Carrier VoIP

CICM Administration and Security

NN10252-611

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

Contents

New in this release

The following sections detail what's new in *CICM Administration and Security* for (I)SN09U.

Features

There have been no feature updates to the document in this release.

Other changes

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

- "CICM software backups" (page 33)
- "Restoring backup files" (page 24)
- "Admin and client LAN security" (page 11)

CICM Administration and Security

This document provides the administration and security tools, utilities, and procedures for Centrex IP Client Manager (CICM) nodes (gateways) and CICM Element Managers (CICM-EM). This document is part of the CICM customer documentation suite. The complete list of documents in the suite is identified in *CICM Basics* (NN10044-111).

Navigation

Administration for CICM

Administering Centrex IP Client Manager (CICM) consists of Call Server 2000 administration and CICM administration.

Navigation

Call Server 2000 administration

Call Server 2000 (CS2000) administration begins with the installation, when connection values are entered into hardware data tables. After this is done, there should be no reason to alter these values. Refer to the CS2000 documentation for additional information.

CICM administration

Administration of Centrex IP Client Manager (CICM) is done through the CICM Element Manager (CICM-EM), or from an administration PC that provides access to the CICM. CICM does not come equipped with a display or keyboard.

A CICM administration PC is attached to the service provider's administration LAN, and is used to accesses the CICM-EM through a Web interface.

Use the CICM administration interface to:

- view the status of the CentrexIP service
- start or stop the CentrexIP service
- configure the CICM and clients
- collect event logs from the CICM
- backup and restore the CICM configuration

Device administration

A CentrexIP line can be made busy (BSY), installation busy (INB) or returned to service (RTS) in the same manner as a conventional line. Refer to the Call Server 2000 documentation suite for complete procedures.

For Nortel IP Phone and m6350 SoftClient configuration and administration information, refer to *CICM document suite and related documents* in *CICM Basics* (NN10044-111).

Terminal transfers

All terminals (clients) connect to the master Centrex IP Client Manager (CICM) node, and terminal transfers are handled automatically by active call failover (ACF) for any upgrade beginning with release SN08.

When upgrading CICM node software, or rolling back to an earlier version, the terminals on the master node must be manually transferred over to the slave node. This ensures that the terminals can be returned to service when immediately followed by a switch of activity (SWACT) between the master and the slave nodes.

Terminal transfer overview

When software or hardware maintenance or upgrades are being performed on a Centrex IP Client Manager (CICM) node, the node is taken out of service. Terminals on the node to be shut down must be moved to the mate node prior to node shutdown. The mate node is still available to provide service during the node outage, although at a reduced capacity.

The terminal transfer enables the CICM node to shut down in a controlled manner, as explained here:

- The administrator selects a shutdown timeout interval (between 5 and 60 minutes, in 5 minute intervals) and initiates the terminal transfer.
- Terminals attempting to register new sessions with the CICM node will be automatically redirected to the mate node.
- Terminals with no active user login session are transferred to the mate node immediately when the terminal transfer is initiated.
- For terminals with an active user login session:
  - Users are presented with a dialog screen informing them that maintenance is being performed, and requesting permission to perform a terminal reboot.
  - Users have the choice to defer the terminal reboot. If they defer the terminal reboot, after several minutes they will again be presented with a dialog screen requesting permission to perform a terminal reboot.
  - Users that repetitively defer the terminal reboot until the end of the shutdown timeout interval will be forced out. The active call is dropped and transferred to the mate node.
  - When a terminal is transferred, the terminal loses service for a few seconds.
  - The user login session is automatically restored when connectivity is restored on the mate node.
- If all terminals have been moved to the mate node before the timeout occurs, the shutdown will complete at that time instead of waiting for the timeout expiration.

Terminal transfer—client terminals

This feature applies to all of the Nortel IP Phones, the Nortel IP Audio Conference Phone 2033, and the m6350 SoftClient clients. The transfer process differs for the IP Phones and m6350 primarily in the user interface.

For detailed information on the user interface for Nortel IP Phones and the m6350 SoftClient, refer to *CICM document suite and related documents* in *CICM Basics* (NN10044-111).

Limitations and restrictions of terminal transfers

This section provides the limitations and restrictions of transferring terminals from one Centrex IP Client Manager (CICM) node to another.

Cross-hosted call processing Cross-hosted calls that have terminals with active user sessions on the mate node and are using call processing resources on the node that is shut down, will lose active calls without notice when the node hosting the call processing resources is taken out of service.

Network addressing To move the terminal from one node to the other, use the **`UNIStim SwitchServer`** command.

When a terminal connects to CICM, CICM queries the terminal server configuration. The terminal server can be configured manually through the terminal or through DHCP. The CICM identifies which of the server entries corresponds to its own host address, which is the client LAN address on the CICM node.

The CICM then identifies the failover server. If the failover server is not configured correctly to be the mate node, the terminal transfer will fail. The terminal will eventually reconnect to the node that was taken out of service when that node is brought back into service. The CICM does not reprogram the terminal's server configuration.

Example

Failover terminal: If a terminal connected to node B has node A configured for server S0, and node B configured for server S1, then node A is the failover server.

If a static NAT bind is being used to publish private CICM client LAN addresses on a public network, CICM is unable to match its own address to either of the addresses configured on the terminal. This causes unpredictable results when transferring terminals.

Terminal server configuration Terminals with S1 and S2 configured as the same server (for example, both configured with the address of node A) are not candidates for transfer to the mate node. In this case, when a terminal transfer is being performed, a log is generated for these terminals and the terminal is left connected to the node until the node shuts down completely, at which point it loses service.

Security for CICM

The security model for the Centrex IP Client Manager (CICM) mandates two separate networks: the administration network (Admin LAN) and the client network.

Navigation

- "Admin and client LAN security" (page 11)
- "Access privileges and restrictions" (page 11)
- "IIS filter access" (page 12)

Admin and client LAN security

The administration (admin) LAN is a secure environment owned and managed by the service provider. It is used for carrying operation and administration data and does not carry call control data or media streams. No voice services are available from the admin LAN.

The client network also belongs to the telco customer. The client LAN is a nonsecure network that is not under the control and management of the service provider. It carries call control and bearer traffic.

For security purposes, the admin LAN and client LAN are physically isolated from each other within each Centrex IP Client Manager (CICM) cabinet. Routing directly between the admin and client LAN is disabled in the CICM. Only the basic services needed for call control are available from the client LAN connections to the CICM.

