Carrier VoIP

CICM Configuration Management

NN10240-511

Document status: Standard
Document version: 07.02
Document date: 20 October 2006

Contents

New in this release

The following sections detail what's new in CICM Configuration Management (NN10240-511) for release (I)SN09U.

Features

There have been no updates to the document for this release.

Other changes

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

- A new chapter was added "Terminal configuration sanity test" (page 67), with these new procedures
  - "Verifying terminal configuration " (page 67)
  - "Manually transferring terminals" (page 69)
- The procedure formerly called Associating, disassociating, and applying Enterprise and Network profiles, was split into four individual procedures.
  - "Associating a CICM with an Enterprise profile" (page 24)
  - "Associating a Network profile with an Enterprise profile" (page 25)
  - "Disassociating a CICM from an Enterprise profile" (page 29)
  - "Disassociating a Network profile from an Enterprise profile" (page 29)

Overview

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

Navigation

- "New in this release" (page 5)
- "Configuration management strategy" (page 7)
- "Configuration data" (page 8)
- "Configuration management procedures" (page 8)

Configuration management strategy

The Centrex IP Client Manager Element Manager (CICM-EM) and its CICMs are configured during the initial installation by Nortel system installers.

After initial system configuration, the configuration may be changed or additional configuration completed by the service provider.

All configuration is performed directly on the CICM-EM or CICM using the preboot tool. The other configuration procedures are included in this document. The command button to access the former Configuration Wizard still appears in the menu, but has no capabilities.

These CICM-EM Web page menus are used to configure a CICM and its clients.

- profiles
  - Audio
  - Enterprise
  - Network
  - Language

  - User
  - Feature
  - Security
  - Terminal Gain

- users
- client terminals

Configuration data

Configuration data, such as IP addresses and the maximum number of concurrent sessions, resides within the Windows NT system registry. Element managers can be configured to periodically back up the configuration data of all Centrex IP Client Manager (CICM) Element Mangers (CICM-EM) and CICMs. The operating company may use standard tools to ensure that this critical configuration data is archived externally to the CICM or CICM-EM.

Previously backed up configuration data can be restored to the Windows NT registry in the event of data loss or data corruption. Service can then be resumed on a replacement or repaired system with minimal loss of service.

Configuration management procedures

This section contains links to procedures you perform to configure the Centrex IP Client Manager (CICM) Element Manager (EM) .

Nortel CICM products are configured during initial installation by Nortel system installers. Using the OSSGate tool ensures that the gateway, the Succession element, and CS2000 Management Tool server have synchronized the configuration data. Refer to the *OSSGate User's Guide* (NE10004512).

After installation, the service provider must use the tool OSSGate to:

- create users or batch create users
- batch change the configuration of users
- configure users
- delete a user

Navigation

ATTENTION

All of the procedures contained in this document require you to log on to the CICM-EM using the administrator user ID and password.

Configuring PAM on the CICM-EMs

Follow this procedure to configure a pluggable authentication module (PAM) on redundant Centrex IP Client Manager (CICM) Element Managers (EM). This will enable centralized security of the CICM-EMs and their subtending CICM pairs, through an integrated element management system (IEMS).

Prerequisites

- The IEMS must be running and it must have a have a certificate before you can deploy it on either of the CICM-EMs in the pair.
- You must have a working knowledge of UNIX.
- PAM must not be configured on either CICM.

Step	Action

From the CICM-EM

1 Open a Telnet session with the PAM server and gain root access.

2 Enter this command to go to the directory where the keystore file is located:

```
cd /opt/jakarta/dist/tomcat/conf
```

3 To format the certificate before you import it, enter this command:

```
keytool -export -v -alias sesmkey -file sesmkey.cer
-keystore ./keystore
```

4 When prompted for the keytool password, enter:

```
sesmkey
```

5 Transfer the newly-created certificate to the CICM-EM.

6 Telnet or connect to CICM-EM node A and open the command line interface (CLI).

7 On the command line, enter:

```
preboot pamauth /interactive
```

System prompt

```
Will this Element Manager use the PAM on the SSPFS
to authenticate users?  [T/N, default=N]
```

8 Enter **Y**.

System prompt

```
Will this EM connect the PAM server via HTTPS? [Y/N,
default=N]]
```

9 Enter **Y**.

You are prompted to enter the IP address of the PAM server.

10 Enter the IP address of the SSPFS PAM server.

You are prompted to enter the fully qualified domain name (FQDN) of the PAM server.

11 Enter the FQDN of the SSPFS PAM server.

Example

pamserver.nortel.com

System response

```
Do you want to import a certificate?  [Y/N, default
= N]
A Security Certificate is required for communicating
via HTTPS to the PAM server.  If you are using a
certificate purchased from valid signing authority
(e.g.  Verisign, Thawte, etc.)  then answer N
to the following prompt as the certificate will
be automatically trusted.  If you are using a
self-signed or unsigned certificate then answer Y to
following prompt, as it is required to import this
type of certificate.
Do you want to import a certificate?  [Y|N,
default=N] :
```

12 Enter **Y** to import the certificate.

You are prompted to enter the filename of the certificate to import.

13 Enter the fully qualified domain name of the certificate to use to validate the PAM server:

Example

d:\data\cablab.cer

Sample system response

```
d:\data\cablab.cer
Connection to PAM through HTTPS
Primary SSPFS PAM Proxy FQDN:
```

```
ucars0033c.ca.nortel.com
Primary SSPFS PAM Proxy IP Address:
47.135.42.226
Security Certificate
Is this correct?  [Y/N, default=Y]
```

14 Enter **Y** to save.

You are prompted to confirm the command summary, for example:

```
You have entered the name of the primary SSPFS
PAM proxy as:  47.135.42.226 Is this correct?
[Y/N, default=Y]]:
```

15 Perform one of these actions:

- Enter **Y** to confirm the input.
- Enter **N** to make a correction, then **enter Y** when it is correct.

16 For authentication to take effect, you must stop and start the PAM service. At the command line enter these commands:

```
net stop pamauthservice
```

```
net start pamautheservice
```

17 Beginning with step 5, repeat this procedure for node B the redundant pair.

18 Test PAM by logging on to the CICM-EM, by using the **central database** user name and password as well as **.administrator**.

—End—

Configuring the Apache proxy server for the CICM-EM

Follow this procedure to configure an Apache proxy server for redundant Centrex IP Client Manager (CICM) nodes.

As a proxy server, the integrated element management system (IEMS) on a Succession Server Platform Foundation Software-based (SSPFS) server can provide secure access to either node of a CICM-EM redundant pair. Use the procedure to configure the proxy (HTTPS connection) between the IEMS and the CICM-EMs.

A maximum of six IP addresses can be configured on the HTTPS proxy server. The maximum number includes CICMs and any other components in the network.

Prerequisites

- You must have the floating HTTPS IP address of the master and slave CICM-EMs.
- You must have the root user ID and password to access the IEMS.

Step	Action

From the PC to access IEMS server

1 Enter this command to open a Telnet session and log on to the IEMS server:

```
telnet <ip_address_server>
```

where

<ip_address_server> is the IP address or host name of the SSPFS-based server on which the proxy is being configured.

2 When prompted, enter your user ID and password.

3 Enter this command to change the root user:

```
su - root
```

4 When prompted, enter the root password.

From the IEMS server on which you are configuring the proxy connection

5 Enter this command to start the command line interface.

```
cli
```

6 At the prompt, enter the number to select **Configuration**.

7 At the prompt, enter the number to select **Apache Proxy Configuration**.

8 At the prompt, enter the number to select **add_proxy_conf**.

You are prompted for the proxy IP address.

9 Enter the floating HTTPS address of the master CICM-EM.

You are prompted for the associated hostname/tag.

10 Enter the same floating HTTPS address for the CICM-EM.

The next prompt is optional.

11 Press enter to omit the entry.

You are prompted for the port number.

