CICM Series 7.0 CICM Basics

Purpose

This document provides an overview of the Centrex IP Client Manager (CICM) Series 7.0 release. It describes the hardware components, software components, and user interface of the Series 7.0 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

CICM Series 7.0 is a component of the (I)SN07 Succession release.

The CICM product is described in seven separate documents, collectively known as the CICM document suite. These seven documents are:

- *NN10044-111 CICM Basics*
- *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 Basics* document provides an overview of the CICM 7.0 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.

(I)SN07 CICM 7.0 Describes the CICM 7.0 product, and provides a description of the new and enhanced features as compared to the last (CICM 6.0) release.

Engineering information Defines the platform for the 7.0 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 seven documents in the CICM document suite are:

- ***NN10044-111 CICM Basics***
- ***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 Nortel Networks IP Phone 200X 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 XP and XPe, refer to the Microsoft Web site:
http://www.microsoft.com/windowsxp/default.asp/
http://www.microsoft.com/window/embedded/xp/default.asp

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:
SAM16:
http://mcg.motorola.com/cfm/templates/product.cfm?PageID=893&ProductID=32&PageTypeID=1,

SAM21:
http://mcg.motorola.com/cfm/templates/product.cfm?PageID=939&ProductID=173&PageTypeID=1

5370:
http://mcg.motorola.com/cfm/templates/product.cfm?PageID=1841&ProductID=201&PageTypeID=1

5385:
http://mcg.motorola.com/cfm/templates/product.cfm?PageID=2149&ProductID=249&PageTypeID=1

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.

Administration LAN
The Administration (Admin) LAN is Operations, Administration, Maintenance, and Provisioning (OAM&P) subnet in the CICM 7.0 LAN in the carrier Central Office network. This subnet hosts the OAM/P interfaces of the CICM and the CICM-EM.

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 all the CICM resource cards (Motorola CPN5385 processor board) on a SAM21 chassis, associated with a single CS 2000. The CICM resource cards are always in pairs. There is one active card and one hot standby card in the pair, providing redundancy. The term “CICM” is synonymous with gateway in a CICM environment.

Chassis
The CICM is hosted on a Motorola SAM21 chassis. A chassis may contain multiple CICM CPN5385 card pairs. 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 CPN5385 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 Client LAN is the public signaling subnet in the CICM 7.0 CS-LAN in the carrier Central Office network. In the carrier-hosted deployment, this public signaling subnet houses the public interfaces of the CICM. These public interfaces are accessed by Centrex IP clients (IP Phones 200x and Softclient m5360) from the enterprise or CPE network, for communication of signaling messages (e.g. UNIStim registration, call processing, firmware download, etc.).

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, designed to provide fault tolerance on the Succession architecture (as well as the TDM architecture in (I)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 (EM)
The CICM Element Manager (CICM-EM) is the device used to configure, monitor, and manage a group of CICMs and their clients.

In a SAM21-based CICM 7.0, the CICM-EM is a pair of Motorola CPN5385 resource cards, one active and the other hot standby for redundancy. Only one pair of the CICM-EM resource cards is required for each CS2000, which is capable of supporting up to 100 pairs of the CICM resource cards. The hot standby CICM-EM resource card is equivalent to the Secondary Element Manager (SEM) chassis in the SAM16-based CICM releases.

Frame
A SAM21 CICM/GWC chassis can be housed on one of the two PI tested, NEBS-2 compliant frames: the SAM21 frame (SAMF) and the Call Control Frame (CCF). One SAMF frame may house (a) up to three SAM21 CICM/GWC chassis; or (b) up to two SAM21 CICM/GWC chassis, plus up to six MEdia Server chassis (AudioCodes MS2010 IP chassis). The CCF frame supports one of the following two configurations: (a) up to two SAM21 CICM/GWC chassis, or (b) up to two SAM21 CICM/GWC chassis, up to six MS2010 IP chassis, plus one STORM chassis for STORM storage systems.

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 (MBS) is the Nortel brand name for the electronic keyset terminals used for delivering Centrex services (i.e. M6320, M5216, etc.)

MGC
Media Gateway Controller

Nodes
Each chassis domain contains a CPN5385 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.

Nodes
Each chassis domain contains a CPN5385 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

This section provides a brief introduction to the CICM product, the purpose of which is to deliver Centrex capabilities to users connected to an IP network, using VoIP technology.

CICM Components and functionality

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 Series 7.0 CICM consists of the following components:

- One Motorola SAM 21 chassis hosting the CICM software, containing a pair of CPU cards
- An Element Manager (EM), which provides the functionality to configure and monitor CICMs and their clients
- Client hardware and software

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.