Because of the separation between the admin LAN and the client LAN, an administrator would have to do the following to test whether a client PC, or Nortel IP Phone, is visible on the client LAN:

- open a cicmconnect session and log on to the CICM on which the user is registered, or
- issue the **`ping`** or **`tracert`** command from the cicmconnec command line to verify the IP address of the client.

ATTENTION

Do not use the **`Ping`** and **`Tracert`** commands in cases where the CICM and its clients are separated by firewalls. The **`Ping`** and **`Tracert`** messages cannot traverse the firewall or the NAT.

Access privileges and restrictions

The following access privileges are protected by user names and/or passwords:

- access to Centrex IP Client Manager Element Manager (CICM-EM) and CICM nodes through the admin LAN
- access to the administration Web pages on the Element Manager
- login to terminals on the client LAN

To access the CICM Element Manager (EM) Web pages, a user must be a member of the Centrex IP administrators group, which is configured as part of the installation process. As a member of the administrators group, the administrator password can be used for access to the administration PC, the Element Manager Web pages, and for Telnet access.

Refer to the specific procedure in this document for instruction on how to configure up user and administrator groups.

IIS filter access

Internet Information Services (IIS) can filter access to Web services based on selected IP addresses or domain names. Having only a small set of client addresses in the filter minimizes the chance of infraction.

Read-only shared resources

The Centrex IP Client Manager Element Manager is initially configured with three shared directories, one for firmware, one for backup, and one for patching. All of these should be read-only. If directories are created for other purposes, ensure these are made writable for the minimum required period of time.

Authenticated Web access

The Web server can be configured to only permit access to authenticated NT users within the Centrex IP Client Manager (CICM) domain, or other domains where trust relationships have been established.

Secure Web access

The Web server supports secure Web access using Secure Sockets Layer (SSL) when provided with a signed Certificate. This requires the administrator to obtain a Certificate from a provider. IIS supports client certificates that are manually distributed to trusted clients and entered into the browser. SSL can be configured using the Internet Service Manager.

Firewall and NAT traversal

Firewalls and network address translation (NAT) devices are widely used by enterprises to maintain their network security and integrity.

For detailed information, see *CICM Basics* (NN10044-111).

NAT traversal

Nortel Centrex IP supports all types of NATs, full cone NAT, restricted cone NAT, port-restricted NAT, and symmetric NAT. There is no change needed on existing NAT functions or NAT devices of enterprises.

UNIStim signaling NAT traversal Centrex IP UNIStim signaling messages can traverse any type of NAT, because UNIStim messages are always initiated by Centrex IP clients from the private side of the enterprise NAT. That initial UNIStim message creates a binding on the NAT to allow UNIStim message traversal from the CICM from the public side of the NAT.

Keep NAT binding alive for UNIStim signaling Each Nortel IP Phone is configured with the IP address of its hosting CICM. When the IP Phone powers on, it sends a Resume Connection message to the CICM. A path through the NAT device is set up for UNIStim signaling.

After the initial connection is made, the IP Phone starts the Watch Dog timer. The default value of the timer is 2.5 minutes.

To keep the firewall pinhole open for the UNIStim signaling path throughout the user session, the CICM has a built-in global terminal Watch Dog timer.

Once every minute, the CICM sends a UNIStim reset watchdog message to the client IP Phone, to reset the timer on the client. The client responds with an ACK message. This ACK message goes through the firewall and resets the firewall (NAT) timer, which keeps the firewall pinhole open and the NAT binding alive.

The NAT binding (firewall) timer value can be configured. Nortel recommends a timer value of 3 minutes. As a guideline, set the Watch Dog timer a minimum of 30 seconds less than the firewall timer.

RTP media NAT traversal Two uni-directional RTP media streams are needed to set up a VoIP call. The outgoing RTP media stream from Centrex IP clients to the CICM can traverse the NAT because it is initiated from the private side of the NAT. However, the incoming RTP media stream initiated at the CICM (the public side of the NAT) and destined to the clients cannot traverse the NAT because there is no address binding established at the NAT. As a result, the call fails.

The challenge of a NAT on any VoIP application, is in how the incoming Border Control Point stream traverses the NAT.

Nortel NAT traversal solution

The Nortel network address translation (NAT) traversal solution is summarized by these following four factors

- CS2000-routed calls
- intraswitched calls behind a single NAT
- calls between two enterprises
- keeping NAT open for RTP media

UNIStim security

Centrex IP Client Manager (CICM) clients communicate with a CICM server using the Nortel proprietary UNIStim (Unified Networks IP Stimulus) protocol. The UNIStim security feature, introduced in the CICM 2.5 MR6 release, provides the infrastructure required for secure communications between the CICM server and its clients. Security configuration is available through the security function on the CICM Element Manager (CICM-EM) Web page, and allows administrators to

- manage RSA keys for the CICM-EM and its associated CICM servers
- view security policies of associated CICM servers
- view security policies of enterprises

Security configuration consists of setting the following security parameters:

- security policy—indicates if the communications between a CICM server and its clients are secure or nonsecure
- nonsecure client threshold— indicates the number of clients permitted to connect in non-secure mode to a CICM server that has a security policy of secure
- secure client threshold—indicates the number of clients permitted to connect in secure mode to a CICM server that has a security policy of nonsecure
- reset security—clears the security objects that ties clients to a particular CICM server, and therefore facilitates moving multiple secure clients (terminals) from one CICM server to another

The security parameters for CICM servers associated with an enterprise are specified as part of the enterprise's profile.

To set up secure communications between CICM servers and their clients, see "Setting security parameters at a CICM level" (page 26). To remove security objects, see"Clearing security objects" (page 19).

Tools and utilities for CICM

The Web interface is the primary user interface to the Centrex IP Client Element Manager (CICM-EM). The CS2000 Line Maintenance Manager (LMM) Interface may be used to perform administration and maintenance of the CS2000 components that relate to the CICM.

In addition to the Web interface, a number of standard administration tools, such as SNMP and WMI, can be used on the administration PC for remote management of CICM nodes.

Web interface

Centrex IP Client Manager Element Manager Element Manager (CICM-EM) Web interface is designed for use with Microsoft Internet Explorer 5.0 or higher, and uses standard Microsoft navigation techniques.

Use the Web interface to configure and monitor CICM nodes and clients Web pages that area hosted on the CICM-EM. The Web pages are password protected, and can also be accessed from a remote Web-enabled terminal.

The Web interface is made up of two basic components: a menu of commands appears on the left side of the page, and the context panel with dynamic displays and additional commands appears on the right side of the page.

The left menu is arranged upon installation, and offers full administration of the CICM. For example, configuration and status Web pages that are applicable to a particular CICM can be selected from the CICM menu.