12 Enter the IEMS IP port number **443** for the public side of the IEMS.

13 Enter **Y** (yes) to accept the values and continue.

System response

```
Stopping group using servstop
Apache Web Service Stopping
WEBSERVER Stopped
Starting WEBSERVER through servstart
Found valid security certificate, starting
Web Services with SSL support...
Apache Web Service Starting
WEBSERVER Started
=== add_proxy_conf completed successfully
```

14 Repeat steps 8 through 13, for the second CICM-EM of the redundant pair.

15 Exit each menu level until you exit the CLI by entering:

```
x
```

—End—

Configuring Audio profiles

An audio profile specifies audio parameters for making or receiving a call. Audio profiles simplify the way in which users control the audio parameters that are used when making a call. The parameters which can be configured include voice coding type, voice activity detection and the voice packet size. These parameters are configured according to the specific network conditions that exist between the customer site and the Centrex IP Client Manager (CICM) node. Having several profiles available to users means that they can select the most appropriate profile for each call.

Examples of audio parameters are:

- voice activity detection (VAD) capability with G.729A
- packet size (that is, the number of voice frames per packet)
- quality of service (QoS) parameters to be applied to the IP packets originating from that terminal or destined for that terminal
- jitter buffer setting on the terminal

The CICM administrator can adjust the parameters in an audio profile to compensate for different types of conditions in the network. For example, a telecommuter's IP voice packets may encounter one set of network conditions when a call is placed from the home, and a different set of conditions when a call is placed from the office. In this case the telecommuter would need two different audio profiles, one for each terminal.

When an IP Phone user or the CICM administrator selects an audio profile for a terminal, the following occurs:

The CICM administrator controls the audio profiles and determines which ones are available for CICM client users to select on their terminals. When a user logs into a CICM through a specific terminal, CICM updates the items on the audio profile selection menu and applies it to that specific terminal.

- the terminal implements the parameters for all outgoing voice traffic
- the CICM implements the parameters for all voice traffic destined for that terminal

Audio profiles may be created, changed or deleted. Changes to an audio profile take effect with the next call. They may be applied to a CICM or to a terminal.

CODEC negotiation rules

In Centrex IP Client Manager (CICM), the Audio profile allows you to specify a list of one or more supported CODECs (compression/decompression algorithms). During call setup, each side of the call (an endpoint) is assigned its role. One half of the call is assigned the rule of master, the other side of the call is assigned the role of slave.

1. The gateway controller (GWC) makes a request to the slave endpoint for its list of audio capabilities.

   The list consists of CODECs, packetiztion rates, RFC2833, and so on. The request from the GWC contains its Local Connection Options (LCO), which is a list of CODECs that reflects the CODECs/order of preference in the GWC audio profile. When reporting its audio capabilities, it must report which CODECs it supports, from the CODECs list sent from the GWCs.

2. The slave sends its CODEC list to the master gateway.

   The master receives two CODEC lists. One is its gateway controllers LCO, and the second is the list from the slave gateway. The master selects a CODEC that is common to both the LCO and the slave gateway, for the call.

3. CICM always report its CODEC preferences in the order specified on the GWC. The CICM audio profile never overrides the order of preference sent from the GWC.

Navigation

- "Applying an audio profile to a CICM" (page 18)
- "Applying an audio profile to CICM users" (page 19)
- "Changing an audio profile on a CICM" (page 20)
- "Creating an audio profile on a CICM-EM" (page 21)
- "Deleting an audio profile from a CICM" (page 21)

Applying an audio profile to a CICM

Follow this procedure to apply an audio profile to a specific Centrex IP Client Manager (CICM) node.

Step	Action

From the CICM-Element Manager home page

1 From the **profiles** menu on the left, select **audio**.

The audio profile home page opens.

2 From the menu on the right, click **apply one or more profiles stored on the CICM-EM to one or more CICMs**.

The apply audio profile page opens.

3 From the **Range of Profiles** box, click a radio button to select to:

- **apply only the selected audio profile**

  or

- **apply all existing audio profiles**

4 From the **Profile Selection** box, choose the profiles to apply. Press **Shift+click** to add a range of consecutive of CICMs, or **Control+click** to select multiple, non-consecutive CICMs.

5 From the **Range of CICMs** box, click a radio button and select:

- to apply the profiles only to the selected CICM or CICMs

  or

- to apply the profiles to all CICM

6 From the **CICM Selection** box, click to select the CICMs. Press **Shift+click** to select a range of consecutive CICMs, or **Control+click** to select multiple, nonconsecutive CICMs.

7 Click **apply profile(s)**.

A status page opens when the process is complete, and shows the result of the action.

—End—

Applying an audio profile to CICM users

Follow this procedure to apply an audio profile to Centrex IP Client Manager (CICM) users.

Step	Action

From the CICM-Element Manager users home page

1 From the **browse users on** field, open the **CICM** pick-list select the user's node.

2 Click the **browse users on** text.

The section expands, showing the VMG and user ranges.

3 Select the applicable user range.

4 Click **browse users on** again.

A page opens showing a list of CICM users.

5 Click the user name to which to apply an audio profile.

An user page opens for you edit the audio profile.

6 From the **Audio profiles for recent terminals** section at the bottom of the page, click to select the user terminal to which to apply the audio profile.

The terminal page opens.

7 From the **Terminal defaults** section, select the audio profile to apply from the **Audio Profiles** pick-list.

8 Click **save**.

The audio profile is saved to the selected CICMs and users.

—End—

Changing an audio profile on a CICM

Follow this procedure to change an audio profile applied to a Centrex IP Client Manager (CICM) node.

Step	Action

From the CICM-Element Manager Audio Profile page

1 From the **change the profiles stored on the following CICM** pick-list, select the CICM.

A page opens.

2 Click to select the audio profile to change.

The audio profile page opens.

3 Edit the audio profile by modifying the fields. For detailed descriptions and decision criteria for each field, click the **?** icon.

4 To save the profile, click **save your changes to this profile**.

The profile is saved.

—End—

Creating an audio profile on a CICM-EM

Follow this procedure to create an audio profile for a Centrex IP Client Manager element manager (CICM-EM).

The Audio profile allows you to specify a list of one or more supported CODECs (compression/decompression algorithms). During call setup, each side of the call (an endpoint) is assigned its role. One end of the call is assigned the role of master, the other end of the call is assigned the role of slave. See "CODEC negotiation rules" (page 18) before you begin this procedure.

Step	Action
	From the CICM-Element Manager home page
1	From the **profiles** menu, select **audio**. *The audio profile home page opens.*
2	Click **change the profiles stored in the CICM-EM**. *A page opens for you modify the audio profile.*
3	From the **add new profile of the following type** pick-list, choose **Succession**. *The audio profile creation page opens.*
4	In the **Audio Profile Name** field, type a name for the new profile.
5	Create the profile by datafilling each field. For detailed descriptions and decision criteria for each field, click the **?** icon.
6	After values are selected for the fields, click **create profile**. *The profile creation results page opens.* The profile is stored on the CICM-EM. Profiles must be applied to CICMs to be activated.

—End—

Deleting an audio profile from a CICM

Follow this procedure to delete an audio profile from a Centrex IP Client Manager (CICM) node.

Step	Action

From the audio profile home page of the CICM-EM Web pages

1 From the **change the profiles stored on the following CICM** pick-list, choose the identifier CICM.

The audio profiles modification on page opens, showing a list of audio profiles stored on the CICM.

2 To delete an audio profile, click the trash can icon in the **Delete** column.

Your are prompted to confirm the deletion.

3 Confirm the action.

—End—

Configuring Enterprise profiles

Use enterprise profiles to create groups of network profiles and Centrex IP Client Manager (CICM) nodes.

Enterprise profiles and network profiles are created through the CICM Element Manager (EM) and stored on the CICM node. An enterprise profile is a collection of network profiles and the CICM nodes that serve that enterprise.

The Enterprise profile supports the selective CICM log on feature (Hot Desking capability). This feature makes it possible for users of an Enterprise served by multiple CICM nodes to select a node to log on to, from a list of available CICM nodes. The user can also log on to any terminal connected to the selected CICM node.