Note: H.248/MEGACO 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.

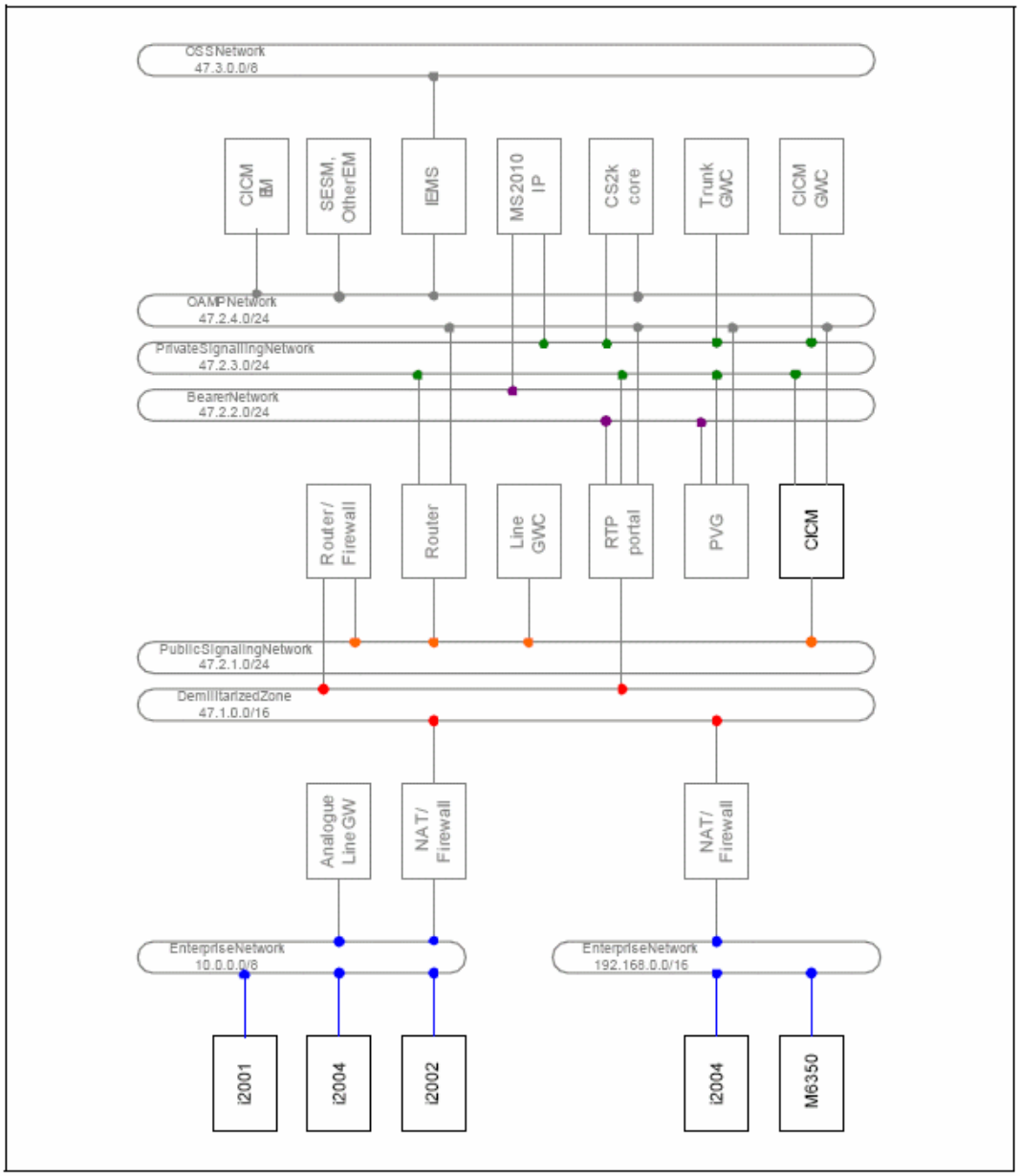
The CICM is not a media gateway. It is better described as a terminal server or signaling gateway. Media streams in a Succession IP solution are routed directly between media end-points. The CICM terminals (e.g. IP Phone 200x) are media end-points. Other media end points in a Succession IP network include:

- 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

Figure 1 shows a generic Succession IP network with a CICM serving IP terminals, in two Enterprise customer networks. Network Engineering details are not included in this diagram; it illustrates general connectivity only. 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.

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), wireless 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 Networks IP Phone 200x).

