CICM Series 6.12 Product and Technology Fundamentals

Purpose

This document describes the hardware components, software components, and user interface of the Series 6.12 Centrex IP Client Manager (CICM) product.

Audience

The intended audience for this document is the administrative and maintenance personnel of the CICM in both International and North American deployments.

Document structure

Document suite

Previous to this CICM 6.12 release, the CICM product was described in one document, *NN10027-111 CICM Product and Technology Fundamentals*, which contained seven sections: *Overview*, *Configuration, Security and Administration, Performance, Fault, Accounting*, and *Upgrade*.

With this 6.12 release, the *NN10027-111 CICM Product and Technology Fundamentals* is now published as seven separate documents, collectively known as the CICM document suite. These seven documents are:

- *NN10044-111 CICM Product and Technology Fundamentals*
- *NN10240-511 CICM Configuration*
- *NN10252-611 CICM Security and Administration*
- *NN10248-711 CICM Performance Management*
- *NN10233-911 CICM Fault Management*
- *NN10244-811 CICM Accounting*
- *NN10230-461 CICM Upgrades*

Document outline

This *NN 10044-111 CICM Product and Technology Fundamentals* document provides an overview of the CICM 6.12 product. It is organized into the following sections:

Purpose Provides a statement of document purpose.

Audience Defines the intended audience of the document.

Document structure Defines the document structure.

References Provides the key references for the user.

Terminology Provides a brief reference guide for terminology used throughout the document suite.

Introduction to CICM Provides an introduction to the CICM, including a description of Centrex, Voice over IP, and Call Server 2000.

Centrex features Provides a description of Centrex features.

CICM 6.12 Describes the CICM 6.12 product, and provides a description of the new and enhanced features as compared to the last (CICM 2.5) release.

Engineering information Defines the platform for the 6.12 CICM, including software loads and central office requirements, and briefly describes the Admin and Client LANs, security approaches, performance criteria and other engineering considerations.

International and North American products Compares the differences between the International and North American versions of the CICM.

Hardware Details the hardware components, configuration and capabilities.

Software Defines the software loads, delivery, upgrades and patches.

CICM clients Describes the CICM clients.

User interfaces Describes the primary and alternative user interfaces.

Network interfaces Defines the IP and Succession network interfaces.

Protocols Provides a summary of the protocols used by the CICM.

CICM configuration data Provides an overview of configuration management of the CICM.

CICM line maintenance Provides an overview of line maintenance for the CICM, including line provisioning of CICM clients.

Customer resources Provides additional customer resources.

Appendix A Glossary

References

The *NN10027-111 CICM Product and Technology Fundamentals* is now published as seven separate documents, collectively known as the CICM document suite. These seven documents are:

- ***NN10044-111 CICM Product and Technology Fundamentals***
- ***NN10240-511 CICM Configuration***
- ***NN10252-611 CICM Security and Administration***
- ***NN10248-711 CICM Performance Management***
- ***NN10233-911 CICM Fault Management***
- ***NN10244-811 CICM Accounting***
- ***NN10230-461 CICM Upgrades***

For information about the m6350 SoftClient and TAPI service provider, refer to:
NN10182-113 CICM m6350 Client Installation Guide,
NN10183-114 CICM m6350 SoftClient Branding Kit, and
NTP 297-5551-901 m6350 TAPI Service Provider Installation and Troubleshooting Guide.

For information about the CS2000, refer to:
CS2000 Product Description

For information about the i200X clients, refer to:
NN10027-113 CICM Etherset Installation Guide and User Manual

For engineering information and specifications to support VoIP, refer to:
NTP 297-5551-100 Centrex IP Client Manager Engineering Guide

For information on Microsoft Windows NT, refer to the Microsoft Web site:
http://www.microsoft.com/ntserver/

For information about the CICM chassis and processor card, refer to: ***http://www.mcg.mot.com/us/products/docs/pdf/cpx1205i.pdf***, and ***http://www.mcg.mot.com/us/products/docs/pdf/cpv5370a.pdf***

For information about Centrex feature support, refer to: ***Centrex Feature Support on Centrex IP Client Manager***

Terminology

This section is a reference guide for terminology used throughout this document.

Admin LAN

The Administration network infrastructure (Admin LAN) is a local area network (LAN) that the CICM connects to. The Admin LAN is usually the service provider's existing central office LAN.

CICM and client configuration and monitoring functions are performed via the Admin LAN. These functions cannot be performed via the CICM itself.

Centrex IP Client Manager (CICM)

The CICM refers to a single SAM 16 chassis containing two processors running as a single network entity (one CPU is the master, the other is a warm-standby slave). The term "CICM" is synonymous with gateway in a CICM environment.

Chassis

The CICM is hosted on a Motorola CPX8216T chassis. The terms gateway, chassis, and CICM may be used interchangeably.

Chassis domains

A chassis consists of two CompactPCI domains, referred to as Domain A and Domain B (or node A and node B).

The two domains of a single chassis provide a high availability (but not fault tolerant) host architecture for CICM software.

Each chassis domain contains a CPV5370 processor card (CPU), and a hot swap controller (HSC) card.

CICM-MG

Centrex IP Client Manager - Media Gateway (CICM-MG) is the Succession variant of the CICM.

The Succession variant of the CICM is not strictly speaking a "media gateway." It is better described as a "terminal server" or "signalling

gateway” as there are no media processing resource cards in the Succession CICM frame. Despite this, the term “media gateway” most closely describes the role of the CICM as it fits into a Succession network. The Succession variant of the CICM is therefore referred to as the CICM-MG, and the TDM variant of the CICM is referred to as the CICM-TDM.

Client LAN

The CICM is connected to a Client LAN that supports the CICM clients: the m6350 SoftClients or i200x Ethersets.

Since public interfaces of the CICM belong to the Client LAN, for security purposes there is no access to the Admin LAN from the Client LAN.

CXIPNET

CXIPNET is a software utility that monitors the state of the network by continuously sending small UDP packets to the mate node. These packets contain state information about the node, so CXIPNET is also used for obtaining information about the software running on the mate node (e.g. version or current activity state information).

DNR

Dual Node Redundancy. A key feature of CICM 6.12 designed to provide fault tolerance on the new Succession architecture (as well as the TDM architecture in SN07.

E1/T1 CICM

CICM is designed for both the International and North American markets. In the International product, the CICM connects to a PLGC via an E1 link. In the North American product, the CICM connects to an LTC or LGC via a T1 link. When it is necessary to refer specifically to the International or North American version of the product, they will be referred to as the E1 CICM or T1 CICM, respectively

EBS

Electronic Business Set. An name used for Nortel Centrex line terminals in its initial deployments. Also referred to as Meridian Business Set (MBS), or Peripheral Phone (PPhone).

Element Manager

The Element Manager (EM) is the device used to configure, monitor, and manage a group of CICMs and their clients. The EM is based on a Motorola 5370 processor board in a CPX8216T 4-slot cPCI chassis, and can be ordered as part of the 19” cabinetized frame containing one or more CICMs.

Frame

The frame refers to a single 19” frame or cabinet that is fitted with up to two CICM chassis, an Element Manager, and support equipment (e.g. power distribution).

Gateway

The gateway refers to the contents of a single SAM 16 chassis containing two processors running as a single network entity. The term is synonymous with CICM in a CICM environment.

LGC

The Line Group Controller (LGC) is a peripheral that the CICM connects to for the North American market. The LGC provides T1 connectivity.

LTC

The Line/Trunk Controller (LTC) is a peripheral that the CICM connects to for the North American market. The LTC provides T1 connectivity.

MBS

Meridian Business Set. The Nortel brand name for M6320, M5216, etc., the electronic keyset terminals used for delivering Centrex services.

MGC

Media Gateway Controller. The MGC replaces the DMS for Series 6.12.

Nodes

Each chassis domain contains a CPV5370 processor card. This card hosts the Windows NT Embedded operating system and CICM software. The card and its software is referred to collectively as a node.

North side

The GWC facing side of the CICM.

PLGC

The PCM-30 Line Group Controller (PLGC) is the line peripheral that the CICM supports in the International markets. The PLGC provides E1 link connectivity.

South side

The terminal facing side of the CICM.

VLCM

A Virtual Line Concentrating Module or Virtual LCM is an emulation of a DMS Remote Line Concentrator Module (RLCM). A single CICM can support multiple VLCMs, thereby representing to the DMS a number of RLCM peripherals.

VMG

A Virtual Media Gateway emulates multiple instances of media gateways. It is supported by the Media Gateway Manager component.

Introduction to CICM

The CICM delivers Centrex capabilities to users connected to an IP network, using VoIP technology.

Centrex

Centrex is an abbreviation for “Central Office exchange service.” Centrex is a set of capabilities that allows a Succession platform to make Private Branch Exchange (PBX) facilities directly available to Meridian Business Set (MBS) lines.

Centrex provides the following benefits:

- Eliminates the requirement for installation and maintenance of PBX hardware
- Provides a wider choice of features than a PBX can support, such as Automatic Call Distribution, Call Forwarding, and Conference Calling
- Provides automatic access to switch upgrades

Refer to the **www.NortelNetworks.com** Web site for a complete list of Centrex features.

Voice over IP

Voice over IP (VoIP) is a technology that allows voice to be carried over a data network. Analog voice signals are digitized, compressed, and transmitted as internet protocol (IP) packets over an IP network.

Some of the benefits of VoIP are:

- **Universal access:** The network over which VoIP calls are carried can be any kind of IP data network (e.g. corporate intranet, corporate Local Area Network (LAN), corporate Wide Area Network (WAN), dial-up modem or cable modem).
- **Cost reduction:** Corporations can move voice traffic onto their existing data network, thereby reducing the cost of long distance and international calls.

- **Consolidation:** The merging of voice and data traffic onto a single network.
- **Increased efficiency:** Compression of the digitized voice traffic results in more efficient use of bandwidth on the combined voice/data network.

A VoIP call can be initiated from:

- A PC equipped with suitable IP telephony client software (such as the m6350 SoftClient), or
- A LAN-capable telephone (such as the Nortel i200x Etherset).

An IP gateway provides various functions for telephony, such as:

- Conversion between Media Gateway and IP
- Compression and decompression of digitized signals
- Connection and negotiation
- Configuration and administration functions
- Access control
- Additional non-voice services

CICM

The CICM provides the control interface between the GWC and distributed CICM IP clients on a managed IP network. It communicates with the GWC using the H.248 IP interface.

H.248 is a joint ITU-T / IETF protocol defined in ITU-T Recommendation H.248 and IETF RFC3015. It fully supports the same basic device/media control capabilities as protocols such as ASPEN. More importantly, it is based on a more flexible functional mode that provides better support for multimedia and conference capabilities.

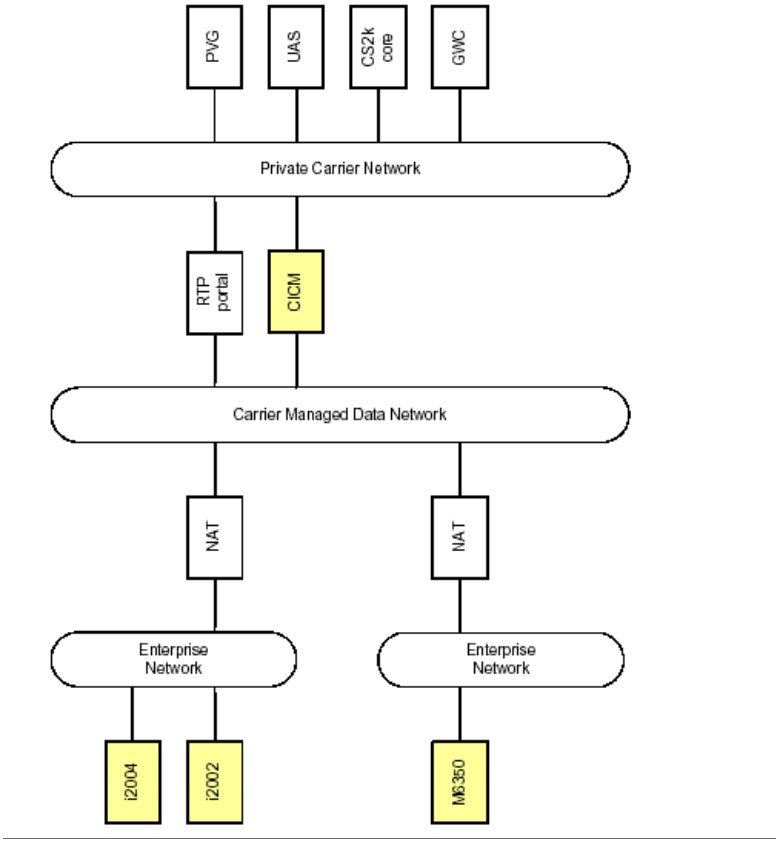
The CICM is not a media gateway. It is better described as a terminal server or signaling gateway. Media streams in a Succession IP solution are routed directly between media end-points. The CICM terminals (e.g. i2004 Internet Telephone) are media end-points. Other media end points in a Succession IP network include:

- Analogue line gateways (e.g. MG9000, Mediatrix 1124)
- Voice processing servers (e.g. UAS)
- IP Terminals hosted off another CICM

The following Figure 1 shows a generic succession IP network with a CICM serving IP terminals in two enterprise customer networks. The

finer details of network engineering are not included in this diagram; it is provided to illustrate general connectivity only. All OAMP devices and networks are also omitted from the diagram.

Figure 1 Role of the CICM and clients in a Succession network



The CICM acts as a “lights out” server. That is, it has no monitor, keyboard, or mouse. Once it is connected and powered up, all maintenance is performed remotely from a PC on the Admin LAN, via a Web-based interface, using the procedures provided in the CICM document suite.

The Centrex IP Client Manager (CICM) product delivers Centrex capabilities to users connected to an IP network, using VoIP technology.

The CICM performs the following functions:

- Provides the interface between the Centrex feature set and an IP network
- Transcodes voice between IP data from the client network and PCM data from the Succession XPM.

The CICM consists of the following components:

- One Motorola SAM 16 chassis hosting the CICM software, containing a pair of CPU cards
- The Element Manager (EM), which provides the functionality to configure and monitor CICMs and their clients
- Client hardware and software

CICM clients

The CICM client is the mechanism that allows a user to initiate and receive VoIP calls, and to receive Centrex features from CS2K. CICM clients are called clients, terminals, or client terminals.

Two types of CICM client are supported:

- The m6350 SoftClient application, which is an IP telephony software client installed on a PC (with Windows 2000 operating system) attached to a LAN. It works with a headset and adapter which plugs into a USB port on the PC.
- The Nortel Networks i200x Etherset telephones, which connect directly to a client LAN or to a telephony switch module. The i2002 and i2004 models are supported.

CICM and the IP network

The CICM connects to clients using the IP protocol on its client side network interface. IP connectivity is provided by 100baseT Ethernet.

The CICM controls terminals using the Nortel Network's proprietary Unified Network IP Stimulus (UNIStim) protocol.

Note: The Unistim protocol that carries information about client key presses between the client and the CICM is not secured. In order to ensure operational security, it is recommended that the CICM be situated in a secure telco WAN or an enterprise LAN, rather than on the public Internet.

Voice is encoded using one of three standard voice encoding algorithms: G.711, G.729 or G.723.1. The encoded voice packets are transmitted across the IP network using the RTP protocol.

Refer to the *Centrex IP Client Manager Engineering Guide* for a detailed description of CICM network engineering.

Call Server 2000

CS2000 (CS2K) is a communication server providing call processing capabilities. In terms of the MEGACO network architecture, it provides

Media Gateway Controller (MGC) functionality. Together with various types of gateway and server, it can support VoIP or VoATM (Voice over ATM), depending on the type of backbone packet network to be used.

A CS2K can be regarded as a single node, but it is composed of separate components. The CS2K capabilities listed below are provided by separate CS2K components, of which the most important are Gateway Controllers (GWCs). The GWCs are used for two main purposes:

- To serve as controllers for media gateways, controlling their operation via device/media control signalling based on packet network protocols.
- To support communication between peer communication servers for the handling of networked calls. This is accomplished via inter-CS signalling, also based on packet network protocols.

CS2K capabilities include:

- Basic connectivity and network element control
- Call processing
- Service support

CS2K Connectivity and network element control
CS2K provides for control over the media gateways that provide the bearer connection interface between the packet network environment and other TDM or access networks. In ISN06, CS2K supports the following types of access via media gateways:

- CCS7 trunk access to/from the PSTN or another TDM network
- PRI and QSIG access for digital PBX's and other PRI-enabled devices
- V5.2 access, currently for analog subscriber lines only
- Analog line access via a variety of gateway types, including CPE gateways attached to customer LANs or cable networks
- ADSL access via terminations on high-capacity line media gateways

CS2K call processing
Call processing capabilities of CS2K include:

- A wide range of internationally proven call processing agents and protocols
- Translations and routing for calls entering, leaving, and crossing the packet network

- Support for requests to apply tones and announcements
- Support for billing, event reporting and performance monitoring

CS2K service support

CS2K service support capabilities include:

- Support for specific sets of value-added features
- Support for general-purpose service delivery platforms
- Support for regulatory features (e.g. number portability)

Centrex features

This section describes Centrex feature support, Centrex IP enhancements over Centrex, and restrictions of Centrex feature support.

Centrex feature support

A client connected via the CICM appears to the CS2K as a conventional Meridian Business Set (MBS) line agent. Most call types and Centrex features that can be provisioned on an M5216 business set are supported by a CICM client, with a few restrictions. (For example, a CICM client can be provisioned as an ACD client in exactly the same manner as an M5216.)

The following table lists Centrex features and indicates whether the feature is supported or not supported for CICM 6.12. System, attendant console, and some ACD features are not supported.

Table 1 Centrex feature support

Feature Name	Supported
Call Disposal Features	
Call Hold	Y
Permanent Hold	Y
Call Waiting / Camp-On for Business Set (BS)	Y
Dial Call Waiting / Dial Call Waiting for BS	Y
Call Waiting Originating / Call Waiting Originating for BS	Y
Blind Transfer Recall	Y
Blind Transfer Recall Identification	Y

Table 1 Centrex feature support

Feature Name	Supported
Call Park / Call Park for BS	Y
Directed Call Park	Y
3-Way Calling / Call Transfer for BS	Y
Call Pickup Features	
Call Pickup / Call Pickup for BS	Y
Directed Call Pickup, No Barge-In	Y
Call Forwarding Features	
Call Forward / Call Forward for BS (unconditional)	Y
Call Forward / Call Forward for BS (busy)	Y
Call Forward / Call Forward for BS (doesn't answer)	Y
Call Forward / Call Forward for BS (station activation)	Y
Speed Calling Features	
Speed Calling / Speed Calling for BS (individual short list)	Y
Speed Calling / Speed Calling for BS (individual long list)	Y
Business Set Display and Function Key Features	
Six-Port Conference (MBS)	Y
Ring Again Features	
Ring Again / Ring Again for BS	Y
Single Digit Activation of RAG/CBWF	Y
Network Ring Again	Y
Automatic Call Distribution (ACD) Features	
Answer Agent Key (AAK)	Y

Table 1 Centrex feature support

Feature Name	Supported
ACD Not Ready (ACDNR)	Y
Answer Emergency Key (AEMK)	N
Agent Status Lamp (ASL)	Y
Call Agent (CAG)	Y
Controlled Interflow (CIF)	Y
Call Supervisor (CLSUP)	Y
Display Agent Status (DASK)	Y
Display Queue Status (DQS)	N
Display Queue Threshold (DQT)	N
Extended Call Management (ECM / ICM)	N
Emergency Key (EMK)	N
Forced Agent Availability (FAA)	Y
Line of Business (LOB)	Y
Night Service (NGTSRVCE)	Y
Observe Agent (OBS)	N
Supervisor (SUPR)	Y
Uniform Call Distribution (UCD) Features	
UCD Login (UCDLG)	Y
UCD Logged In Indication (UCDLI)	N
UCD Signal Distributor (UCDSD)	N
Miscellaneous Features	
Bridged Night Number (BNN)	Y
Automatic Recall (AR)	Y

Table 1 Centrex feature support

Feature Name	Supported
CLI with Flash/Malicious Call Hold/Malicious Call Hold for BS	Y
Distributed Line Hunt (DLH)	Y
Directory Number Hunt (DNH)	Y
Multiple Appearance Directory Number (MADN)	Y
Meet-Me Conference (MEETME)	Y
Multi-Line Hunt (MLH)	Y
Make Set Busy (MSB)	Y
Make Set Busy Intragroup (MSBI)	Y
Message Waiting Indication (MWIDC)	Y
Preset Conference (PRESET CONF)	N

The complete list of Centrex features is provided in the feature library, which is available on the **http://www.nortelnetworks.com/products/01/centrex/library/overview/** Web site. A search tool is available that will provide a feature description for each feature name entered.

Centrex IP enhancements over Centrex

Centrex IP provides the following capability enhancements over the standard Centrex:

- **Geographical freedom.** A user can log on and access their Centrex services from any location that has IP connectivity with the CICM.
- **Choice of client.** Users can choose between the SoftClient or two versions of the physical etherset: the i2002 or i2004. An etherset is recommended for a user based at one location, and the SoftClient is recommended for mobile users to access from a variety of locations.
- **Hot desking.** A user can log in to any terminal connected to the CICM. This provides flexibility and avoidance of costs normally associated with intra-site staff moves.

- **Selective CICM login.** The selective CICM login feature allows a user to log in to a selected CICM from a group of CICMs, and log in to any terminal connected to the selected CICM. Enterprise Profiles allow the administrator to define groupings of CICMs and associated users.
- **Integration of CICM and PC desktop software.** An interface between the terminal and the PC software allows for CICM and PC integration. For example, within Microsoft's Outlook PIM, the user can set up a call by clicking on the person's contact details.
- **Address book for contact numbers.**
- **A list of recent incoming and outgoing calls.**
- **Function key lamp cache.** On a regular MBS set, unplugging the set looses all lamp states. On a CICM client, the status of all function key lamps is cached in the CICM on a per-line basis. When a previously disconnected client is reconnected, the lamp status for features such as call forwarding, message waiting, etc. is correct.

Restrictions to Centrex feature support

System and attendant console Centrex features are not supported.

Although client development is focussed toward presenting an exact replica of MBS terminal functionality over an IP network, client services are subject to certain restrictions. These restrictions are due to the differences in the service paradigm between the physical line interface of conventional Centrex and the network data connection of the CICM.

Certain features (such as Distinctive Ringing) may not operate in the same way, or may be disabled. For example, if local ringing is configured for i2004 sets, distinctive ringing and ring back tones may not originate locally on the set itself, but may originate from the UAS instead. Also, features which involve a one-way speech path as one of their stages will not work exactly as intended with CICM clients because two-way speech is currently enabled by default as soon as a call is received and answered. This applies to features such as Intercom (OCM), Group Intercom for BS (GIC) and Group Intercom All Call (GAC).

The i2004 has 6 feature keys. Up to 11 features are available from these 6 keys by using the page up/page down keys. The i2002 has 4 feature keys and acts in a similar manner.

The Call Server can support multiple feature assignments to each feature key, but the CICM supports only one feature assignment per key.

The following restrictions apply only to the m6350 client:

- The speech path represents the headset mode of MBS operation. Hands-free mode is not directly supported by the m6350, since hands-free operation can be simulated using the speaker/microphone hardware on the PC platform.
- Incoming ringing and ringsplash are implemented in the following two ways simultaneously:
  - a pop-up dialog box
  - an audio prompt from the client PC system speaker

CICM 6.12

The CICM 6.12 release represents the evolution of the CICM from the TDM version to a Succession based CICM. To accomplish this evolution, much of the CICM architecture has been re-organized. The reorganization more readily allows the C-side facing components of the CICM to be replaced and/or adapted to use the H.248 protocol and Succession call control methodology.

The Succession variant of the CICM is not strictly speaking a “media gateway.” It is better described as a “terminal server” or “signalling gateway” as there are no media processing resource cards in the Succession CICM frame. Despite this, the term “media gateway” most closely describes the role of the CICM as it fits into a Succession network. Hence the Succession variant of the CICM is sometimes referred to as the CICM-MG, and the TDM variant of the CICM is referred to as the CICM-TDM.

CICM 6.12 New Features and Enhancements

To accomplish this evolution of the CICM from the TDM version to a Succession based CICM, much of the CICM architecture has been re-organized.

The CICM Series 6.12 contains the following new features:

- Base Re-architecture
- Succession Architecture
- Authority component of Gateway Services
- Audio Tones Profiles
- SDP Negotiation
- Dynamic Feature Keys
- CxipNet and Gateway Services Enhancements

- Dual Node Redundancy
- Multi-tenanted Enterprise Support (VMG)

Base Re-architecture feature

The Base Re-architecture feature addresses the re-architecture of the base CICM software to support a single software stream for both TDM and CS2K versions. Much of the core CICM functionality is common between the TDM and CS2K product variants, so a single software stream will significantly reduce the support required.

The purpose of this feature is to change the base architecture to support the addition of new components that will provide the interface to the CS2K. This feature does not explicitly discuss the design of those components.

Re-architecture for Succession

In Succession, the CICM interfaces to the CS2K via a Gateway Controller (GWC). From a signaling perspective, the GWC performs a role analogous to the PLGC/LTC in the TDM product. The CICM presents itself to the GWC as a line gateway, and operates at a level similar to an LCM in the TDM product.

Figures 2 and 3 below illustrates TDM and CS2K CICM networks, respectively, for comparison purposes. In a CS2K network, the GWC controls the CICM using the H.248 call signaling protocol. PPhone messaging primitives are tunneled between the GWC and CICM using a custom H.248 package.

Figure 2 TDM CICM connectivity

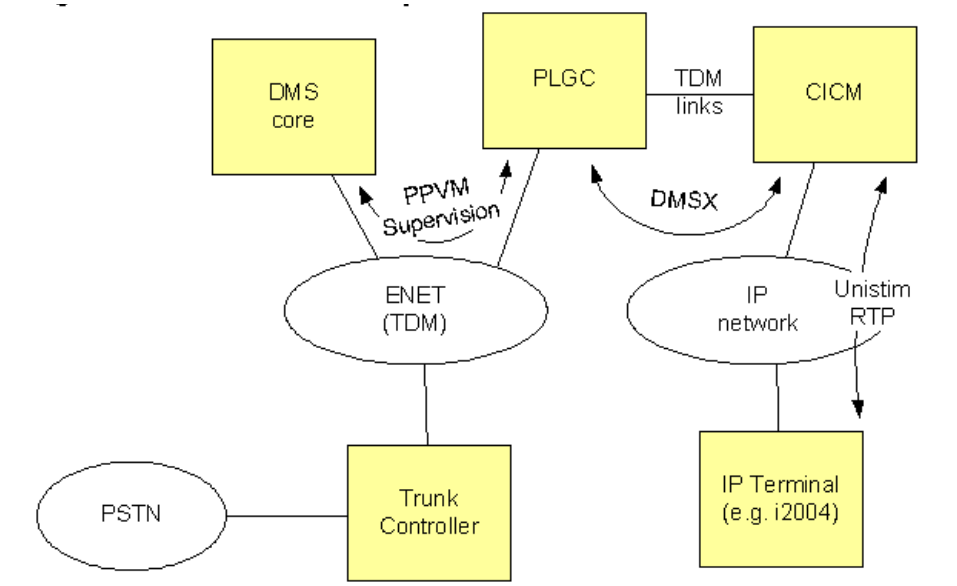
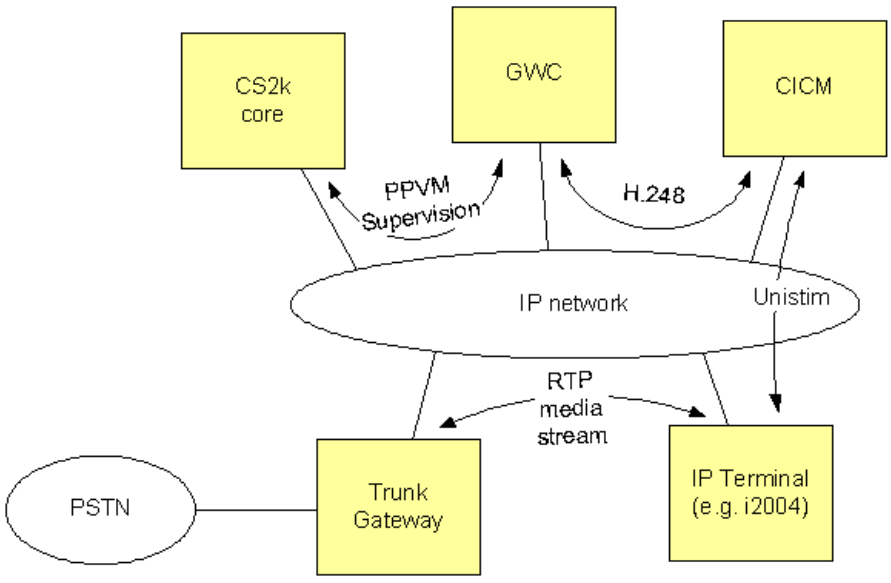


Figure 3 CS2K CICM connectivity



Neither the CICM nor the GWC processes media packets in the Succession network. In Succession, the CICM is not a gateway. A gateway provides interworking across different media boundaries (e.g. Media Gateway to ATM or IP). The CICM provides a virtual emulation of Meridian terminals, driven by the PPhone stimulus received by the GWC. CICM projects the functions of these virtual terminals, to terminals out in the network using the Unistim protocol. The packets

forming the media stream for a call are routed directly between the two end-points of the call.

For example, these two end points could be:

- two IP terminals connected to a homogeneous network
- an IP terminal and a gateway providing access to a Media Gateway network or POTS terminals
- an IP terminal and a gateway providing secure interworking to another IP network

CICM core services

There are six core services that make up the CICM software load. These services are controlled (started, stopped and upgraded) by another service, CXIPBOOT. These core services will remain unaltered for CICM 6.12 release, except for CXIPNET and Gateway Service enhancements.

These seven services are:

- **CXIPBOOT**
  The CXIPBOOT service is automatically started when the OS has booted. CXIPBOOT is used to start, stop and upgrade the other software components on the CICM node.
- **CXIPAGT (CXIP01)**
  The CXIPAGT service provides SNMP services for the CICM. It polls critical system functions and sends traps when thresholds are exceeded. It also responds to SNMP Get and Set functions from SNMP clients in the network.
- **CXIPNET (CXIP02)**
  The CXIPNET service maintains a routing path between the two nodes of the CICM. It monitors the two network interfaces on each port of each CPU, and selects the most appropriate route for inter-unit messaging.

  CXIPNET monitors the state of the network by continuously sending small UDP packets to the mate node. These packets contain state information about the node, so CXIPNET is also used for obtaining information about the software running on the mate node (e.g. version, current activity state).

  See the CXIPNET enhancements section below for a description of enhancements for CICM 6.12.