For the Web Interface to be correctly displayed, a PC with a resolution of at least 800 x 600 pixels and a color depth of at least 256 colors should be used.

LMM interface

The Line Maintenance Manager (LMM) interface on the Communication Server 2000 (CS2000) is the primary interface between administration personnel and the CS2000. The LMM interface is used to perform administrative and maintenance tasks on the CS2000, including:

- general maintenance
- network management
- operational measurements
- service analysis
- trunk tests
- data modification
- line tests

Refer to the CS2000 documentation suite for detailed procedures on the LMM Interface.

CICM SNMP agent

Simple Network Management Protocol (SNMP) is an industry standard management interface. An SNMP agent provides a standard interface for status monitoring and fault reporting.

Centrex IP Client Manager (CICM) provides an SNMP interface for remote status monitoring. Each CICM node will send SNMP traps to a set of management systems when specific events occur.

An SNMP browser can be used to view the standard MIB-2 MIBs, and Nortel-specific CICM MIBs.

CICM WMI agent

WMI is a management interface from Microsoft, and is a standard component of the NT-embedded operating system. The WMI management system provides the capability to monitor the status of Centrex IP Client Manager nodes (CICM). The WMI Agent does not need configuration.

WMI management systems are available from companies such as Hewlett-Packard.

Administration and security procedures

Administration and security procedures are performed through the Centrex IP Client Manager Element Manager (CICM-EM) Web interface, a Telnet connection to the administration LAN, and the Microsoft desktop.

For all procedures provided in this document, it is required to use administrator user IDs and passwords to login to the EM.

Navigation

- "Accessing the CICM-EM home page" (page 17)
- "Adding a CICM node" (page 18)
- "Creating an IEMS user account" (page 21)
- "Clearing security objects" (page 19)
- "Deleting a CICM node" (page 21)
- "Editing the list of CICM nodes" (page 22)
- "Monitoring the status of a CICM node" (page 22)
- "Performing a sanity check on a CICM node" (page 24)
- "Restoring backup files" (page 24)
- "Setting security parameters at a CICM level" (page 26)
- "Setting security parameters at an enterprise level" (page 27)
- "Starting service on a CICM node" (page 28)
- "Viewing CICM-EM synchronization" (page 31)
- "Viewing information at the node level" (page 31)
- "Viewing Language profiles" (page 32)

- "Viewing terminal status" (page 32)

Accessing the CICM-EM home page

Follow this procedure to open the Centrex IP Client Manager Element Manager (CICM-EM) home page.

The Centrex IP Client Manager (CICM) home page consolidates access to all of the user administration procedures. You can access these administrative Web pages from the home page:

- CICM home
- CICM-element manager home
- Configuration—described in *CICM Configuration Management* (NN10240-511)
- Terminals—described in *CICM Configuration Management* (NN10240-511)
- Users—described in *CICM Configuration Management* (NN10240-511)
- Maintenance
- Audio Profiles—described in *CICM Configuration Management* (NN10240-511)
- Language Profiles—described in *CICM Configuration Management* (NN10240-511)
- Network Profiles—described in *CICM Configuration Management* (NN10240-511)
- User Profiles (described in *CICM Configuration Management*, NN10240-511)
- CICM upgrades (described in *Upgrading CICM* (NN10230-461)
- synchronization
- diagnostics

Prerequisites

You must have the administrator user name and password to perform this procedure.

Step	Action
	In the Internet Explorer address line
1	Type the IP address of the Element Manager, followed by **`/centrexip/`**, then press **Enter**.

Example
http://47.73.240.176/centrexip/

You are prompted to enter the user name and password appears.

2 Type your administrator user name and password, and press **Enter**.

The welcome page opens.

3 In the CICM menu, click **status** .

The CICM home page opens.

—End—

Adding a CICM node

Follow this procedure to add a Centrex IP Client Manager (CICM) node to the list of nodes on the CICM Element Manager (CICM-EM).

When a CICM server is added, it has a default security policy of nonsecure. If you want secure communications between the CICM server and its clients, see "Setting security parameters at a CICM level" (page 26).

Step	Action

From the CICM home page

1 Click **Change the list of CICMs stored on the CICM-EM**.

The CICM modification page opens.

2 Click **add new CICM**.

The CICM creation page opens.

3 In the **Name** field, type the identifier of the node.

where

`CICM name` refers to both sides of the CICM.

4 In the **node A IP address** and **node B IP address** fields, enter the IP addresses of node A and node B.

where

`nodes` are the names of each side of a CICM.

5 Click **save new CICM**.

The CICM creation page displays the progress of the action. A confirmation message appears when the process is complete.

—End—

Clearing security objects

After a client is connected to a secure Centrex IP Client Manager (CICM) server, it has a security object that associates it to that particular CICM server. To move a secure client from one CICM server to another, you must first clear the associated security object from the client. This is done through the Reset Security parameter at any one of the following three levels:

- enterprise level
- CICM server level
- client level

The following table shows the impact of setting the Reset Security parameters:

Security object parameters

Enterprise	CICM server	Client	Reset security value	Impact
No	No	No	No	No security objects are cleared from the clients.
No	No	Yes	Yes	Security objects are cleared from the specified client only.
No	Yes	No	Yes	The security objects are cleared from all the clients associated with the CICM server.
Yes	No	No	Yes	The security objects are cleared from all clients under this enterprise.
Yes	No	Yes	Yes	The security objects are cleared from all clients under this enterprise.
Yes	Yes	No	Yes	The security objects are cleared from all clients under this enterprise.
Yes	Yes	Yes	Yes	The security objects are cleared from all clients under this enterprise.

Step	Action

At the CICM-EM home page

1 From the profiles section, click **security**.

The security configuration page opens.

2 Perform one of these actions. To clear a security object at the:

- enterprise level, go to step 3.
- CICM server or client level, go to step 4.

3 Perform theses steps to clear the security object from all clients associated with CICM servers within an enterprise:

a. On the **security configuration** page, click **View security policies of enterprises on this CICM-Element Manager**

The security summary for enterprises page opens.

b. Click on an Enterprise link.

The enterprise profile page opens.

c. Open the **Enterprise Reset Security** field pick-list and select **Yes**.

d. Click **save**.

You can now move all the clients associated with each CICM server within the enterprise to other CICM servers.

To clear the security object from one or more clients associated with a CICM server

4 On the **security configuration** page, click **View security policies for CICMs**

The security summary for cicms page opens.

5 Perform one of these actions. If you want to clear the security object at the

- CICM server level, go to step 6.
- client (terminal) level, go to step 7.

6 Perform these steps to clear the security object from all clients associated with a CICM server:

a. On the security summary for cicms page, click CICM server link.