A CICM can be associated with more than one Enterprise profile, as long as the profiles are served by the node. However, a Network profile can only be associated with a single Enterprise profile.

During the client session setup, the hosting CICM node checks the source IP address of the packet against the list of Network profiles stored on the node. If a Network profile contains that source IP address and the Network profile is also associated with an Enterprise profile, the user is presented with a list of all the nodes associated with that profile. The Enterprise profile, in conjunction with the Network profile, enhances security.

The source IP address does not have to be the client IP address. If the client is behind an enterprise Network Address Translation (NAT), then the source IP address is the public IP address of the NAT.

The Enterprise profile is created, edited and deleted on the CICM element manager. Neither the Enterprise profile or its associated Networks profiles, cannot be edited on the CICM node to which they have been applied.

Navigation

- "Auditing an Enterprise profile" (page 24)

Auditing an Enterprise profile

Follow this procedure to audit an Enterprise profile to generate an audit report of its associated Network profiles and Centrex IP Client Manager (CICM) nodes.

Step	Action
	From the CICM-Element Manager home page
1	From the **profiles** section, select **enterprise**. *A modification page opens, showing the current list of Enterprise profiles.*
2	From the list of current profiles, click to select the Enterprise profile to audit. *A page opens for you to edit an enterprise profile.*
3	Click **audit enterprise profile**. *The system checks the properties of the Enterprise profile and its associated CICMs. The report is displayed.*

—End—

Associating a CICM with an Enterprise profile

Follow this procedure to associate a Centrex IP Client Manager (CICM) node with an Enterprise profile.

Step	Action
1	From the **enterprise profile edit** page, click **associated CICMs**. *A page opens, showing the current CICM associations.*
2	Click **associate one or more cicms**. *A page opens, showing a list of available CICMs.*

3 Select the CICMs to associate.

4 Click **associate selected CICMs**.

A page opens, showing the results of the action.

ATTENTION
This step is required to apply all profile association changes to the CICMs.

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

—End—

Associating a Network profile with an Enterprise profile

Follow this procedure to associate a Network profile with an Enterprise profile.

Step Action

From the CICM-Element Manager home page

1 From the menu, select **enterprise profiles**.

A page opens for you to modify an enterprise profile.

2 Click to select an Enterprise profile from the list.

A page opens showing the Network profiles and CICMs that are currently associated with this Enterprise profile.

The Profile up to date on the Associated CICMs field identifies if the selected profile is downloaded to its associated CICMs.

3 Click **edit network associations**.

A page opens, showing the current associations.

4 Identify the Network profile to associate with the Enterprise profile.

5 In the **Associated** column of the Network profile, click the check box.

6 Click **update associated network locations**.

The system updates the network associations.

ATTENTION
This step is required to apply all profile association changes to the CICMs.

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

—End—

Creating an Enterprise profile

Follow this procedure to create an Enterprise profile.

Step	Action

From the CICM-Element Manager Home page

1 From the **profiles** section, select **enterprise**.

The enterprise profile page opens.

2 Click **add new profile**.

A page opens for you to create an enterprise profile.

3 Type a name for the new profile in the **Enterprise Name** field, and then populate the remaining fields to create the profile. See Enterprise profile fields for a description of the fields.

The **Associated Networks** and **Associated CICMs** fields cannot be edited. The Network Profiles and CICMs are not associated on this **Enterprise Profile Creation** Web page. You must create the Enterprise profile name first.

A page opens showing the result of the creation.

4 Click **create profile**.

5 Go to "Associating a CICM with an Enterprise profile" (page 24) and perform that procedure to associate an Enterprise profile with Network profiles and CICMs.

—End—

Procedure job aid

Enterprise profile fields

Field	Entry	Description
Enterprise Name	User-defined name with a maximum length of 20 alphanumeric characters.	The profile name is chosen during creation and cannot be edited later.

Field	Entry	Description
Profile up to date on Associated CICMs	Read-only. Yes or No	Indicates if the profile is up-to-date on all of its associated CICMs. The state changes to No when a change is made to the Enterprise profile. The state changes to Yes when it is successfully applied to all of the CICMs in the Associated CICMlist. If the Enterprise profile is not kept up-to-date on the associated CICMs, it will be automatically deactivated and must be re-associated.
Transfer Connection Retries	0 or 1 Default is 0	Recommended setting: 0 This is the number of times a terminal redirecting to another CICM triesto reconnect to each node of the target CICM. The value should be set to zero (the default) for most applications.
Enterprise secure policy	Secure or Nonsecure	Indicates if the communications between the CICM servers within the enterprise, and their clients are secure or nonsecure.
Enterprise Nonsecure Client Threshold	0 to 9999	Indicates the number of clients permitted to connect in nonsecure mode to their secure CICM servers within the enterprise (enterprise has security policy of Secure).
Enterprise Secure Client Threshold	0 to 9999	Indicates the number of clients permitted to connect in secure mode to their nonsecure CICM servers within the enterprise (enterprise has a security policy of Nonsecure).
Enterprise Reset Security	Yes or No	Indicates whether all clients under the enterprise will have their security object cleared (yes). Clearing the security object from a client facilitates moving the client from one CICM server to another.
Associated Networks (Network Profile)	Read-only	Terminals are associated with an enterprise based on their network location. Some terminals can automatically discover their location (for example, from a DHCP server) and provide it to the CICM. For terminals that do not or cannot report an automatically discovered network location to the CICM, a mapping, called a Network profile, can be created to assign a network location based on the terminal's IP address. This is the list of network locations that are associated with the enterprise defined by this profile. A noneditable list of Network profiles that are associated with this Enterprise profile. When a CICM is disassociated from the Enterprise profile, it will remain in this list with the postfix

Field	Entry	Description
		disassociated until the updated information is successfully applied to the CICMs. It will be blank for a new profile with no associations defined.
Associated CICMs	Read-only	A non-editable list of CICMs that are associated with this Enterprise profile. It will be blank for a new profile with no associations defined.

Deleting an Enterprise profile

Follow this procedure to delete an Enterprise profile.

The state of the Enterprise profile must be set to Yes before the Enterprise profile can be deleted. See the **Up To Date** field to determine the state.

Prerequisites

Apply the Enterprise Profiles to the associated Centrex IP Client Manager (CICM) nodes to change the Profile Up To Date on Associated CICMs field to Yes, before deleting the Enterprise profile. See Enterprise profile fieldsfor a definition of this field.

CAUTION
Risk of service loss
You must disassociate all CICMs and Network profiles from the Enterprise profile before it can be deleted. Go to "Disassociating a CICM from an Enterprise profile" (page 29) and perform that procedure before you begin this procedure.

Step Action

From the CICM - Element Manager home page

1 Select **enterprise profiles**.

A page opens showing the current list of enterprise profiles.

2 In the **Delete** field, click the trash can icon corresponding to the Enterprise profile to delete.

The results of the action are displayed, and the deletion is confirmed.

—End—

Disassociating a CICM from an Enterprise profile

Follow this procedure to disassociate a Centrex IP Client Manager (CICM) from an Enterprise profile.

Step	Action
	From the CICM-EM home page
1	From the menu, select **enterprise profiles**. *A modification page opens.*
2	Click to select the Enterprise profile name from the list. *A page opens showing the Network profiles and CICMs that are currently associated with the Enterprise profile.*
3	From the **enterprise profile edit** page, click **associated CICMs**. *A page opens showing the current CICM associations.*
4	Click the check box in the **Disassociate** field to select the CICMs.
5	Click **disassociate selected CICMs**. *The results of the action are displayed.*

—End—

Disassociating a Network profile from an Enterprise profile

Follow this procedure to disassociate a Network profile from an Enterprise profile.

Step	Action
	From the CICM-Element Manager home page
1	From the menu, select **enterprise profiles**. *The enterprise profiles modification page opens.*
2	Click to select the Enterprise profile name from the list. *A page opens showing the Network profiles and CICMs that are currently associated with the Enterprise profile.*
3	From the **enterprise profile edit** page, click **edit network associations** *A page opens showing the current associations.*

4 Identify the Network profile that you want to disassociate from the Enterprise profile.

5 In the Associated column of the Network profile, click to remove the check mark and disassociate the profile from the CICM.