- **Chassis Manager (CXIP03)**
  The chassis manager is responsible for maintaining the resources provided by the chassis. Its functions include:

  — controlling the LEDs on the alarm panel

  — monitoring the temperature of the CPUs and adjusting the fan speeds accordingly

  — monitoring the chassis fans for failures

  Other software components on the CICM are responsible for changing the state of the alarm panel; the chassis manager simply provides the hardware control to change the LED state.

  Hardware restrictions require that only the chassis manager on Node A can control the system status LEDs on the alarm panel, so the chassis manager service on Node B continually communicates with the chassis manager service on Node A to ensure the alarm state is correct. When Node A is out of service, the system status alarm LEDs are left in an indeterminate state.

  Changes to the LEDs on the alarm panel are also written back into the MIB so that they can easily be displayed on the CICM-EM.

- **MibSync (CXIP04)**
  The MibSync service has two roles. At system startup, it is responsible for performing a bulk synchronization of the MIB data with the mate node. While the system is running, it acts as a server for replication requests from the mate node.

- **UFTP server (CXIP05)**

  The Unistim File Transfer Protocol (UFTP) service provides two functions for terminals:

  — firmware upgrades

  — configuration services for the M6350 soft client

- **Gateway Service (CXIP06)**
  The Gateway service performs the bulk of the processing on the CICM. All the other services listed here can be considered auxiliary services to the Gateway service.

  The Gateway service itself is a simple process that launches and monitors four sub-components: Media Control, VMG, Lines, and Sessions. If one of these sub-components terminates unexpectedly, the Gateway service initiates a system reset to attempt to regain service.

  Each of the sub-components is controlled through an interface called IAdmin. IAdmin has methods to initialize, start, shutdown,

stop and query the status of the sub-components. It can also be used to notify the subcomponents of significant events such as the mate node starting up or shutting down.

See the Gateway Service enhancements section below for a description of enhancements for CICM 6.12.

CICM Miscellaneous services

The following miscellaneous services will also remain unaltered for CICM 6.12 release:

- **PREBOOT**
  The PREBOOT utility is used to provide the initial configuration of the CICM (e.g. network identity) after a node as been provided with an initial software image. It is executed directly on the command line through a Telnet session.
- **CXIPDBGLOG**
  The debug log service is automatically started when the OS has booted. It spools system debug outputs to a set of rotating files.
- **CENTREXIPMIB**
  CENTREXIPMIB provides a scriptable interface to configure and administer the CICM node from the CICM-EM. It is launched upon demand by the system.

  The RemoteMib component exported by CENTREXIPMIB provides facilities to query the MIB data in XML format. It also provides functions for updating, creating and deleting MIB nodes and attributes.

  The RemoteAdmin component exported by CENTREXIPMIB provides access to administration functions. It can be used to stop and start the services on the CICM node and control subsystems within these services. It also acts as an interface for CXIPBOOT to perform software upgrades.
- **CXIPMATEPROXY**
  CXIPMATEPROXY fields all DCOM requests from the mate node and proxies them to the appropriate component on the local node. It is required because DCOM bindings cannot be reset when IP addresses have to be moved to maintain inter-node communication after network elements have failed.

  CXIPMATEPROXY is launched automatically on demand by the system. It is terminated by CXIPNET when address bindings change, which causes a new instance to be created using the new bindings.

CXIPNET Enhancements

The CXIPNET service has been enhanced for the new architecture. The CXIPNET component advises the Gateway manager component of mate state change events. Such events directly result in various actions that must be performed by subcomponents. (For example, during a controlled Switch of Activity (SWACT) the transition must be done using multiple steps. All this is controlled by the CXIPNET component.)

The CICM communicates with the GWC using a single IP address and port. The two redundant halves of the GWC are managed in a hot-standby configuration so that the address is always available.

The GWC expects gateways to present a single IP address and port for signaling. Therefore in the new 6.12 architecture, CICM dynamically binds the IP address to one or the other CICM node, depending on network connectivity and node state.

CXIPNET constantly monitors network connectivity and the state of the mate node and manages the election of a single master between the pair of nodes. Both of these functions (monitoring connectivity and managing the master election) are key to providing IP address sharing across the nodes.

> ***Note:*** Master/Slave elections are not dependent on the state of the gateway service; they only depend on the status of the CXIPNET on each node. Therefore it is recommended to watch out for both nodes starting up simultaneously, and during a controlled shutdown.

CXIPNET has been enhanced so that applications can request particular IP addresses that are bound to specific adapters. CXIPNET provides facilities to automatically manage the binding across the two nodes.

Gateway Service enhancements

The key features and enhancements of the Gateway Service components are:

- The login control functionality has been moved from the Lines component to the new Authority component.
- A new Terminations component is provided that acts as the common interface to the CS2K specific components. The overall architecture has been improved by providing all Pphone specific functionality in the Terminations component rather than having a split between the Lines and Sessions components.

- The Media Control component is unchanged in the new architecture. The Lines component acts as a bridge between the existing Media Control component and the new Terminations component.
- The new Terminations component provides an interface for dynamically adding and removing media gateways to the system, while maintaining service on the other gateways.

Terminations component

The Terminations component of the Gateway Service provides a single generic interface for media gateway instances. The Terminations component expects media gateways to implement a single generic interface for communications in the opposite direction. The methods of these interfaces provide a superset of functionality required by the CS2K media gateway components.

The following new facilities have been added in CICM 6.12:

- The capability of the terminal to generate a range of tones.
- Support for multiple simultaneous audio streams being directed to a single terminal. Only one audio stream can be active.
- New interfaces to drive the sessions at a functional level rather than having the session process Pphone primitives directly (e.g. UpdateFeatureIndicator and DisplaySetLine)].

Succession Architecture feature (CICM-TDM re-architecture for Succession CICM)

This feature evolves the TDM version of the CICM to a Succession based CICM, by developing and incorporating the components and functionality required for a Succession CICM.

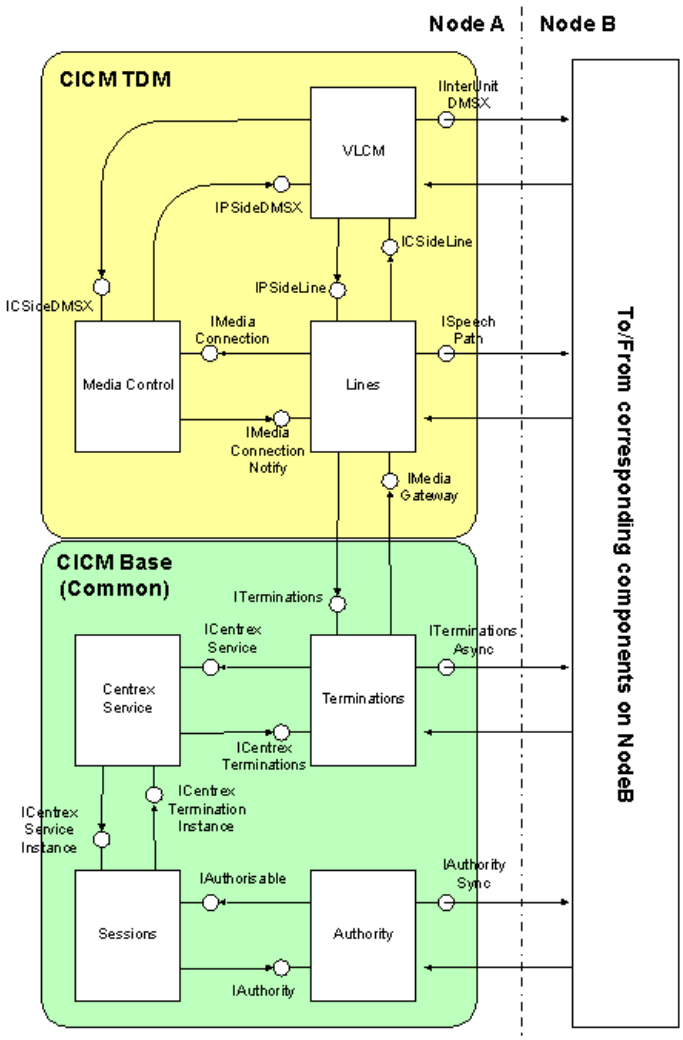
In order to accomplish this evolution, much of the CICM architecture has been re-organized. The re-organization more readily allows the C-side facing components of the CICM to be replaced and/or adapted to use the H.248 protocol and Succession call control methodology.

The new architecture of the TDM variant of the CICM (which will be available in the SN07 release) is summarized in the following Figure 4, *Architecture of CICM-TDM*. The various components that make up the system are now organized into two layers. The TDM specific components (in the upper yellow frame) encompass the DMSX protocol functionality needed to communicate with the DMS as well as the media control component that manages the TDM and DSP cards.

The CICM base components (in the lower green frame) encompass the

functionality common to both TDM and Succession variants of the CICM product, such as session management and authentication.

Figure 4 Architecture of CICM-TDM



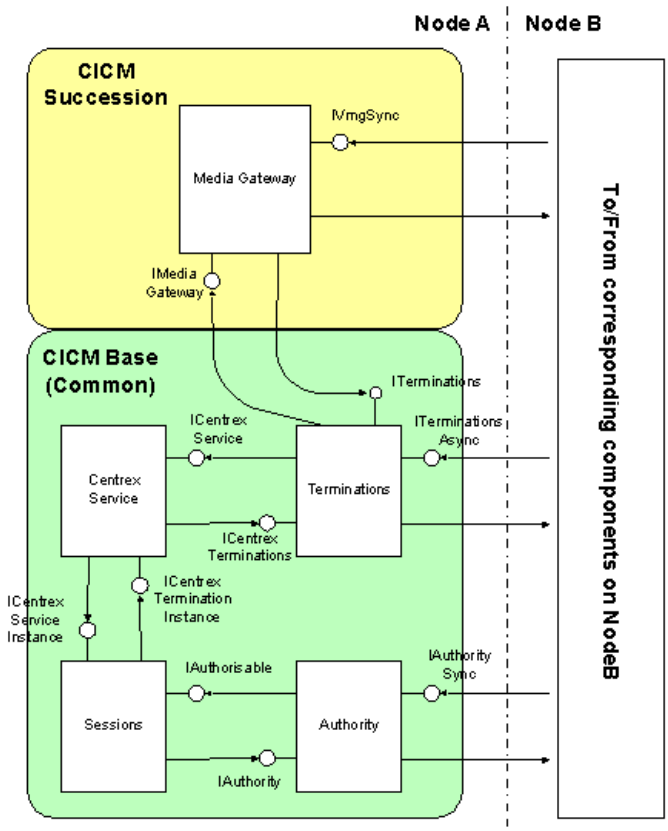
There are two parts of this re-architecture that is relevant for this SN06.2 release and beyond:

- the new Terminations component
- the modification to the existing Lines component

Much of the functionality of the old Lines component that is common to both variants of the CICM has been moved to the new Terminations component. This now allows for the natural evolution of the product to support Succession by simply removing the TDM specific components and replacing them with a Succession equivalent. This is illustrated in the following Figure 5, *Architecture of Succession CICM*.

The Succession specific component (layer) of the CICM is contained within the yellow area in Figure 5. Components that are part of the base layer (in green) will only be discussed in this document as needed to address Succession specific issues.

Figure 5 Architecture of Succession CICM



Note: Figure 5 is a simplified view of the actual system architecture for purposes of discussion. It is not intended as the true architecture that incorporates VMG support.

Since media streams do not traverse a Succession CICM, there are no hardware resources (DSPs, etc.) to manage. The primary responsibility of the Succession specific layer of the CICM is communication to the GWC using the H.248 protocol.

Media Gateway

The central component of this Succession CICM architecture is the integration of the Media Gateway (MG) and its associated elements. The MGF includes the H.248 stack and the functionality needed by any Media Gateway.

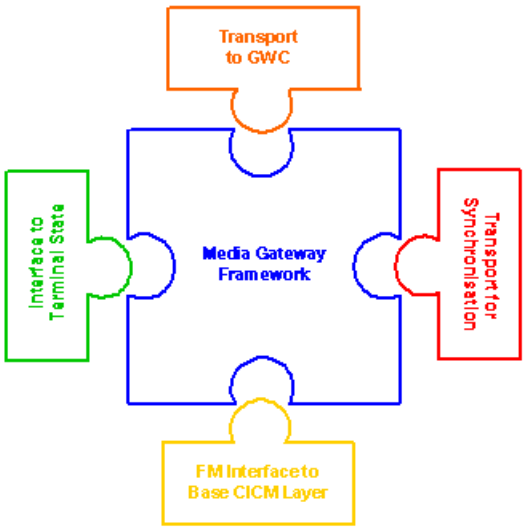
The Media Gateway Framework (MGF) is a term referring to what is commonly called the “H.248 stack.” Since this component also implements everything else needed by a Succession media gateway, this document will refer to it as the MGF.

The functionality provided by the MGF is:

- parses incoming H.248 messages from a GWC
- generates outgoing H.248 messages to the GWC
- manages call contexts (including the NULL context)
- manages physical, ephemeral and the root terminations (including state)
- isolates “hardware specific” details from the core H.248 functionality by providing “neutral” interfaces
- implements a synchronization mechanism with a peer MG
- provides QoS reporting abilities

The Media Gateway Framework is illustrated in the following figure.

Figure 6 Media Gateway Framework



The MGF allows the following platform-specific components to be implemented by the CICM:

- Transport layer to GWC. Transport mechanism to communicate with GWC.
- Transport layer to mate node. Transport mechanism to communicate with mate node (call state synchronization).

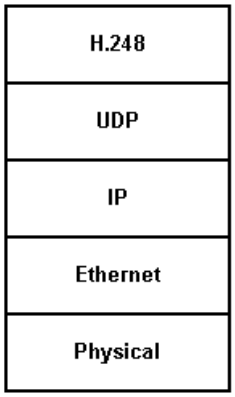
- Functional Manager (FM) layer. Functional Managers are required to process telephony primitives.
- Service state controllers
- System timers
- Error handlers

Transport layer to GWC

The MGF makes no assumption about the mechanism used to send and receive H.248 messages to and from the GWC. It is up to the platform to provide this mechanism and pass received H.248 from the GWC to the framework, and vice versa.

Since the CICM works in an IP based Succession network, it uses UDP over IP as its transport mechanism to the GWC. UDP is used because H.248 provides its own reliability mechanism. The H.248 protocol stack is illustrated in the following figure.

Figure 7 H.248 Protocol Stack



Transport layer to mate node

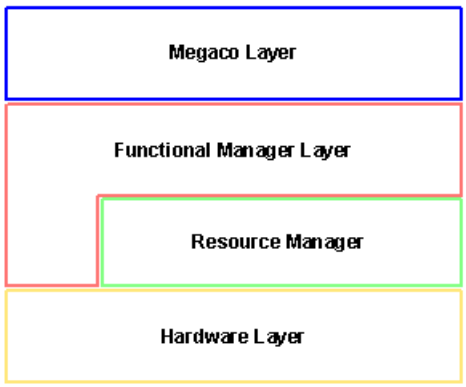
The MGF assumes the existence of an inactive mate node. The inactive node is intended to take over the call processing function in the event of a failure of the active node. For this purpose, the active node constantly maintains the inactive node in a synchronized state with itself by sending it each successfully processed H.248 message. In this manner, the inactive node's data structure contents exactly matches those of the active node.

To send H.248 messages to the mate, the CICM must provide a transport mechanism to the MGF. In keeping with the existing design of the CICM, a COM interface is used for this purpose. The interface is named IVmgSync and supports a single method called SendMsg.

Functional Manager layer

The Functional Manager (FM) layer is the most important aspect that the CICM must implement for the MGF. The following figure illustrates the relationship that exists between the various call processing layers of the MGF.

Figure 8 MGF Call Processing Layers



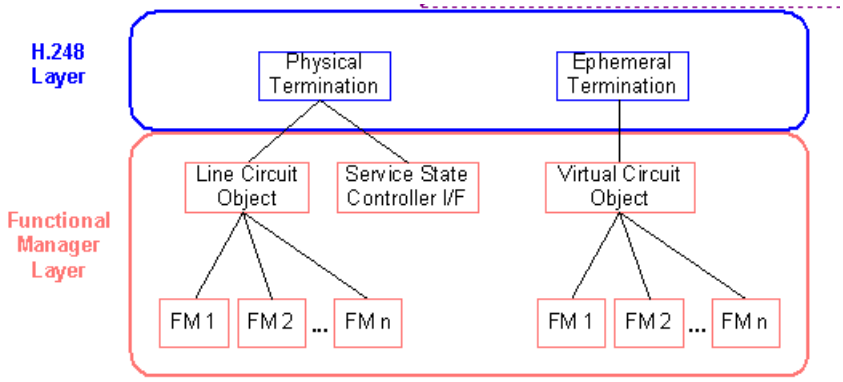
In the case of the CICM, the FM layer acts mostly as a protocol conversion layer. The CICM FM implementations perform whatever work they can, and use the ITerminations interface implemented by the Terminations component to accomplish the remaining work needed.

The CICM FM layer must also implement the IMediaGateway interface to allow the Terminations component to report terminal events that are generated.

Therefore, the interface into the Resource Manager layer and Hardware layer for the CICM is the ITerminations interface implemented by the Terminations component.

The Functional Manager layer's relationship to the H.248 layer is illustrated in the following Figure 9.

Figure 9 Functional Manager layer relationship to the H.248 layer



Service State Controllers

Each termination object in the MGF has an associated Service state Controller (SCC). The purpose of the SSC is to track the state of a termination, and also to handle GWC requests to perform maintenance or state changes. Three SSC types exist: root, physical and ephemeral.

The SSCs reside at the H.248 layer described in Figure 9 above. The MGF hides as much of the SSC functionality as possible and handles the cases that are common among all media gateways. In a similar manner to functional managers, the MGF uses SSC interfaces to allow platform specifics to be carried out in the event of state changes.

Service State Controllers support 3 states:

- In Service
- Out Of Service
- Testing (not supported by CICM)

A service state controller interface is available for the root termination and the physical terminations.

- Root termination SSC interface.
  The Root SSC keeps track of the CICM's current working state.
- Physical termination SSC interface.
  The physical termination SSC keeps track of the hardware specific details of all physical terminations.

Virtual Media Gateways

The emulation of multiple instances of media gateways is achieved by the virtual media gateway (VMG). VMG support is provided through the Media Gateway Manager component.

The CICM software architecture in Figure 5 above, *Architecture of Succession CICM*, is a simplified illustration and does not show the multiple instances of media gateways possible. It shows a single running instance of the Megaco Media Gateway component encapsulating a single instance of the MGF. From the GWCs point of view, the CICM appears as a single media gateway.

Due to existing GWC limitations, a single media gateway cannot be provisioned with more than 1024 lines. Such a limitation can be restrictive should the CICM processor card be capable of handling many more lines.

It is therefore desirable for the CICM to emulate multiple instances of media gateways, thus bypassing the GWC limitation and allowing it to achieve its full processing potential. This is achieved by the VMG.

Inter-node cooperation

The resiliency of the CICM is assured by its dual node configuration. The term “processor pair” refers to the pair of CPU cards that cooperate to achieve the redundancy required by highly available telephony systems.

The Succession CICM processor pair has a dual purpose. The GWC-facing side of the CICM runs in a warm take-over configuration that kicks in on failure of the active node. The terminal facing side of the CICM architecture runs in a load-sharing mode while both nodes are active.

In CICM 6.12, load sharing occurs while both nodes are active. In the case of a node failure, the remaining active node will take over any terminals hosted by its mate.

Interfaces

The Media Gateway Manager (MGM) communicates with other CentrexIP components through a series of COM interfaces.

The interfaces implemented and/or used by the MGM component are:

- IAdmin
- ITerminations
- ITerminationsAsync
- ICentrexTerminations
- IMegacoMG
- IMediaGatewayMgr

- IMediaGateway
- IMediaGatewayState

IAdmin This interface is common among all components of a CentrexIP gateway and is used to administer the component. The MGM implements this interface to allow it to be integrated to the existing architecture. This allows the new component to be started, stopped and managed by current processes.

ITerminations The ITerminations interface is implemented by the Terminations component. Its purpose is to enable the MG to communicate with the Gateways terminals. Methods on this interface are called as a result of messages sent by the Media Gateway Controller (MGC). Once the MG component parses a message, it makes the appropriate call(s) against this interface to its local Terminations component.

> ***Note:*** The MG does not need to go through the MGM to get to the Terminations component; all MGs hold a pointer to their local ITerminations interface.

ITerminationsAsync The ITerminationsAsync interface is implemented by the Terminations component. The interface is a remote interface, meaning that calls are made from one machine to another. In this case, the two machines are the two sides of the BSCM Gateway. Calls coming down into Terminations may be passed into the other side of the Gateway if the terminal is connected to that side.

ICentrexTerminations The ICentrexTerminations interface is implemented by the Terminations component. The interface is used by the Sessions component to communicate information (on a termination logged into that Sessions component) to the MGs, and reply to previous calls to the ICentrexService interface. ICentrexTerminations is comparable to the ICSideLines interface.

IMegacoMG The IMegacoMG interface is implemented by the MG Unit component. The interface is wholly local, in that all calls made to it are made by the local MGM component.

MediaGatewayMgr This interface is implemented by the MGM component. It is a remote interface and is used by MG Units on the remote side of the node to communicate with their peers on the local side of the node.

IMediaGateway IMediaGateway is implemented by the MegacoMGMgr component. The class that actually implements the

interface is CMediaGateway, a base class which CMegacoMGMgr inherits from. This interface is exposed to the Terminations component.

IMediaGatewayState IMediaGateway is implemented by the MegacoMGMgr component.

Authority Component feature

The Authority Component of the Gateway Services is a new feature for CICM Series 6.12 release. The Authority component is responsible for the authentication of users. It does not manage user configuration.

The Authority component is a COM component, an instance of which runs on each side of the gateway. The two instances talk to each other using DCOM.

The Authority component is used mostly by the Sessions component and as such, it is packaged in the same executable: sessions.exe.

Users

A single user can have multiple active instances at any one time. There are two types of user instances: master and slave. The type of instance is predetermined from the type of terminal used by the user. Users cannot have active instances on both nodes of the gateway at the same time.

The following combinations are permitted for an individual user on a single node:

- No instances
- Master instance only
- Slave instance only
- master instance and a co-existent slave instance

Interfaces

The Authority Component has three interfaces:

- IAuthority
- IAuthoritySync
- IAdmin (plus IUnknown)

A component that wishes to use Authority must support a fourth interface:

- IAuthorisable

IAuthority interface
The IAuthority interface is used by other components to request user authentication from the Authority. The other components that use IAuthority are:

- AuthenticateUser
- Login
- ReleaseUser
- ChangePassword

AuthenticateUser component The AuthenticateUser component checks that the supplied username is valid and that the password matches the password stored in the user mib. Checks are also made to ensure that excessive failed password attempts cause the user to have their account disabled temporarily. If the user is authenticated, a handle is created and returned. This handle contains a unique identifier for the user and a cookie for the user's current session.

The AuthenticateUser component definition is provided in the following table.

Table 2 AuthenticateUser component

Direction	Parameter Type	Description
in	String	Username
in	String	Password
in	tAuthInfo	Provides a handle for call backs through IAuthorisable and some information for auditing. Also has a terminal type which decides if the session is a master or slave.
out	tAuthHandle	If the result is successful, it contains a handle which can be used for future calls to Login, ReleaseUser or ChangePassword
out	tLoginResult	Provides an enumerated return code describing what happened.

When a user is authenticated, an entry is made into two data stores. The first is the user map, which contains a single entry for each user and records the user's current state. The second contains an entry for

every instance of a user, and stores the tAuthInfo structure for that instance.

Login component The Login component attempts to login an authenticated user using the specified login type. Three login types are available:

- **Unique logins** can only succeed if the user is currently idle (has no other instances logged in).
- **Join logins** can only succeed if the user has another instance of a different type already logged in on the local node (the master can join the slave, and vice versa).
- **Takeover logins** will cause existing login sessions on either node to be forced out of their login session. These will always succeed, unless a race condition occurs whereby a takeover login is being attempted on both nodes at the same time.

The Login component definition is provided in the following table.

Table 3 Login component

Direction	Parameter Type	Description
in	tAuthHandle	A handle identifying a unique instance of this user, returned by a successful call to AuthenticateUser
in	tLoginRequestType	The type of login that is required (Unique, Join or Takeover)
out	tLoginResult	If the call type is synchronous, this contains an enumerated return code describing what happened.
out	tCallType	A flag indicating if the call executed synchronously or not.

Login can be called indefinitely for a valid authentication handle until the login succeeds. The result of the login indicates why the login failed and can be used to decide if a further login attempt of a different type should be made.

In general, the login sequence is as follows (assuming this is the master; the slave sequence is analogous):

- Attempt a Unique Login.
- If the Unique Login failed because there is already a slave instance on the local node, attempt a Join Login.
- If the Unique Login failed because there is another master instance on the local node, or there are instances on the remote node, attempt a Takeover Login.

A takeover login will cause existing login sessions on either node to be forced out of their login session.

A Login call does not always complete synchronously. This is because, if both nodes of the gateway are active, the local node needs to exchange user login state with the remote node and remote communications are always asynchronous on the gateway. If the call cannot complete synchronously, the result of the call will be delivered through IAuthorisable::LoginAck().

When a Takeover Login is being performed to force out instances on the remote node, the remote instances will be forced out before the call completes. This ensures that two unsupported instance types will not exist at the same time, which would cause race conditions.

ReleaseUser component ReleaseUser takes just one parameter that identifies the user instance. The method revokes the authentication handle for the user instance. If the user instance is actively logged in, ReleaseUser logs the user out. There is no explicit logout function needed.

The ReleaseUser component definition is provided in the following table.

Table 4 ReleaseUser component

Direction	Parameter Type	Description
in	tAuthHandle	A handle identifying a unique instance of this user, returned by a successful call to AuthenticateUser.

ChangePassword component ChangePassword changes the user's password. Password changes only succeed when the user is logged in. The result of the password change is indicated in the HRESULT return value, S_OK if successful and S_FALSE if not.

The ChangePassword component definition is provided in the following table.

Table 5 ChangePassword component

Direction	Parameter Type	Description
in	tAuthHandle	A handle identifying a unique instance of this user, returned by a successful call to AuthenticateUser.
in	String	The user's old password
in	String	The user's new password

IAuthoritySync interface

This interface is used between instances of the Authority component on different nodes to keep them in synchronization. This interface is intended to be used over machine boundaries and has no return parameters, so it can be asynchronous.

LoginNotify component LoginNotify is called to notify the remote node that a user has logged in on the local node. If there are no active user instances on the remote node, the remote node updates the state of the user. If there are active user instances on the remote node, these instances are forced out. This process always results in a LoginNotifyAck message being called back from the remote node to the local node indicating if the operation completed as expected. Any forced logouts will occur before LoginNotifyAck is called.

The local node calls IAuthorisable::LoginAck() to return the result to the user when LoginNotifyAck() is called.

The LoginNotify component definition is provided in the following table.

Table 6 LoginNotify component

Direction	Parameter Type	Description
in	Long	The high order index of the user that is logging in.
in	Long	The low order index of the user that is logging in.

LoginNotifyAck component Refer to LoginNotify component section above.

The LoginNotifyAck component definition is provided in the following table.

Table 7 LoginNotifyAck component

Direction	Parameter Type	Description
in	Long	The high order index of the user that is logging in.
in	Long	The low order index of the user that is logging in.
in	tLoginResult	The result of a call to LoginNotify

LogoutNotify component LogoutNotify is called when the last instance of a user logs out on the local node. This enables the remote node to permit local logins once more without needing a takeover login. There is no response to this method call.

The LoginNotifyAck component definition is provided in the following table.

Table 8 LogoutNotify component

Direction	Parameter Type	Description
in	Long	The high order index of the user that is logging in.
in	Long	The low order index of the user that is logging in.

Synchronise This method call has no parameters. When the authority is started it is told if the mate node is already running. If it is, the node will call Synchronize to request that all the user state data is transferred across so that the nodes will start in synchronization. Subsequent changes to user state while both nodes are running are synchronized through the LoginNotify and LogoutNotify methods.

SynchroniseAck SynchroniseAck is called on the remote node in response to a call to Synchronize from the remote node. The local node iterates all the users and creates an array containing any user that is currently logged in. Calls to LoginNotify and LogoutNotify are only made once a request for synchronization is made.

The SynchroniseAck component definition is provided in the following table.

Table 9 SynchroniseAck component

Direction	Parameter Type	Description
in	Long	The size of the array in the second parameter.
in	tAuthoritySync	An array containing users which are active on this node.

IAdmin interface

IAdmin is used by other components in the system to control start-up and shutdown. It can also be used to force userlogouts for users.

The authority component must be told what state the two nodes of the gateway are in when it is initialized so it knows whether synchronization is necessary or not. IAdmin::Init takes a parameter indicating if the node is a master or slave and the Authority uses this to control synchronization.

Individual users can be administered by calling IAdmin::Select and supplying the class “user” and the username as an instance. Calling IAdmin::Stop on a user causes active instances of that user to be forced out of the gateway.

IAuthorisable interface

The IAuthorisable interface must be implemented by components using the Authority so that they can receive asynchronous call backs when significant events occur.

LoginAck LoginAck is used to return a login result when a login attempt could not be completed synchronous.

Table 10 LoginAck component

Direction	Parameter Type	Description
in	Long	A handle identifying the session instance to which the method corresponds to. This matches the handle supplied in the tAuthInfo structure during a call to AuthenticateUser.
in	tLoginResult	The result of the login attempt; an enumerated return code describing what happened.

ForceLogout ForceLogout is called when a login session is terminated abnormally. An abnormal termination can be, for example, a takeover by another user instance, or an intervention by the administrator to delete a user account.

Table 11 ForceLogout component

Direction	Parameter Type	Description
in	Long	A handle identifying the session instance to which the method corresponds to. This matches the handle supplied in the tAuthInfo structure during a call to AuthenticateUser.
in	tSessionLogoutReason	The reason why the session is being forced to logout.

Data structures

There are two main data structures used by the Authority component:

- User State Map
- User Instance Information Map

User State Map Usernames are strings of numeric digits composed of 4 to 15 characters. The Authority must hold state information for each user (described by the CUserState class). To index the data using strings would be slow, so the username is converted into two 32-bit indexes that can uniquely represent the full range of usernames. Leading zeros are significant to usernames so the two indexes preserve leading zeros. The User State Map maps usernames into CUserState indexes.

UserInstance Information Map User instances are also stored in a C++ STL map. The index to the map is also an integer but it is a randomly generated cookie. When an AuthenticateUser is called successfully, an entry is made to the user instance information map for that user instance. The map contains information such as master or slave user instance, and auditing information such as the terminal IP address. It also contains the user's high and low order indexes so that the user state map can be referenced easily. When ReleaseUser is called, the user instance is removed from the map.

Audits

The LM_LOGIN_AUDIT and LM_LOGOUT_AUDIT event logs are generated when user logins and logouts occur.

Tone generation and SDP negotiation feature

CICM up to and including Series 2.5 fitted into a telephone network which relied on the DMS for tone generation. In Series 6.12 the DMS is replaced by a Media Gateway Controller (MGC) which will not generate tones for the terminals.