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

- Conversion between TDM and IP
- 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

Centrex

Centrex is an abbreviation for “Central Office exchange service.” Centrex is a set of capabilities that allows a Call Server 2000 (CS2000 or CS2K) or Call Server 2000 for Enterprise Networks (CSE2K) 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.

Call Server 2000

Call Server 2000 (CS2000 or CS2K) is a communication server providing call processing capabilities. In terms of the MEGACO.H.248 network architecture, it provides Media Gateway Controller (MGC) functionality.

Together with various types of gateway and server, CS2K can support VoIP or VoATM (Voice over ATM), depending on the type of backbone packet network to be used.

Specific CS2K capabilities 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 (I)SN07, 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 MS 2010 IP.

— Originations and terminations for inter-CS signalling across the packet network to/from other CS2000s and compatible MGCs such as the Multimedia Communications Server (MCS).

— Originations and terminations for TDM-side CCS7 signalling.

- Call processing
  - — A wide range of 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 CS2K can be regarded as a single node, but it is composed of separate components. The CS2K capabilities listed above 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.

For additional information on the CS2K, refer to the *CS2000 Product Description*.

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)

CS-LAN

For the SAM21-based Succession CICM 7.0, both the CPN5385 resource cards and the CICM-EM CPN5385 cards on the SAM21 CICM/GWC chassis will be collocated with the CS2000 complex in the standard Succession Communication Server LAN (CS-LAN).

This standard Succession CS-LAN consists of two high-density, high-throughput, high-resilience, NEBS-3 compliant Passport 8600 routing switches that provide Ethernet connectivity to the CICM and the CICM-EM. The CS-LAN also functions as the default gateway router to support the CICM and the CICM-EM WAN communication.

In CICM 7.0, the Client LAN interfaces and the Admin LAN interfaces of the CICM and the CICM-EM are added to the Public Signaling Subnet and the OAM/P Subnet, respectively, in the standard Succession (I)SN07 PP8600-based CS-LAN.

Refer to the *CICM Engineering Guide* for details on the PP8600 routing switches and the standard Succession (I)SN07 PP8600-based CS-LAN.

Element Manager

The Element Manager is the principal management platform for the CICM, performing the following functions

- Hosting the web pages that provide the web-based interface for configuring and monitoring the CICM and its clients.
- Providing the database for CICM configuration data.
- Providing storage for user profiles and CICM software upgrades.
- Providing an open API for IEMS and third party OAM solutions.

In the SAM21-based CICM 7.0, the CICM-EM is a pair of Motorola CPN5385 resource cards, one active and the other hot standby, providing redundancy. Only one pair of the CICM-EM resource cards is required per CS2K, which is capable of supporting up to 100 pairs of the CICM resource cards. The hot standby CICM-EM resource card is equivalent to the Secondary (or Backup) Element Manager (SEM) chassis in the SAM16-based CICM releases.

Refer also to the Hardware Section of this document for additional hardware-related details of the CICM Element Manager.

CICM Clients

The CICM client is the component 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 attached to a LAN. It works with a headset and adapter which plugs into a USB port on the PC. The Windows XP and 2000 operating systems are supported for the m6350.
- The Nortel Networks IP Phones 200x, which connect directly to a client LAN or to a telephony switch module. The 2001, 2002, and 2004 models are supported.

CICM clients use the Nortel proprietary UNIStim (Unified networks stimulus) protocol to communicate with the CICM. This allows the clients to deliver the full range of CS2K Centrex services.

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 (10 ms), G.729 A/B (10 ms), and G.729 A/B (20 ms). 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.

CS2000 and TDM versions of CICM

The SN07 CICM supports both the CS2000 version of the product, and the TDM, DMS-interfacing version.

Deployment

CICM is designed for both International and North American (NA) customers. CICM can be deployed in countries where a First Market Application (FMA) for Centrex has been carried out.

The supported tone sets on the CICM are:

- United Kingdom
- North America
- Spain
- Australia
- German

The CICM supports the following languages:

- English
- Spanish
- Italian
- French
- German

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 or M5316 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 1 lists some key Centrex features and indicates whether the feature is supported or not supported for CICM 7.0. It is not a complete feature list. 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.

Table 1 Centrex feature support for CICM 7.0

Feature Name	Supported
Call Disposal Features	
Call Hold	Y

Table 1 Centrex feature support for CICM 7.0

Feature Name	Supported
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
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

Table 1 Centrex feature support for CICM 7.0

Feature Name	Supported
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
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	

Table 1 Centrex feature support for CICM 7.0

Feature Name	Supported
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
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

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 three versions of the physical etherset: the IP Phone 2001, 2002 or 2004. 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 IP Phone 2004, distinctive ringing and ring back tones may not originate locally on the set itself, but may originate from the UAS instead.

