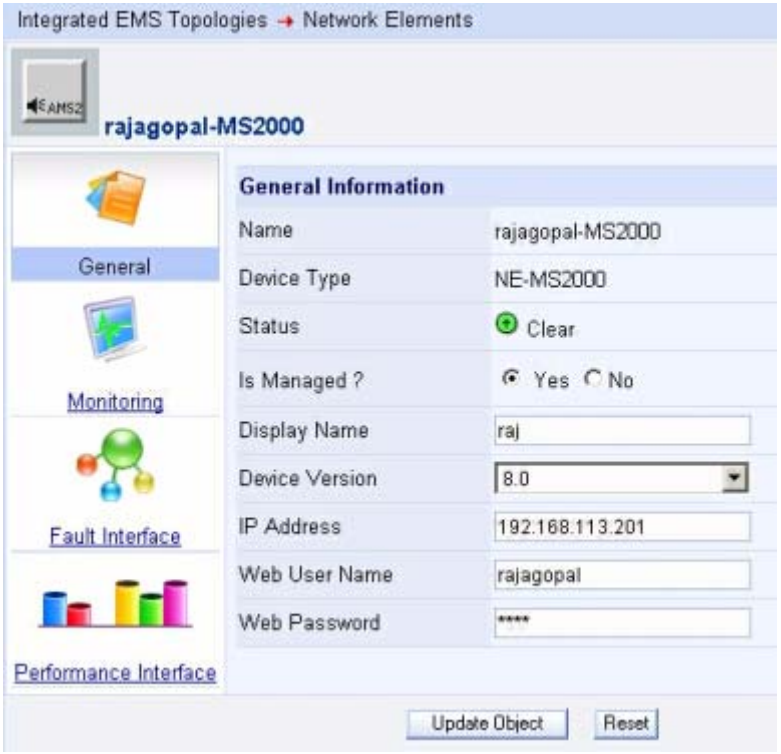
Action

At the IEMS workstation

1. Launch the IEMS Web Client. Refer to Launching the IEMS Web Client in *IEMS Basics*, NN10329-111.
2. Select the **Integrated EMS Topologies** tab.
3. Navigate to the required topology node in the Integrated EMS Topologies tree.
4. Click the map symbol label to open the **General Information** window.

   Note: The object properties displayed can differ for each component.

   A window similar to the following figure opens.



5 Select each vertical tab and modify the object properties listed in the table below if required.

Managed object properties in Web Client

Field	Description
General	
Name	Displays the unique object name of the managed object
Device Type	Displays the type of object (element manager, EMS, EMS platform or NE)
Status	Displays the status of the object
Is Managed?	Indicates whether the object is managed or unmanaged
Display Name	Displays the name or label displayed in map symbol
Device Version	Select the version of the device from the drop-down list

Managed object properties in Web Client

Field	Description
IP Address	Modify the IP address of the object
Web User name	Enter your web user name
Web Password	Enter your web password
Monitoring	
Last Status Update Time	Displays the time when the status of the managed object last changed
Last Status Change Time	Displays the time when the status of the managed object last changed
Status Polling Interval (secs)	Modify the Poll Interval for status updates

Managed object properties in Web Client

Field	Description
Fault Interface	
If the details are present for the selected object, the details can be modified.	
Performance Interface	
If the details are present for the selected object, the details can be modified.	

6 Click the **Update Object** button to update the changes.

7 You have completed this procedure.