Tone generation

The tone Generation aspect of this feature makes changes to the CentrexIP Gateway so that the tones (e.g. dial tone, ring tone) are produced at the terminal itself.

A new Tone Profile section on the EM allows the administrator to configure and modify sets of tones into a profile. These tone profiles can be applied to the user profiles.

The user is presented with a choice of tone profiles they may select.

In series 6.12 release, tones are produced locally by the i200x SoftClient by playing sets of frequencies and cadences (stream-based tones) downloaded by Sessions. The i2004 has the ability to store up to 16 separate stream IDs, each of which comprise up to 4 frequency pairs and cadencies. The SoftClient is capable of the same storage.

Upon starting the gateway, Sessions will read all tone set profiles stored in the MIB and store them in a static storage area accessible by all users. When a user logs into the gateway, Sessions reads which tone set profile they are associated with from the MIB. Sessions will check the following areas for a tone set profile, in this order:

- User
- User Profile
- Gateway Default

If Sessions cannot find a tone set profile to associate with a user, or the tone set profile found is invalid, hard-coded default tones will be used.

Standard tone set profiles are datafilled on the gateway when the **install.bat** command is run during gateway installation. The English and Australian tone sets have been created for this feature.

When a tone is required, Sessions downloads the frequencies and cadencies to the client for that specific tone ID.

A test screen is provided on the i200x (which is available to users with the administrative permissions) to test tones.

Tones are grouped in sets (tone sets) and are configurable using a Tone Profile Web page on the EM and stored locally on the gateway. A Tone Profile Home page is available to the administrator, which provides the following options:

- Apply tone profiles to a gateway.
- An option is available to create a new tone profile.
- Change tone profiles stored on the element manager. This displays a tone profile name list to allow the administrator to edit or delete existing tone profiles stored on the element manager.
- Change the tone profiles stored on a specific gateway. This displays a tone profile name list to allow the administrator to edit or delete existing tone profiles stored on the gateway.

SDP negotiation

Session Descriptor Protocol (SDP) negotiation provides for codec negotiation subject to a selection of preferred and default codecs. This provides the ability to set up a selected codec (and parameters) within the audio profile web page for the administrator to setup.

The audio profile Web page has been enhanced to provide the ability to set up a preferred codec and associated parameters. The administrator can create an audio profile, which may be applied to either a TDM gateway or a CS2K gateway. A selection of separate codecs is available (applicable for a TDM gateway) and a selection of preferred and default codecs is available (applicable to a CS2K gateway).

Codec negotiation is carried out as shown in the following table.

Table 12 Codec negotiation

Codec choice in SDP from GWC	CICM Audio Profile Codec choice	Negotiated Codec sent back to GWC in SDP
G.711	G.729	NACK
	G.729, G.711	G.711
	G.711, G.729	G.711
	G.711	G.711

Table 12 Codec negotiation

Codec choice in SDP from GWC	CICM Audio Profile Codec choice	Negotiated Codec sent back to GWC in SDP
G,729, G.711	G.729	G.729
	G.729, G.711	G.729, G.711
	G.711, G.729	G.711
	G.711	G.711

Note 1: The GWC will only accept G711 as the default codec.

Note 2: In some cases the response is one codec, when both codecs are sent from the GWC on our codec choice. This is done in order to allow the preferred codec to be the codec that is sent to the other party. Without this, the GWCs preferred codec would always be chosen which may be incorrect for a particular gateway.

The QOS options are still located on the Audio Profiles Modification EM Web page for CICM 6.12.

New logs for tone generation

The new logs introduced for this feature are listed in the following table.

Log type	Log number	Description
Warning	N/A	Invalid tone received + "tone ID received"
Warning	N/A	Tone + "tone ID received" + not datafilled

Audio path codec negotiation feature

The Audio path codec negotiation feature enables the Succession CICM to select a codec to use for the RTP audio stream between two terminals, based on negotiations with the other party in a call. This is required to make optimum use of the IP network and to ensure the RTP media stream between terminals is set up correctly.

The negotiations take place using the SDP protocol, and include the audio compounding algorithm (G.711 or G.729), packet size, and DTMF capability (in-band or out of band).

When a call is on take up, the GWC will specify to the CICM either its default codec capabilities, or (if known) the remote party's codec capabilities, or both. The CICM takes this information and compares it

with what the local party supports, and responds to the GWC with either its codec capabilities, or its chosen codec for the call.

Succession supports two audio codecs: G.711, which is high quality high bandwidth, and G.729, which is a lower bandwidth and quality. G.711 has two variants: a-law for the international market, and mu-law for the North American market.

The TDM version of the CICM gateway allows one codec to be selected in an audio profile. Succession needs to be able to associate two codecs with a profile: a primary and a secondary for use in codec negotiation. It also needs to be able to support more than one Packet size, as Succession supports Packet sizes of 10ms and 20ms. The Audio Profiles Modification Web page is illustrated in the following Figure 10.

Figure 10 Audio Profiles Modification

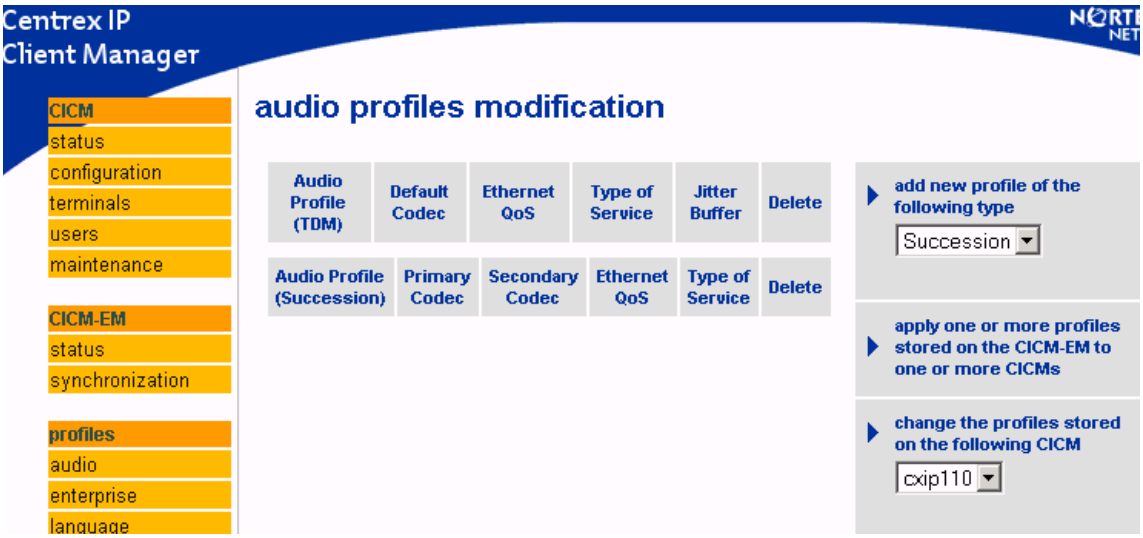


Table 13 provide is the primary and secondary codec choices that fit network requirements. Table 14 provides the choice of packet sizes that fit network requirements

Table 13 CICM 6.12 codecs

Primary codec	Secondary codec	Quality
G.729	G.711	Optimal bandwidth
G.711	G.729	Best Quality
G.729	-	Low bandwidth

Table 14 Packet size choices

Primary packet size	Secondary packet size	Quality
10 ms	20 ms	Best quality
20 ms	10 ms	Optimal bandwidth
10 ms	-	Low bandwidth

The CICM gateway must respond to the SDP sent from the GWC using the negotiation rules defined below in Table 15. this illustrates the choices made by the CICM gateway based on the codecs in the local audio profile, and the received codecs in the remote SDP message. This is for an H.248 ADD message.

Table 15 Codec negotiation for an H248 ADD message

Codec choice in SDP from GWC (either local, remote, or intersection of both)	CentrexIP - Audio Profile Codec choice	Supported codec(s) to be sent back to GWC in local SDP (if SDP from GWC was local only)	Chosen codec to be sent back to GWC in local SDP (if SDP from GWC was remote only or both local and remote)
G.711	G.729	NACK	NACK
	G.729, G.711	G.711	G.711
	G.711, G.729	G.711	G.711
	G.711	G.711	G.711
G.711, G.729	G.729	G.729	G.729
	G.729, G.711	G.711, G.729	G.711
	G.711, G.729	G.711, G.729	G.711
	G.711	G.711	G.711
G.729, G.711	G.729	G.729	G.729
	G.729, G.711	G.729, G.711	G.729
	G.711, G.729	G.729, G.711	G.729
	G.711	G.711	G.711
G.729	G.729	G.729	G.729
	G.729, G.711	G.729	G.729
	G.711, G.729	G.729	G.729
	G.711	NACK	NACK

If the chosen codec is sent to the GWC in the local SDP message, the audio path can be set up between the two clients, as negotiation has taken place and the codec to be used for the call is known.

If the supported codec(s) are sent to the GWC in the local SDP message, the CICM can expect to receive an H.248 Modify message containing Remote SDP. The audio path will then be set up between the

two clients using the codec information contained within, as negotiation has taken place and the codec to be used is known.

RFC2833 tone support can be set in the audio profile. However if RFC2833 tone support is set, the CICM will verify that the terminal can actually support them, and it will override the setting if it finds the terminal is incapable.

The Succession audio profile in Series 6.12 is illustrated in the following Table 16.

Table 16 Succession audio profile parameters

Parameter	Profile setting
Primary codec *	G.711 Auto, G.711 a-law, G.711 mu-law, G.729
Secondary codec *	G.711 Auto, G.711 a-law, G.711 mu-law, G.729
RFC2833 *	Yes/No
G.729 VAD	On/Off
G.711 BFI	On/Off
Primary packet size *	10, 20
Secondary packet size *	10, 20

Note 1: * These parameters are negotiated during a call.

Note 2: If the primary and secondary codecs are left blank, the default is: primary G.711 and no secondary.

For comparison purposes, the TDM audio profile is provided in Table 17

Table 17 TDM audio profile parameters

Parameter	Profile setting
Primary codec	G.711 Auto, G.711 a-law, G.711 mu-law, G.729, G.723
VG.729 or G.723 VAD	On/Off
G.711 BFI	On/Off
G.711 packet size	10, 20

Table 17 TDM audio profile parameters

Parameter	Profile setting
G.729 packet size	20, 40
Out of band ringing	Yes/No

Jitter Buffer information is not needed for the Succession profile. Quality of Service information will remain the same.

Before creating a profile, the administrator must specify if it is a Succession or a TDM profile. The Audio Profile Modification page contains two tables, one for Succession profiles and one for TDM profiles. The Audio Profile edit page will only allow relevant parameters to be datafilled for the specific Audio Profile. For example for a Succession profile, only packet sizes of 10 or 20 will be allowed.

Upon profile application, the Element Manager ensures that TDM and Succession profiles are applied to the relevant gateways. TDM profiles will not be applied to Succession gateways and vice versa.

If a user is not logged in to their session, the CICM responds to the GWC with default codecs to make it appear to the CS2K that the call is successful. This allows feature interactions such as sending the call to voicemail. The supported codecs sent back in this situation are primary G.729 and secondary G.711, with a packet size of 20ms. This default of G.729 saves bandwidth, but G.711 can be used if necessary. The packet size of 20ms is the Succession default.

Table 18 illustrates the expected packet sizes for the supported Succession codecs. It can be used to verify that the correct codec choice has been made between clients by analyzing the packet stream.

Table 18 Packet sizes for supported Succession codecs

RTP payload size (bytes)	Codec
2	G.729 silence frame (10 ms or 20 ms)
4	G.729 silence frame (20 ms only)
10	G.729 silence frame (10 ms or 20 ms following silence)
12	G.729 data and silence frame (20 ms only)
20	G.729 data frame (20 ms only)

Table 18 Packet sizes for supported Succession codecs

RTP payload size (bytes)	Codec
80	G.711 data frame (10 ms only)
100	G.711 data frame (20 ms only)

Dynamic Feature Key Assignment feature

The Dynamic Feature Key Assignment feature provides for the display of only those feature keys which may be used in a particular state (idle/non idle). This feature also includes the extended feature key functionality, which uses certain feature keys to gain access to extended functionality provided by the CICM.

This feature applies to the i200x client. Refer also to *NN10027-113, CICM Etherset Installation Guide and User Manual*.

Dynamic feature keys

The i200x clients have limited feature key real estate. The CICM provides emulation of a 14 key M5216 terminal, plus up to 2 optional M522 22 key extension modules. All feature keys may be configured so they are displayed dynamically on the i200x terminal(s).

Prior to 6.12 release, the CICM provided access to the 14 feature keys by using pages of feature keys. The number of pages was determined by the number of physical feature keys on the terminal.

A large majority of CICM supported features can only be used when the client is in a particular state (idle or busy). Therefore many feature keys which are displayed in the limited area on the terminal screen cannot actually be used when the client is on a call, or when the terminal is idle. By dynamically showing or hiding the feature keys which can or can't be used, the need to scroll across feature key pages can be reduced. Thus the Dynamic Feature Key feature is introduced to minimize confusion from the multiple pages of feature keys.

Feature key options

Using the Element Manager, each feature is assigned a set of options to control the hide/show functionality of a specific type of feature key. These options are:

- DN feature
- Hide Mode

The DN feature option may be configured as shown in table 19, and the Hide Mode feature option may be configured as shown in table 20.

Table 19 DN feature option

DN feature option	Result
Yes	• This feature key will behave like a DN key • It will toggle the DN activity state for the dynamic feature keys hiding/showing. • It will have an active inbox associated to it by default (NOTE: If an inbox is not required for a particular DN this can be deactivated through a user profile or user override setting).
No	• This feature key will behave like a normal feature key (non DN key).

Table 20 Hide Mode option

DN feature option	Result
Never	• The feature key will always be displayed and available.
When DN is active	• This feature will be hidden from the user when the DN key is active. An example is the “call forward universal” feature, used to program call forwarding. You can't program call forwarding while on a call.
When DN is in active	• This feature is hidden from the user when the DN key is inactive. An example is the “make set busy” feature, used to make the set appear to be busy. This can be configured so it can only be activated when a set is idle.

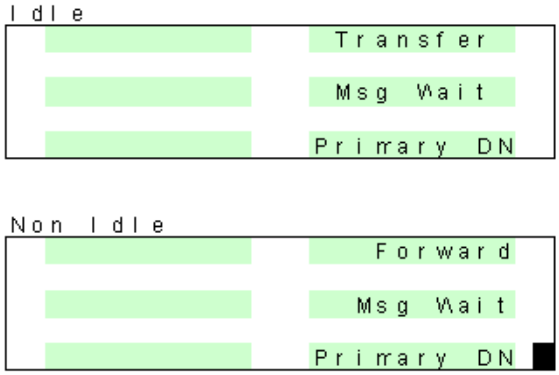
The CICM only displays the features that can be operated in the current phone state. The terminal is considered to be idle when there are no active DN features. In this case, the lamps associated with DN features are off.

An example feature key configuration is shown in Figure 11 below. The corresponding feature key display for i2004 is shown in Figure 12.

Figure 11 Example feature key configuration

Feature Name	DN feature	Hide Mode
Primary DN	Yes	Never
Msg Wait	No	Never
Call Transfer	No	When DN is active
Call Forward Universal	No	When DN is inactive

Figure 12 Example feature key display



Feature profiles configuration

The feature key type rules for all CICM supported features are configurable via a Feature Profile Web page on the CICM EM.

Refer to the CICM Configuration Management document for configuration procedures. The following Figures 13, 14, and 15, display the configuration pages required to set up the feature profile for a gateway.

Figure 13 Feature Profile home

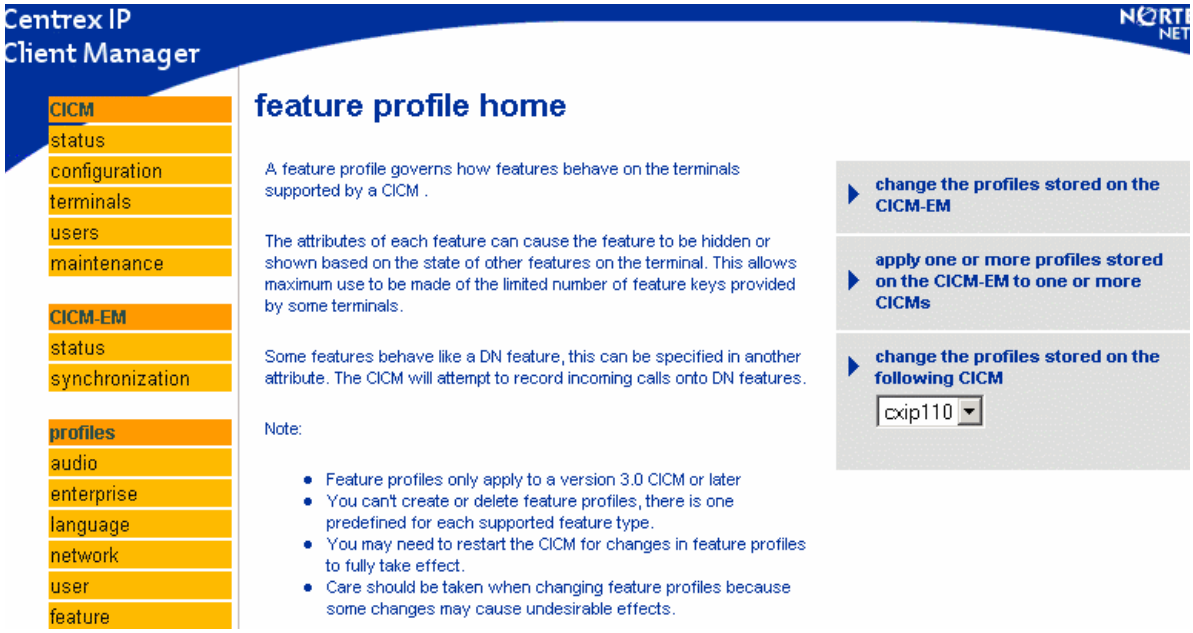


Figure 14 Feature Profiles modification page

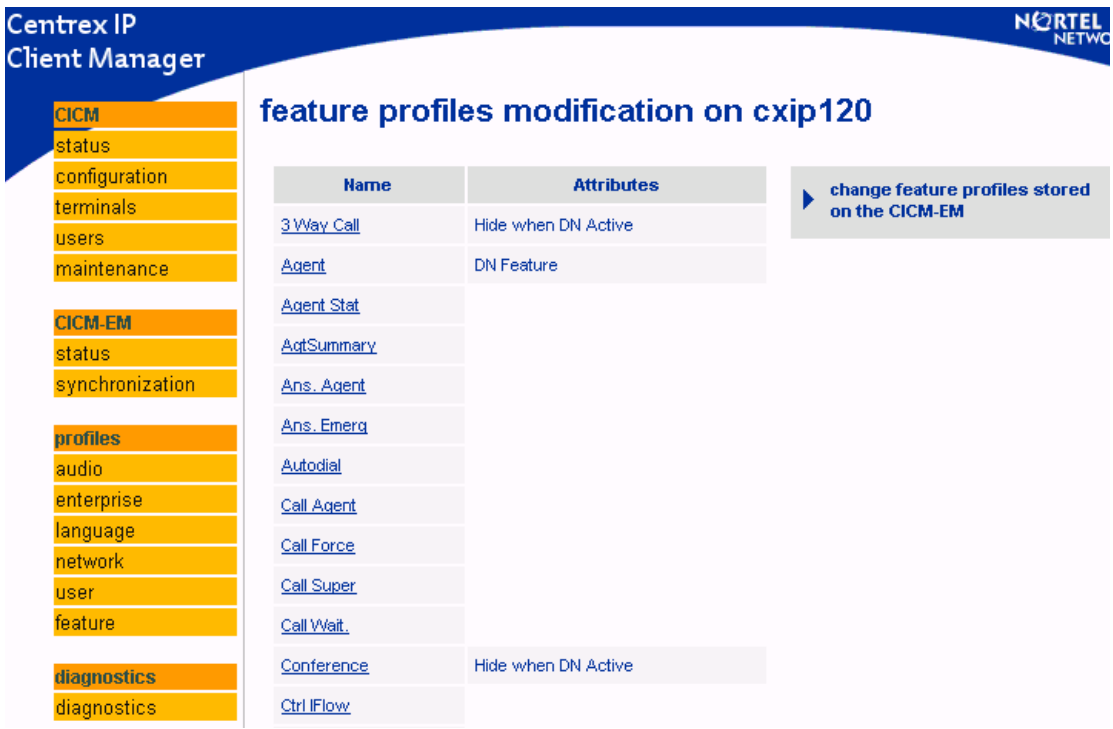
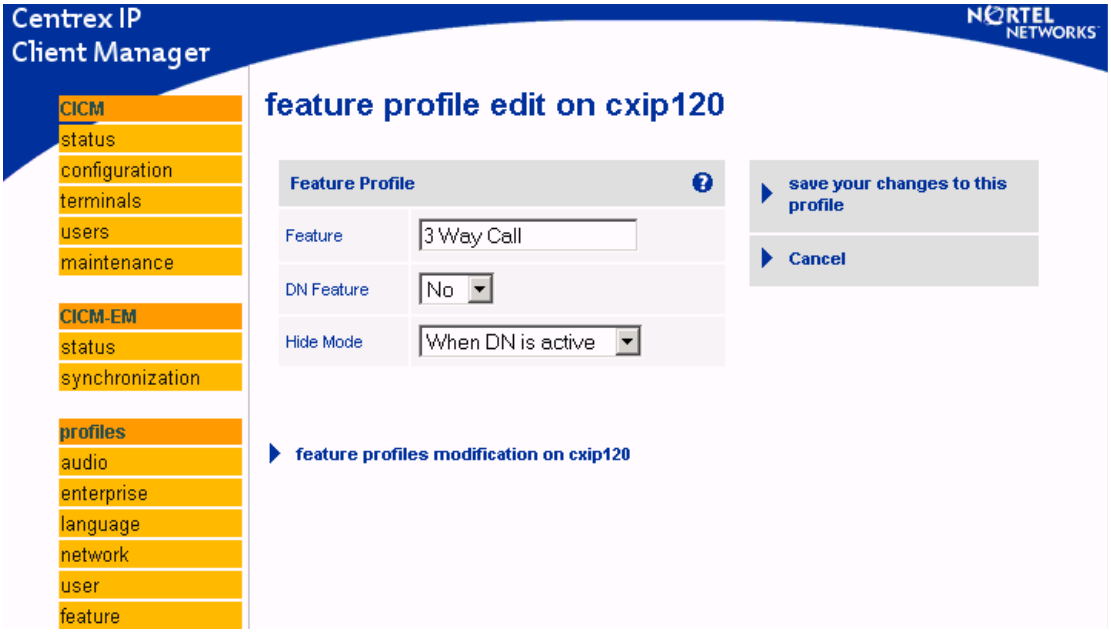


Figure 15 Feature Profile edit on cicm_name page



Refer to:

- the CICM Configuration Management document for the *Feature Profiles configuration* procedures
- the CICM Security and Administration document for the *Enable/Disable dynamic feature key functionality* procedure.

Dual Node Redundancy feature

This section provides a brief overview of the Dual Node Redundancy feature. For additional details, please refer to:

- *NN10233-911 CICM Fault Management*
  for a discussion of manual shutdowns, node failures, and network adapter failures related to DNR functionality.
- *NN10252-611, CICM Security and Administration*
  for Administration procedures related to DNR functionality, including the *Take a node out of service* procedure
- *NN10248-711 CICM Performance Management*
  for event monitoring and logs information.

CICM 6.12 is a Succession-only solution, and represents an interim step in the CICM re-architecture.This re-architecture will be complete in CICM 7.0, which will support both TDM and Succession. Dual Node Redundancy is the key feature in this re-architecture, which has started in CICM 6.12 and will be fully implemented in CICM 7.0.

Any carrier grade platform provides some level of redundancy. In TDM, there is no concept of a master/slave relationship at the LCM (or ILCM) level. Instead, both halves of the peripheral (LCM/ILCM) operate in a full load-sharing mode with the core (DMS CM), communicating with both nodes equally.

In Succession, only one side of the peripheral is expected to communicate with the core (CS2K). Therefore there is a master/slave relationship between the two nodes of the CICM. A modification of the CICM's architecture is needed to support this design.Specifically, an ability to perform a switch of activity (SWACT) is necessary.

The DNR feature implements the DNR functionality of the CICM by enabling the master/slave relationship and switch of activity required in the Succession paradigm. The basic purpose of the DNR feature is to achieve redundancy through the required Succession architecture.

The implementation of Dual Node Redundancy means that both nodes of the CICM gateway are capable of processing H248 messages and behave in a master and slave capacity. The master node will be responsible for processing H248 messages received via the H248 IP address bound to one of its VLAN adapters. The slave node will function as a "hot standby," ready to become the master should it become necessary.

Key aspects of the DNR feature for 6.12

The key aspects of this DNR feature are:

- Only a single node, the master, can communicate with the CICM gateway controller (GWC) at any time. The CICM will ensure the IP and port are moved to the appropriate interface as needed.
- In a failure scenario on the active node, the CICM will automatically initiate a switch of activity in order to maintain service.
- The CICM will differentiate between failure scenarios in which a SWACT is desirable. For example, should a loss of communication with the GWC occur, the CICM will only initiate a SWACT if it determines that the failure has occurred with the H.248 link or an interface on the active node. The SWACT will occur only if such action is likely to resolve the loss of communication.
- All stable calls will survive a SWACT. A stable call is one that is in the "talking" state. In this state, CODEC negotiation has been completed and the voice path has been setup such that no further action is required. No call-processing feature is active in a stable call. An idle terminal is also considered a stable call.
- Unstable calls may survive a SWACT.

- Only the North side of the CICM supports hot-swap takeover. The South side of the CICM will continue to operate in a load-sharing mode as with the CICM 2.5 TDM version. This means that even stable calls mainly hosted on the recently out-of-service master node may be lost in a failure scenario.
- A facility is available for the operator to determine which node is currently the active node.
- An operator may initiate a SWACT at any time.
- Once started, an operator-initiated SWACT cannot be cancelled. To return the system to its original pre-SWACT state, a second SWACT must be performed.
- The EM Web interface has been updated as follows:
  - The maintenance page has been updated so that an administrator can monitor and control SWACT activity.
  - The restart/reboot functionality has been moved to the maintenance page.
  - The main menu has been reorganized for improved userability.
- The changes to the CXIPNET and gateway services that are necessary for the implementation of DNR are outlined in the CXIPNET and Gateway Enhancements feature described below.

CICM software components

The redundancy provided by the CICM is best understood in terms of the software components that make up the CICM, as illustrated in the following Figure 16.

Figure 16 CICM redundancy model in Succession

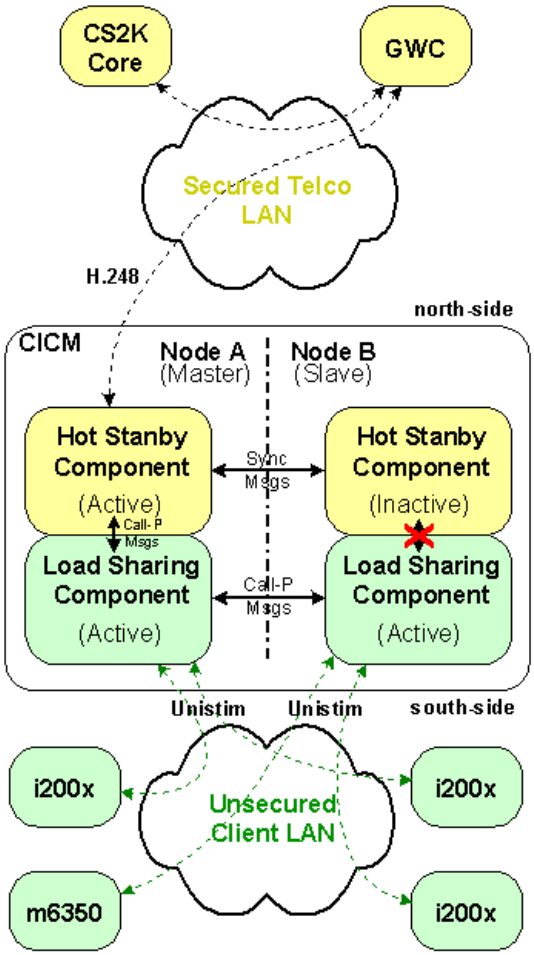


Figure 16 illustrates that each CICM node (i.e. each half of the gateway) executes an identical software load.

The GWC facing side of the CICM (or north side) operates in a hot standby mode. This component ensures proper communication with the gateway controller using the H.248 protocol over UDP/IP1. As the GWC knows only about a single entity, it does not expect to communicate with more than one component. To this end, only one half of the CICM may communicate with the GWC at any one time (the master).

The inactive hot standby component must keep in constant synchronization with the active side. The double-headed arrow connecting both hot standby components of the CICM illustrates this. This is necessary to ensure that both nodes have an accurate view of

the state of call processing at any time, thus allowing the inactive side to take over control of these functions should the need arise.

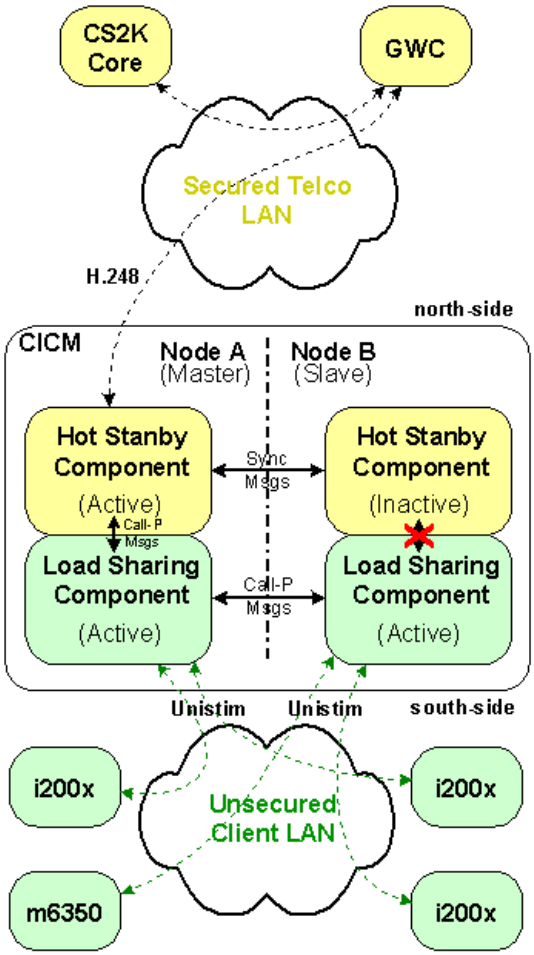
The terminal facing side (or south side) of the CICM operates in a load sharing fashion. For this software component, each node hosts roughly one-half the terminals connected to the CICM, thus balancing the load. The arrows identified as Call-P messages show the messaging path between the various components in typical call scenarios.