The global settings modification on cicm page opens.

b. Open the **Reset Security** field pick-list and select **Yes**.

c. Click **Save changes to the CICM**.

You can now move all the clients associated with this CICM server to another CICM server.

This procedure is complete.

The procedure to clear the security object at the CICM server level is complete.

7 To clear the security object from a client associated with a CICM server, click **View Terminal Settings** for a particular CICM server.

The terminal audit results on cicm page opens.

8 Click the **MAC address** for the client (terminal) on which you want to reset the security parameter.

*The **terminal** page for the selected CICM opens.*

a. Open the **Reset Security** field pick-list and select **Yes**.

b. Click **Save**.

—End—

Creating an IEMS user account

Step	Action

At the terminal

1 Use a Web browser to access port 9090 of the IEMS, and log on.

2 Click the **Admin** tab.

3 From the Admin pick-list, click **Add User**.

The Add User page opens.

4 On the Add User page, enter a user name and password for this account.

5 From the **Available Group Names** pcik-list, select the user authentication levels.

6 Datafill the other fields, and click **Add User**.

—End—

Deleting a CICM node

Follow this procedure to delete a Centrex IP Client Manager (CICM) node from the CICM Element Manager.

WARNING
Loss of all service
Perform this procedure under the direction of Nortel technical support only

Completing this procedure will delete a CICM node, and cause a loss of all Centrex IP service on that CICM.

Step	Action

From the CICM-EM home page

1 Click **Change the list of CICMs stored in the CICM-EM**.

The CICM modification page opens.

2 In the **Delete** column, click the trash can icon of the CICM to delete.

A status window displays the progress of the operation, and confirms the action when it is complete.

—End—

Editing the list of CICM nodes

Follow this procedure to edit the list of Centrex IP Client Manager (CICM) nodes.

Prerequisites

The nodes of a CICM correspond to the IP address of each side of the CICM. Unit 0 = Node A and Unit 1 = Node B. The CICM Element Manager (CICM-EM) uses this IP addresses to access the CICM nodes. Make sure that the addresses you enter in step 3 are correct. The CICM name is a reference only and is not used for communication with the CICM.

Step	Action

From the CICM-EM home page

1 Click **Change the list of CICMs stored in the CICM-EM**.

The cicm modification page opens.

2 From the list of CICMs, click to select the CICM to change.

The edit cicm page opens.

3 Enter the node IP address for Node A and/or Node B.

4 Click **Apply Changes**.

—End—

Monitoring the status of a CICM node

Use this procedure to monitor the status of a Centrex IP Client Manager (CICM) node.

The CICM status page emulates the alarm bar panel on the physical CICM. Alarms that appear on the physical CICM card are reported on the CICM status page within 30 seconds.

Nortel recommends that you use the CICM status page to monitor CICM nodes. Nortel also recommends that you periodically monitor the event logs of paired nodes, and the CICM Element Manager (CICM-EM). View the event logs to identify the cause of a fault, if an error occurs.

Step	Action

At the CICM-EM home page

1 Click **View the status of the CICMs**.

The cicm status page opens, showing a summary of critical, major, and minor faults.

2 To view additional details, click **view brief status of**.

The information is updated to show additional node and card status information.

3 To view the complete CICM status information, click **view complete status of**.

The information is updated to add additional VMG, node, and network information. You must scroll down in the details sub-window to view all information.

4 To view details of the chassis components, click **view status of chassis components** for each option that appears in the menu on the right.

Each time you select another component, the cicm status page updates to show the new information.

5 To view performance monitoring information about connections, terminals, or packets, perform one of these actions. From the cicm status page:

- click **Connections**
- click **Terminals**
- click **Packets**

6 Click **performance monitoring**.

*The **cicm status** page updates to display the information.*

—End—

Performing a sanity check on a CICM node

Follow this procedure to perform a sanity check on a CICM node. It results in a display of the software release version.

Step	Action
	At the CICM-EM home page
1	Click **diagnostics**. *The diagnostics home page opens.*
2	From **sanity check on a CICM** field pick-list, select the CICM. *The verify CICM page appears, with the results of the sanity check.*

—End—

Restoring backup files

There is no restriction on the time at which backups can be executed; they can be done on a regular schedule or on demand. Be aware of these restrictions when you restore a backup file.

- Backup files can only be restored to Centrex IP Client Manager (CICM) nodes that are running the same version of the software as that of the backup files.
- Restoration of backup files should be done only when
  - — there is an accidental loss or deletion of portions of the MIB, on a pair of fully configured CICM nodes
  - — there is a fresh re-image of both CICM nodes, after having fully run preboot on one node

The restore functionality is not supported and Nortel does not recommend restoring backup files when these conditions apply:

- across software upgrades within the same product release (for example, 8.11 to 8.12)
- software upgrades across two different product releases, for example, from release SN08 to SN09

A version check is built into the restore facility, to prevent accidentally restoring a backup file that falls outside the scope intended by this feature; specifically restoring a file that does not match the current software.

This functionality does not provide direct support for automated restores of CICM backups. This means that, in order to apply any previously saved configuration, the operator must connect directly to both the Centrex IP

Client Manager Element Manager (CICM-EM) and the Centrex IP Client Manager (CICM), because the CICM-EM does not include a restore interface.

To restore a backup file: locate the applicable XML file on the CICM-EM. If necessary, decompress the file (compressed files have a .gz extension). Transfer the .xml file to the correct node of the system you want to restore. From the target node, copy the file from the CICM-EM using the (secure) FTP application. Use the restore tool to apply the backup file.

1. Decompress the file.
   - To decompress a file on a Windows system, use Winzip or a similar utility to unzip the file.
   - To decompress a compressed backup file on a UNIX system type

     `gzip -d backupconfig_01.xml.gz backupconfig_01.xml`
   - To decompress a file on a CICM-EM, type

     `cxipgzip decompress backupconfig_01.xml.gz backupconfig_01.xml`
2. From the CICM-EM, use the cicmconnect tool to open a Telnet session with the CICM.
3. Pull the .xml file from the CICM-EM to the CICM, using psftp.
4. Restore the MIB using one of these commands:

   `cxiprestore <xml_backup_file> /norestart`

   or

   `cxiprestore <xml_backup_file> /restart`

   where
   `<xml_backup_file>` is the full pathname of the backup file to use to restore the node
   `/norestart` is specified to restore on fully configured CICM nodes,
   `/restart` is used for freshly re-imaged CICM nodes, following completion of preboot.