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 IP Phone 2004 has 6 feature keys. Up to 11 features are available from these 6 keys by using the page up/page down keys. The IP Phone

2002 has 4 feature keys and acts in a similar manner. The IP Phone 2001 does not have assignable feature keys.

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

Following are the Key Expansion Module (KEM) support restrictions:

- The KEM is an expansion of the main set. All the KEM messages should be treated as main set messages, so while the Net6 session is active, any key press from the KEM or KEM message from the KEM will terminate the Net6 session and return the control to the TPS.

  Note: When the Net6 is active, the KEM messages cannot be passed to the TPS because the NEt6 session doesn't release the control to the TPS.

- Currently, 22 features on the KEM out of the 24 buttons/features are supported.

The RTP Portal restriction is:

- The CICM requires an RTP Portal, even if there are no NATs in the network. The reason is that the RTP Portal is required to land the media paths for calls to terminals that are not logged in.

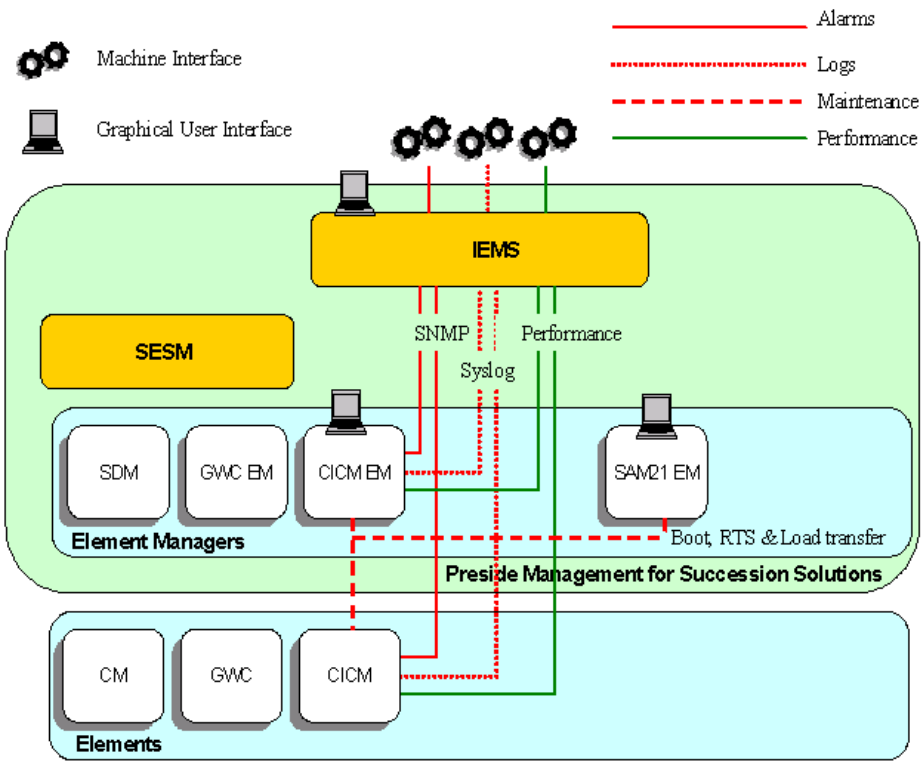
(I)SN07 CICM

The (I)SN07 version of the CICM 7.0 product provides substantially enhanced Operations, Administration, Maintenance, and Provisioning (OAM&P) capabilities, particularly when it comes to being able to interface to the service provider's OSS equipment. This is done by making the CICM and CICM EM products compatible with Succession's Integrated Element Management System (IEMS).

Integrated Element Management System (IEMS)