6 Click **Update associated network locations**.

The system updates the network associations.

ATTENTION

This step is required to apply all profile association changes to the CICMs.

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

—End—

Configuring Feature profiles

Follow this procedure to configure Feature profiles.

The Hide attribute of the Feature profile determines under what conditions a feature is available for use on Centrex IP Client Manager (CICM) client terminals. The state of other features on the terminal, and the state of the terminal itself, can affect feature availability. The ability to hide features when they cannot be used allows some terminals to maximize the use of a limited number of feature keys.

Step	Action

From the CICM - Element Manager home page

1 From the **profiles** section, select **feature**.

The feature profile home page opens.

2 Select the CICM identifier from the pick-list, then click **change the profiles stored on the following CICM**.

The feature profiles modification page opens, showing the feature profile for the selected CICM. The feature profile is a list of features, each of which has a set of attributes that can be configured.

3 From the **Name** list, click to select the features you want to configure.

A feature profile page opens for each feature chosen.

Click the **?** icon for help performing the next step.

4 Perform one of these actions:

- To configure this feature as a dynamic (DN) feature, choose **Yes** from the **DN Feature** pick-list.
- If you do not want to designate this as a dynamic feature, choose **No**.

5 Click **save your changes to this profile**.

6 To configure the **Hide Mode**, perform one of these actions. From the **Hide Mode** pick-list, choose one of these profiles:

- Never
- When DN is active
- When DN is inactive

A page opens showing the results.

7 Repeat steps 4 through 6 to modify the profile of each feature you selected in step 3.

—End—

Enabling or disabling the dynamic feature key (terminal type)

Follow this procedure to enable or disable the dynamic feature key on a specific type of Centrex IP Client Manager (CICM) node.

This setting cannot be overridden by any other setting. That means that if the dynamic feature key functionality is disabled on a particular terminal type, the feature cannot be activated on that type of terminal in any other way.

Users logged into the Centrex IP Client Manager (CICM) node when the functionality is enabled or disabled are not affected by the change. The change goes into the effect the next time they log onto the CICM. If you want the change to effect immediately, perform procedure Enabling or disabling the dynamic feature key (user overrides).

The user may also disable the functionality from the terminal itself through the CICM client menu. These setting changes take effect immediately.

Step	Action

From the CICM - Element Manager home page

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

A terminal page opens.

2 Select the CICM identifier from the pick-list.

3 Click **go to terminal configuration on CICM**.

The page opens showing the terminal configuration for the selected CICM.

4 On the **terminals on** page, from the **configuration** pick-list, select the terminal type.

5 Click **configuration**.

A configuration page opens for you to configure the terminal.

6 To configure this terminal type as a dynamic (DN) feature, choose **Yes** from the **Automatically hide features** pick-list in the **Feature Key Attributes** field.

7 Click **Apply changes**.

The updating terminal configuration page opens to confirm the changes.

—End—

Enabling or disabling the dynamic feature key (user overrides)

Follow this procedure to immediately enable or disable the dynamic feature key on a specific type of Centrex IP Client Manager (CICM) node. If you do not want users to be immediatelyaffected by the change, perform procedure Enabling or disabling the dynamic feature key (terminal type).

Step	Action

From the CICM-Element Manager home page

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

The **user home page** opens.

2 In the **User** input box, enter the user ID that you want to apply overrides to, or remove overrides from.

3 Select the correct CICM in the pick-list immediately under the **User** input box.

4 Click **edit user's**.

A user page opens.

5 Click **User overrides**.

A page opens for you to edit user profile overrides.

6 Perform one of these actions in the **User Settings** field:

- To enable dynamic feature key functionality, choose **Yes** in the **Auto-hide feature keys User Setting** field.
- To disable dynamic feature key functionality, choose **No** in the **Auto-hide feature keys** field.

7 Click **save changes**.

The change takes affect immediately.

—End—

Configuring the Language profile

IP Phones and Centrex IP Client Manager (CICM) SoftClients support multiple languages, through the Language profile. A Language profile must be enabled or disabled for the specific CICM in order for the IP Phones to access a particular language.

A list of the available Language profiles can be found on the CICM-Element Manager (CICM-EM) Web pages, but they cannot be created or changed. New languages are added through new software releases or language patches.

Although multiple languages are available on the m6350 SoftClient, it does not support the Language profile. For information on language selection on the CICM SoftClient, refer to the *m6350 SoftClient Installation Guide,* (NN10182-113).

Step	Action
	From the CICM-Element Manager home page
1	From the **profiles** section, select **language**. *The language profile home page opens.*
2	From the **view the profiles stored on the following CICM** pick-list, select the CICM identifier.
3	Click **view the profiles stored on the following CICM**. *A page opens for you to select a language profile.*
4	Enable or disable the language on the selected CICM through the **Action** column. Before disabling an enabled language, the system warns you if the language is used by global settings, user profiles, or user overrides. You are prompted to replace the references to the language being disabled with a language which is currently enabled.
5	After enabling or disabling a language, reboot both CICMs.

—End—

Configuring Network profiles

Network profiles define the IP address domains that are supported by the Centrex IP Client Manager (CICM) node. An IP address domain is identified by the network device that connects it to the public IP address space that contains the CICM. Typically, this is a network address translation (NAT) device. Only terminals within a valid IP address domain can be connected to the CICM. Refer to the section *NAT and firewalls* in *CICM Administration and Security* (NN10252-611).

Centrex is a carrier-hosted featured voice service offered to enterprises. Centrex IP maintains feature transparency to CS2K Centrex. One key difference between Centrex and Centrex IP is that with Centrex IP, enterprises are served over a converged IP network instead of a CS2K network. Each enterprise has its own enterprise IP network. It normally uses private IP addresses for communication within the enterprise, and public IP addresses for communication outside the enterprise through a NAT associated with its gateway router.

Each enterprise IP network is uniquely represented by a network profile on the CICM that serves this enterprise. A Network profile identifies the IP address domain of the enterprise, represented by the public IP address of the enterprise NAT, along with an associated network location for this enterprise.

Network Profiles provide an effective means for authentication and control of Centrex IP traffic. Centrex IP traffic is only allowed to flow between the CICM and the IP address domains that are specified by the Network Profiles on the node.

Network profile configuration changes are immediately effective for new terminal connections. You do not need to restart the CICM to implement the changes; they are immediate. However, you must restart terminals if they are assigned a new network domain.

Network Profiles can only be created, changed, and deleted by an administrator. They are stored on the CICM-EM and applied to a CICM.

Enterprise IP address domain representation

For terminals behind a network address translation (NAT), the NAT presence must be defined in the Network profile. The Network profile specifies the public IP address and the subnet of the NAT.

For an enterprise that uses public IP addresses (no NAT is needed), the administrator can still create a Network profile for it, by using the network domain 0.0.0.0, 0.0.0.0, or by specifying the subnet from which those customers originate (for example, 47.165.169.0, 255.255.255.0). Nortel recommends to lock down the allowed range of valid terminal IP addresses in this way, to prevent denial-of-service attacks from unknown subnets.

Network domain addressing

Assume that two enterprise nodes are configured through the CICM-EM Network profile Web page using these IP addresses:

- Enterprise 1 with 47.165.168.100 and 255.255.255.255
- Enterprise 2 with 47.165.168.200 and 255.255.255.255

The mask 255.255.255.255 informs the CICM to consider only clients originating from the single IP address 47.165.168.100 to be in Enterprise 1.

Network address translations (NAT) often only have a single IP address into which they multiplex the active connections by mapping them to unique ports. A NAT with four interfaces, for example, would be datafilled with the two least significant missing bits. Therefore, for address 47.165.168.100, the mask 255.255.255.255 would permit addresses 47.165.168.100, 101,102, and 103 to be considered part of the network domain.

If network domain licensing is enabled, a terminal can log in only if its IP address falls within one of the Network profiles datafilled on the CICM to which it is connected.