When the ***/restart*** option is used, the main CICM services are stopped prior to restoring the data. The services restart again when the restore operation is complete. If you do not to want to stop the service, use the***/norestart*** option, which has no impact on the services running at the time the restore is performed.

ATTENTION

For the restore procedure to succeed on newly re-imaged CICM nodes when the **/restart** option is used, the node being restored must be the only one running. This means it must be the master node of the pair, with no slave presently connected to the network or switched on. This is essential to ensure that the newly restored MIB content is not accidentally deleted by a premature synchronization with the mate node, and that it will be properly replicated across following the re-imaging of the slave node at a later stage.

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

ATTENTION

Although there are other command line options available for the **cxiprestore** tool, they are not documented here because they are not relevant to this activity. Using them should be avoided.

A version check is built into the restore facility, to prevent accidentally restoring a backup file that falls outside the scope intended by this feature; specifically restoring a file that does not match the current software.

Setting security parameters

You can set the security parameters at a Centrex IP Client Manager (CICM) server level or at an enterprise level. All CICM servers within an enterprise must have the security feature provided in the MR6 release in order for the enterprise to have its security policy set to secure. If one or more CICM servers within the enterprise do not have the security feature, then the security policy for the enterprise can only be set to nonsecure. All CICM servers within an enterprise, are either all secure or all nonsecure as the CICM servers security policy defaults to the security policy of the enterprise. All CICM servers within an enterprise share the same security parameters, which cannot be overridden on a CICM server basis.

Follow one of these procedures to set up secure communications between a CICM server and its clients:

- "Setting security parameters at a CICM level" (page 26)
- "Setting security parameters at an enterprise level" (page 27)

Setting security parameters at a CICM level

Follow this procedure to select the security policy used by the Centrex IP Client Manager (CICM) server.

Step	Action

From the security configuration page

1 Click **View security policies for CICMs**.

The security summary for cicms page opens.

2 Click to select a CICM server link.

The global settings modification page opens.

3 From the **Default Security Policy** field pick-list, select **Secure**.

You can only set the Default Security Policy parameter to Secure if the CICM server has an RSA key. If the CICM server does not have an RSA key, you are prompted to generate one.

If the CICM server is within an enterprise, the enterprise security policy takes precedence.

4 From the **Nonsecure Client Threshold** pick-list, select the number of clients permitted to connect in a non-secure fashion to this secure CICM server.

If you do not want to allow any clients to connect to the secure CICM server in non-secure mode, set the Nonsecure Client Threshold value to 0 (zero).

5 Click **Save changes to the CICM**.

After the security parameters are set, the CICM server propagates the RSA key to its clients and transitions the clients to secure mode. This involves a hard reset.

The first time the CICM server propagates the RSA key to its clients, it will be done in the clear without encryption. The clients only allow a one-time push of the RSA key in the clear. All other RSA key pushes are ignored unless the push is done over a secure connection.

—End—

Setting security parameters at an enterprise level

Follow this procedure to select the set security parameters used by the enterprise associated with the Centrex IP Client Manager (CICM) server.

Step	Action

From the security configuration page

1 Click **View security policies of enterprises on this CICM-Element Manager**.

The security summary for enterprises page opens.

2 Click to select an Enterprise link.

The enterprise profile cicm-em page opens.

3 To set the security parameter for the enterprise to secure, from the **Enterprise Security Policy** field pick-list, select **Secure**.

You can set the Enterprise Security Policy parameter to Secure only if all the CICM servers within the enterprise support the security feature provided in the MR6 release.

4 From the **Enterprise Nonsecure Client Threshold** field pick-list, select the number of clients permitted to make a non-secure connection to a secure CICM server, within this secure enterprise.

If you do not want any clients to make a non-secure connection to a secure CICM server, set the Nonsecure Client Threshold value to 0 (zero).

5 Click **save**.

6 Click **apply enterprise profile to all associated CICMs**.

The security parameters are propagated to all the CICM servers associated with the enterprise, and in turn the CICM servers propagate the RSA key to their clients and transition the clients to secure mode, which involves a hard reset.

The value displayed in the Profile up to date on Associated CICMs field changes from No to Yes. This indicates that all CICM servers within the enterprise are using the latest settings in the enterprise profile.

—End—

Starting service on a CICM node

Follow these procedures to start a Centrex IP Client Manager (CICM) service in order to minimize service outage.

CAUTION
Loss of service
Perform this procedure under the direction of Nortel technical support only

Pressing the Restart button can result in loss of service if a terminal transfer is not performed prior to this procedure.

Step	Action

At the CICM-EM home page

1 From the CICM menu, click **status**.

The cicm home page opens.

2 From the **view the status of the following CICM** pick-list, select the CICM.

3 Click on **view the status of the following CICM**.

The cicm status page opens.

4 Click **perform maintenance on cicm**.

The maintenance status page opens.

5 From the **Node A Service Control** or **Node B Service Control** pick-list, click **Restart**.

You are prompted to confirm the action.

6 Select **Yes** to confirm restart.

The CICM resets and attempts to start the service on the node.

The Status field updates to display the current service state. Possible states have this syntax x (y) where:

x
is one of the following:

- master
- master (no slave)
- slave
- slave (no master - isolated)
- swact complete
- swacting master -> slave
- swacting slave -> master
- unavailable

y
is one of the following:

- running
- start pending
- stop pending

- stopped
- unknown state

The node is in the "Start Pending" state while the hardware is being initialized.

7 Monitor the node service status from the maintenance status page.

When the service state changes to running the service has been restored.

8 Repeat this procedure to start the second node.

9 If the service fails to start, refer to the CS2000 documentation *Remote Line concentrating Module Maintenance Guide*, to restore service to the CICM node.

—End—

Stopping service on a CICM node

Follow this procedure to stop the call service on a Centrex IP Client Manager (CICM) and avoid raising alarms.

Stopping service on a Centrex IP Client Manager (CICM) node may be necessary when upgrading or during routine maintenance such as changing cables. When the service is stopped, CICM terminals cannot log on to the server and call processing is interrupted.

CAUTION
Loss of service
Perform this procedure under the direction of Nortel technical support only

Do not perform this procedure on a master node. Perform this procedure on a slave node only.

Stopping the CICM service raises alarms. To prevent these alarms, take the CICM offline at the CS2000 before powering down the CICM. Refer to the documentation *Remote Line Concentrating Module Maintenance Guide*.

Step Action

From the CICM-EM home page

1 From the CICM menu, click **status**.

The cicm home page opens.

2 Select the CICM to view from the drop-down list and click **view the status of the following CICM**.

The page cicm status opens.

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

The maintenance status page opens.