The illustration also shows that although both load sharing components host terminals, the message path ensures that all terminal events from either side are routed to the master hot standby component as only it may communicate with the GWC.

Note that the south side's role and functionality remain effectively the same as in the TDM variant of the CICM (SN06.1/CICM 2.5).
It is the north side of the CICM that changes significantly in SN06.2/CICM 6.1. In the TDM variant of the product, both nodes communicate equally with the PLGC (DMSX over TDM links) whereas in Succession only one node assumes the master role and communicates with the GWC.

SWACT
A switch of activity (SWACT) occurs when the role of the master node is transitioned from one node to the other. This implies that following a SWACT, communication with the GWC is maintained by the newly promoted master (in this case node B). This is illustrated in Figure 17.

Figure 17 CICM following a SWACT



A SWACT is considered “controlled” when initiated manually by the administrator. Following a controlled SWACT, the master and slave nodes assume each other’s previous role. A manual SWACT is usually executed in order to perform maintenance activities.

An uncontrolled SWACT is automatically initiated by the system upon failure of the master node. No immediate operator intervention is required for the slave node to assume the role of the master.

During a switch of activity (whether controlled or uncontrolled) only the hot standby components shown in Figure 17 exchange roles and will perform special processing in this circumstance. The south side components continue normal operations. No automatic terminal handover is carried out during a SWACT.

During the SWACT, only stable calls are guaranteed to survive. A stable call is a call in which the parties have achieved the talking state, and for which no user interaction is in progress. Anything else is considered to be an unstable call. Unstable calls may or may not survive.

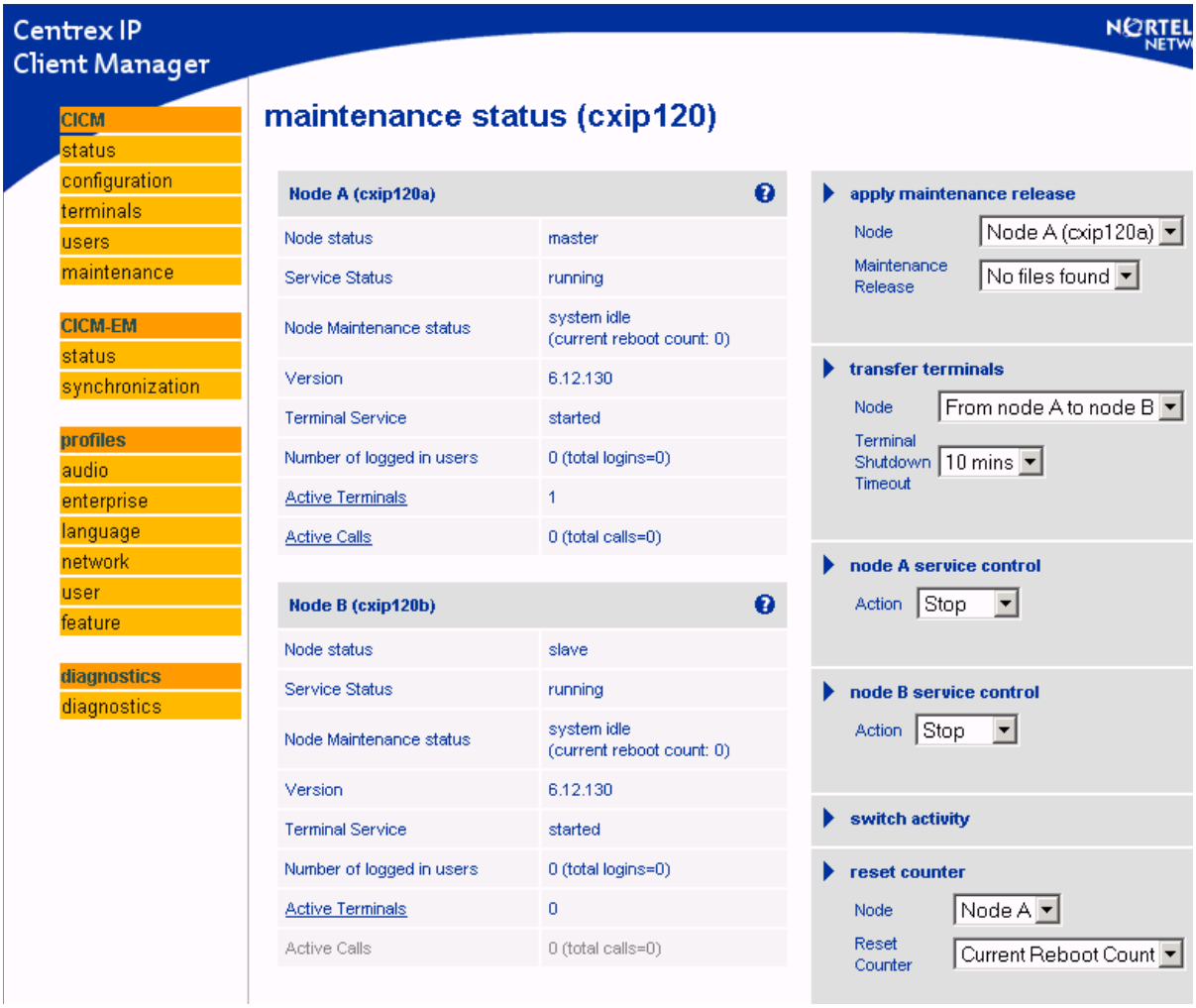
The following list provides a few examples of possible effects that could occur during a SWACT:

- A call in the middle of being setup may not terminate and could be lost.
- A user in the process of using a feature (such as setting up a 3 way call) could loose both parties, if a SWACT occurs before the speech path is established between all parties.
- General terminal stimulus could be lost during a SWACT, which could result in a misdialled call.

User interface

All controllable aspects of the dual-node redundancy functionality can be accessed from the **Maintenance Status** Web page of the element manager, illustrated in Figure 18 below.

Figure 18 Maintenance status Web page



The new **Node status** field indicates the mastership state of each node. It assumes one of the following values:

- Initializing
- Master
- Slave
- Transition in progress (master to slave)
- Transition in progress (slave to master)
- Slave (takeover not available)

The **switch activity** (or **SWACT**) option in the right menu is only displayed when the functionality is actually available. Once this option is chosen, a number of automated tests are performed before the

system proceeds. The operator is generally provided with a number of warnings and recommended preparation activities if they haven't already been carried out (e.g. transferring terminals). A confirmation must be made to proceed with the operation.

Following a SWACT, the mastership roles of both nodes are exchanged. Initiating this switch of activity manually is useful for maintenance purposes just prior to taking a node out of service (e.g. to swap a faulty CPU blade).

The **node A/B service control** option has moved to this **maintenance status <cicm_name>** page, from the **CICM status** page in CICM 2.5. The functionality is the same; the following 3 options are available (context sensitive) for each node:

- **Restart**
  Stop all services on this node and reinstalls the CPU card. Services restart automatically following the nodal restart, and call processing service are also resumed.
- **Stop**
  Stops the CICM service from running, thus halting call processing on the node. The CPU card remains active.
- **Start**
  Starts a stopped CICM service and resumes call processing on the node.

System start-up and shutdown
The behavior of the CICM in normal circumstances during start-up and shutdown is summarized in this section.

First node start-up (master) As the first node of the CICM initializes and begins operation, it broadcasts periodic heartbeat messages on its Admin LAN, directed to its mate node. Because it does not observe corresponding heartbeats from its mate, it assumes the role of the master.

The north side begins sending H.248 messages to the GWC and advises it when it is available for service. A number of initialization messages are exchanged between the CICM and the GWC. Meanwhile, the south side enables its Unistim interface and begins accepting incoming connections from terminals.

Once in service, users at connected terminals may login, make and receive calls, and use other available CICM services.

Second node start-up (slave) As the second node initializes, it also begins broadcasting periodic heartbeats directed to its mate node. As the master is already broadcasting, it recognizes this and assumes the role of the slave.

As the north-side operates in hot standby, the slave's standby component initializes, but does not begin communicating with the GWC. Instead, it requests a bulk synchronization of call processing state from its mate. Once completed, the master node continues dynamically sending synchronization information to keep the slave constantly up to date.

The south-side on the slave initializes in a similar manner to the master. As this component operates in a load-sharing mode, it begins accepting incoming connections from terminals as soon as it is ready. Users at connected terminals may login, make calls and use CICM services.

Only when all software components have started and the bulk synchronization has completed is it possible to initiate a switch of activity.

Manual shutdown of a node A node may be shutdown or restarted using the Element Manager's maintenance Web page. For the purpose of dual-node redundancy, both shutdown and restart are effectively equivalent, and are treated as such in the software. For simplicity this section will refer to a system shutdown and ignore node restarts.

Three scenarios may exist:

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

These 3 scenarios are treated as failures of the respective nodes. No special processing is done to automatically initiate a SWACT, even though such an action may be desirable. It is the responsibility of the operator to ensure that the node is in the desired state before initiating any node shutdown.

However, initiating the shutdown from the CICM Element Manager (as is recommended) will result in system verification. The operator will be presented with an appropriate warning message and recommended courses of action in order to minimize any impact on service. Refer to the following *Node failures* section for details on the expected behavior of a node on failure.

Node failures The two important scenarios to consider are:

- Both master and slave nodes are running, and the master node fails
- Both master and slave nodes are running, and the slave node fails

The only other case in which a failure is possible is that of a node running in standalone mode and subsequently failing. In this case, as the node is running on its own, it would have already assumed the role of the master. If a standalone node fails, no action can be taken. There is no redundant node to fall back on.

A node failure may have a number of possible causes. The term applies equally to both hardware and software failures. Possible node failures include, for example:

- A general failure of the CPU card
- A software component that makes up the CICM load experiences a software exception (i.e. trap). The monitoring software automatically initiates an immediate restart of the node

From the remaining nodes perspective, these node failure cases are identical in that its mate suddenly stops providing heartbeats. The remaining node takes appropriate action as follows:

- **Master fails**
  When the master node experiences an unexpected failure, the slave hot standby component (refer to Figure 17) detects it and automatically SWACTs to assume the role of the master. This occurs transparently to the GWC as the new master node binds H.248 IP address. Some inbound messages from the GWC may be lost during the takeover, but the retransmission algorithm built in to H.248 ensures that they are eventually delivered.

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

  Terminals hosted off the node that fails (the master node before the failure) do lose connectivity to the CICM, as the south side operates in a load-sharing mode and does not support hot hand-over in SN06.1. These terminals eventually reboot and begin searching to connect to the mate node. If the terminal is on a call (stable or unstable), the call is lost.

- **Slave fails**
  When the slave node experiences an unexpected failure, the master hot standby component (refer to Figure 17) detects it, but does

nothing except make note of the failure. No SWACT occurs, therefore no H.248 messages from the GWC are lost.

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

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

Network adapter failures LAN adapter failures on the CPU cards are treated differently from other types of failures. There are four cases that call for special consideration:

- **Master looses adapter hosting H.248 interface**
  When the master node detects that it has lost layer-2 connectivity (typically representing a physical loss of a network adapter) on the physical adapter hosting the H.248 interface, the master initiates an automatic SWACT. This is done to conserve connectivity to the GWC, thus maintaining call processing.

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

  Terminals hosted on the new master node (previously slave) remain connected to their node, but unstable calls may experience problems due to the SWACT.
- **Master looses both adapters**
  If the master node detects layer-2 loss of connectivity on both its physical adapters, it determines that it is at fault, and demotes itself to the slave state. The original slave determines that the master has failed, and promotes itself to master.

  When either of the isolated node's adapters becomes available, the node looks for its mate. If found, the node restarts itself in order to refresh itself as the slave and ensure that all its MIB data is synchronized with the master node.

  If, upon regaining either physical adapter, the node does not find a mate, it re-promotes itself to the master state. Appropriate monitoring software ensures that only one node is ever master at any given time.

  In these cases, terminals hosted on this node lose their connection

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

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

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

- **Slave loses both adapters**
  If the slave detects layer-2 loss of connectivity on both its physical adapters, it acts almost exactly as in the above-described scenario: *Master looses both adapters*. The only difference is that the node does not need to demote itself. It is already the slave.

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

DNR related event logs
The three basic severity level of logs have not been changed. They are:

- **Error logs**
  Serious and often unrecoverable events
- **Warning logs**
  Unexpected but recoverable events
- **Information logs**
  Expected but significant events

New Information logs related to DNR are generated for the following normal start-up events:

- On the master node, when the master node comes into service
- On the slave node, when the slave node comes into service
- On the master node, on detection of the slave node coming into service
- On the slave node, on start-up and the detection that master node is running

Information logs are generated during an operator-initiated switch of activity, at the following points:

- On the slave node, when the SWACT command is first received
- On the master node, when the slave requests the master to relinquish its role
- On the master node, when the master completes transition to slave
- On the slave node, when the slave completes transition to master

In node failure scenarios, the mate detects when the failed node dies, and generates a warning log. If the failure is software related, the failed node generates an error log before dying. The remaining node will also generate logs informing the operator of any remedial action(s) to take.

If the operator manually stops a node, the mate will detect it as a failure and generate log(s).

All types of link failures result in the generation of the following system logs:

- On the master node, when H.248 connectivity to the GWC is lost
- On the affected node, when any link is lost

DNR related SNMP
The 6.1 CICM builds upon the existing 2.5 CICM SNMP MIB. This section discusses the differences between these two releases.

A single new MIB node is introduced in 6.1 to allow the operator to determine whether a node is the master or slave. This new node is added to the existing CICM SNMP hierarchy under:
…\cicm\cicmCpuCards\cicmCpuCardTable\cicmCpuCardEntry

The name of the new node is **cicmCpuCardMastership**. When queried on a given node, it may return one of the following states:

- **uninitialized(0)**: Reported when the node/service is first started until it fully assumes a working role (master-no-slave or slave). This is a transient state.
- **master(1)**: Reported by the master node when a slave node is also present. The node reporting this state behaves as master by controlling H.248 interface and communicating with GWC, etc.
- **slave(2)**: This node is the slave (hot-standby).
- **master-to-slave(3)**: The node is transitioning from a master to a slave state. This is a transient state.

- **slave-to-master(4)**: The node is transitioning from slave to master state. This is a transient state.
- **takeover-complete(5)**: As the last step in a SWACT, this state is reported on the newly demoted slave for a very brief period. This is a transient state.
- **master-no-slave(6)**: The node is running as master, but without the presence of any mate node (i.e. no slave). No redundancy is available.
- **slave-no-master(7)**: Represents a specific error condition.
- **error(8)**: Represents a general error condition.

The transient states listed above are reported only temporarily. Should these transient states be reported for a significantly longer delay, the problem should be reported to Nortel Networks. The error states above should also be reported to the appropriate support staff.

A new SNMP trap is introduced to the hierarchy under:
…\cicm\cicmTraps
and is named **cicmMastershipStateChange**. This trap is generated for each transition of the **cicmCpuCardMastership** node described above and reports the new state of the node. The alarm state field in this trap is always reported as **ok(2)**.

The **cicmVMGUnit0State** and **cicmVMGUnit1State** nodes are located in the MIB hierarchy under:
…\cicm\cicmVMG\cicmVMGTable\cicmVMGTableEntry
and are used to reflect the 6.1 status of the VMG (instead of the 2.5 VLCM). The nodes may have one of the following states:

- **inService(0)**: VMG is in service as master
- **stopped(1)**: Node is not running
- **outOfService(2)**: VMG is not in service
- **hotStandby(3)**: VMG is in service as slave

Indirectly, the state of this MIB node on the master tracks the CICMs H.248 connectivity with the GWC. When connectivity to the GWC is lost, the masters state reports **outOfService(2)**. When the connection is restored, it returns to reporting **inService(0)** once it has successfully transitioned back to that state (i.e no additional problems exist).

The 6.1 CICM also updates the contents under the hierarchy:
…\cicm\cicmVMG\cicmVMGTable\cicmCritProcesses

The names of the critical processes listed when walking this node are (in order):

- sessions.exe
- mgm.exe
- megacomg.exe
- cxipdbglog.exe
- tlntsvr.exe

The two nodes:
…\cicm\cicmDspCards
…\cicm\cicmTdmCards
are not used by the 6.1 CICM, since neither DSP nor TDM cards are needed or supported by this configuration.

DNR related alarms

The alarms of CICM 6.1 continue to behave as in CICM 2.5. However, the following alarms are most significant and specific to the dual node functionality of CICM 6.1:

- The CICM 2.5 alarm behavior of the VLCM also applies to the CICM 6.1 VMG. A card fault is raised if the VMG is out of service and the CPU card's alarm light glows red when in this state.
- A chassis alarm is raised as major if a single VMG is out of service, and critical if the VMGs on both nodes are out of service.
- The loss of a nodes critical link hosting the H.248 and Unistim interfaces is raised as a card fault and a major chassis alarm. The loss of both critical adapters results in a critical chassis alarm.

Systems engineering

Table 21 summarizes the lengths of times various maintenance activities related to DNR may require to complete.

Table 21 Timing of DNR related maintenance activities

	Call Processing Load	
	Average - High	**Low**
Master node start-up delay	N/A	< 30 seconds
Slave node start-up delay	> 10 minutes	3-4 minutes

Table 21 Timing of DNR related maintenance activities

	Call Processing Load	
	Average - High	**Low**
Switch of activity	< 3 seconds	< 1 second
SWACT at risk period	< 10 seconds	< 2 seconds

A switch of activity, from start to finish, lasts no more than 3 seconds, but typically lasts less than a second. The at risk period is the time during which unstable calls are in danger of being lost. This period begins when the SWACT is initiated, and lasts no more 10 seconds even with a high call processing load.

Limitations and restrictions of DNR functionality

Following is a summary of the limitations and restrictions of the DNR functionality:

- Hot takeover functionality is provided only at the H.248 communication side of the CICM. Terminal handover does not occur on loss of a node. Terminals connected to the failed node will lose any active calls and services until they reboot themselves and re-establish communication with the mate node.
- Only stable calls are guaranteed to survive a SWACT. Unstable calls may or may not survive.
- No client LAN redundancy is provided at the CICM with this feature.
- Initiating a SWACT at the EM will not automatically initiate other maintenance activities (such as transferring terminals). It is the operator's responsibility to perform these tasks as appropriate. However, the EM will perform checks and warn the operator of the possible effects of proceeding.
- Performing a shutdown or restart of a node from the EM will not automatically initiate a SWACT. It is the operator's responsibility to ensure the node is in the desired state before performing the shutdown. The EM will, however, warn the operator of the possible effects of proceeding with any potentially service-affecting actions.
- Once initiated, an operator initiated SWACT cannot be cancelled. To return the system to its original pre-SWACT state, a second SWACT must be carried out.
- It is not possible to upgrade any existing TDM CICM load to the 6.1 (Succession) CICM load. In order to make such a conversion, it is necessary to re-install and datafill both nodes.

However, the 6.1 EM load may be applied over an existing 2.4 or 2.5 EM load. The 6.1 EM may also be used to manage 2.4, 2.5 and/or 6.1 CICMs.

CXIPNET and Gateway enhancements for DNR feature

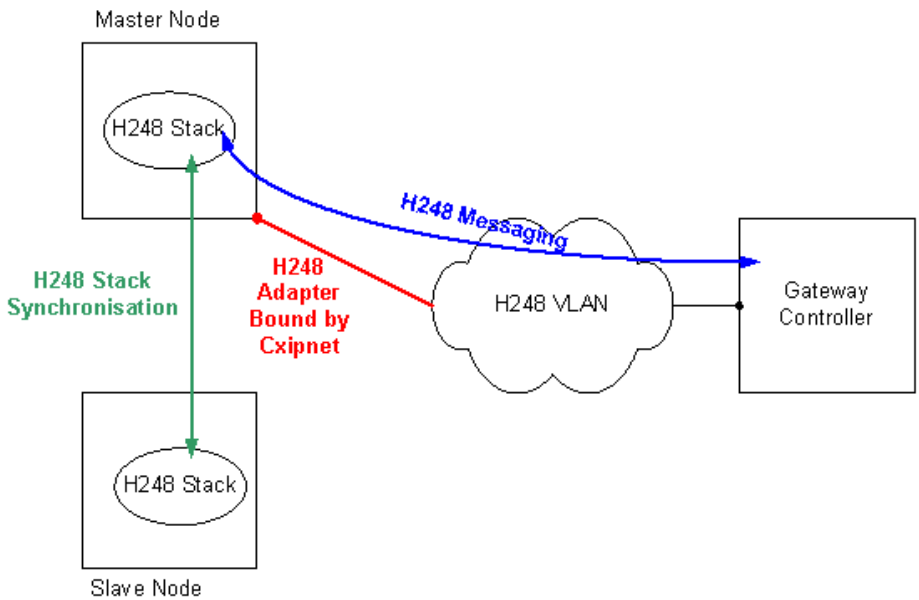
The CXIPNET and Gateway services enhancements are required to provide the functionality for Dual Node Redundancy that is introduced in CICM 6.12.

The implementation of Dual Node Redundancy means that both nodes of the CICM gateway are capable of processing H248 messages and behave in a master and slave capacity. The master node is responsible for processing H248 messages received via the H248 IP address bound to one of its VLAN adapters. The slave node functions as a hot standby, ready to become the master should it become necessary.

H248 Messaging

The following Figure 19 shows the operation of the DNR CICM gateway under normal conditions. The H248 Stack on the master node communicates with the Gateway Controller via an IP adapter bound to a physical interface held especially for it by CXIPNET. At the same time the H248 stack on the slave node is kept synchronized with the H248 stack on the master node in case it needs to take over as master itself.

Figure 19 H248 Messaging before SWACT



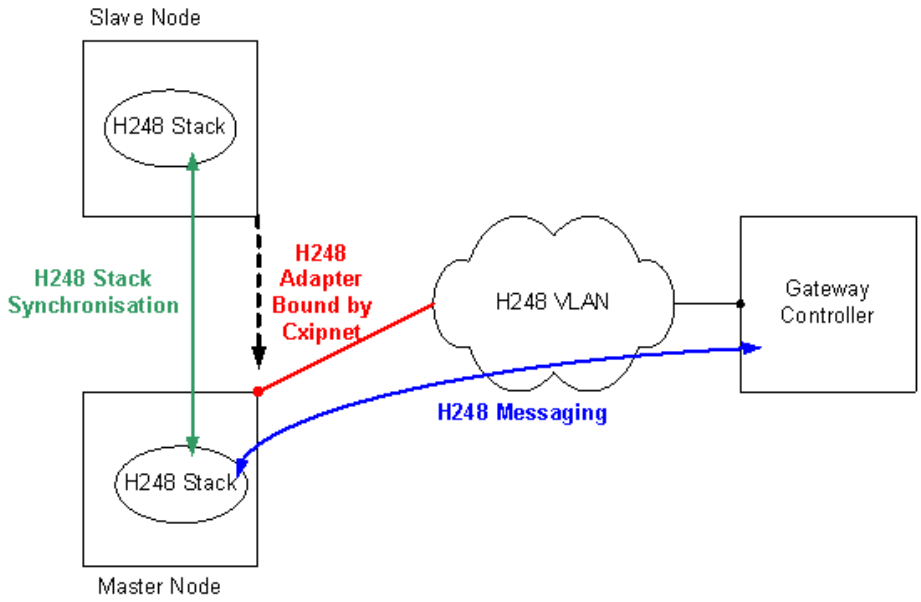
H248 Messaging after SWACT

Figure 20 below shows the action taken by the CICM in the event of a SWACT. CXIPNET co-ordinates the transition of the two H248 stacks from slave to master and master to slave. When the H248 stack on the new master node is ready to take over processing of the H248 message stream, CXIPNET will unbind the H248 Adapter from the previous master node and bind it to the new master node.

Since the H248 adapter will have the same IP information regardless of which node it is bound to, the overall result is that the IP address (virtually) moves from one node to the other. At that time the newly active H248 stack takes up signalling from where the previously active stack left off).

From the Gateway Controllers' point of view, the SWACT is transparent. The GWC will continue to send and receive H248 messages without interruption, to and from the same Gateway IP address, both before and after the SWACT.

Figure 20 H248 Messaging after SWACT



Changes to CXIPNET

CXIPNET, in CICM 2.5 and previous releases, already contained a state machine that was used to resolve conflicts arising from LAN failures. The state machines on CICM nodes work in tandem and are synchronized by sending information about their current state to each other within the ping messages that CXIPNET uses to detect network failures. This synchronization ensures that the two state machines will

always try to transition to a state where one is master and the other is slave.

In CICM 2.5 this state machine was driven by two external stimuli:

- the state of the other node
- manual intervention (for example, entering **cxipnet /swact start** from a command line)

In CICM 6.12, the enhancements to CXIPNET for Dual Node Redundancy is the extension of the state machine so that it can co-ordinate the necessary steps needed to support H248 stacks on each node in a manner that provides a degree of fault tolerance.

To this end, the master/slave state relationship of the two nodes is used by the H248 stacks to define whether they should function in an active manner (i.e. processing real-time H248 messages), or as a hot-standby (i.e. providing fault tolerance for the other active stack).

To achieve this fault tolerance, CXIPNET was modified for CICM 6.12 in the following three ways:

- First, handlers were added to the state machine so that CXIPNET ensures that if it is the master (and hence has the active stack). Then the necessary H248 VLAN adapters are bound to one of the master node's IP interfaces. This ensures that the active stack is able to communicate with the Gateway Controller.
- Second, the CXIPNET state machine capability was upgraded to handle scenarios and events which were not present in the pre-6.12 TDM versions of the CICM. New states, transitions and handlers were added based on identified needs from possible Dual Node configuration scenarios.
- Third, the state machine was modified to be capable of coordinating its actions. For example, SWACTing between its local H248 stack and the remote H248 stack (via CXIPNET on the other node). This co-ordination is two-way. In some instances a change in state of CXIPNET requires an event to be sent to the stack to request that an action be taken. In other circumstances, the stack may need to notify CXIPNET of an event which would require CXIPNET to change state (and possibly invoke a handler, as described above).

The interfaces needed to support communication between the CXIPNET state machine and the H248 stack are INetworkStatus (for incoming requests and notifications from the VMG to CXIPNET), and INetworkStatusNotify (for outgoing notifications from CXIPNET to the VMG).

Changes to the NT Embedded OS, Preboot, and the EM

For series 6.12, Preboot was modified to enable the user to assign either the existing Client VLAN adapter to be used for H248 messaging, or to define a separate H248 VLAN adapter for H248 messaging.

In 6.12, the H248 VLAN adapter pre-defined in the NT OS is at Preboot either re-configured or disabled, depending on which configuration the user selects. The Element Manager then auto-datafills the selected IP address when the user adds a VMG, forcing the VMG to use the H248 adapter that was defined at Preboot.

In Series 6.12, during Preboot the user still defines which VLAN adapter to use. However, the Element Manager now allows another IP address to be defined as the Floating H248 Adapter. This new IP address is bound as an additional address, when required, onto either the Client or H248 Adapter that was defined in Preboot.

Gateway Services changes

CXIPNET does not communicate directly with the H248 stack. The INetworkStatus and INetworkStatusNotify interfaces are used to send and receive messages to and from the Gateway Service which acts as a router for inter-process communication. These messages are then in turn relayed to the MegacoMgMgr service via the IAdmin and IAdminSink interfaces.

In addition, the MegacoMgMgr on the slave node ensures that its hot standby H248 stack remains synchronized with the active H248 stack on the master node, in case a SWACT is needed.

In order to support the coordination of the two stacks, additional methods were added to the INetworkStatus, INetworkStatusNotify, IAdmin and IAdminSink interfaces.

H248 adapter binding

In Series 6.11 the NT OS image was modified to include an additional VLAN adapter for use with H248. Preboot was also modified to give the user a choice of whether they wished to use this adapter for H248 messaging, or whether they wished to use the existing client VLAN adapter for H248 messaging.

If the user selected to use the H248 VLAN adapter they were then prompted for the relevant IP information, which was then assigned to the adapter. If the user selected to use the client VLAN for H248 messaging, then the H248 VLAN adapter was removed from the system. A virtual adapter D within the mib was then pointed at either the Client or H248 adapter to indicate which of the adapters should be used for H248 messaging.

In Series 6.12 CICM, the function of adapter D has been changed slightly. Adapter D still points to the VLAN adapter which is intended to be used for H248. However, it now holds its own IP address (the IP address of the floating H248 adapter) that is datafilled from the Element Manager. This IP address is returned when queried, instead of the IP address of the adapter at which it is pointing.

Figures 21 & 22 show the adapter mapping for Series 6.12. In both cases, the D adapter stores the floating IP address which is bound, when needed, as an additional IP address to either the Client or H248 Adapter. In Figure 21 the VLAN 3 adapter would have both the 47.165.76.190 and 47.165.76.105 addresses bound. In Figure 22 the VLAN 4 adapter would have the 47.165.200.100 and 47.165.200.105 addresses bound.

Figure 21 Series 6.12 with Client LAN adapter used for H248

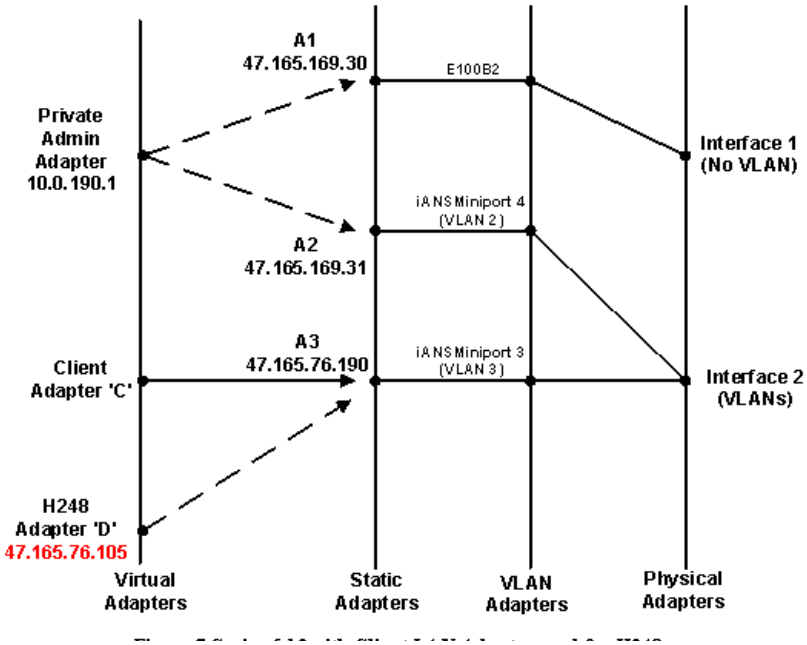
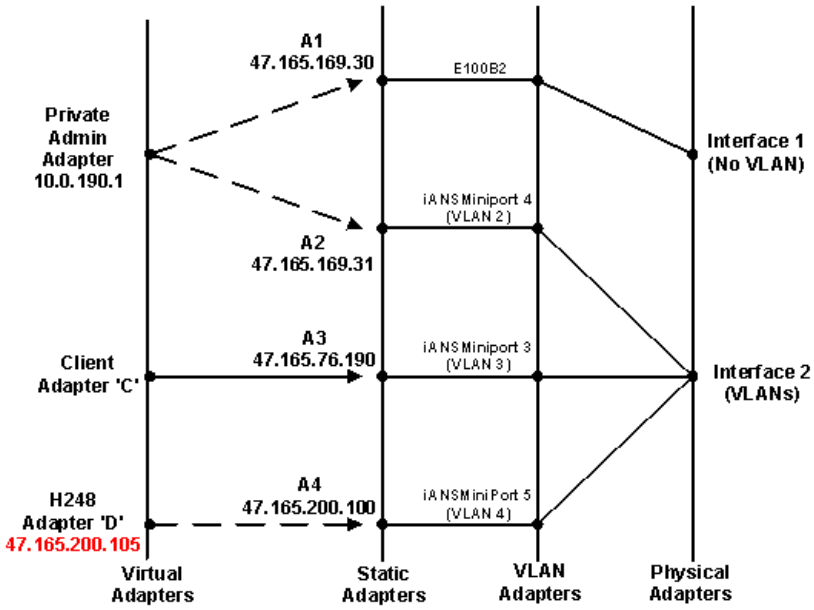


Figure 22 Series 6.12 with separate H248 adapter



Multi-tenanted Succession CICM (Virtual Media Gateway) feature

The purpose of this Multi-tenanted Succession feature is to enable secure media path communication between devices in different enterprise networks, and to improve the traversal of Network Address Translation (NAT) devices.