Media routing in a CS2000 environment with NAT

When possible, media routed between Centrex IP Client Manager (CICM) client phones stays within the Enterprise network. Staying within the same network:

- improves voice quality
- Increases CICM capacity
- reduces bandwidth requirements from the enterprise to the carrier

However, intraswitched calls cannot traverse the boundaries of a network address translator (NAT) because:

- routing will likely be blocked by a security setup, such as fire wall rules

- RTP packets use nonroutable private IP addresses that are either overlapped between two Enterprises, or viewed as unreachable

It is the associated network location fields that is part of the network profiles that determines if calls can be routed directly between each other or if they have to go through a proxy.

Navigation

- "Changing a Network profile" (page 39)
- "Creating a Network profile" (page 40)
- "Deleting a Network profile" (page 41)
- "Enabling or disabling network domain address licensing" (page 42)
- "Updating auto-discovery networks" (page 42)

Changing a Network profile

Step	Action

From the CICM-Element Manager home page

1 From **profiles**, select **Network**.

A network profile page opens.

2 Click to select the IP address of the network profile to edit.

A page opens for you to modify the network profiles.

3 In the **Details** section, edit the fields as required. Click the **?** icon for help.

4 Click **save your changes to this profile**.

The update to the profile is confirmed.

To edit default location information:

5 Perform these substeps to edit the default location.

a. Click **edit default location**.

The edit default location information page opens.

b. Datafill the fields in the **Type of Location, Civil Location,** and **Spatial Location** sections.

Click on the **?** icon for help.

c. Click **save changes**.

—End—

Creating a Network profile

Step	Action

From the CICM-Element Manager home page

1 From **profiles**, click **network**.

A network profiles page opens.

2 Click **add new profile**.

A page opens for you to create a network profile.

3 Populate these fields to create a network profile. Click the **?** icon for help populating a field.

- In the **Address** field, specify the network address of the subnet that contains the range of public addresses available to a network address translations (NAT) device.
- In the **Subnet** field, specify the subnet mask for the subnet that contains the range of public addresses available to a NAT device.
- In the **Lease period (min)** field, enter the period for which any UDP port mapping is maintained.

  For release SN08 CICM-EMs and gateways, the lease period is variable and the field can be specified.
- In the **Retry count** field, specify the number of times a terminal attempts to connect to a CICM before it fails, and attempts to connect to the other node.

  A terminal connecting to a CICM with an IP address described by this Network profile will have this retry connection count. To take effect, this Network profile needs to be applied to the CICM or to be associated with an Enterprise profile that is applied to the CICM. Leaving the field blank means that the value of the Retry count is taken from the terminals settings for that CICM.
- Read only field. Cannot be edited—the **Associated Enterprise Profiles**.

  If this field is not blank, the Network profile is already associated with an Enterprise profile. The Network profile must be dissociated from the Enterprise profile before you can edit it.

- Set the field **Associated network location** to CS-LAN (no NAT), Manually defined (when the Associated Limited Bandwidth Link Identifier is also to be set), or to one of the Auto-Discovery Networks that have been downloaded to the CICM-EM in the procedure Updating auto-discovery networks.
- Perform one of these actions:
  - If you selected **Manually defined Limited Bandwidth Link** in the **Associated Network Location** field, in the **Associated Limited Bandwidth Link Identifier** field, enter the global middlebox identifier of the Limited Bandwidth Link .
  - If you selected CS-LAN or Auto-Discovery Network Location as the Associated Network Location, this field is ignored. Derive the value of this field from the Succession Element and Sub-Element Manager (SESM).

4 Click **create profile**.

The profile creation results page opens, showing the results of the action.

—End—

Deleting a Network profile

Step	Action

From the CICM-Element Manager home page

1 From **profiles**, select **Network**.

A page opens for you to select a network profile.

2 Click the trash can icon in the **Delete** field of the Network profile to delete.

The action is confirmed.

3 Click the trash can icon in the **Delete** field of the network IP address to delete.

The status page confirms the results of the action.

—End—

Enabling or disabling network domain address licensing

Step	Action

From the CICM-EM network profiles modification page

1 Select the CICM from the **change the profiles stored on the following CICM** pick-list.

2 Click **change the profiles stored on the following CICM**.

A page opens for you to modify the network profile.

3 Click **Enable/Disable Network Domain Address Licensing** text bar to toggle between **enable** and **disable**.

A status page opens, confirming the action.

—End—

Updating auto-discovery networks

Step	Action

From the CICM-Element Manager home page

1 From the **profiles** menu, click **network**.

A page opens for you to modify the network profile.

2 Click **update auto-discovery networks**.

A page opens for you to update the global middlebox IDs.

3 Enter the details for the Call Server 2000 Management Tools (CMT formerly known as the SESM).

4 Click **Update middlebox ids**.

You are prompted to confirm the action.

5 Confirm the action.

—End—

Configuring Terminal Gain profiles

Terminal Gain profiles provide a means of increasing the volume levels of the Centrex IP Client Manager (CICM) terminals. To adjust the default factory gain parameters, configure the these parameters:

- send loudness rating (SLR)—defines the level of amplification applied to the voice signal recorded by the microphone by the DSP in the terminal before the voice signal digitized and sent on the network.
- receive loudness rating (RLR)—defines the level of amplification applied to the digitized voice signal received from the network by the DSP before the reconstructed voice signal is played through the output device speaker. Volume adjustments made by the user or through configuration are relative to the nominal level.

All configuration data related to the use of terminal gain profiles is backed up by the CICM and CICM-EM backup facilities. The configuration data can be restored using the CICM and CICM-EM restore procedures.

Restrictions

- Terminal gain profiles are not supported on third-party terminals or the m6350 SoftClient.
- Handsfree gain parameters cannot be adjusted.
- Headset settings apply only to terminals with native headset capabilities, for example IP Phone 2004 and IP Phone 2002.

Navigation

- "Applying terminal gain profiles" (page 44)
- "Creating or editing a terminal gain profile" (page 44)
- "Configuring the CICM to use a terminal gain profile" (page 44)
- "Deleting terminal gain profiles" (page 46)
- "Viewing terminal gain profiles" (page 46)

Applying terminal gain profiles

Follow this procedure to apply a terminal gain profile to a Centrex IP Client Manager (CICM) terminal.

Before terminal gain profiles can be configured and used on the CICM, you have to download the profile from the CICM-EM. Nortel recommends that you download all profiles to all the CICMs to simplify management.

Step	Action
	From the apply terminal gain profile page
1	In the **Range of Profiles** field, click to select **Apply all existing terminal gain profiles**.
2	In the **Range of CICMs** field, click to select **Apply to all CICMs**.
3	Click **apply profile(s)**. *All of the existing terminal gain profiles are applied to all of the CICMs.*

—End—

Configuring the CICM to use a terminal gain profile

Follow this procedure to configure a terminal gain profile on a Centrex IP Client Manager (CICM).

Prerequisites

A terminal gain profiles must be created and applied to a CICM before you begin this procedure.

Step	Action
	From the terminals on cicm page
1	From the **Terminal Settings** section, open the pick list and select a gain profile. *If there are no terminal gain profiles available, this message appears No profile stored on the CICM.*

—End—

Creating or editing a terminal gain profile

Follow this procedure to create or edit a terminal gain profile.

Profile creation guidelines

- The profile name must be wholly alphanumeric, and has a maximum length of 20 characters.
- You cannot change the name of a profile after it is created.
- The send loudness rating (SLR) and receive loudness rating (RLR) parameters for the handset and headset can be specified in the profile.
- Each parameter has a predefined range of supported values, specified in decibels. Higher numeric ratings indicate higher perceived volume levels.
- A default setting for any parameter instructs the CICM not to adjust the parameter on the terminal. This means that the terminal continues to use the factory default setting.
- Changing the RLR affects the minimum base level from which volume adjustments on the CICM terminal were made. Any volume adjustments made to increase the volume prior to the introduction of a terminal gain profile, may need to be readjusted.
- Changing the RLR affects the nominal level from which volume adjustments are made using the volume controls on the terminal or the default volume settings on the CICM. If volume adjustments have been made prior to the introduction of terminal gain profiles to compensate for low nominal levels, default volume levels may be too high and will need to be adjusted.