4 Click **node A service control** or **node B service control**.

Stop should be displayed on the pick-list. If the node is running, Restart appears.

5 Click either **node A service control** or **node B service control**.

The node begins the shutdown process. The result of the action is displayed.

On the maintenance status page, the Status field the node selected displays stop pending. The node remains in this state while the hardware is shutting down.

6 Monitor the node service state from the **maintenance status** page.

The service has correctly been shut down when the status changes from stop pending to stopped.

7 Repeat this procedure to stop the mate node.

—End—

Viewing CICM-EM synchronization

Follow this procedure to view and check the synchronization between the primary and backup Centrex IP Client Manager Element Managers (CICM-EM).

Step	Action

From the CICM-EM home page

1 From the CICM-EM menu, select **synchronization**.

The cicm - element manager synchronization page opens.

—End—

Viewing information at the node level

Follow this procedure to view node-level statistics.

The Web interface can be used to collect statistics about the number of calls that are handled by the Centrex IP International Gateway. These statistics are collected and displayed per node.

Step	Action
	From CICM-EM home page
1	From the **CICM** menu, click **status**. *The cicm home page opens.*
2	From the **view the status of the following CICM** pick-list, select the CICM to be view.
3	Click **view the status of the following CICM**. *The cicm status page opens.*
4	Click **perform maintenance on cicm**. *The maintenance status cicm page opens.*

—End—

Viewing Language profiles

Follow this procedure to view the language profiles available to a Centrex IP Client Manager (CICM) node.

Step	Action
	From the CICM-EM home page
1	From the profiles menu, select **language**. *The language profile home page opens.*
2	Select the CICM from the pick-list and click **view the profiles stored on the following CICM**. *The language profiles modification page opens, showing the list of available language profiles.*

—End—

Viewing terminal status

Follow this procedure to view the status of a Centrex IP Client Manager (CICM) terminal.

Step	Action
	From the CICM-EM home page
1	Click **terminals**. *The terminal configuration page opens.*
2	Select the CICM from the pick-list of and click **go to terminal configuration on CICM**. *The terminals on cicm page opens.*
3	Click **terminal audit**. *The terminal audit on cicm page opens.*
4	Select the terminal details to display by checking the appropriate check box.
5	Click **display results**. *The terminal audit results on cicm page opens.*
6	To view terminal values, networking information, and terminal defaults for a specific terminal, click **MAC Address**. *The terminal page opens.*

—End—

CICM software backups

Follow these procedures to back up a Centrex IP Client Manager Element Manager (CICM-EM) prior to an upgrade or maintenance activity.

Backing up the software on a CICM-EM and CICM nodes is a contingency plan to allow you restore a software image. Applying the backup files to a pair of CICM nodes or a pair of CICM-EMs restores the former software configuration.

Creating backup files can be done at any time, manually or automatically. The application that does a CICM node backup resides on the CICM and is controlled by a scheduler through the CICM-EM.

For either backup method, the result is a compressed *.gz file that, after issuing a restore command, contain either the file name *backupconfig_<day_number>_em.xml* for a CICM-EM, or *backupconfig_<day_number>.xml* for a CICM.

Navigation

- "Backup overview" (page 34)

Backup overview

Backup files contain the Centrex IP Client Manager Element Manager software and configuration information. The backup procedure stores all elements of the MIB registry that are static data and that are directly relevant to the configuration of the CICM-EM or CICM node. Transient data is not stored because it is not essential. 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 endpoint equipment, including the global profile overrides stored on the CICM
- scheduled tasks
- the UNIStim security setup

Where backup files are stored

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.

Backup files are stored with a file name that conforms to one these formats:

- For a CICM-EM—*backupconfig_<day_number>_em.xml*
- For a CICM node—*backupconfig_<day_number>.xml*

On even numbered days of the month, the backup files from the paired CICM nodes pairs and paired CICM-EMs, are sent to one CICM-EM while on odd numbered days the files are sent to the other. The files are sent through anonymous FTP and stored in this node-specific folder on the D drive of the personal computer (PC) with CICM software:

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

where

day_number
is from the current month
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 run, the node-specific folder is automatically created.

The CICM-EM has a limited amount of storage space for the backup files. You are responsible for moving or copying the backup files from the CICM-EM folders to a different and safer storage location, if you do not want the backup file overwritten.

When to restore a backup file

Use the backup files to restore the software image to both nodes of a Centrex IP Client Manager Element Manager (CICM-EM) pair or CICM node. Be sure to follow these rules when restoring a backup file.

- Each file is dedicated to a particular node and must be used only on that node.
- The software version on a backup file must match the version that was most recently running on the node, for example, 8.10.xxx. Accidental restoration by an invalid backup file is prevented by the system.
- See the procedure *Restoring the CICM node registries* is in *Restoring the software configuration of a CICM-EM or a CICM node CICM Fault Management* (NN10233-911) before you attempt to restore a backup file.

Automatic backups

Automatic backup files for the Centrex IP Client Manager Element Manager (CICM-EM) and node pair occurs daily, according to a user-defined time. The default time is for 2:00 AM. The backup schedule is set during the initial configuration of the CICM.

To suspend the automatic backup schedule, open a Telnet session with the CICM-EM and enter this command:

```
cxiptaskserver /task delete schedulebackup
```

To restore the automatic backup schedule, enter this command:

```
preboot time /interactive
```

The previously scheduled time is re-enabled even if you accept the default time.

Changes to the date, time, or both on the CICM node, CICM-EM, or Microsoft Windows of the PC, can affect when the next automatic backup is run. For example, the next backup might inadvertently be skipped or a backup that has already occurred is not repeated. After release 8.10.MR2, manual changes to the date or time take immediate effect. Otherwise you need to enter the commands **`cxiptaskserver`** and **`preboot`** consecutively.

Manual backups

Manual, or on-demand backup files, are done through Centrex IP Client Manager Element Manager (CICM-EM) master or slave node Web pages. Both nodes of a CICM node pair or CICM-EM pair must be backed up. A backup file can only be restored to the node from which is was derived.

On-demand backups can be done independently from, or in addition to the automatic daily backups. Taking a backup file does not affect the active services of a node. Changing the date, time, or both for a CICM node does not affect the on-demand creation of a backup.

Backing up the CICM nodes

Follow this procedure to create a backup file for each node of a redundant Centrex IP Client Manager (CICM) pair.

Prerequisites

- Read and understand the information in "CICM software backups" (page 33).
- Run the backup procedure on each node of a CICM pair. The backup file can only be applied to the node it was taken from.
- Each backup file name must remain the same as the copied file.
- The backup files must be used only with the identical software release that they were created from.
- The duration of a backup procedure varies according to the amount of datafill configured on the CICM node. The backup 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.