Each node (media gateway) being controlled by the Gateway Controller (GWC) is associated with an enterprise network. If the two end-points for any call are hosted by different nodes associated with different enterprises, the GWC inserts the RTP portal into the call, which is used to forward packets.

A CICM processor can host up to 1024 users. To configure the CICM as a single node on the GWC would mean that all of these 1024 users would need to be in the same enterprise network. This would significantly limit the deployment potential of the CICM.

Dynamic end-point discovery

To implement the Multi-tenanted Succession feature, dynamic end-point discovery has been implemented. The CICM automatically detects the network association for each terminal that is connected to it. Dynamic discovery allows users to roam across different networks and still obtain service.

The TDM CICM has a table of sub-networks that is used to make decisions about NAT traversal. Each NAT is described as a sub-network

of the public network that the CICM is connected to. A NAT with a single address is described as a sub-network of one address (mask is 255.255.255.255). When a terminal connects to the CICM from behind a NAT, the source IP address for the terminal will appear to be the public address of that NAT. The CICM checks in the sub-network table for a match and uses the entries in this table to check for NAT-specific settings (such as the UDP lease timeout).

A similar approach is used for the CS2K CICM. The GWC has a table of sub-networks and the CICM allocates each end-point against a sub-network so NAT traversal (and other internet transparency functions such as bandwidth counting) can take place.

When a terminal is powered up, it will connect to the CICM. The CICM then associates that terminal with a sub-network through the sub-network table, using the source address of the packets from the terminal. When a user logs into the terminal, the user also becomes associated with that sub-network. Users have a one-to-one mapping with end-points, so end-point to sub-network mapping can be established. The GWC is notified at user login time of the end-point to sub-network mapping. A new set of messages is defined for this purpose (an H.248 package or set of events). The GWC provides a table mapping each end-point to a dynamically discovered network identifier.

Provisioning considerations

Each CICM processor is configured as a single large gateway node and associated with a single line group. All of the 1024 TIDs in the line group will be datafilled in table LNINV and registered as end-points on the GWC.

There are additional provisioning requirements, depending on the chosen solution for mapping IP address-based sub-networks with the logical names used in the GWC.

Element Manager Web site enhancements

The CICM EM Web interface has been enhanced to support the new features. It has also been reorganized to improve userability. This section provides a brief overview of the enhanced Web interface.

CICM Home

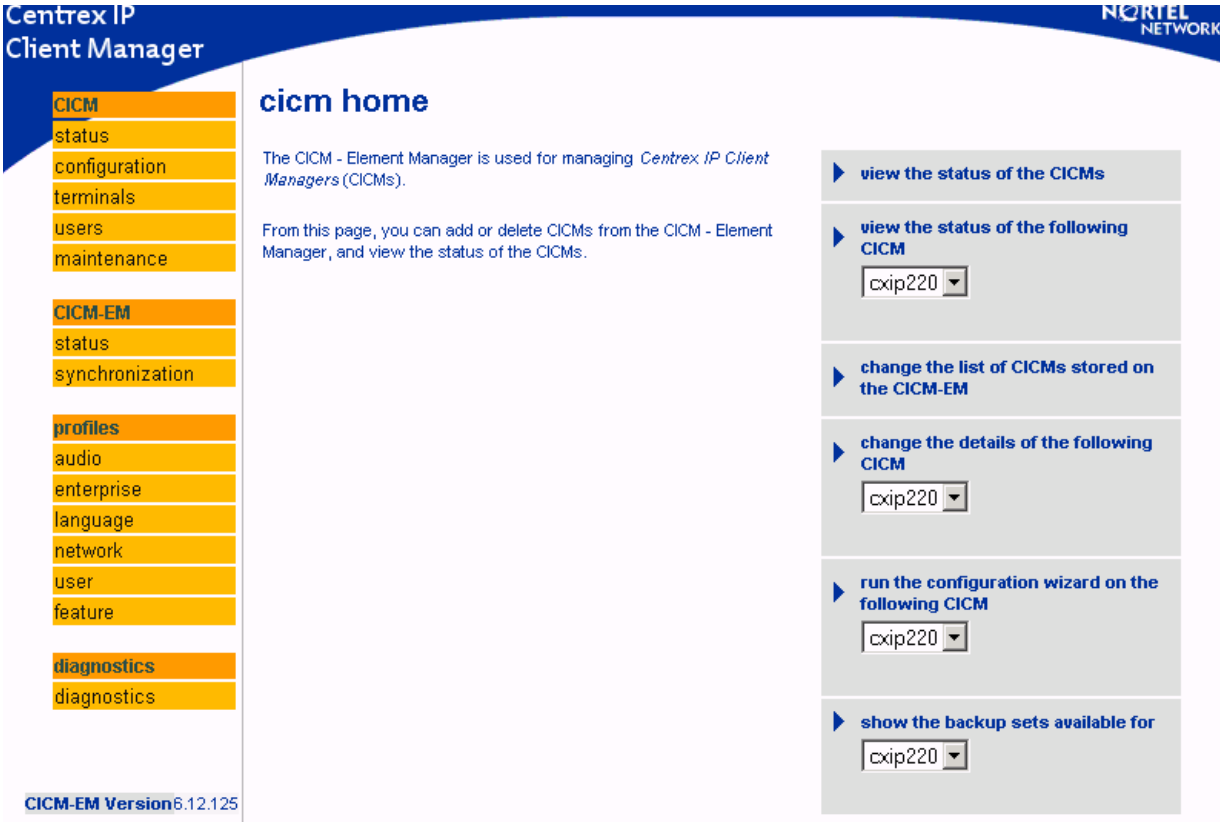
The **CICM Home** page is the first page presented after entering the CICM-EM URL into the Web browser and logging on to the Web site. This page can also be accessed by selecting **status** from the **CICM** section of the left menu bar. It is illustrated in the Figure 23 below.

The main menu on the left has been reorganized into four sections:

CICM, CICM–EM, Profiles, and Diagnostics.

From this **CICM Home** page you access pages to add or delete CICMs from the CICM EM, to view the status of a CICM, or to change IP addresses of a CICM.

Figure 23 CICM Home

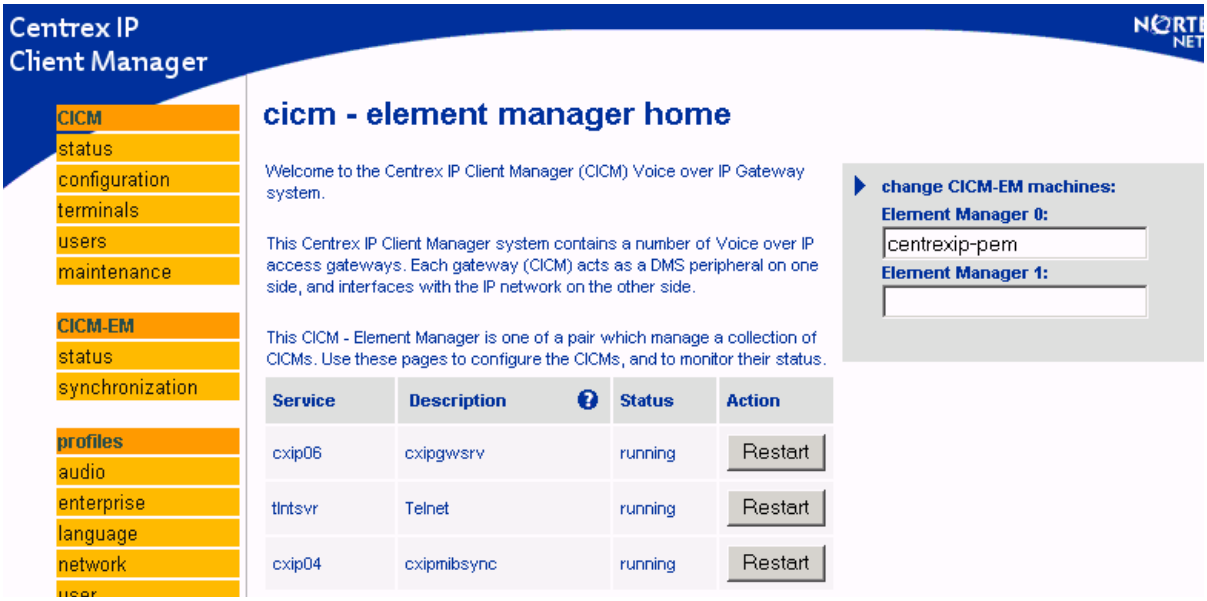


The **CICM – Element Manager Home** page is accessed by selecting the **status** option in the **CICM-EM** section of the left menu bar. This is the home page of one of a pair of CICM EMs which manage a collection of CICMs. This page is used to configure and monitor the CICMs.

This page also displays a list of the services that can be restarted from the Web, such as the Telnet service that allows a Telnet client to connect across a network and access the CICM.

Note: Click on the **?** icon for additional information about these services.

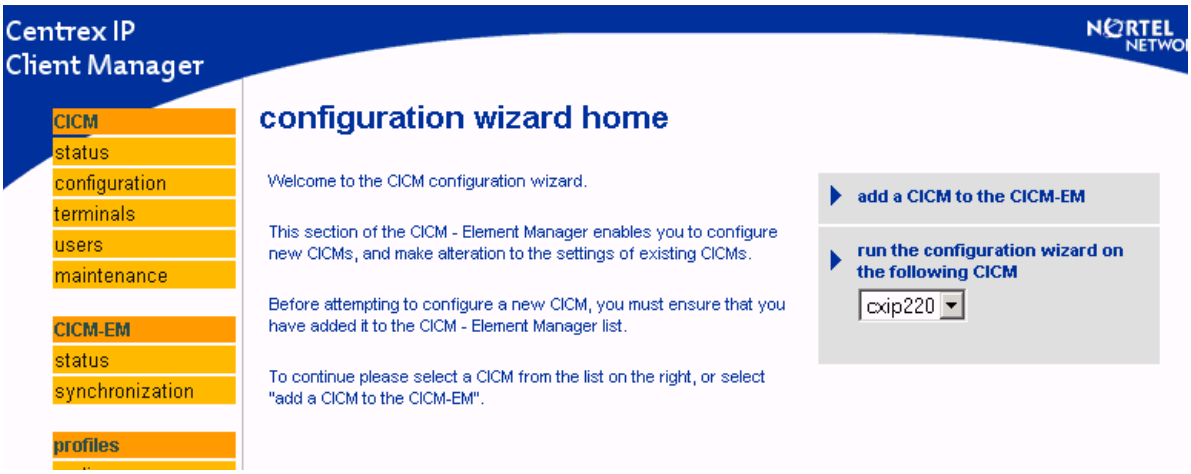
Figure 24 CICM – Element Manager home



Configuration Wizard home

The **Configuration Wizard home** page is accessed by selecting the **configuration** option from the **CICM** section of the left menu bar. It is illustrated in the following figure.

Figure 25 Configuration Wizard home

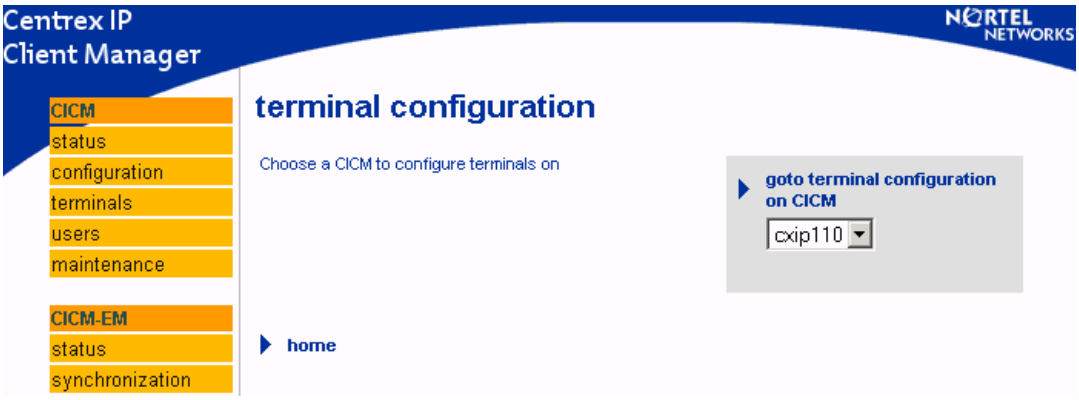


Terminal configuration

The Terminal configuration page is accessed by selecting the **terminals** option in the **CICM** section of the left menu bar. It is illustrated in Figure 26 below.

From this **Terminal configuration** page, configuration pages are accessed for each CICM, where attributes for each terminal type are specified.

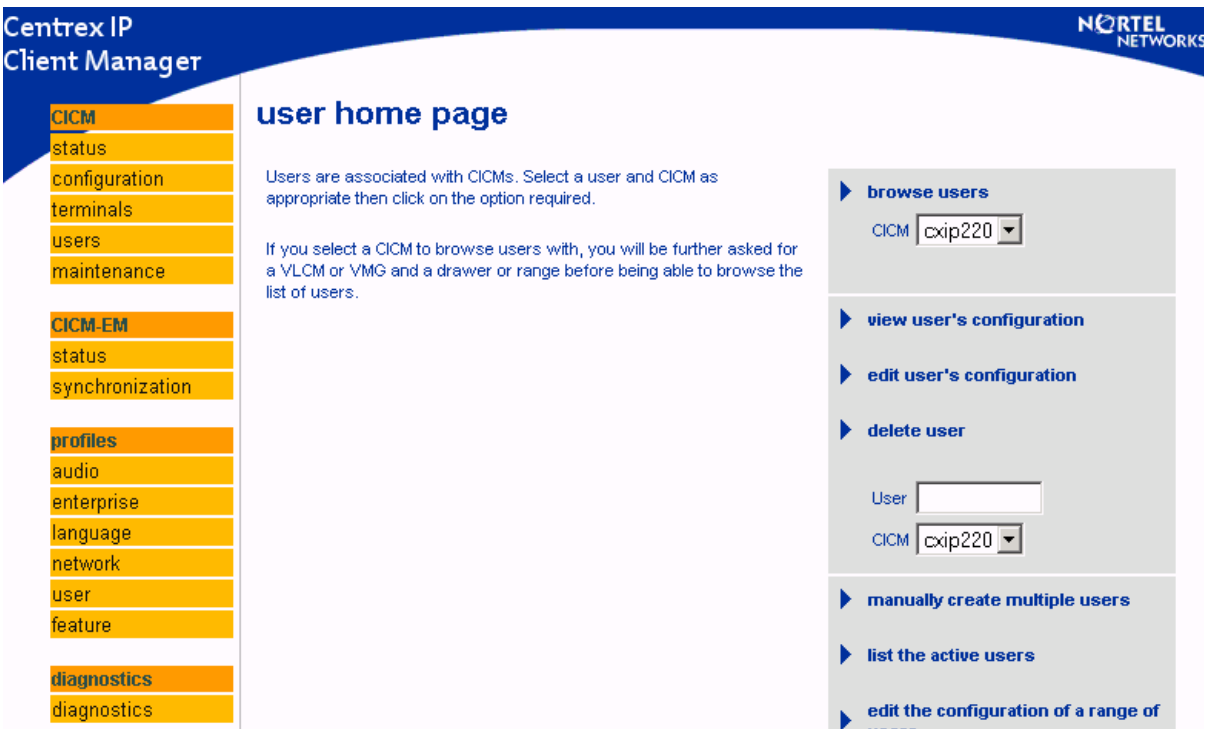
Figure 26 Terminal configuration



User home page

The **User home page** is accessed by selecting the **Users** option of the **CICM** section of the left menu. From this page users can access web pages to add or delete users on a CICM, configure users, and view or edit user configuration.

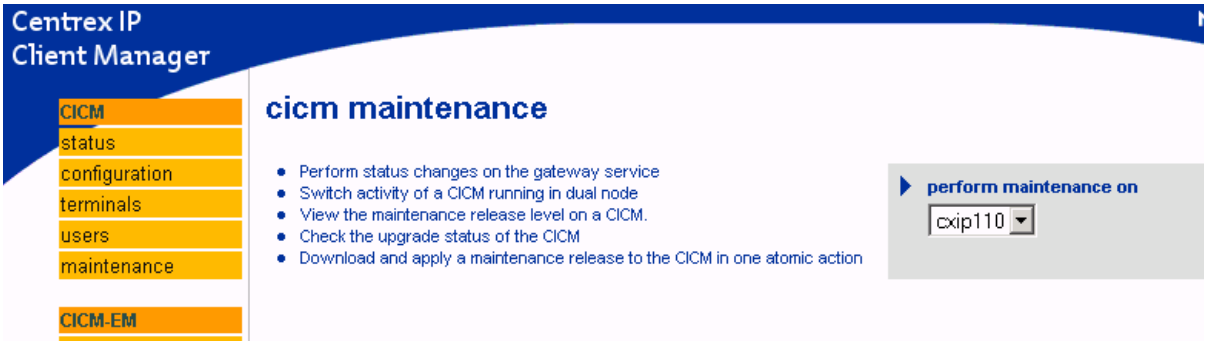
Figure 27 User home page



CICM maintenance

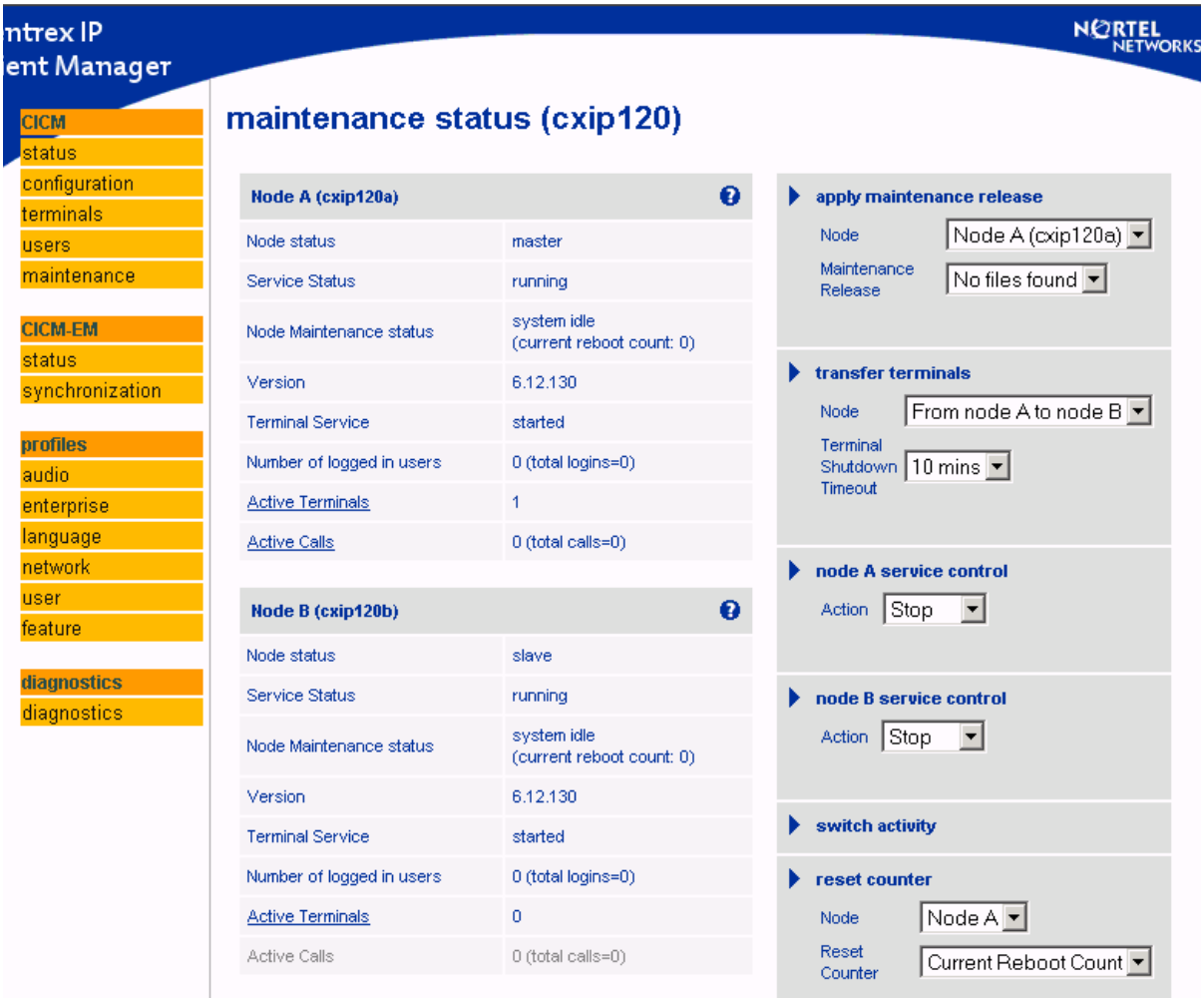
The **CICM maintenance** page is accessed by selecting the **maintenance** option from the **CICM** section of the left menu bar. It is illustrated in the following Figure 28.

Figure 28 CICM maintenance



From this **CICM maintenance** page, a CICM is selected and the **maintenance status <cicm_name>** page is accessed to perform a variety of tasks, including SWACT, a maintenance release upgrade, and a status change on the gateway. This **maintenance status <cicm_name>** page is illustrated below.

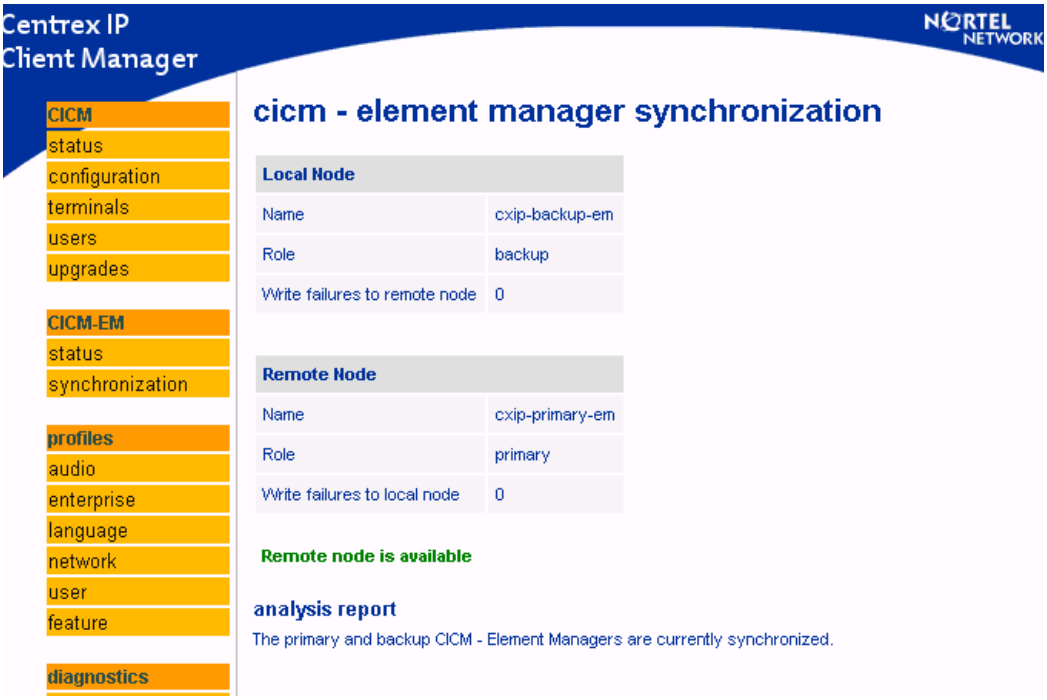
Figure 29 Maintenance status <cicm_name>



CICM – Element Manager synchronization

The **CICM – Element Manager synchronization** page is accessed by selecting the **synchronization** option from the **CICM – EM** section of the left menu bar. This page is used to check synchronization between the Primary and Backup Element Managers.

Figure 30 CICM – Element Manager synchronization

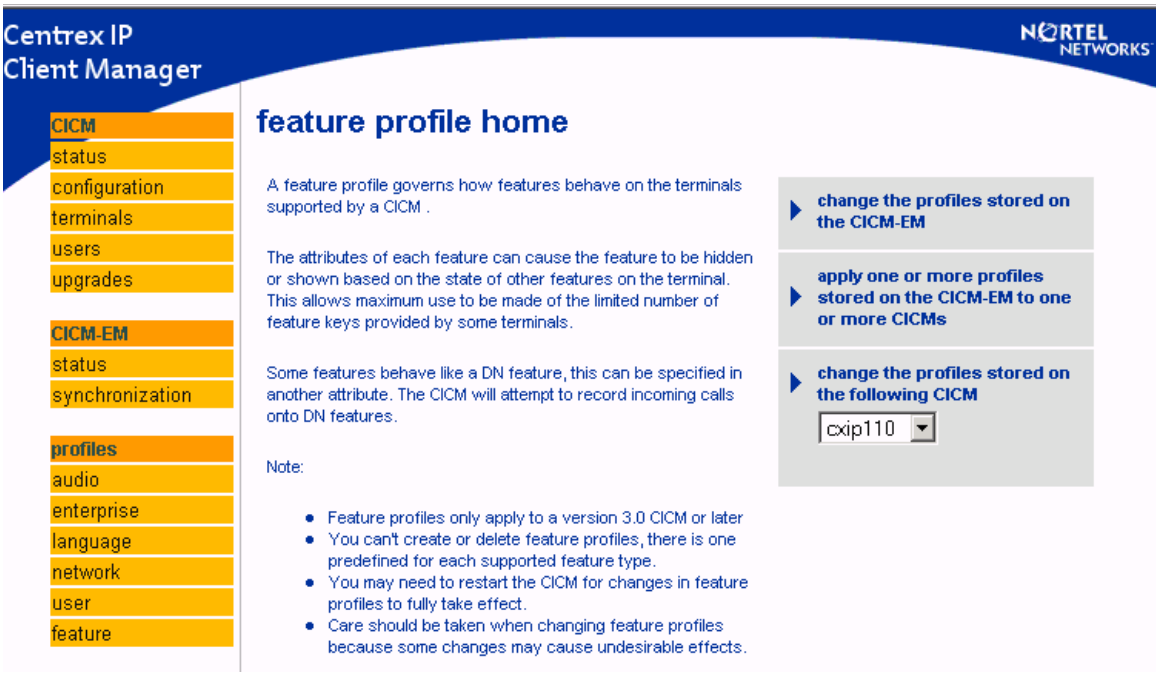


Feature Profile home

The **Feature Profile home** page is accessed by selecting the **feature** option of the **Profiles** section of the left menu. This is a new Web page for 6.12 release. A **Feature Profile** defines how features behave on the terminals supported by a CICM. A profile defines, for example, whether a feature may be hidden or shown, based on the state of related features. This allows maximum use of the limited number of feature keys.

Features profiles are not user-defined; they are pre-defined for each supported feature. Feature profiles may be selected to be stored on a CICM EM, and among those stored on the EM, they are applied to a CICM.

Figure 31 Feature Profile home



Engineering information

This section provides general engineering information, including the Succession platform, the Telco Central Office requirements, and the Admin and Client LANs. For detailed engineering information, refer to the *Centrex IP Client Manager Engineering Guide*.

Succession platform

The Series 6.12 release of the CICM is a combined hardware and software release based on Succession release SN06.2. It is applicable to both International and North American customers.

Administration LAN

The Telco's private network infrastructure is used for all administrative functions of the CICM that are not related to Voice over IP (VoIP) traffic. It is referred to as the Administration or Admin LAN in this document.

The Admin LAN is controlled by the Telco and must be a secure network not available for public access. It therefore must be physically separate from the Client LAN.

The Admin LAN is an Ethernet LAN that allows the Telco's network elements to communicate operations, administration, maintenance, and provisioning data with each other. It allows the two nodes of the CICM to communicate with each other.

The Admin LAN connects directly to the Primary Element Manager (PEM) and the (optional) Backup Element Manager (BEM). The Admin LAN connects PCs or workstations for remote access to the CICM. It is used for all administrative and access functions of the CICM. The Admin LAN does not carry call signaling (UNIstim messages) or voice traffic.

The Telco Administration LAN must provide the following resources:

- direct connection to the PEM and (optional) BEM
- a PC for performing configuration, administration and monitoring
- isolation of the Administration LAN from the Client LAN
- secured remote access to the EM(s) for Nortel Networks support

Client LAN

The Client LAN refers to a logical network that supports communication between Centrex IP clients and the CICM. This logical network extends from the carrier's Central Office network (CO-LAN) to the enterprise network, through carrier and enterprise data transport networks. The Client LAN is also referred to as the traffic data network.

In the carrier's CO-LAN where the CICM is located, the Client LAN refers to the subnet that public interfaces of the CICM belong to. These public interfaces are reachable by Centrex IP clients that may be located in enterprise networks. In the CO-LAN, the Client LAN interfaces to the CICM through a pair of redundant Ethernet switches.

In the enterprise network, the Client LAN is the enterprise LAN segment that hosts Centrex IP clients.

The Client LAN carries TCP/IP and UDP/IP packets containing call signaling (UNIStim messages) and voice traffic between the client terminals and the CICM. This LAN may also carry IP packets containing data traffic that is not related to call processing.

Because the Client LAN in the CO is reachable by clients from enterprise networks, it must be kept physically separate from the Admin LAN.

The Telco must ensure that sufficient bandwidth is available to support the number of deployed CICM clients (terminals) within all elements of the network.

Each CICM client configured on the CICM has a permanent bi-directional control messaging connection. This channel requires minimal bandwidth when the terminal is not being used.