Step	Action

From the terminal gain profile page

1 Perform one of these actions:

- If this is a new profile, in the **Profile name** field, enter the name of the profile.
- If you are editing a profile, in the **Profile name** field select the name of the profile to edit.

2 In the **Handset Properties** field,

- open the **Send Loudness Rating** pick list and select an option.
- open the **Receive Loudness Rating** pick list and select an option.

3 In the **Headset Properties** field,

- open the **Send Loudness Rating** pick list and select an option.

- open the **Receive Loudness Rating** pick list and select an option.

4 Click **save your changes to this profile**.

The profile is created, or the changes are save to the profile.

—End—

Deleting terminal gain profiles

Follow this procedure to delete a terminal gain profile from a Centrex IP Client Manager Element Manager (CICM-EM).

If you delete profiles that are currently in use, the terminals that have logged on users continue to use the configured settings of the deleted profile.

Users logging on to a CICM terminal after the profile is deleted revert to the default configuration. The CICM terminal settings show that the default profile is in use.

Step	Action

From the CICM Element Manager home page

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

2 Click **change the terminal gain profiles stored on the CICM-EM**.

A list of profiles appears.

3 In the **Delete** column of the profile to delete, click the trash can icon.

The profile can only be deleted from the CICM-EM if the CICM-EM successfully deletes the profile on all the CICMs.

The results of action are confirmed.

—End—

Viewing terminal gain profiles

Follow this procedure to view the terminal gain profile that is stored on a Centrex IP Client Manager Element Manager (CICM-EM).

Step	Action

From the CICM Element Manager home page

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

2 To view of the list of profiles stored on the CICM-EM, click **change the terminal gain profiles stored on the CICM-EM**.

A list of profiles appears.

3 Perform these steps to view a list of profiles stored on the CICM,

a. From the CICM pick list below the link, select the node identifier of the CICM to view.

b. Click **change the profiles stored on the following CICM**.

A list of profiles pushed down to the node appears.

—End—

Configuring User profiles

A User profile is a collection of default settings that can be applied to a group of users. A User profile can contain feature key settings, language preference, time zones, and permissions.

User profiles may be created, changed, and deleted. They are stored on the Centrex IP Client Manager-Element Manager (CICM-EM) and applied to a selected CICM.

Unless overridden locally, a user inherits settings from the User profile configured for the CICM client terminal. The administrator can override local changes to a User profile.

To create users, refer to *CICM Administration and Security* (NN10252-611).

Navigation

Applying a User profile to a CICM

Step	Action
	From the CICM-Element Manager user profile home page
1	Click **apply one or more profiles stored on the CICM-EM to one or more CICMs**. *The apply user profile page opens.*
2	Select the profiles to apply to the nodes. Click the **?** icon for help.

3 Select the CICM to nodes to which to apply the profiles. Use the **CTRL** key to select more than one CICM.

4 Click **apply profile(s)**.

The profile apply results page opens, showing the results of the action.

—End—

Applying or removing User profile overrides

Step	Action

From the CICM-Element Manager element manager home page

1 From the **CICM** list, select **users**.

The user home page opens.

From the user home page

2 In the **User** field, enter the user ID that you want to apply overrides to, or remove overrides from.

3 From the pick-list immediately under the **User** field, select the CICM.

4 Click **edit user's**.

The page opens for you to edit a user.

5 Click **user overrides**.

The profile overrides for user page opens. The fields are populated with the data from the user's current profile, if one exists.

6 Datafill or edit the contents of the fields that you want to override for this user. Click the **?** icon for help populating a field.

The User Settings you specify here override the default settings on the user's profile.

If a User Settings field is blank, it defaults to the user profile.

7 To remove an override in a particular field, set the field to blank.

8 To remove all overrides, click on **remove all overrides**.

9 Click **save changes**.

The status page opens, confirming the action.

—End—

Changing a User profile

Step	Action
	From the CICM Element Manager user profile home page
1	Select **change the profiles stored on the CICM-EM**. *A page opens for you to select a user profile.*
2	Click to select the name of the user profile that you want to modify. *The user profile edit page opens.*
3	Edit the fields. Click the **?** icon for help.
4	Click **save your changes to this profile**. *The status page opens and confirms the action.*

—End—

Creating a User profile

Step	Action
	From the CICM Element Manager home page
1	From **profiles**, select **user**. *The user profile home page opens.*
2	Click **change the profiles stored on the following CICM-EM**. *A page opens for you to select to add a new profile.*
3	Click **add new profile**. *A page opens for you to create a user profile.*
4	Datafill the fields. Click the **?** icon for help.
5	Click **create profile**. *A page opens confirming the creation of the file. The User profile is stored on the CICM-EM.*

—End—

Deleting a User profile

Step	Action

From the CICM Element Manager user profile home page

1 Click **change the profiles stored on the CICM-EM**.

A page opens for you to select a user profile to delete.

2 Click the trash can icon in the **Delete** field, for the profile you want to delete.

A page opens for you to select to delete the user profile.

3 Click **delete this profile on the element manager and ALL CICMs**.

You are prompted to confirm the action.

4 Click **Yes**.

A status page opens and confirms the deletion.

—End—

Enabling or disabling Daylight Savings Time

Follow this procedure to manually enable and disable Daylight Savings Time on the Centrex IP Client Manager Element Manager (CICM-EM).

Some regions observe Daylight Savings Time, which means the clock is changed twice a year. This requires the administrator to manually change the time on the CICM-EM so that the change is reflected on the IP Phones. Enabling and disabling Daylight Savings Time cannot be done automatically because a CICM-EM might support IP Phones in more than one time zone, or the IP Phones themselves may be in a time zone that is different from the CICM-EM.

There are two different methods to enable or disable Daylight Savings Time on the CICM-EM, through the Global Settings, or the User Profiles.

Enabling or disabling Daylight Savings Time through Global Settings

Step	Action
1	Log in to the CICM-EM.
2	Navigate to the **Global Settings** page.
3	Perform one of these actions: • To change to Standard Time — In the **Locale Settings** field, change **Default Daylight Savings** to **No**. • To change to Daylight Savings Time — In the **Locale Settings** field, change **Default Daylight Savings** to **Yes**.
4	Click **save changes to the CICM**.

—End—

Enabling or disabling Daylight Savings Time through User Profiles

Step	Action
1	Log in to the CICM-EM.
2	Navigate to the **User Profiles**.
3	Click **change the profiles stored on the CICM-EM**.
4	Select the profile you wish to change.
5	Perform one of these actions: • To change to Standard Time — In **User Settings**, change **Daylight Setting** to **No** or blank. If the Daylight Setting field is blank, the IP Phone uses the Global Setting. • To change to Daylight Savings Time — In **User Settings**, change **Daylight Setting** to **Yes** or blank.
6	Click **save your changes to this profile**.
7	Click **user profile modification**.
8	Repeat steps 4 through 7 for each User profile you want to change.
9	Click **apply one or more profiles stored on the CICM-EM to one or more CICMs**.
10	Select the profiles and the CICMs to download.
11	Click **apply profile(s)**.

—End—

Enabling or disabling QoS reporting for a CICM

Follow this procedure to enable or disable the reporting of Quality of Service (QoS) statistics from a CICM to a collection server.

Prerequisites

- Refer to *Quality of Service reporting for CICM node calls* in *CICM Basics* (NN10044-111), for the method of reporting, and a list of IP Phones that support QoS reporting.
- See the description, *Basic and extended QoS statistics reporting for CICM nodes* and the procedure *Viewing QoS statistics of CICM nodes*, in *CICM Performance Management* (NN10248-711).
- The gateway controller (GWC) to which the CICM connects, must be configured to enable basic QoS reporting.
- The CICM-EM of the CICM must be configured to enable extended QoS reporting.
- You need to know the IP address of the extended QoS server equipment.
- Adding or changing the IP address for the destination of the extended QoS reports takes effect within approximately 2 minutes. It does not require a reboot.
- Disable QoS reporting by removing the check mark from the Enable box of the CS2000 Management Tool and by removing the data from two fields in the CICM-EM Web page.