Step	Action

From the PC desktop with remote access to the CICM-EM

1 Access the CICM-EM of the CICM node to back by entering:

```
https://<unique_admin_ip_address_of_cicmem>/centrexip
```

From any CICM-EM Web page

2 From the CICM menu, click **status**.

3 From the pick-list, select the CICM to backup and click **run the backup on the following CICM**.

4 From the **run the backup on the following CICM** pick-list, select CICM node A or node B.

5 Click **run backup on which node of cicm-nnn**, where nnn is the node you selected in step 4.

6 Wait for the back up message to appear, which indicates the backup was successful:

Example
The backup of the configuration for <cicm-nnn_IP_addr> completed successfully.

7 Copy the backup file called *backupconfig_<day_number>.xml* from the CICM-EM folder called *D:\\CentrexIP\\support\\backups\\<cicm-nnn>* to a storage location, such as 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. Make sure that the copied backup has the same name as the original file.

8 Repeat steps 2 through 7 for the mate node.

9 If you were sent to this procedure from another procedure, return to that procedure.

—End—

Viewing the backup record

Follow this procedure to view the record of backup execution times, for a Centrex IP Client Manager (CICM).

Step	Action
	From the CICM-EM home page
1	From the **show the backup sets available for** pick-list, select the CICM name
2	Click **show the backup sets available for**. *The backup sets on cicm page opens, showing a table of backup sets for the CICM.*
	—End—

Backing up the CICM-EMs

Follow this procedure to back up each node of a redundant Centrex IP Client Manager Element Manager (CICM-EM) pair to prepare for restoring a former software configuration when you want a more recent snapshot than the scheduled backup file.

Prerequisites

- Read and understand the information in "CICM software backups" (page 33).
- Back up each node of a CICM-EM pair. The backup file can only be applied to the node it was taken from.
- The backup file name must remain the same as the copied file. Manually created backup files have follow this format: *EMDUMP_CICMEM-<node>_<day_number>.xml*. Automatically created backup files follow this format: *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 backup file instead of the manual backup file.
- The duration of backing up varies according to the CICM-EM configuration and your access to the CICM-EM. The backup application runs at a low level of software priority to minimize the impact on the CICM-EM.
- Backup files for CICM-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.

Step	Action

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

1 Access the CICM-EM to back up by entering:

```
https://<unique_admin_ip_address_of_cicmem>/centrexip
```

At any CICM-EM Web page

2 From the CICM menu, click **status**.

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

4 From the response, make a note of

- the folder path that appears in the **Creating file** field.
- the name that appears in the **Creating secondary file** field.

See "Example of the cicm-em backup page" (page 40) for details.

5 Wait for the back up message to appear, which indicates the backup was successful:

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

6 Copy the backup file (on-demand or automatically created) 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, sudh as 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.

Make sure that the copied backup file has the same name as the original.

7 Access the CICM-EM mate node by entering this in the Web browser address field:

Example

```
https://<unique_admin_ip_address_of_mate_cicem>
/centrexip
```

where

unique-admin-ip-address-of-mate-cicm-em is the IP address of the CICM-EM mate.

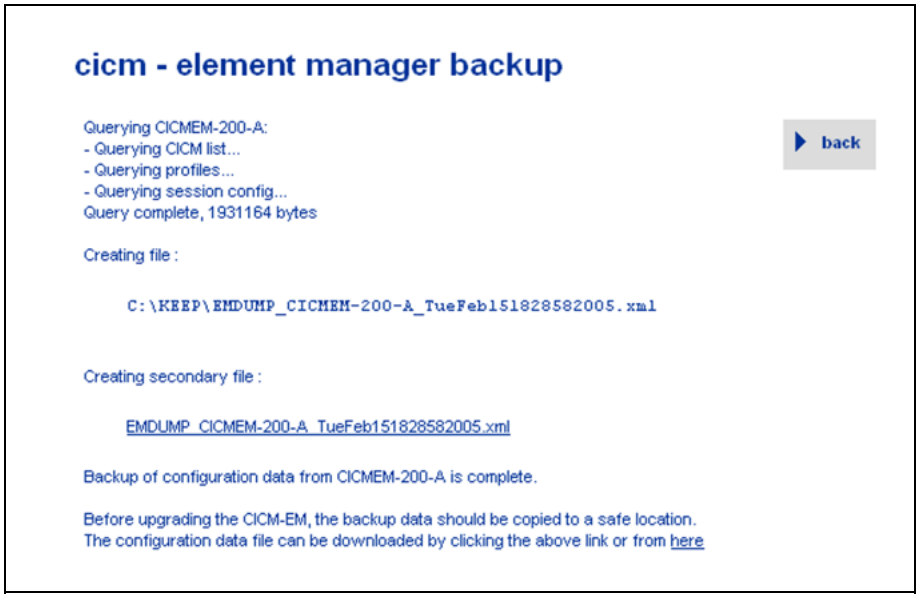
8 Repeat steps 2 through 6 for the mate node.

9 If you were sent to this procedure from another procedure, return to that procedure.

—End—

Procedure job aid

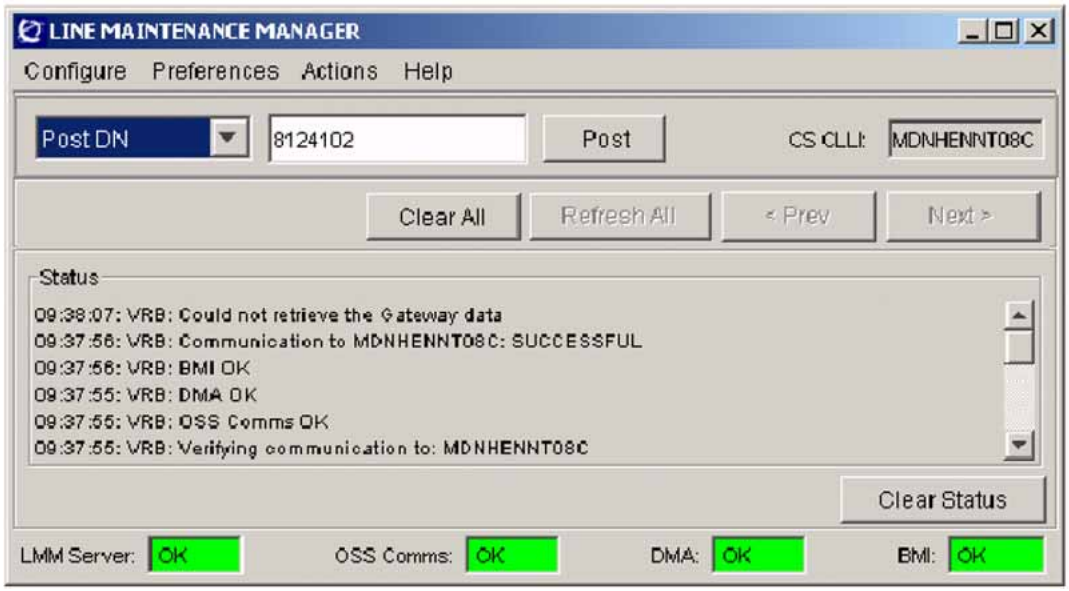
Example of the cicm-em backup page



Line Maintenance Manager

The Line Maintenance Manager (LMM) is a graphical user interface provided by the CS2000 Management Server to replace/emulate the function provided by the MAPCI tool on the CS2000 Core.