When a call is initiated, a bi-directional voice stream is set up between media end points. Media end points in a Succession IP network include:

- the originating terminal
- TDM trunk gateways (e.g. PVG)
- analogue line gateways (e.g. MG9000, Mediatrix 1124
- voice processing servers (e.g. UAS)
- IP terminals hosted by the same CICM (e.g. an i2004 Internet Telephone)
- IP terminals hosted on another CICM

Detailed traffic capacity information is provided in the *Centrex IP Client Manager Engineering Guide*.

Security of the Admin and Client LANS

To prevent disruption of the Admin LAN by the Client LAN, or vice versa, the Client LAN is physically isolated from the Admin LAN.

Routing directly between the Admin and Client LAN is disabled in the CICM. For an administrator to test whether a client PC or i200x is visible on the Client LAN, they would have to:

- use Telnet to log into the CICM on which the user is registered
- use the **ping** or **tracert** commands from the Telnet command line to attempt to reach the IP address of the client

Note: **Ping** and **tracert** commands may not be used for deployments where the CICM and its clients are separated by firewalls and NATs, because **ping** and **tracert** messages are not able to traverse firewalls and NATs.

Pint and tracert are the only commands that have any effect on the Client LAN. No other commands are installed on the CICM, and no applications that use anything other than IP (without TCP or UDP) can be invoked because of the port filtering rules on the Client LAN interface. Only a limited set of UDP ports are allowed on the Client LAN. Other ports are blocked by the CICM CPU card.

Access to the CICM and EM via the Admin network is password protected. Access to the administration web pages on the EM is also password protected. Login to terminals on the client LAN is protected by usernames and passwords.

Firewall and NAT traversal

Firewalls and Network Address Translators (NATs) are widely used by enterprises to maintain their network security and integrity.

In a typical deployment where a Carrier provides Centrex IP as the Carrier-hosted Centrex solution to its various enterprise customers, the CICM is normally located in the Private Signalling Network in the Carrier's managed IP network, as part of the Carrier's IP address space, while IP phones reside on the Enterprise Network as part of the enterprise private IP address space behind the enterprise firewall and NAT. The IP phones communicate with the CICM through the De-militarized Zone. The firewalling and NAT functions may be provided via software residing on the enterprise edge router, or by a separate device linked to the edge router. The NAT is normally part of the firewall.

To enable a Carrier to provide Centrex IP as the Carrier-hosted Centrex solution to its various enterprise customers, it is critical that the Carrier's Centrex IP services must be able to traverse enterprise firewalls and NATs.

Firewall traversal

Nortel Networks has the following specific recommendations for firewall traversal:

- Enterprises that will use Carrier Centrex IP services should activate the "minimally restricted UDP policy" on their firewalls that normally perform dynamic stateful packet filtering, to allow a UDP packet via pre-defined Centrex IP UDP port into the enterprise if and only if the incoming packet is in response to an outgoing UDP packet.
- For Carrier's Centrex IP services, the pre-defined UDP ports must allow flow through of the following packets:
  - UNISTIM for Centrex IP control and signaling
  - RTP (Real-time Transport Protocol) for voice media streams
  - RTCP (RTP Control Protocol) for periodic network performance monitoring
  - UNISTIM FTP packets for IP phone firmware download from server to Centrex IP clients

For details on UDP port assignments, see the *Centrex IP Client Manager Engineering Guide*.

NAT traversal

Nortel Networks' Centrex IP supports all types of Network Address Translation (NAT) (also referred to as a NAPT – Network Address and Port Translator), regardless of whether it is a full cone NAT, restricted cone NAT, port-restricted NAT or symmetric NAT. Every NAT must have at least a two-minute UDP lease period.

The RTP portal provides secure interworking for calls between end points in different enterprise networks and provides NAT traversal capabilities for these end points.

For the correct operation of the CICM when using the RTP portal, the NAT must be provisioned on both the SESM and the CICM Element Manager.

For details of RTP portal usage and how NAT traversal works, please refer to the *Centrex IP Client Manager Engineering Guide*.

CICM performance criteria

For an overview of traffic loading and other performance considerations, refer to the *CICM Performance Management* document. For other and related engineering details, refer to the *Centrex IP Client Manager Engineering Guide*.

Robustness

The design goal of the CICM is to minimize the customer service impact for any single point of failure. However, particular failures may cause a degradation in the service provided. For an overview of how CICM copes with failure conditions, refer t*o the CICM Fault Management* document.

Situating the CICM

The CICM 6.12 should be co-located with the CS2000. When co-located, the CICM 6.12 can leverage on the CS2000 CS-LAN infrastructure, which consists of two Passport 8600 routing switches. In addition to supporting the CS2000 Core and other CS2000 components, the dual-PP8600's provide the LAN connections between the CICM and:

- The Telco's administrative LAN, which includes the Primary and Backup Element Managers.
- The client LAN.

The CentrexIP Client Manager can be co-located with or sited remotely from the CS2K GWC. Nortel recommends co-locating the CICM with the CS2K.

Each CICM must have an Admin LAN connection that is available permanently for the CICM to remain in service.

Product standards and regulatory requirements

This section provides an overview of product safety standards, EMC standards, and telecom center installation standards (including NEBS and ETSI).

Product safety standards

The international product safety requirements are:

- EN 60950 (1992) including Amendments 1, 2, 3, 4, and 11. Specification for Safety of information technology equipment, including electrical business equipment.
- IEC 60950, Second Edition, 1991 including A1-A4 | Safety of Information Technology Equipment
- TS001 (AS3260 + A1) Australia Product Safety Standard

North American safety requirements are:

- UL 1950 3rd Edition, Rev. 6/22/98 - Information Technology Equipment
- CSA C22.2 No 950-95, 3rd Edition - Information Technology Equipment

EMC standards

International EMC requirements are:

- EN 55022: 1998 Class A Emissions
- EN 55024: 1998 Immunity

North America EMC requirements are:

- FCC Verification Rules contained in Title 47 of the CFR, Part15, Subpart B for a Class A Digital Device CISPR22

Telecom center installation standards

The international Telecom center installation standards requirements are:

- EN300-386-2
- ETS 300 019-1-1, 2, 3, 2-4 pr A1

The North America Telecom center installation standards requirements are:

- NEBS GR-63 Core tests Physical Protection
- NEBS GR-1089 Core tests EMC and Electrical Safety - Generic Criteria for Networked Telecommunications Equipment
- SBC Local Exchange Carrier Equipment Requirements #TP76200MP, latest version
- AT&T NEDS MILD# 9069, latest version
- Verizon RNSA-NEBS-95-0003, Rev 10A, Verizon Conformance Requirement

International and North America products

CICM is designed for both International and North American (NA) customers.

Hardware

This section describes the hardware components of the Series 6.12 CICM.

Hardware overview

The Series 6.12 CICM hardware platform provides the functionality that allows CICM clients to access the full range of MGC Centrex services using VoIP.

The CICM is based on a CompactPCI architecture. It contains features that provide support for high availability, serviceability, and upgrade without incurring a total loss of service. The CICM provides runtime status information by means of visible alarms and remote alarm reporting consistent with the Minor/Major/Critical alarm schema of the CS2K Core.

Hardware frame

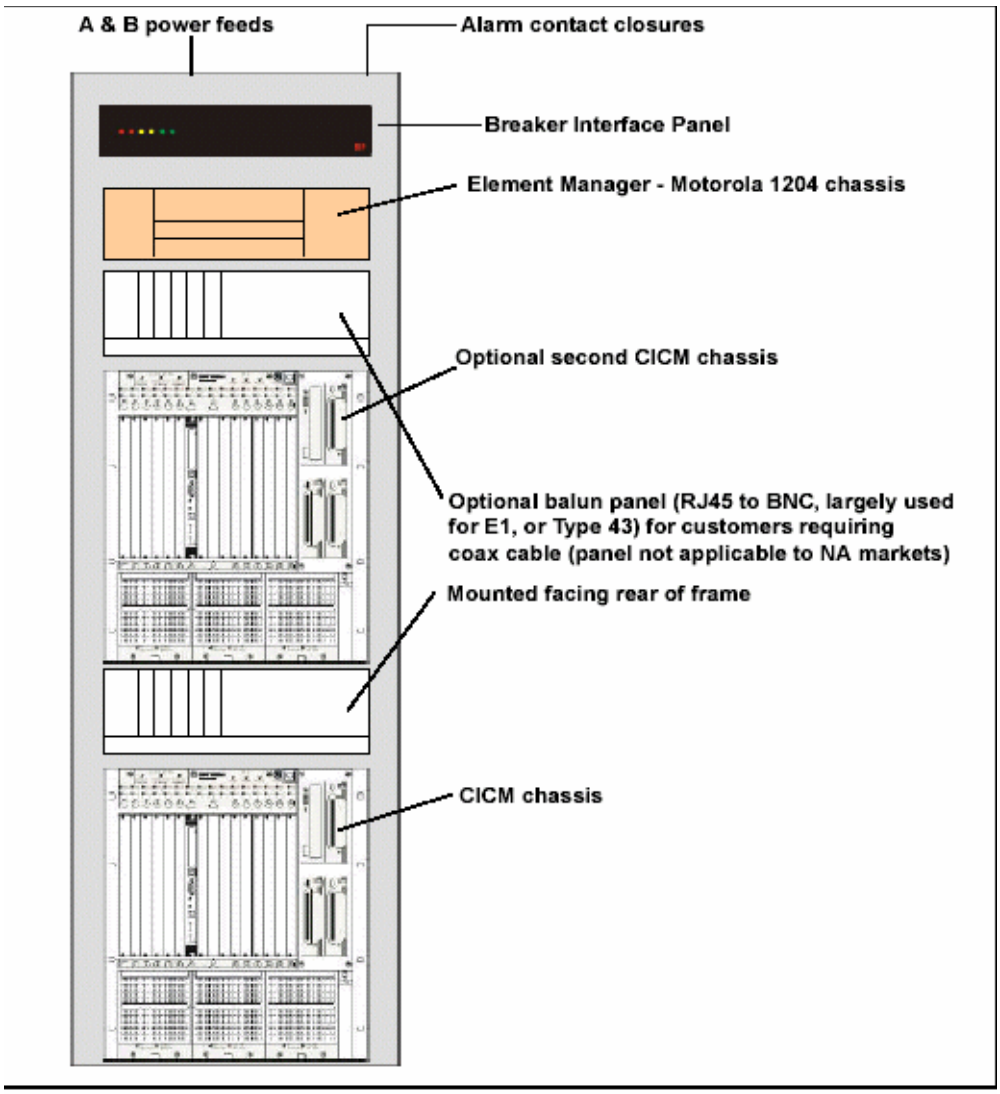
The CICM is shipped as a series of components fitted into a standard NEBS compliant 19” frame (also called a cabinet). The frame used is the PTE2000. The components of the frame are:

- **A Primary Element Manager.** This component is optional in the sense that a CICM can be ordered with no Element Manager installed. However, an Element Manager is essential to CICM operation, and the customer must provide the Element Manager platform described in the *Platform* section of this document. A backup Element Manager can be installed in an additional rack.
- **One or two CICM chassis.** Each chassis contains processor cards.

Where an Element Manager is already in place (e.g. when expanding an existing network), a CICM can be ordered without an Element Manager installed in the chassis, since an Element Manager can support up to 100 CICMs.

The following Figure 32 shows the component arrangement in the CICM cabinet.

Figure 32 Component arrangement in the CICM cabinet



The specifications of the PTE2000 frame are summarized in the following table:

Table 22 PTE2000 Frame Specifications

Parameter	Specification	
Height	2128.62 mm	83.8 in
Width	598 mm 653.62 mm	23.5 in 25.7 in (with side panels)
Depth	604 mm	23.8 in
Weight (estimated)	295 kg	650 lbs
	320 kg (with shipping pallet & sleeve)	700 lbs (with shipping pallet & sleeve)
Power	Voltage: -41.5 to -57 VDC	
	Inputs rated to 65A	
	Typical current drain: 21A (for 2 fully loaded CICM chassis and 1 EM)	
	Maximum current drain: 22A @ 50.25 VDC per feed (assuming one power feed failure, for 2 fully loaded CICM chassis and 1 EM)	

Installations with AC power supplies will require AC to DC power conversion equipment to interface with the frame. Two suitable options are:

- Astec Power Min3500 (see www.astec.com for details)
  This is the standard deployment, if required.
- C & D Technologies AGM-600 (see www.cdpowercom.com for details)

The DC powered NEBS-compliant hardware configuration or the earlier AC powered configuration are both supported and have identical software features. The DC and AC hardware configurations interwork.

The following table provides a comparison of the DC powered NEBS hardware configuration versus the AC powered hardware configuration.

Table 23 Comparison of DC to AC powered NEBS hardware

DC Powered NEBS Compliant Hardware Configuration	AC Powered Hardware Configuration
CICM chassis (Motorola CPX8216T), DC powered with updated CPU card	CICM chassis (Motorola CPX8216T), AC powered
Balun panels (Cambridge Connectors)	Balun panels (Cambridge Connectors)
Element Manager updated: • NEBS compliant • DC powered	Updates N/A
Frame PTE2000 (Solectron) updated: • NEBS compliant • Supports A & B DC power feeds	Updates N/A
Breaker/Alarm panel (Astec Breaker Interface Panel)	N/A
Removed: • Baystack data switch • In frame screen & keyboard	N/A

Element Manager

The Element Manager (EM) is the principal management platform for the CICM. The EM is the device used to configure, monitor, and administer CICMs and their clients. Although the CICM's call processing operates without the Element Manager, the EM is required as the administrative interface to the CICM.

The functions of the EM include:

- acting as a Web server for the Web-based user interface used to configure, monitor, and administer the CICM and its clients
- performing security checks and authorizations.
- providing the database for CICM configuration data

- serving as a backup device for CICM configuration files by storing the backup configuration files and executing the automatic backup process
- providing storage for user profiles and CICM software upgrades
- storing the firmware upgrade files for the i2004/2002 Ethersets and the software upgrades for the m6350 SoftClients.
- polling the CICMs at regular intervals for status information
- providing SNTP time synchronization for a network of CICMs over different timezones. The Element Manager supplies the absolute time and each CICM applies local timezone corrections.

The EM is usually co-located with the CICM; it can be installed in the same hardware rack as the CICM.

Element Managers are normally configured in redundant pairs: a Primary Element Manager (PEM) and a Backup Element Manager (BEM). Although a CICM requires only one Element Manager, Nortel Networks recommends configuring EMs in redundant pairs to provide redundancy and to avoid a single point of failure.

The PEM is ordered with, and assembled into, the first 19” frame shipped to the customer. The BEM is normally ordered with and assembled into the second 19” frame shipped to the customer. The two frames containing the PEM and BEM do not need to be co-located on the same site, but routing must be available via the Admin LAN such that the PEM, BEM, Admin PC(s) and all CICMs are directly addressable via IP.

Each EM or pair of EMs can support up to 100 CICMs. The Element Manager connects directly to the Admin LAN. The 6.12 Element Manager with 6.12 hardware runs Windows 2000 Server with Terminal Services.

Element Manager and CICM backup and restore
Series 6.12 release includes a Backup/Restore tool that allows the administrator to take offline disk images of both the CICM and Element Manager. Since this tool requires a shutdown of the Element Manager, its use temporarily prevents access to the Web-based administration interface for customers not equipped with a Backup Element Manager.

Element Manager platform

In Series 6.12 the Element Manager is based on the Motorola CPX8216T 4-slot cPCI chassis hardware platform. This is a NEBS compliant system with the following characteristics:

Table 24 Motorola CPX8216T Chassis Specifications

Characteristic	Specification
Dimensions	Height: 133.35 mm (5.25 in) Width: 480 mm (18.9 in) Depth: 381 mm (15 in)
Weight (estimated)	13.6 Kg (30 lb) unloaded 15.9 Kg (35 lb) fully loaded
Slots	4 CompactPCI slots (1 system processor, 3 hot swap I/O slots)
Power supply	-36 to -72 VDC 6.4A maximum input current at -36VDC 4.5A maximum input current at -48VDC

The system processor slot holds a Motorola CPV5370 CompactPCI processor board, which uses a Pentium III BGA2 processor at 700MHz with 512Mb of RAM.

The Element Manager runs Windows 2000 Server with Terminal Services. A Series 6.12 CICM EM can manage Series 2.4, 2.5, and 6.1x CICMs

The Element Manager is supplied with a backup/restore tool that allows the administrator to take offline disk images of both the CICM and Element Manager. Since the tool requires a shutdown of the Element Manager, its use will temporarily prevent in any access to the Web-based CICM configuration interface for customers not equipped with a Backup Element Manager.

The EM also has the ability to perform automatic in-service backups of CICM configuration data.

Element Manager security

Access to the web-based Element Manager interface is controlled by Internet Information Services (IIS). The following security safeguards are in place (by default) to eliminate various security threats:

- authentication is required to obtain access to the element manager
- users cannot access directories or manipulate files

The following additional security options are also available:

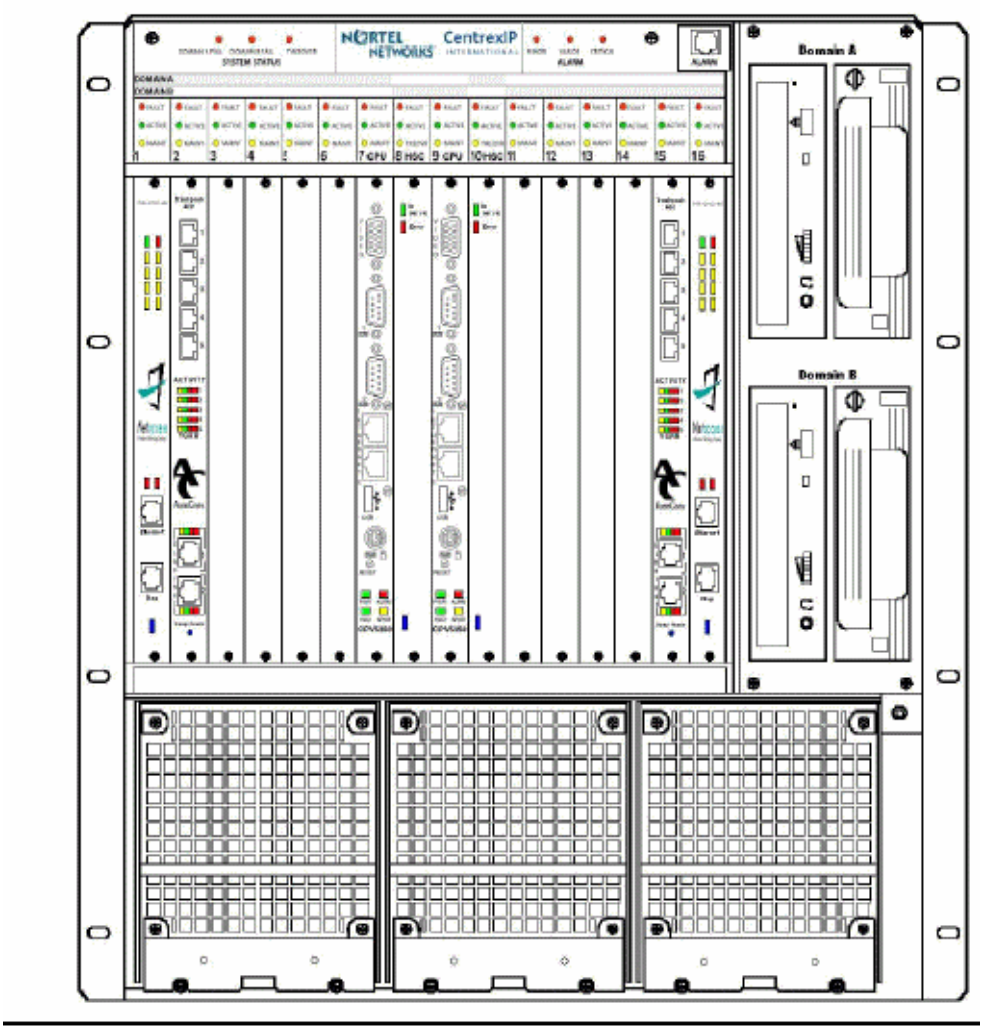
- SSL encryption may be configured to provide privacy of sensitive information
- certificates may be configured to provide additional authentication
- auditing may be configured to monitor security activities for unauthorized access

CICM chassis

The CICM is housed in a Motorola CPX8216T chassis. An example of the chassis is shown in the following Figure 33.

Note: This illustration is an example only. The position, number and version of each card in the chassis may not be precisely as shown.

Figure 33 CICM chassis



The 6.12 CICM is designed based on the CS2000 philosophy of duplicating hardware and software resources in order to provide high reliability and availability without incurring total loss of service.

The CICM is split into two domains: Domain A and Domain B. Each domain is controlled by its own processor card running the Windows NT Embedded operating system and CICM software. From the software perspective, each domain is regarded as a separate CICM node.

The CICM monitors its own internal status. Each CICM node can be restarted individually, if necessary, to provide resilience in the event of software failures. Refer to the *Restart (soft reboot) the node* procedure in the *Fault Management* section of this document.

All major hardware components of the CICM are hot-pluggable (i.e. they can be removed and replaced without powering down the chassis).

> ***Note:*** Although hot-pluggable cards can safely be inserted in or removed from powered-up hardware, a WinNT restart is required before an inserted card is available for use by the CICM software.

These major components are also hot-swap capable (i.e. they can be removed, replaced, and brought back into service without restarting the software or powering down the chassis). However, the current operating system does not support hot swapability. When appropriate support becomes available in the operating system, the hot-swap feature will be operational.

Processors

The single backplane chassis contains two separate cPCI bus domains (A and B), each with its own CPV5370 processor card running the Windows NT operating system (Windows NT Embedded 4.0 Class 3 Server). Each card has a Pentium III BGA2 processor at 700MHz with 512Mb of RAM. Each domain can be independently hardware reset and rebooted without affecting the other domain (except for alarm bar behavior, where system and telco alarms function only when domain A is running).

The processor handles such tasks as:

- UNIStim session management
- Client interfacing
- Media stream control
- Remote configuration of the CICM

Administration Ethernet and LAN interfaces

Access to CICM administrative functions is provided via an Ethernet interface, which is physically separate from the LAN interface that carries VoIP traffic and client signalling.

CICM software is administered (configured and managed) from:

- Any Windows NT machine with the appropriate access rights on the service provider's Admin LAN, using a combination of native Windows NT remote management functions (e.g. Windows NT Event Viewer), and the Nortel CICM management tools accessed

via the Element Manager Web pages. Refer to the *CICM Configuration* and *CICM Administration and Security* documents.

- Any PC running Microsoft Internet Explorer (IE), version 5.0 or later. Note that other Web browsers can use the Web-based management interface, but only Internet Explorer is supported.

The Administration interface can also be used to gain access using Telnet to the base operating system from which tools can be run and various logs can be viewed.

Admin LAN redundancy Protection against a single point of failure in the Ethernet network is achieved by connecting the CICM to two Ethernet switches rather than one. These switches connect the CICM to the rest of the Telco network.

If all the CICM Ethernet ports are connected to a single Ethernet switch, this switch becomes a potential single point of failure. If the switch fails for any reason, or a cable or adapter becomes faulty, the two nodes of the CICM would no longer be able to communicate with each other. In this situation, each CICM node incorrectly reports the mate node to the MGC as missing. The MGC would then put the CICM out of service and report that the nodes are reporting a state mismatch. Avoidance of this is achieved by installation of two Ethernet switches.

There are four Ethernet networks possible:

- The **CICM Admin LAN** is a private network for inter-node and Element Manager communications. The traffic on this LAN is not secured, so the Admin LAN is isolated to provide security.
- The **CICM Client LAN** is the network on which all media and call signalling is carried. This network extends to the customer sites where terminals are located.
- The **Network Operations LAN** is an optional LAN used to administer network devices such as routers and switches. Network device administration should be disabled on all other LANs.
- The **Telco Administration LAN** is an optional LAN used by the Telco to administer its captive office equipment. The EM is connected to this LAN as the Operations, Administration, and Maintenance (OAM) platform for the CICM devices.

Of these four possible LANs, the Admin and Client LANs are mandatory. The two optional LANs, the Network Operations LAN and the Telco Administration LAN, may be combined with the Admin LAN, depending on the security requirements of the Telco.

Telephony bus

The Motorola CPX8216T chassis includes an integrated H.110 telephony bus.

CPU cards

For Series 6.12, the single backplane chassis contains two separate PCI bus domains (A and B), each with its own CPV 5370 Intel processor card running the Windows NT operating system (Windows NT Embedded 4.0 class 3 server).

Each Central Processor Unit (CPU) card has a Pentium III BGA2 MMX processor at 700Mz with 512 Mb of RAM. Each domain can be independently hardware reset and rebooted without affecting the other domain (except in the case of alarm bar behavior: system and telco alarms function only when domain A is running).

The CPV 5370 processor card has provision for supporting a single PMC daughter card, which can be used to provide additional processing power.

The CPU tasks includes:

- Layer 3 signalling
- Call control
- Media stream control
- VMG emulation
- UNIStim session management
- Client interfacing
- Communication with the host
- Communication with the client terminals using the UNIstim protocol
- Load sharing between the CPU pair
- Remote configuration of the CICM
- Responding to regular polls from the PEM

Dual node operation

Under normal operation, each CICM node appears to the CS2K as a VMG unit.

A client can initially log on to either CICM node and receive service. With one unit busied, the CS2K will only send messages to one side of the CICM.

If one of the CICM nodes becomes unusable (e.g. due to a hardware failure or during an upgrade), the non-failing node can still provide service. When one node becomes unusable, all current calls on the failed node will be dropped, and clients may need to log in again to regain service.

Ethernet switch

An Ethernet switch is required to provide the LAN connections between the CICM and:

- the service provider's Admin LAN, which supports the PCs through which the service provider configures and monitors the CICM and its clients, and
- the client LAN

Although the CICM requires only one Ethernet switch to operate, two Ethernet switches are required to provide Admin LAN redundancy, and to separate client and admin traffic for security purposes.

Note 1: With one switch, if there is failure, the two CPU cards will not be able to communicate with each other via the Admin LAN. Each CPU card will then tell Succession that its mate node is missing, and Succession will take both nodes out of service.

Note 2: Two Ethernet switches do not provide Client LAN redundancy. If a switch is lost, the Ethersets active on that switch will drop and then recover.

The CICM 6.12 should be collocated with the CS2000. As such, the CICM 6.12 can leverage on the CS2000 CS-LAN infrastructure, which consists of two Passport 8600 routing switches. In addition to supporting the CS2000 Core and other CS2000 components, the dual-PP8600's provide the LAN connections between the CICM and:

- the service provider's Admin LAN, which includes the PRimary and Backup Element Managers
- the client LAN

The base configuration of the PP8600 being used in Succession CS2000 CS-LAN deployment is:

- A10-slot Passport 8010CO chassis on Passport 7480 Universal Frame
- One Passport 8691SF CPU Module
- Two (2) Passport 8632TXE Routing Switch Modules, each supporting 32 Fast Ethernet ports

Depending upon the application and actual deployment requirement, the remaining seven slots may be used to add additional I/O modules for supporting expanded Ethernet connections and diversified Gigabit Ethernet, 10 Gigabit Ethernet, ATM, or Packet over SONET (or SDH) WAN interfaces. Some of these expansion modules are:

- Passport 8632TXE Routing Switch Module supporting 32 Fast Ethernet ports
- Passport 8648TXE Routing Switch Module supporting 48 Fast Ethernet ports
- Passport 8608GBE GBIC Routing Switch Module supporting eight (8) Gigabit Ethernet ports (mostly for WAN interface)
- Passport 8672 ATME 2-Slot MDA Baseboard, supporting up to eight (8) OC-3 or two (2) OC-12 ports for ATM WAN interface.

The key features of the dual-PP8600 based CS2000 CSLAN are:

- NEBS-3 compliance
- Superior reliability with 99.99999% availability
- Up to 128 Gbps switching bandwidth per switch
- Wire-speed routing of 96 million packets per second
- Support for IEEE 802.1p (Priority Marking)
- Support for IEEE 802.1Q (VLAN Tagging)
- Support for IETF DiffServ
- 802.1p to DiffServ mapping
- Equal Cost Multi-Path (ECMP)
- Multi-Link Trunking (MLT)
- Split Multi-Link Trunking (SMLT)
- Distributed Multi-Link Trunking (DMLT)
- Virtual Router Redundancy Protocol (VRRP)
- Support for high FE port density: up to 300 FE ports per switch through expansion modules, or 600 FE ports per CS-LAN
- Support of diversified WAN interfaces such as Gigabit Ethernet, 10 Gigabit Ethernet, ATM, or Packet over SONET (or SDH)

The Ethernet switches must be purchased separately, and can be supplied by the service provider or by Nortel Networks. The Ethernet switches must provide support for 802.1Q VLANs. The CS2000 deployment uses dual Passport 8600 Ethernet switches, and Nortel

Networks recommends that the CICM 6.12 also utilize these switches to provide network connectivity.

Note 1: The switch cannot be installed in the frame containing the CICMs, since this would invalidate its electromagnetic compatibility (EMC) compliance.

Note 2: If Admin LAN redundancy is required, two Ethernet switches must be provided.

Nortel recommends the BPS2000 Ethernet switch or equivalent. Following is a list of the primary features of the BPS2000. Any Ethernet switch provided by the service provider must provide at least an equivalent functionality.

- NEBS-3 compliance
- Aggregate frame forwarding rate 3.2 million pps
- Support for 802.1p (Priority)
- Support for 80201Q (VLAN tagging)
- Support for IETF DiffServ
- Multi-Link trunking
- IP traffic shaping
- Four hardware-based queues
- Web-based GUI management tools
- Support for remote monitoring (RMON)
- Support for SNMP V3
- Common Open Policy Support (COPS) via Optivity Policy Services
- 2.5 Gbps backplane capacity
- 24 10/100 BaseT Ethernet ports
- Gigabit Ethernet uplink
- 802.1 p to DiffServ mapping
- Up to 8 BPS2000 may stack up to perform as a single switch.

Refer to the *CICM Series Engineering Guide* for a detailed definition of Ethernet switch requirements and additional engineering details.

Call Server 2000

Call Server 2000 (CS2000 or CS2K) is a communication server providing call processing capabilities. In terms of the MEGACO network architecture, it provides Media Gateway Controller (MGC) functionality.

Together with various types of gateway and server, it can support VoIP (Voice over IP) or VoATM (Voice over ATM), depending on the type of backbone packet network used.

Capabilities of the CS2000 include:

- Basic connectivity and network element control.
  - Control over the media gateways that provide the bearer connection interface between the packet network environment and other TDM or access networks. In ISN06, CS2000 supports the following types of access via media gateways:
    - CCS7 trunk access to/from the PSTN or another TDM network.
    - PRI and QSIG access for digital PBXs and other PRI-enabled devices.
    - V5.2 access, currently for analogue subscriber lines only.
    - Analogue line access via a variety of gateway types, including CPE gateways attached to customer LANs or cable networks.
    - ADSL access via terminations on high-capacity line media gateways.
  - Control over media servers supporting capabilities such as announcements and conferencing over the packet network, for example the Universal Audio Server (UAS).
  - Originations and terminations for inter-CS signalling across the packet network to/from other CS2000s and compatible MGCs such as IMS.
  - Originations and terminations for TDM-side CCS7 signalling.
- Call processing.
  - A wide range of internationally-proven call processing agents and protocols.
  - Translations and routing for calls entering, leaving and crossing the packet network.