Step	Action
From the CS2000 Management Tool	
1	Access the CS2000 Management Tool.
2	Open the **Device Types** folder and select folder **Gateway Controller**.
3	Select the GWC identifer under the window **Gateway Controllers**.

4 Click the **QoS Collectors** tab.

5 Click to check the **Enable QoS Collection** check box.

6 From the File menu, select **Save**, to save the configuration.

From the CICM home page

7 From the **change the global settings for the following CICM** pick-list, select the CICM identifier.

8 Click **change the global settings for the following CICM**.

The page appears for you to modify the global settings.

From the global settings modification page

9 In **Extended QoS server Ip Address** field, enter the IP address of the QoS server.

10 In **Extended QoS server por**t field, enter **34367**.

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

12 Repeat step 7 to step 11 for each CICM for which you want to enable extended QoS reporting.

13 To verify that statistics are being collected, perform this procedure *Viewing QoS statistics of CICM nodes*, in *CICM Performance Management* (NN10248-711).

—End—

Forcing a user log off from a CICM

Follow this procedure to force the log out of a user from a Nortel Centrex IP Client Manager (CICM) node.

Step	Action
	CICM Element Manager users home page
1	Select the CICM identifier from the **browse users on** pick-list.
2	Double-click **browse users**. *A page opens for you to identify a user.*
3	Enter a user name in the **delete users on** field.
4	Click **edit a user's configuration**. *A page opens for you to select to force a logout of the user.*
5	Click **force user logout**. *A status message shows the result of the action.*
	—End—

Provisioning a line for a CICM client

Follow this procedure to provision a line for a Nortel Centrex IP Client Manager (CICM) client.

Step	Action

From the CICM Element Manager desktop

1 Connect to the CS2000 Management Server for the chosen CS2000.

2 Ensure that the gateway controller (GWC) is provisioned to support Large Lines Gateways.

3 In the *Associate Media Gateway* dialog, select a CICM gateway to associate with the chosen GWC.

4 Enter a number in the *Reserved terminations* field.

The maximum number of reserved terminations is 1023 for SAM16, and 3069 for SAM21.

5 Click **OK**.

Response 1: The Gateway List displays a registration of the CICM gateway against the GWC.

Response 2: A logical group is automatically created in table LGRPINV on the CS2000.

For a SAM16, only one tuple is created for its 1023 supported terminations. For a SAM21, three tuples are created (in table LGRPINV) to accommodate its 3069 supported terminations.

6 Log on to OSSGATE and enter the command **`NEW`** to create new lines

where

`8500001` is the directory number (DN).
`m5216` is the name of the line class code (LCC).
`IPCLIENT OTHER` specifies the kind of phone service. OTHER indicates any of the Nortel IP phone sets.
`PUBGRPA` is the customer group.

151 is the simplified numbering plan area (SNPA).
CICM 500 0 00 01 is the line equipment number (LEN)
1 userid 000001 $ is the user id of the CICM client (terminal).
1 passwd 1234 is the password of the user id.
1 LNR 2 3WC IPCLIENT OTHER 3 MWT Y ALL N 4 CFU N 1 $ 5 INSPECT $ is the list of features assigned to the line. Use OTHER to include any version of an IP phone for option IPCLIENT.

—End—

Resetting user counters

Follow this procedure to reset these user counters to zero:

- Total login failures
- Login count
- Login failure count
- Total call count

Step	Action

From the CICM Element Manager user home page

1 Select the CICM identifier from the **browse users on** pick-list.

2 Double-click **browse users**.

A page opens for you to select a user..

3 Click the user name for which you want to reset the counters.

A page opens where you can select to reset the counters for the user..

4 Click **reset user counters**.

A status page displays the results of the action.

—End—

Security profiles

For details and procedures, refer to *UNIStim security* in *CICM Administration and Security* (NN10252-611).

Security configuration is available through the Centrex IP Client Manage-Element Manager (CICM-EM). Security profiles allow administrators to:

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

Security configuration consists of setting these security parameters:

- security policy - indicates whether 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, which facilitates moving multiple secure clients (terminals) from one CICM server to another

Setting the global m5216 emulation mode

Follow this procedure to set the m5216 emulation mode.

The m5216 emulation mode is automatically used by any terminal with GIC or GIAC features assigned to it. If the global m5216 emulation mode flag is set, this emulation mode is used for all terminals, regardless of whether they have GIC or GIAC features assigned. This ensures that all terminals behave in a consistent manner.

Step	Action
	From the CICM Element Manager home page
1	From the **CICM** menu, select **Status**. *The cicm home page opens*
2	Click **change the global setting for the following CICM**. *The global settings on page opens.*
3	Scroll down the **global settings modification on** page, to the **Terminal settings** section, and select **yes** in the **M5216 Emulation Mode** field.

—End—

Terminal configuration sanity test

Perform the procedures in this section to verify that the network and terminal configuration is correct.

Nortel recommends that you perform these procedures before you attempt to upgrade from release SN07 to a later Centrex IP Client Manager (CICM) release. If there is a problem with either the network or the S1/S2 IP address on the terminals, the terminal transfer cannot be completed. As a result, some terminals could be left without service after a CICM upgrade is completed.

For additional information about terminal transfers, see *Administration and Security* (NN10252-611).

Navigation

- "Verifying terminal configuration " (page 67)
- "Manually transferring terminals" (page 69)

Verifying terminal configuration

Perform this procedure to transfer Centrex IP Client Manager (CICM) client terminals from one CICM to another to ensure that service is maintained, or can be restored after a service interruption or software upgrade.

CAUTION
Risk of service interruption

Performing this procedure may result in a temporary loss of service. Nortel recommends that you perform this procedure outside of normal working hours.

Allow for up to 5 minutes per 1000 connected terminals.

Step	Action
1	Perform a terminal transfer from node A to node B. See "Manually transferring terminals" (page 69).

2 Verify that the node A count value shown in the **Active Terminal** field decrements to zero, and that the **service status** of the terminal changes to **stopped**.

From the maintenance status page

3 Click **re-start terminal service on node A** to restart service on node A.

You are prompted to confirm the action.

4 Click **Yes** to confirm the action to restart the node.

5 Click **start auto refresh**.

6 Verify that **Started** appears in the **Terminal Service** field.

If the Active Terminals value did not decrease to zero, it indicates a problem with the configuration of one or more of the terminals, or that there is a network problem. Either cause will prevent a terminal transfer to the mate node. This has an adverse impact on service for affected terminals during a network or node failure or upgrade.

Contact Nortel technical support for help to identify the terminals that failed to transfer.

Perform a terminal transfer from node B to node A

7 Begin at step 1 and repeat this procedure, making these changes at the appropriate step:

- At step 1, perform a terminal transfer from node B to node A.
- At step 2, verify that the node B count value decrements to zero, and the node B service status changes to stopped.
- At step 3, click **re-start terminal service on node B**.

If the Active Terminals value did not decrease to zero, it indicates a problem with the configuration of one or more of the terminals, or that there is a network problem. Either cause will prevent a terminal transfer to the mate node. This has an adverse impact on service for affected terminals during a network or node failure or upgrade.

Contact Nortel technical support for help to identify the terminals that failed to transfer.

—End—

Manually transferring terminals

Follow this procedure to transfer CICM client terminals from one CICM to another to ensure that service is maintained, or can be restored after a service interruption or software upgrade.

ATTENTION

Perform this procedure only in conjunction with the *Verifying terminal configuration* procedure.

CAUTION

Risk of service interruption

This procedure may cause a temporary loss of service. Nortel recommends that you perform this procedure outside of normal working hours.

Step	Action

From the CICM maintenance status page

1 Ensure that **start auto refresh** is showing in the menu on the right.

If **stop auto refresh** appears in the menu, click it to toggle to **start auto refresh**.