Example: Line Maintenance Manager



The LMM provides for the following commands:

- BSY
- RTS
- FRLS
- INB

The LMM also provides the functionality to post a gateway in addition to individual lines.

Downloading firmware to the CICM Element Manager

Follow this procedure to copy a new firmware load onto the CICM Element Manager (CICM-EM). To upgrade to a new CICM release, see *Upgrading CICM* (NN10230-461).

Nortel may occasionally find it necessary to issue a new firmware load for a CICM release to correct a minor problem. In this circumstance, follow this procedure to download the firmware to the CICM-EM.

- This procedure assumes that you are using an FTP client to copy the firmware from the PC that downloaded it, to the CICM-EM.
- In this procedure, the firmware is downloaded from the Nortel site to a folder on the C drive, called firmware.

Step	Action

Copying the firmware file from the Nortel Web site

1 Go to www.nortel.com and perform these steps to download the firmware for the specific terminal type, such as IP Phone 1140E.

a. From the home page, select **Support and Training** > **Technical Support** > **Software Downloads**.

b. From the Technical Support page, click the **Browse product support** tab.

c. In field **1**, open the pick-list and click **Products A-Z** and then click **I** in the list box.

d. In field **2 ...choose a product...**, scroll down the list and click to select the IP Phone, for example IP Phone 1140E.

e. In field **3 ... and get the content...**, click **Software**.

f. Click **Go**.

The Software tab appears.

g. Click to select the firmware.

h. When prompted, log in to the site.

i. From the software page, click the file to download.

j. When the File Download dialog opens, click **Save**.

k. Browse the PC to select a location to which to save the file.

l. Create a new folder at this location, for the file.

m. Click **Save**.

The file is downloaded.

n. Unzip to extract the product bulletin and the binary file.

o. Read the product bulletin.

Downloading the firmware file to the CICM-EM

2 On the PC Desktop, click **Start** > **Run**.

The Run dialog appears.

3 In the **Open** field, type **cmd**.

The Microsoft cmd.exe application is launched.

4 On the command line, type the command to access the CICM-EM.

Example

```
C:\firmware>ftp <cicm-em ip address>
```

5 When prompted, enter the administrator user name and password.

6 Use the **cd** command to change to the CICM-EM firmware directory.

Example

```
ftp> cd firmware
```

Sample output

```
250 CWD command successful.
```

7 Use the **dir** command to verify the name of the directory to which to download the firmware.

Example

```
ftp> dir
```

Sample output

```
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
02-16-06 09:55PM <DIR>  i1110
02-16-06 09:56PM <DIR> i1120e
02-16-06 09:56PM <DIR> i1140e
02-16-06 09:56PM <DIR> i2007
```

```
02-21-06 04:33PM <DIR> i2033
02-16-06 09:55PM <DIR> i221x
02-16-06 09:56PM <DIR> m6350
02-16-06 09:56PM <DIR> phase1
02-16-06 09:56PM <DIR> phase2
226 Transfer complete.
ftp:  418 bytes received in 0.00Seconds 418000.00Kby
tes/sec.
```

8 Use the **cd** command to change to the directory to which to download the firmware.

Example

```
ftp> cd i1140e
```

Sample output

```
250 CWD command successful.
```

9 Use the **dir** command to view the contents of the directory.

Example

```
ftp> dir
```

Sample output

```
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
12-06-05 09:39AM 2371136 IP_Phone_1140e_Rel_2_1A.bin
226 Transfer complete.
ftp:  136 bytes received in 0.00Seconds 136000.00Kby
tes/sec.
```

10 Use the **bin** command to force the system to download the file as a binary file and not ASCII.

Example

```
ftp> bin
```

Sample output

```
200 Type set to I.
```

11 Use the **put** command to copy the firmware to the directory on the CICM-EM.

Example

```
put 0625C1C.bin
```

Sample output

```
200 PORT command successful.
150 Opening BINARY mode data connection for
0625C1C.bin.
226 Transfer complete.
```

```
ftp:  2233462 bytes sent in 0.28Seconds 7976.65Kby
tes/sec.
```

12 Use the **dir** command to view the results of the file transfer.

Example

```
ftp> dir
```

Sample output

```
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
02-28-06 10:22AM 2233462 0625C1C.bin
12-06-05 09:39AM 2371136 IP_Phone_1140e_Rel_2_1A.bin
01-26-06 07:09AM 2373206 IP_Phone_1140e_Rel_2_1B.bin
226 Transfer complete.
```

Overriding the current firmware load on the CICM-EM

13 Log onto the Element Manager of the CICM to which to download the firmware.

14 From the CICM menu, click **terminals**.

The terminal page opens.

15 Open the firmware update pick-list and select the terminal type.

The ip phone terminal firmware configuration page opens.

16 From the **Recommended firmware load name** field, open the pick-list and select the file you downloaded in step 11.

17 Click to check the **Overwrite** check box.

18 Perform these steps to ensure that the minimum and maximum firmware levels reflect the level of firmware that you want downloaded to the IP Phones.

a. Change the value of the **Recommended supported firmware level** field to that of the new firmware, for example 2.1C.

b. If you downloaded this firmware to solve a problem, change the value of the **Min Supported firmware level** field to that of the new firmware. Replace 2.1A with 2.1C for example.

The next time users log in to their IP Phones, they are notified that a firmware upgrade is available.

19 Click **Apply changes**.

A Please wait message appears. The clock shows the progress of the firmware as it is pushed from the EM to both CICM nodes.

A box appears, showing the results and confirming the successful completion of the actions.

—End—

Carrier VoIP

CICM Administration and Security

Publication: NN10252-611
Document status: Standard
Document version: 06.04
Document date: 20 October 2006

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

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