  - Support for requests to apply tones and announcements.
  - Support for billing, event reporting and performance monitoring.
- Service support.
  - Support for specific sets of value-added features.
  - Support for general-purpose service delivery platforms.
  - Support for regulatory features (e.g. number portability).

A CS2000 can be regarded as a single node, but it is not monolithic. The capabilities listed above are provided by separate CS2000 components, of which the most important are Gateway Controllers (GWCs). These are used for two main purposes:

- To serve as controllers for media gateways, controlling their operation via device/media control signalling based on packet network protocols.
- To support communication between peer communication servers for the handling of networked calls. This is accomplished via inter-CS signalling, also based on packet network protocols.

For additional information on the CS2000, please refer to the *CS2000 Product Description* document.

CICM in the Succession network

The CICM provides the control interface between the GWC and distributed CICM IP clients on a managed IP network. It communicates with the GWC using the H.248 IP interface.

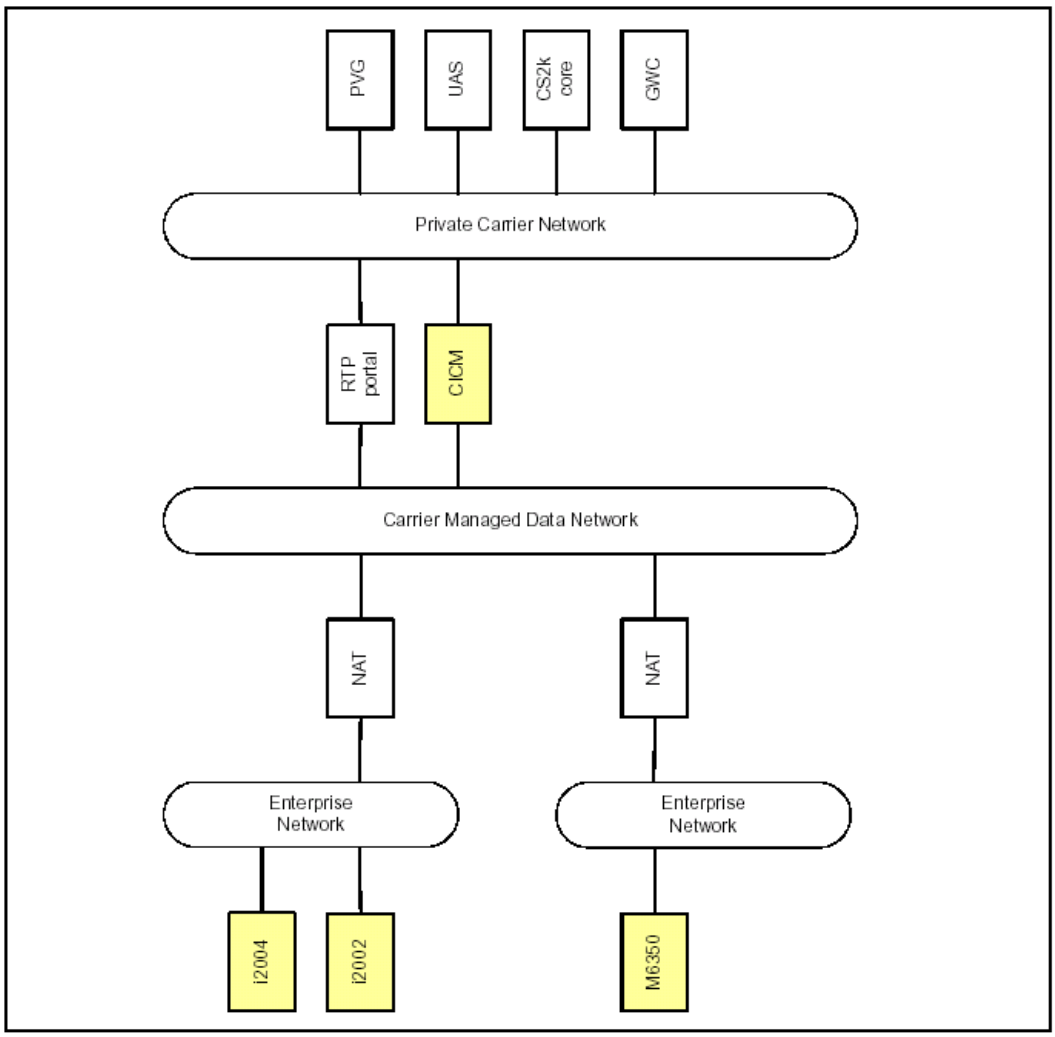
H.248 is a joint ITU-T / IETF protocol defined in ITU-T Recommendation H.248 and IETF RFC3015. It fully supports the same basic device/media control capabilities as protocols such as ASPEN. More importantly, it is based on a more flexible functional mode that provides better support for multimedia and conference capabilities.

The CICM is not a media gateway. It is better described as a terminal server or signaling gateway. Media streams in a Succession IP solution are routed directly between media end-points. The CICM terminals (e.g. i2004 Internet Telephone) are media end-points. Other media end points in a Succession IP network include:

- TDM trunk gateways (e.g. PVG)
- Analogue Line gateways (e.g. MG9000, Mediatrix 1124)
- Voice processing servers (e.g. UAS)
- IP Terminals hosted off another CICM

The following Figure 34 shows a generic Succession IP network with a CICM serving IP terminals in two enterprise customer networks. The diagram illustrates general connectivity only, and not the details of network engineering.

Figure 34 CICM and clients in the Succession network



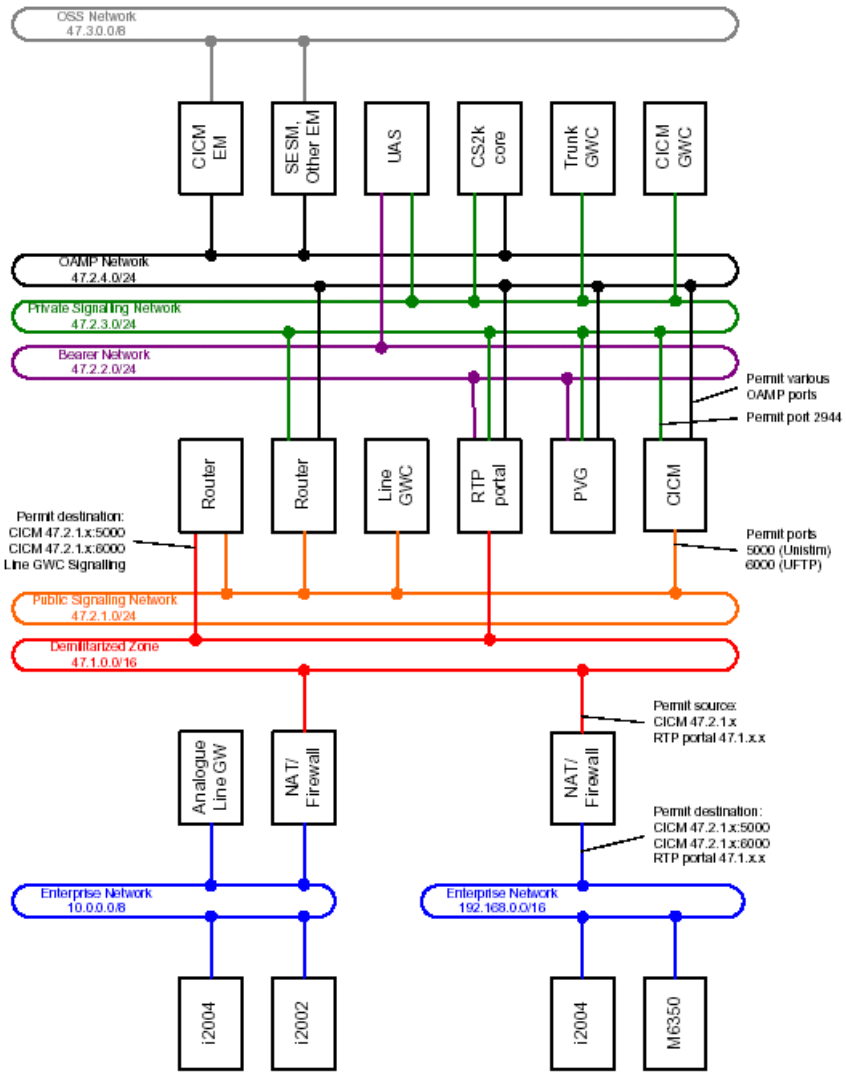
The CICM operates as a “lights out” server; that is, it has no keyboard, mouse, or monitor. Once it has been connected and powered up, all further maintenance is performed remotely from a PC on the admin LAN via a Web-based interface.

Network engineering

Protection against a single point of failure in the Ethernet network is achieved by connecting the CICM to two Ethernet switches rather than one. These switches can then be connected to the rest of the Telco

network. The following Figure 35 provides a reference network for CICM in the CS2000 network.

Figure 35 CICM in the CS2000 network



The sub-networks shown in Figure 35 are described as follows:

- The Operations Support System (OSS) network provides administrator access to Operations, Administration, Maintenance and Provisioning (OAMP) functions.
- Element managers manage their elements (and potentially each other) using the OAMP network.
- The Private Signaling Network is used for all call signaling between servers (e.g. CS2K core to trunk GWC) except those that require

connectivity to devices outside the Central Office (e.g. GWC serving remote analogue line gateways).

- All voice packets inside the Central Office are transmitted on the Bearer Network.
- The Public Signaling Network hosts call servers needing to transmit call signaling directly to devices outside of the Central Office.
- The Demilitarized Zone (DMZ) is a non-secured network connecting multiple enterprises to common resources (such as the Succession network and the Internet).
- Two enterprise networks are shown in Figure 35. Each network uses a private addressing scheme and is isolated from the DMZ by a NAT device and firewall.

Figure 35 does not make a distinction between physical connectivity (a dedicated network adapter) and logical connectivity (VLANs used to multiplex functions onto a single adapter while maintaining isolation at layer 3).

Although the diagram shows a single GWC dedicated to serving the CICM, this is not a restriction. A single GWC can serve many media gateway nodes as long as they are the same basic type. A CICM is a large IP lines gateway type. Currently the only other large lines gateway is the MG9K. Therefore a CICM can share a GWC with another CICM or an MG9K, but cannot share with small line gateways such as a Mediatrix 1124. The location of the media gateway nodes being served determines the positioning of the GWC in the network.

In the carrier network where the CICM is located, a carrier firewall is recommended to protect CICM from the public interfaces that are reachable from clients in enterprise networks. This carrier firewall must meet the following requirements:

- It must be a statefull inspection firewall with incoming and outgoing firewall rules. The firewall connects through a set of pre-defined UDP ports to only allow Centrex IP signaling traffic to flow between authorized Centrex IP clients in enterprise networks and the CICM located in the carrier CS-LAN.
- It must be QoS-enabled to maintain enterprise-to-carrier QoS consistency.
- It must have high throughput and high reliability.
- It must have diversified WAN interfaces to support the carrier MAN/WAN technologies.

Refer to the *CICM Engineering Guide* for further details.

Network interfaces

CICM processors work in pairs. The two processors are referred to as Node A and Node B. Each processor has two network adapters: primary and secondary. The primary adapter is reserved for OAMP functions and inter-node communications.

Each CICM processor requires three logical network interfaces (other than OAMP):

- H.248 call signaling to and from the GWC
- Unistim/UFTP signaling to terminals
- Redundant connection for inter-node signaling

To achieve the highest degree of isolation between these functions, they are multiplexed onto the secondary adapter using VLANs.

Each CICM processor has four logical network interfaces. They are called A1-A4 on Node A and B1- B4 on node B. The interfaces are summarized in Table 25

Table 25 CICM Network Interfaces

Interface	IP Addresses	Usage	Restrictions
A1/B1	This interface on each node has one IP address on the OAMP network.	Administrative functions from CICM-EM. Primary interface for inter-CICM node communications.	None
A2/B2	This interface on each node has one IP address on the OAMP network.	Backup interface for inter-CICM node communications. Can be used for some OAMP functions from CICM-EM.	None
A3/B3	Each node has one IP address on the public signalling network.	Unistim and UFTP signaling to terminals	Permit port 5000 and 6000
A4/B4	One IP address on the private signaling network shared between node A and node B.	H.248 call signaling to GWC.	Permit port 2944

All inter-node CICM communications are carried out on a private IP sub-network. Each CICM processor has a single private IP address that is bound to one of the administration interfaces. A software component on the CICM processor monitors the state of the administrative network

interfaces. When a failure occurs, the processor moves the binding of this private address so that connectivity between the two nodes is maintained. This functionality is described in more detail in the *Centrex IP Client Manager Engineering Guide*.

Network Connectivity

The OAMP network, private signaling network and public signaling network are commonly referred to collectively as the CS-LAN. A pair of Passport 8600 routers provides the connectivity and routing capabilities of the CS-LAN.

The CICM 6.12 should be co-located with the CS2000. When it is co-located, the CICM 6.12 can leverage on the CS2000 CS-LAN infrastructure, which consists of two Passport 8600 routing switches.

In addition to supporting the CS2000 Core and other CS2000 components, the dual-PP8600's provide the LAN connections between the CICM and:

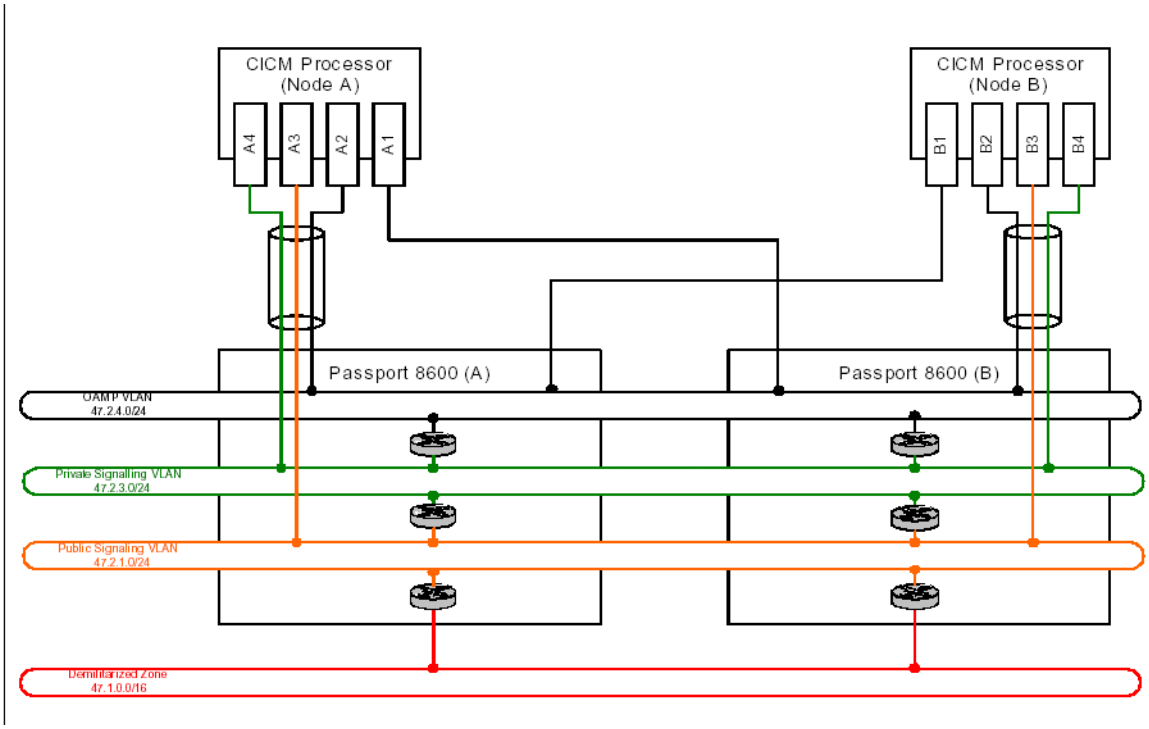
- The Telco's administrative LAN, which includes the Primary and Backup Element Managers.
- The client LAN.

Each of the network functions is implemented as a VLAN. Routing between the different network functions is required for devices like the GWC that do not support direct VLAN capabilities. The passport restricts the routing capabilities to achieve the highest available level of security.

The pair of Passport 8600 have a limited number of Ethernet ports, so any significant deployment of CICM will require additional Ethernet connectivity.

Figure 36 below shows a typical deployment scenario for the Succession CICM in a central office. Figure 36 should be considered in conjunction with Figure 35, *CICM in the CS2000 Network*. Each CICM processor is cross-connected across the two switches so that in the event of any single network element failure, there is still a routing path between the pair of CICM processors.

Figure 36 Network connectivity for LAN redundancy



IP Addressing

Assuming the network configuration provided in Figure 36 above, Table 26 provides an example of the IP addresses required by a pair of CICM processing nodes.

Table 26 IP Addressing Example

Network	IP Address	Interface	Description	DHCP Support
OAMP	47.2.4.100	A1	Node A primary OAMP address	No
	47.2.4.101	A2	Node A secondary OAMP address	No
	47.2.4.102	B1	Node B primary OAMP address	No
	47.2.4.103	B2	Node B secondary OAMP address	No
Private Call Signaling	47.2.3.100	A4 or B4	H.215 signaling address	No

Table 26 IP Addressing Example

Network	IP Address	Interface	Description	DHCP Support
Public Call Signaling	47.2.1.100	A3	Node A Unistim address	Yes
	47.2.1.101	B3	Node B Unistim address	Yes
Private inter-node signaling (on OAMP network at layer 2)	10.0.0.100	A1 or A2	Node A private address	No
	10.0.0.101	B1 or B2	Node B private address	No

Network redundancy

The following table summarizes the redundancy model used for each network interface on the CICM.

Table 27 CICM Network interfaces

Function	Client	Description	Approximate Failover Time
OAMP	CICM-EM	CICM-EM can communicate with interfaces A1 and B1 on the CICM. When A1 or B1 is unavailable, most OAMP functions can still be performed through the mate node. Some OAMP functions can also be performed through A2 and B2 (e.g. Telnet for support functions).	N/A
Unistim signaling	Terminals	Each terminal is configured with both of the addresses of the public signaling interfaces (A3 and B3) on each node. When either interface fails, the terminal resets and attempts to reconnect to the other interface. In scheduled maintenance windows, terminals can be gracefully moved from one node to the other.	1-2 minutes, depending on the activity on the terminal and the configuration of the terminal reliability parameters.
H.248 signaling	GWC	The Dual Node architecture of the CICM is hidden to the GWC – a single address is shared across the two nodes. The state of the private signaling interfaces (A4 and B4) is monitored by the CICM and the address is bound to the most available interface. When the active interface fails, it is switched to the other interface without loss of H.248 messaging (messages are retransmitted during the outage).	1-2 seconds
Inter-node communications	Mate CICM processor node	A virtual private network between the two nodes is maintained across adapters A1, A2, B1 and B2.	1-2 seconds

Dual Node Operation

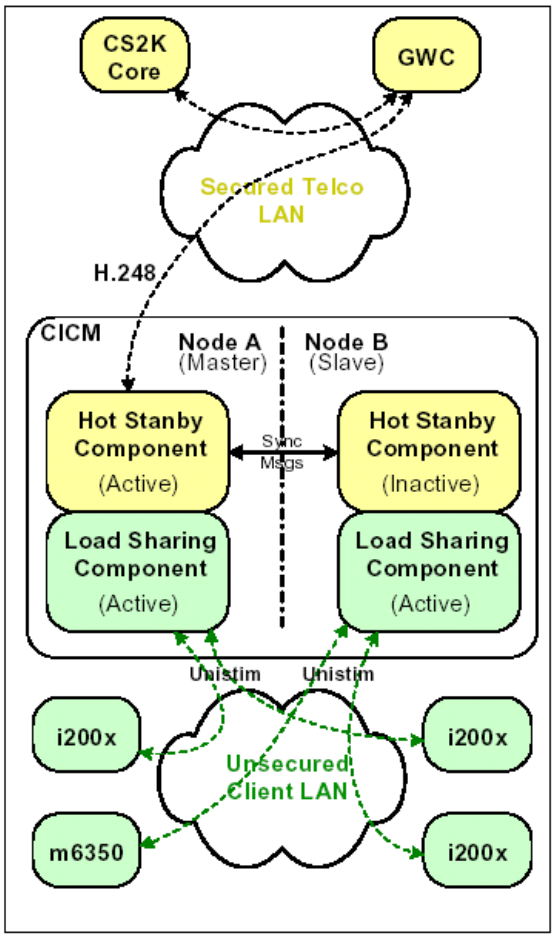
Pairs of CPU cards provide hardware redundancy for the CICM applications. The two CPU cards present themselves to the GWC as a single network entity (one CPU is the master, the other is a warm-standby slave).

The terminals are configured with the address of both CPUs. The terminal will failover between them when a failure occurs. In Series 6.12, only one pair of CPU cards is supported in the chassis (one CICM processor).

If one of the CICM nodes becomes unusable (e.g. due to a hardware failure or during an upgrade), the non-failing node can still be used to provide service. When one node becomes unusable, all current calls on the failed node will be dropped and clients may need to log in again to regain service.

The following Figure 37 shows the model used for Dual Node Redundancy.

Figure 37 Dual Node Redundancy model



Hardware configurations

The series 6.12 hardware configuration includes:

- 2 Motorola CPV5370/5350 Intel CPU Cards
- 2 or 4 Brooktrout Netaccess NS300 or NS301 Cards

Software

This section defines the software loads, delivery, upgrades and maintenance releases applicable to the Series 6.12 CICM.

Software loads

The base load for Series 6.12 CICM is SN06.2.

Coexistence of Series 6.12 and previous releases

Series 6.12 CICM systems can coexist with Series 6.1, Series 2.5, and Series 2.4 systems, as follows:

- A minimal outage upgrade can be performed from Series 2.5 to 6.12, or from Series 2.4 to Series 6.12.
- A Series 6.12 EM can manage Series 6.1, 2.5, and 2.4 CICMs.
- The recommended firmware release for the i200x client on Series 6.12 CICMs is 1.39.

Software requirements or dependencies

Series 6.12 includes the NetAccess IISDN 7.5 library that allows support for the NS301 card.

C2000 Platform software dependencies

The CICM uses Microsoft Windows NT Embedded Server Version 4.0 Operating System. The CICM-EM uses Microsoft Windows 2000 Server Operating System.

The software dependencies of CICM 6.12 are listed in the following table.

Table 28 CICM 6.12 software load configuration

System	Minimum Software Load	Comments
CS2000 Core	ISN06	
GWC	GWC09.1	CICM will function with GWC09 without support for multi-tenanted NAT
CICM	6.1	
CICM-EM	6.1	
SESM	SESM06.1	
i2002, i2004	1.57	Older releases supported (1.38+) without support for RFC 2833
M6350	6.1	

Software ordering and delivery processes

CICM software is ordered from Nortel Networks via a standard software ordering process.

Nortel Networks provides customer information on a CD ROM. Documentation for CICM is delivered on a CD with supporting MGC documentation. The full suite of MGC documents is available through Helmsman Express.

Product and Maintenance Release upgrades

There are two types of upgrades: product upgrades and Maintenance Release upgrades. Product upgrades involve upgrading the release number. Maintenance Release upgrades involve build number upgrades, within the same release. Refer to the *Upgrade* section of this document for information and procedures.

CICM Clients

This section provides an overview of the CICM clients. For detailed information, refer to:

- *NN10182-113 CICM m6350 Client Installation Guide*
- *NN10183-114 CICM m6350 SoftClient Branding Kit.*
- *NN10027-113 CICM Etherset Installation Guide and User Manual*

The CICM client is the mechanism that allows a user to initiate and receive VoIP calls, and to receive Centrex features from CS2K. CICM clients are called clients, terminals, or client terminals.

Two types of CICM client are supported, both are supplied by Nortel Networks exclusively:

- The m6350 SoftClient application, which is an IP telephony software client installed on a PC (with Windows 2000 operating system) attached to a LAN. It works with a headset and adapter which plugs into a USB port on the PC.
- The Nortel Networks i200x Etherset telephones, which connect directly to a client LAN or to a telephony switch module. The i2002 and i2004 models are supported.

Both of these types of CICM clients use the Nortel Networks proprietary Unified IP networks Stimulus (UNIStim) protocol to deliver the full range of CC2K Centrex service set which would not be possible to deliver with standardized protocols and terminals.

Note: Stimulus protocols reflect the user's input stimulus ((key presses) and reflect display commands sent from the network (which

drive displays and lamps on the device). This allows the clients to deliver the full range of MGC Centrex services.

CICM lines are datafilled on the CS2K as standard MBS lines, using the M5216 template. There is no distinction between a normal MBS line and one connected to a CICM.

Feature key assignments are made by the SERVORD through the MAP interface (like traditional MBS sets). Feature assignments on a client must be labeled to match the features provisioned. This feature key labeling can be made directly via the client itself, or through the Element Manager Web interface.

The CICM Element Manager Web interface provides two ways of labeling the assigned feature keys. You can label the feature keys of a specific phone or use a User Profile to do a bulk labeling of several phones. Refer to the *Configuration* section of this document, and the *Apply/remove user profile overrides* procedure.

Clients support the following codecs:

- G.711 (full rate 64Kbit/s)
- G.729A (compressed, 8Kbit/s)
- G.729AB (compressed, 8K bit/s with VAD/silence suppression)

A codec is assigned to a terminal via an audio profile by the Element Manager Web-based interface. The profile (and hence the codec used) can be overridden from the client's interface.

Nortel Networks i200x Etherset client

Two versions of the Nortel Networks Etherset client are supported: the i2002 and i2004. Both Ethersets are MBS-like handsets that connect directly to a LAN. The Ethersets are shown in the following Figure 38.

Figure 38 i2004 Etherset (left) and i2002 (right)

The Nortel Networks i200x Etherset is an MBS-like telephone that connects directly to a LAN. The functional components of the i200x are:

- A handset
- A speaker and headset connector for hands-free operation
- A standard keypad, including Release, Hold, Volume Control and Mute keys
- A function display area with a set of keys for scrolling

Etherset user interface

To use the i200x, the user logs on to the CICM, supplying a user name and password. Once logged in, the handset and standard keypad of the i200x behave in the same way as a standard MBS telephone. Additional services and features can be accessed via the soft keys of the function display area. Each of the soft keys corresponds to a menu option, and the navigation keys can be used to select a particular menu option.

Additional services and features can be accessed via the soft keys of the function display area. Each of the soft keys corresponds to a menu option, and the navigation keys can be used to select a particular menu

option. The following table provides a comparison of the i2002 and i2004 user interfaces.

Table 29 i2004 to i2002 User Interface Comparison

Option	i2004	i2002
Display contrast	Y	Y
Feature key configuration	Y	N
Language selection	Y	Y
Time and date format selection	Y	N
Time settings	N	N
Audio configuration allows for the user to configure and choose their own audio profile from the i200x menu.	Y	Y
Firmware Upgrades	Y	Y
User-created Contacts List that can be associated with feature keys for automatic dialing. There are 6 feature keys. Up to 12 features are available from these keys by using the **page up/down** keys.	Y	N
Call history feature provides access to CICM-hosted inboxes and outboxes. It enables users to display a history of incoming and outgoing calls.	Y	N

Etherset hardware feature comparison

Both the i2004 and i2002 clients support IEEE 802.1p and IETF DiffServ Code Point (DSCP) marking, with IP phone firmware 1.3x. The following table provides a i2004 and i2002 hardware feature comparison.

Table 30 i2004 to i2002 Hardware Feature Comparison

i2004	i2002
Adjustable-angle stand	Fixed-angle stand
N/A	Wall mount
Plug in Ethernet switch available on older models, and built-in Ethernet switch (2 RJ-45 jacks) in more recent version.	Built-in Ethernet switch (2 RJ-45 jacks)
6 line keys	4 line keys

Table 30 i2004 to i2002 Hardware Feature Comparison

i2004	i2002
4 line display area	2 line display area
Extended low-frequency speaker	Standard Stetron LS19 speaker (no tuned cavity)
AEM and ACM accessory port (for key expansion modules)	AEM accessory port (for key expansion modules)
Handsfree microphone for wide-band audio	Standard Primo EM-80 handsfree microphone

m6350 SoftClient

The m6350 software client (SoftClient) is accessed through a Windows interface and uses Microsoft Internet Explorer, version 5 and above. For this release the m6350 is supported only on Windows platforms; other operating systems are not supported.

For detailed information on the m6350 SoftClient and installation procedures, refer to *NN10182-113 CICM m6350 Client Installation Guide.*

The m6350 SoftClient communicates with the CICM over the IP LAN using the proprietary Nortel UNIStim protocol for feature and call signalling. RFC1889 compliant audio streams are used as bearer channels to provide the speech path. Speech in the PC is encoded (using the configured codec) for transmission to the CICM and decoded for reception from the CICM.

It is not possible to guarantee the voice quality provided by the m6350 client, since it is significantly influenced by:

- the sound card hardware and driver software
- the characteristics of the operating system on which the client is installed
- the mix of other computing tasks in progress during the call.

Although it is not possible to guarantee the voice quality of the m6350 client, this client offers the best voice quality available and, unlike the i2004 and i2002 Ethersets, it does not support QoS marking (either 802.1p or DiffServ).

The m6350 supports a 2.1 compliant Telephone Application Program Interface (TAPI) to allow integration with third party applications on Windows. This is a separate component, called the m6350 TAPI

Service Provider (TSP), included with the SoftClient. It provides access to the m6350 from Windows applications such as Microsoft Outlook.

An OEM customizer is available to allow a service provider to create a custom version of the m6350. A service provider can brand the m6350 with their own logo. Refer to *NN10183-114 CICM Series 2.5 m6350 SoftClient Branding Kit.*

m6350 users can view, and in some cases modify, option data on the CICM that is specific to their line or terminal. This includes changing feature key assignments, selecting the active audio profile, viewing the active session's data, and viewing inbox/outbox as part of call history feature.

Client platform requirements

The minimum requirements to run the m6350 SoftClient are:

- A 550 MHz Pentium III-class or equivalent processor
- Microsoft Windows 2000
- 25 MB free RAM (in addition to the memory requirements of the OS and other concurrent applications)
- 60 MB free hard disk space
- A USB Headset

The Nortel Networks recommended hardware and operating system requirements to run the m6350 SoftClient are:

- 1 GHz (or higher) Pentium III-class or equivalent processor
- Microsoft Windows 2000
- 50 MB free RAM (in addition to the memory requirements of the OS and other concurrent applications)
- 60 MB free hard disk space
- A USB Headset
- An IP connection (dial-up or Ethernet) for communications with the CICM

Note: The voice quality of the SoftClient could be degraded if memory, CPU or network intensive applications are used in conjunction with the SoftClient.