2 Open the **Node** pick-list and select the node to which to transfer the clients.

3 Click to open the **Terminal Shutdown Timeout** pick-list.

4 Select the length of time (in minutes) for which to allow CICM clients to log off.

After the time expires, any clients that are still logged on are automatically dropped by the transfer.

5 Click **transfer terminals**.

A confirmation screen appears.

6 Click **confirm terminal transfer**.

The terminal transfer operation begins as soon as you confirm the action. The operation ends when the length of time you specified in step 3 expires.

7 On the **maintenance status** page, click **start auto refresh**.

The item toggles to stop auto refresh.

CAUTION
Wait until the terminal transfer has completed before proceeding. If the transfer does not complete, stop this procedure.

Contact your next level of technical support.

8 When the transfer is completed, all the client terminals should be hosted on the node you selected in step 2.

—End—

Viewing a CICM user list

Follow this procedure to view the list of users for a selected Centrex IP Client Manager (CICM) node.

Step	Action

From the CICM-Element Manager home page

1 From the CICM menu, select **users**.

The user home page opens.

2 Select the node identifier from the **CICM** pick-list in the **browse users on** field.

3 Click the **browse users** text.

A page opens showing a list of current users on the CICM.

4 To view the user list for a different CICM, a different VMG, or a different range, select an item from the **browse users on** pick-list.

The page is refreshed, showing new information.

5 To view a list of active users with node and line number information, click **list the active users**.

A page opens showing a list of active users.

—End—

Viewing user configuration

Follow this procedure to view the configuration settings for a selected user of a selected Centrex IP Client Manager (CICM) node.

Step	Action

From the CICM-Element Manager users home page

1 Select the node identifier from the CICM pick-list in the **browse users** field.

2 Click the **browse users** text.

The VMG and Range fields appear.

3 Click **browse users** again.

The users on CICM page opens.

4 To view a user configuration, click the user name in the list, or enter a user name in the **User** field.

5 Click **view user's configuration** text.

The user page opens where you can view configuration information.

Fields on the page are read only. You cannot make changes on this page.

6 To configure or edit user configuration, refer to the *OSS Guide (ATM) Advance Feature Guide*, PLN-08AT-OSS.

—End—

Installing and initializing IP Phones

Follow this procedure to install and initialize a Nortel Centrex IP Client Manager (CICM) IP Phone. The procedure for installing and initializing CICM IP Phone sets is the same for these models:

- IP Phone 2001
- IP Phone 2002
- IP Phone 2004
- IP Phone 2007
- IP Audio Conference Phone 2033
- IP Phone 1120E
- IP Phone 1140E
- IP Phone 1150E

Navigation

- "Initializing an IP phone" (page 75)
- "Installing an IP Phone" (page 78)

Initializing an IP phone

Initialize a IP Phone to complete the initial installation, and to enable it to operate with a Centrex IP Client Manager (CICM) node.

Prerequisites

- You must have completed this procedure, "Installing an IP Phone" (page 78).

Step	Action
	From the IP Phone
1	Ensure that the IP Phone set is powered. Power is indicated by flashing indicator lights and soft key icons.

If the display is blank:

- verify that the AC outlet has power
- verify that the AC Power adapter has a good connection at both ends
- unplug the AC adapter at the telephone base and plug it in again

When the phone set is powered, it automatically begins initializing.

2 When the Nortel Networks screen appears in the display, begin at the left and press each soft key once to configure the phone.

If this screen does not appear, contact your system administrator to upgrade the phone set.

If the terminal attempts to connect to the server before you press all of the soft keys, you must repeat this step. Unplug the power cord, then plug it in again to restart the initialization.

3 As the prompts for configuration data appear, enter the appropriate information. See IP Phone configuration parameters, for a list of prompts and correct responses.

When inputting data to answer the prompts, labels appear above the soft keys in this order.

OK
Press to record the entry and continue to the next prompt.

Bkspace
Press to edit the current prompt by deleting an entry one character at a time.

Clear
Press to erase the current entry for the prompt so that other data can be entered.

Cancel
Press to terminate the configuration process. Return to step 1 if you cancel the configuration.

Use the number keys on the dial pad to enter numbers for the data. When entering IP addresses, press the star key (*) to represent a period (.).

4 After all the configuration data is entered, the IP phone saves the entries and attempts to connect to the server.

5 Depending on the configuration of your gateway, you may be offered to upgrade the firmware for the IP phone. When there is a new firmware release, this message appears:

```
New firmware available.  Perform upgrade now?
```

Select **Yes** by pressing the nearest key. Downloading takes less than two minutes.

6 When the IP phone has successfully connected to the server, the Login screen appears. Enter your user name and password to log on and begin using the IP phone.

If the IP phone cannot connect to the server, it retries automatically.

If the IP phone cannot connect to the gateway, it may indicate that an invalid parameter was entered during the initialization. In this case:

a. Verify that your entry data is correct. See IP Phone configuration parameters

b. Disconnect the phone from the power source to clear the initialization data. Reconnect the phone to the power source and beginning with step 2, repeat this procedure.

7 If you still cannot connect to the network through the gateway, contact your next level of technical support for assistance.

—End—

Procedure job aid

IP Phone configuration parameters

Prompt	Entry data
1. DHCP? (0—No, 1—Yes)	Enter 1 to use full or partial DHCP. Enter 0 (zero) to manually configure the set.
2. DHCP: 0—Full, 1—Partial	The prompt appears only when full or partial DHCP is selected. For full DHCP, all remaining prompts are automatically configured by the DHCP server. For partial DHCP, prompts 3, 4, and 5 are automatically configured by a DHCP server.
3. SET IP	Enter the IP address for the phone.
4. NETMSK	Enter the network submask.
5. DEF GW	Enter the IP network address of the default gateway.
6. S1 IP	Enter the IP address of the primary server.
7. S1 PORT	Enter **5000** for the port number of the primary server.

Prompt	Entry data
8. S1 ACTION	Enter **1** for the primary action code.
9. S1 RETRY COUNT	Enter **6** for the primary retry count.
10. S2 IP	Enter the IP address of the secondary server.
11. S2 PORT	Enter **5000** for the port number of the secondary server.
12. S2 ACTION	Enter **1** for the secondary action code.
13. S2 RETRY COUNT	Enter **6** for the secondary retry count.

Installing an IP Phone

You install an IP Phone to make it a client of a Centrex IP Client Manager (CICM) node.

Prerequisites

- An IP Phone set can be configured in different ways depending on whether a full or partial Dynamic Host Configuration Protocol (DHCP) server is available in your network. DHCP can be used to provide the IP Phone with an IP address and other information required to initialize the set. Ask your network administrator if DHCP is being used, and if so, is it full or partial.
- Even if DHCP is not used, you must know the information that is identified in the table IP Phone configuration parameters, before you begin the installation.
- You need CAT-5 cable with an RJ45 connector at each end.
- You need an AC power outlet for the phone set. The outlet must provide up to 240 V.

Step Action

From the location for the IP Phone

1 Place the IP Phone in the location where it is to be used.

2 Measure the path from the phone to the IP network connection.

3 Make a CAT-5 cable, with an RJ45 connector at each end, long enough to follow the path.

CAUTION
Risk of equipment damage
Severe damage occurs to an IP phone set that is plugged into an ISDN connection. Ensure that you are plugging your set into a 10 or 100 BaseT Ethernet jack.

4 Connect one end of the CAT-5 cable to the line jack on the telephone base and the other end to an Ethernet jack into the IP voice network.

5 Connect one end of the handset cord to the handset jack on the telephone base. Connect the other end of the cord to the handset.

6 Plug the AC Power adapter into the telephone base and the other end into an AC outlet.

All hard key indicator lights and soft key icons flash to indicate the phone is powered but not initialized. See Initializing an IP phone, and continue the installation.

—End—

Carrier VoIP

CICM Configuration Management

Publication: NN10240-511
Document status: Standard
Document version: 07.02
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.