To guarantee the correct audio transmit and receive levels, distortion, frequency response and echo return loss, and correctly limit peak acoustic pressure as specified in TIA-810 standards, the m6350 is designed as part of a system to be used with the Nortel Networks USB

Headset Adaptor (part number NTEX14AA) and the Nortel Networks (GN Netcom Advantage Plus) headset.

The headset, headset cords, USB adaptor and m6350 audio stack are engineered together as part of a system to meet TIA-810 standards, and should always be used together. It will not be possible to meet these requirements if the user uses a mixture of third party sound cards, headsets, handsets or speakers and microphones.

The m6350 audio stack does not have any form of echo canceller. It manages echo through use of the recommended headset, cords, and careful control of gains. Loudspeakers will introduce large amounts of echo and, if used, the far end will hear their own voice delayed and echoed back to them. Loudspeakers will always result in unacceptable performance.

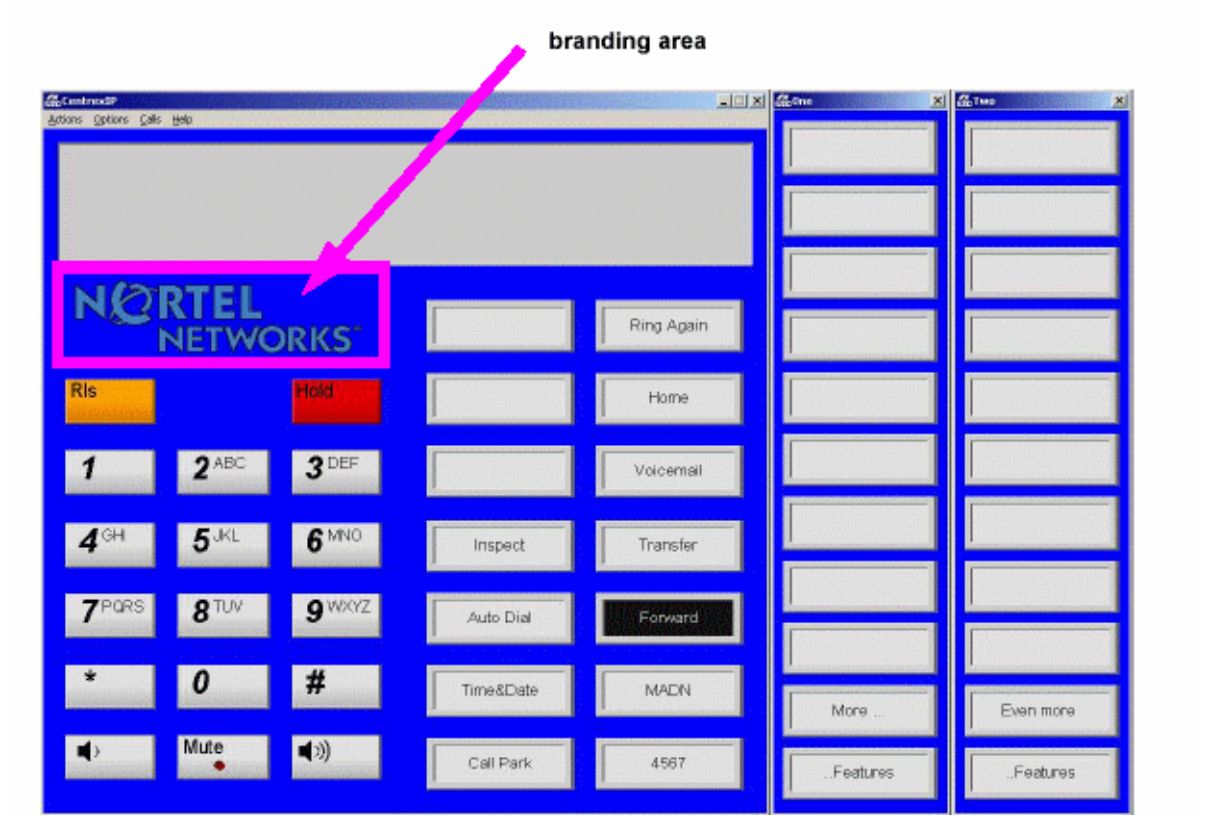
Even using a headset with the m6350 can be problematic. If the volume is turned up too far on the earphone(s), the sound may be picked up by the microphone. The end result will be noticeable echo (perhaps to an unacceptable degree) to all other participants in the call.

m6350 user interface

The m6350 client behaves as a standard Windows program. The user starts the m6350 just like any Windows program. The user then logs in to the CICM with a user name and password.

After login, the user is provided with a GUI that mimics the appearance of an MBS set (as illustrated by the following Figure 39). The m6350 behaves exactly like an M5216 MBS set. To press any of the keys, the user points and clicks the mouse. Keyboard shortcuts are available. Extensive online help is provided.

Figure 39 m6350 SoftClient user interface, with 2 additional banks of feature keys



Features of the m6350 client include:

- On/off-hook menu option
- Release and Hold keys
- 14 feature keys with auto-labels.
  Up to 4 additional banks of feature keys can be added to the interface
- Call history feature, providing access to CICM-hosted inboxes and outboxes
- Quick-dial address book feature, providing access to and dialback from CICM-hosted contact list
- Display area (two 24-character lines) with customizable fonts
- Volume keys
- Mute key with indicator
- Adjustable microphone gain level
- On-hook dialling (provided via a pop-up dialogue)

- Customizable appearance
- TAPI 2.1 Service Provider via TSP
- Multiple language support
- Separately controllable ringing and headset speakers for PCs with more than one sound device.

The m6350 client can be run in parallel with other PC programs. It follows the standards rules about active windows. However, simultaneously running CPU intensive applications may degrade the audio quality of the m6350 client.

Refer to the NN10182-113 CICM Series 2.5 m6350 SoftClient Installation and User Guide for additional information.

TAPI service provider
The m6350 client supports a TAPI 2.1 compliant interface to allow integration with other third party applications on Windows. This is a separate component, called the m6350 TAPI Service Provider (TSP). This component can be installed after the m6350 has been installed and provides access to the m6350 from Windows applications such as Outlook.

For more information on installation and configuration, refer to the *NTP 297-5551-901, m6350 TAPI Service Provider Installation and Troubleshooting Guide.*

Client branding
An OEM customizer is available to allow a Telco to create a custom install version of the m6350 client with the features described in this section.

The m6350 GUI includes an area that contains a configurable brand logo (see Figure 39 above). A Telco can brand this area with a logo in one of two ways:

- a TrueType font file with the logo defined as one of the font glyphs
- a (possibly transparent) bitmap file with an aspect ratio of 7:2

The branding facility allows the Telco to brand the m6350 GUI and produce an installable kit where the company/product/description information and default software placement details have been tailored to represent the Telco rather than Nortel Networks.

Configuring CICM resident options

m6350 users can view, and in some cases modify, option data on the CICM that is specific to their line or terminal. Specifically, m6350 users can:

- change feature key assignments and labels
- select the m6350's active audio profile
- view the active session's data
- view their inbox, outbox and quick-dial address book (part of the call history feature)

The m6350 uses Microsoft Internet Explorer (version 5 or later) to display HTML pages served by the CICM. If the user's PC does not have IE 5 or later installed, the m6350 will continue to function normally, but will not provide access to this new functionality.

Call History and Contacts Directory features

Both the m6350 and i2004 (but not the i2002) clients support a Call History feature, which enables users to display a history of recent incoming and outgoing calls. The feature makes use of inboxes and outboxes hosted by the CICM.

The inbox allows the user to display information about the most recent incoming calls (up to 10 calls). Incoming call in formation is captured regardless of whether the user is logged in at the time.

The outbox allows the user to display information about the most recent outgoing calls, (up to 10 calls).

The contacts directory allows the user to maintain a quick-dial address book (of up to 16 names and numbers). Entries can be copied to the contacts directory directly from the Inbox or Outbox, or can be added to the directory via an edit dialog. Contacts can be dialed from the directory, on the Etherset via a softkey on the Directory display, and on the m6350 from a drop-down list on the main menu.

Interworking between m6350s and i200x Ethersets

A user can be logged in from both an m6350 and an i200x Etherset at the same time, in a cooperative session. The user can dial or answer from either the m6350 or the i200x during a cooperative session. Lamps will light on both clients (e.g. if a call is waiting) and both displays will show the same information.

The audio for such a cooperative session will always be handled by the Etherset client, since the voice quality on an i200x Etherset is usually superior to that of a PC with the m6350 SoftClient. If the user hits the

DN key on the m6350, the etherset will get dial tone, and only the etherset will ring.

If a user is currently logged in and attempts to log in from another client (m6350 or i200x), the user is presented with the following options:

- Join the currently logged-in client in a cooperative session.
- Forcibly log out the currently logged in client(s). Selecting this override option causes the currently logged in client(s) to be logged out, and presents the user with the login screen, with their username filled in.
- Cancel the login attempt.

The following restrictions apply to cooperative sessions:

- Only the Etherset will receive audio.
- A cooperative session can only be established between an m6350 and an i200x; not between two clients of the same type. This option is therefore not available if the user is already logged in on a client of the same type, or if the user is already in a cooperative session with two clients.
- A cooperative session can only be established between clients connected to the same CICM node. If two clients are connected to different nodes, and a user attempts to log in the second client with the same username as the first, then the user can only force out the first client or cancel the login attempt; a cooperative session cannot be established.
- If a logged-in client is making a call and an attempt is made to force it out, the call is cleared.

For detailed procedures, refer to *NN10182-113 CICM m6350 SoftClient Installation and User Guide* and the *NN10027-113 CICM Series 2.5 i2000x Etherset Installation Manual and User Guide.*

DHCP and Centrex IP Clients

Centrex IP clients can have their IP addresses allocated by a DHCP server.

For m6350 clients, standard MS Windows DHCP capabilities can be used, although additional manual configuration is required to enter the CICM addresses. The m6350 must be restarted if the IP address configuration changes (e.g. if a dial-up session is terminated and then re-established, or if a DHCP lease expires and is renewed on a different IP address.

The i200x clients support two modes of DHCP operation:

- Full DHCP, in which the i200x obtains all its configuration data from the DHCP server, including the CICM addresses and ports.
- Partial DHCP, in which the i200x obtains only its IP address, subnet mask, and default router address from the DHCP server. Other data must be configured manually. See the *2.5 Engineering Guide* on the Ethernet configuration via a DHCP server.

The CICM does not care about the IP address of a client as long as it remains constant while the client is logged in to the CICM.

Codecs

A codec is a speech coding/compression standard. The term “codec” refers to either Compression/Decompression algorithm or coder/decoder algorithm. A codec is a coder-decoder (compressor-decompressor) for speech and signalling passing between the LAN and CentrexIP clients.

A client is assigned a codec in an Audio Profile via the Element Manager Web Interface. The profile (and hence the codec) can be overridden from the client interface.

CICM supports three standardized codec types for VoIP:

- *G.711 Speech coding standard*

  This is the standard of the PSTN. Wireless networks also use it. It is the benchmark for conventional-band telephony voice performance. It has a packet loss concealment algorithm to improve its performance under packet loss conditions.

- *G723 Speech coding standard*

  This is a low bit-rate codec which can be used in very low bandwidth applications (e.g. modem).

- *G.729 Speech coding standard*

  This is also a low-bit-rate codec, but uses more bandwidth and provides better audio quality than G.723.

The specific codecs used for speech transmission between the client and the CICM can be configured as any of the following:

- G.711 m-law and G.711 A-law
  (G.711 A-law has a packet loss concealment algorithm to improve its performance under packet loss conditions)
- G.723.1 and G.723.1 annex A
- G.729A and G.729A annex B

Restrictions on CICM clients

The following restrictions exist for CICM 6.12 clients:

- System and attendant console Centrex features are not supported.
- Although client development is focussed toward presenting an exact replica of MBS terminal functionality over an IP network, client services are subject to certain restrictions. These restrictions are due to the differences in the service paradigm between the physical line interface of conventional Centrex and the network data connection of the CICM.
- Certain features (such as Distinctive Ringing) may not operate in the same way, or may be disabled. For example, if local ringing is configured for i2004 sets, distinctive ringing and ring back tones may not originate locally on the set itself, but may originate from the UAS instead. Also, features which involve one-way speech path as one of their stages will not work exactly as intended with CICM clients because two-way speech is currently enabled by default as soon as a call is received and answered. This applies to features such as Intercom (OCM), Group Intercom for BS (GIC) and Group Intercom All Call (GAC). This applies equally to i200x Ethersets and m6350 clients.
- The i2004 has 6 feature keys and up to 11 features are available from these keys by using the page up/page down keys. The i2002 has 4 feature keys and acts in a similar manner.
- The Call Server can support multiple feature assignments to each feature key, but the CICM can support only one feature assignment per key.
- The following restrictions apply only to the m6350 client:
  - The speech path represents the headset mode of MBS operation. Hands-free mode is not directly supported by the

m6350, since hands-free operation can be simulated using the speaker/microphone hardware on the PC platform.

— Incoming ringing and ringsplash are implemented by a pop-up dialog box and an audio prompt from the client PC speaker, simultaneously.

User interfaces

The normal mode of access to the CICM EM is via a PC connected to the Administration LAN. The procedures in the CICM document suite are written based on this primary mode of access.

It is also possible to access the EM locally via a customer-supplied terminal (with keyboard and mouse) directly connected to the EM. In this case, the procedures are the same, except the remote access steps are skipped.

A CICM and its clients can be configured, monitored, and administered in the following ways:

- **Web-based Element Manager interface.** This interface uses a Web browser to access the Element Manager Web pages. Refer to the *Element Manager Web pages procedures* in the *CICM Security and Administration* document.
- **MS Windows Terminal Services Client.** This interface uses the Windows Terminal Services Client for remote access. Refer to the Terminal Services Client procedures in the *CICM Security and Administration* document.
- **Telnet.** A Telnet session may be used to perform certain (but not all) administrative functions. Refer to the Telnet procedures in the *CICM Security and Administration* document.
- **MS Windows Event Viewer.** The Microsoft Windows Event Viewer is used to access event logs for troubleshooting purposes. Refer to the Event Viewer procedures in the *CICM Security and Administration* document.

For all procedures that use all of these interfaces, administrator logins are required.

Web-based Element Manager interface

The Web-based Element Manager interface is a Web site (i.e. collection of Web pages) hosted on the Element Manager. This EM Web site provides most of the functionality necessary for configuring and monitoring a CICM and its clients.

This Web-based EM interface can be run from any platform that supports Microsoft Internet Explorer, version 5.0 or later.

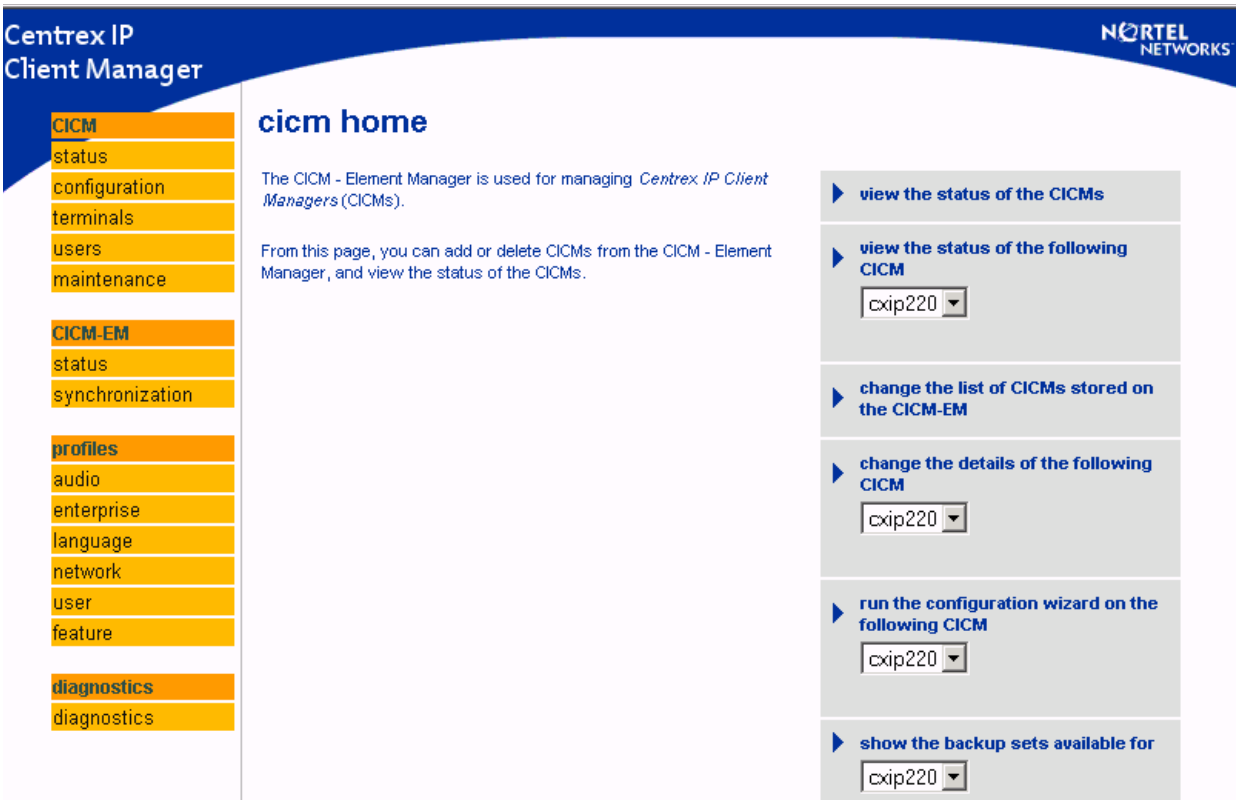
The Element Manager Web site provides the user interface for most of the functionality necessary for configuring and monitoring a CICM and its clients.

The Element Manager Web pages consist of:

- An EM home page, which provides links to:
  - A CICM Status Overview page. This provides a summary of the status of the CICM and its components.
  - Detailed status pages for each CICM element.
- A collection of read-only status pages, which present the current node status
- A CICM configuration wizard for performing initial setup and configuration of the CICM.
- Pages for configuring profiles (user, network, audio, language, feature, and enterprise profiles)
- Pages for configuring users
- Pages for configuring client terminals.

The following Figure 40 shows the CICM home page that opens after initial login to the EM Web site.

Figure 40 CICM home page



For detailed description of the EM Web page interface and procedures, refer to the *CICM Configuration Management* and *CICM Security and Administration* documents.

Windows Terminal Services Client interface

The Element Manager operating system is Windows 2000 Server, which supports remote access via Windows Terminal Services Client. This is the primary remote access mechanism for the Element Manager.

For additional details on the Windows Terminal Services Client, refer to the Web site **http://www.microsoft.com/windows2000/technologies/terminal/default.asp**

Telnet interface

Telnet is a terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the

server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

Telnet provides a method of remote administration of CICM from a PC connected to the Admin network. Telnet can be used to perform the following operations of the CICM:

- check the overall status of the CICM
- monitor and copy event logs from the CICM
- start and stop the service on the CICM
- power up and power down the CICM
- verify the connection of a terminal on the client LAN

For detailed description of the Telnet-based CICM configuration interface and procedures, see the *CICM Security and Administration* document.

Windows Event Viewer interface

The Windows Event Viewer tool can be used to access event logs for troubleshooting purposes.

The CICM software generates Windows NT event logs for various cases such as client session events and initial is at ions. Audits of user login successes and failures are also generated as event logs.

SNMP will also generate event logs when sending out traps. In general, the event logs generated by SNMP will be warning logs for high severity traps, and informational logs for other traps.

There are five categories of logs:

- **Error logs** indicate a critical event or condition, such as failure to initialize hardware, or out of memory.
- **Warning logs** indicate a non-critical event, and are usually generated after a logic error has been detected in the software and recovery action has been taken.
- **Informational logs** provide information about the state of the CICM.

- **Success Audit logs** provide details of successful logins (e.g. a success audit log is generated when a user has successfully logged in.
- **Failure Audit logs** provide details of failed login attempts. A failure audit event is generated when any of the following occur:
  - a user has tried to log in to a currently running session
  - a user has provided incorrect login information
  - a user has exceeded the maximum number of failed login attempts (datafillable at the CICM)

Logs can be reviewed remotely on the Administration LAN by running the Windows NT event viewer. Refer to the *Event Viewer* section of the *CICM Security and Administration* document for Event Viewer procedures.

Network interfaces

CICM and the IP network

The CICM connects to clients using the IP protocol on its client side network interface. IP connectivity is provided by 100baseT Ethernet.

The CICM controls terminals using the Nortel proprietary Unified Network IP Stimulus (UNIStim) protocol. The UNIStim protocol carries information about client key presses between the client and the CICM, and is not secured. Security is established by placing CICM in a secure telco WAN environment or an enterprise LAN, and not on the public Internet.

Voice is encoded using one of three standard voice encoding algorithms, G.711, G.729, or G.723.1. The encoded voice packets are transmitted across the IP network using the RTP protocol.

Protocols

A protocol is a standard way of organizing data transmissions or making connections between devices. The protocols relevant to VoIP services are summarized in the following table.

Table 31 Protocols relevant to VoIP

Network Area	Protocols	Purpose
Call/session & device/CICM control	UNIStim	Ensure that connections are established and determine the set of call features.
Management	SNMP	Essential for monitoring and maintaining the health of IP communication devices.
Quality of Service (QoS)	Diffserv	Ensure that voice traffic gets priority over less time-sensitive services like file transfer and fax.
Device/media control	H.248	Support device control and media control capabilities.

UNIStim

UNIStim (Unified Networks IP Stimulus) is a Nortel Networks proprietary protocol for Internet Terminals (IP telephones) used for Voice over IP (VoIP) telephony services.

CICM clients use the UNIStim protocol to communicate with the CICM. UNIStim allows the delivery of the full range of Centrex features to VoIP devices. It can deliver any new feature to the device without recourse to a software upgrade. It also allows delivery of a wide range of features without having specific feature support in the device itself.

SNMP

Simple Network Management Protocol (SNMP) allows network administrators to manage and monitor IP communications and the performance of devices. It is used to collect valuable information on network routers and CICMs, and to manipulate network configurations. SNMP defines how maintenance information is accessed and sent to various network devices.

Diffserv and RSVP

Differential Services (Diffserv) and Resource Reservation Protocol (RSVP) provide information about network performance requirements in an attempt to ensure appropriate resources are provided for different

types of network traffic such as data, fax, and voice. Prioritization of resources is important because fax and data can tolerate certain amounts of delay without affecting user satisfaction, whereas voice conversations do not tolerate delay. Diffserv marks each individual packet to specify the requested handling priority, which may or may not be honored. RSVP, on the other hand, creates an end-to-end connection that has the performance characteristics that are required by the application.

CICM configuration data

Configuration data (e.g. EM IP addresses, maximum number of concurrent sessions) resides within the Windows 2000 system registry. Therefore, the operating company may use standard Windows 2000 backup tools to ensure that critical configuration data is archived externally to the CICM.

Previously backed up configuration data may be restored to the Windows 2000 registry in the event of data loss or corruption due to a hardware or software failure, so that service may be resumed on a replaced or repaired system with minimal loss of service.

Element Managers can be configured to back up the configuration data of all CICMs on a regular basis (e.g. once a night).

CICM line maintenance

Line provisioning of CICM clients

The procedure used to provision a CICM client on the CS2000 is very similar to the method used to provision a line on other lines gateways. Refer to the *Perform line provisioning for CICM clients* procedure in the *CICM Configuration Management* document.

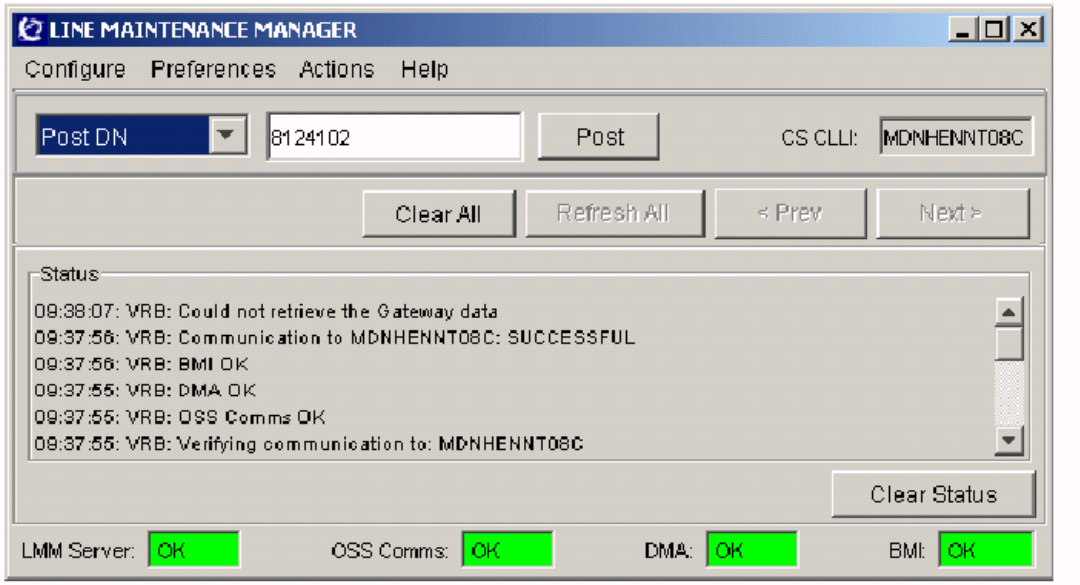
Line Maintenance Manager

The Line Maintenance Manager (LMM) is a GUI provided by the Succession Element and Sub-Element Manager (SESM) to replace and emulate the functionality provided by the MAPCI tool on the CS2000 Core. The LMM provides the functionality to post individual lines as well as to post a gateway.

The LMM main dialog window is illustrated in the following Figure 41. The LMM provides for the input of the following commands:

- BSY
- RTS
- FLRS
- INB

Figure 41 Line Maintenance Manager



For additional information, refer to the *CS2000 Provisioning* documentation.

Customer resources

Nortel Networks customer support

For customer support information, please contact your Nortel Networks account prime.

Customer documentation

Nortel Networks provides customer information on a CD ROM. Documentation for CICM is delivered on a CD with supporting MGC documentation. The full suite of MGC documents is available through Helmsman Express.

Legacy documentation

For legacy information, refer to the MGC suite of documents available through Helmsman Express.

Training information

All course descriptions, prerequisites, schedules and locations can be viewed at www.nortelnetworks.com.

For the most recent curriculum information, please contact your Nortel Networks Training and Documentation representative. For enrollment assistance, contact Training Registration at 1-800-4-NORTEL (1-800-466-7853).

www.nortelnetworks.com

Nortel Networks' Web site, www.nortelnetworks.com, provides information on customer documentation, customer service, professional services and support.

Operations support services

Nortel Networks provides Technical Assistance Service (TAS) and Emergency Technical Assistance Support (ETAS). The TAS and ETAS technical personnel investigate and resolve problems that customers may encounter while operating the covered systems.

Technical support for local customers in each country is 1-800-4-NORTEL.

Appendix A: Glossary

This section provides a glossary of acronyms and terms listed alphabetically in the following table.

Table 32 Glossary

ACRONYM	DEFINITION
ACD	Automatic Call Distribution
AMA	Automatic Message Accounting
BEM	Backup Element Manager
BHCA	Busy-Hour Call Attempts
BHHCA	Busy-Hour Half Call Attempts
Centrex	Central Office exchange service
CICM	Centrex IP Client Manager. The Centrex IP gateway that interfaces with the CS2K and controls etherset and SoftClient terminals.
COM	Common connection
CS	Call Server
CS2000	Call Server 2000
CS2K	Call Server 2000
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DMS	Digital Multiplex System
DMS-X	DMS-XPM Nortel proprietary signalling protocol interface
DNR	Dual Node Redundancy.
DSCP	Differentiated Services Code Point
DSP	Digital Signal Processing
EBS	Electronic Business Set.
EM	Element Manager

Table 32 Glossary

ACRONYM	DEFINITION
EMC	Electromagnetic Compliance
ENET	Enhanced Network
GUI	Graphical User Interface
GW	Gateway
GWC	Gateway Controller. Interfaces between the CS2K CM and the various supported gateways.
HSC	Hot Swap Controller
IETF	Internet Engineering Task Force
IMS	Interactive Media Server
IIS	Internet Information Server
IP	Internet Protocol
LAN	Local Area Network
LCM	Line Concentrating Module
LGC	Line Group Controller
LMM	Line Maintenance Manager
LM(D)	Line Module
LTC	Line/Trunk Controller
MAP	Maintenance and Administration Position
MBS	Meridian Business Set.
MEGACO	
MGC	Media Gateway Controller.
MIB	Management Information Block
MIDCOM	IETF Middle-box Communications Working Group
MMP	Multi-Market Platform

Table 32 Glossary

ACRONYM	DEFINITION
MR	Maintenance Release
NA	North America
NAPT	Network Address and Port Translator
NAT	Network Address Translation
NEBS	Network Equipment-Building System
OA&M	Operations, Administration, and Maintenance
OAMP	Operations, Administration, Maintenance, and Provisioning
OM	Operational Measurement
OSS	Operations Support System
PBX	Private Branch Exchange
PEM	Primary Element Manager
PCM	Pulse Code Modulation
PLGC	PCM-30 Line Group Controller
PM	Peripheral Module
PPhone	Nortel proprietary signalling protocol used between the DMS and Centrex business terminals. Also used as a generic name for line terminals supporting this protocol.
PSTN	Public Switching Telephone Network
QoS	Quality of Service
RCC	Remote Communications Controller
RLCM	Remote Line Concentrating Module
RMM	Remote Maintenance Module
RTCP	RTP Control Protocol

Table 32 Glossary

ACRONYM	DEFINITION
RTP	Real-Time Transport Protocol
SAM	Service Access Module
SDP	Session Descriptor Protocol, used to negotiate audio session information between two or more parties. Used between the CICM and GWC to negotiate codec types and parameters.
SESM	Succession Element and Sub-Element Manager
SIP	Session Initiation Protocol
SLU	Subscriber line usage
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SSL	Secure Sockets Layer
SWACT	Switch of Activity. A term used to describe the process of moving the responsibility from a master device to a hot standby (slave).
TAPI	Telephony Application Programming Interface
TDM	Time Division Multiplexing
Tone set	A group of tones required for a specific market.
TSP	TAPI Service Provider
UAS	Universal Audio Server
UDP	User Datagram Protocol
UDP/IP	A stateless datagram protocol used for transfer of time sensitive data (such as voice) in an Internet-protocol network.
UFTP	Unistim File Transfer Protocol
UNIStim	Unified Networks IP Stimulus protocol. Nortel signalling protocol used for the i200x Etherset

Table 32 Glossary

ACRONYM	DEFINITION
VLAN	Virtual LAN
VLCM	Virtual Line Concentrating Module
VMG	Virtual Media Gateway
VoATM	Voice over ATM
VoIP	Voice over IP
WMI	Windows Management Instrumentation
XPM	Extended Peripheral Module