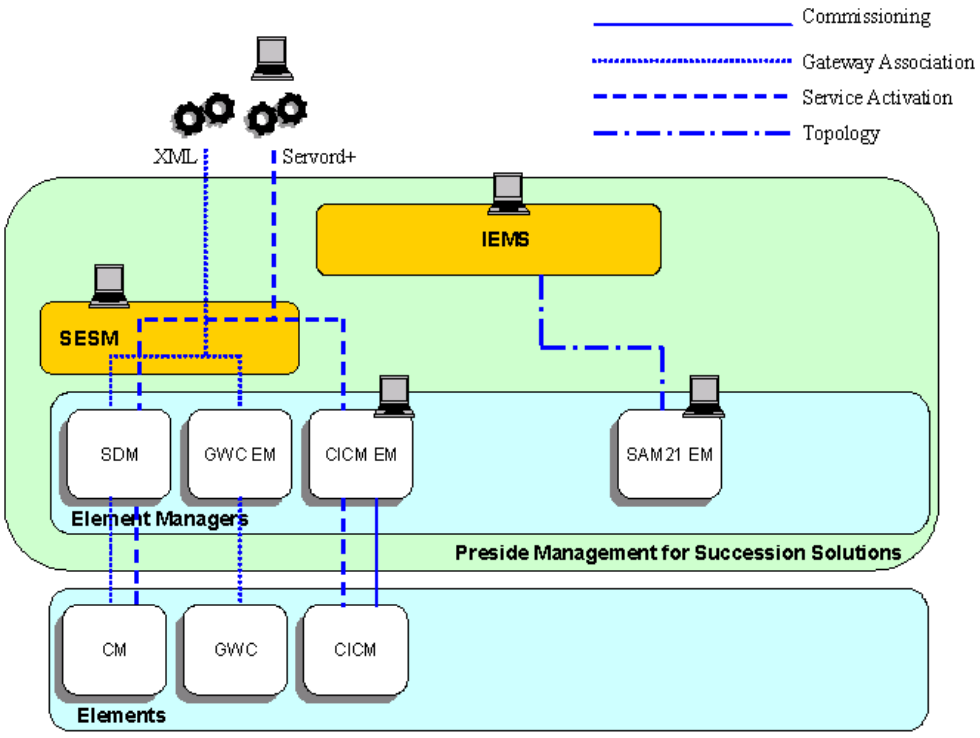
As shown in Figure 2, the IEMS takes the alarms, logs and performance monitoring data produced by CICM and passes it to the OSS systems in a choice of industry standard formats.

Figure 2 Succession CICM Fault and Performance overview



A flowthrough provisioning system is implemented, as shown in Figure 3. It is possible in CICM 7.0 to use the CS2000 Management Server OSSGate or Web interface to associate a CICM with a GWC. Additional Servord+ can be used to add or modify subscribers on a CICM. In both cases, data is automatically propagated to all elements requiring that data, in order to remove the risk of inconsistent data.

Figure 3 Succession configuration overview for CICM



CICM 7.0 New Features and Enhancements

The major changes for the CICM 7.0 release are listed in this section. A description of each new feature is provided in the following sections.

- **Support of the CPN 5385 processor card**
  In 7.0, CICM runs on the Motorola 5385 card, which is a faster version of the older 5365 card.
- **Inclusion within SAM21 chassis**
  CICM no longer requires its own chassis. CICM can be incorporated into the same SAM21 chassis as is used for GWC cards.
- **Capacity increase**
  The number of users and simultaneous calls has been increased substantially. The capacity of the CICM is now up to 3069 end users.
- **E911 support**
  The CICM Emergency Call Service (ECS) location identification feature provides the functionality to report the location of a user from the CICM telephony client to a compatible ECS system.
- **Enhanced FCAPS interfaces and integration into IEMS**
  CICM 7.0 provides enhanced interfaces for provisioning, fault reporting, performance measurements, and security. It provides

capabilities to pass on fault and alarms to the overlaying OSS systems of the service provider.

- **Flow Through Provisioning**
  The Flow Through Provisioning feature provides support for the flow through of line and user provisioning data between the CS2000 Management Server OSSGate provisioning interface and the CICM platform.
- **H.248 Compliancy Extensions**
  The H.248 compliancy extensions support additional H.248/SDP mechanisms.
- **H.248 Call Control Signalling**
  This feature introduces the (I)SN07 version of the H.248 protocol stack software for the CICM product.
- **Multi-Timezone support**
  The Multi-Timezone feature provides the ability to store the local time of the user on the switch so that the features can be activated in terms of the local time of the user. This is a DMS/CS2K feature.
- **UNIStim Security**
  This feature provides the infrastructure for secure signalling communication (i.e. encryption/decryption) between the CICM clients and the CICM Server.
- **Support for interopt**
  This feature provides support for interopt with the Ambit line gateway.
- **Fault and Performance management**
  This section summarizes the alarms, logs and performance changes for (I)SN07
- **GWCEM VCAC Support for CICM**
  GWC-EM Internet Transparency VCAC provisioning support for CentrexIP gateways.
- **Preset Conference on Succession**
  The Preset Conference on Succession feature provides for the functionality of the Preset Conference in the Succession environment.
- **Support of the IP Phone 2001**
  In addition to the IP Phone 2002 and 2004 ethersets, CICM now supports the low-cost IP Phone 2001.
- **IP Phone 2002/2004 Key Expansion Module**
  The Key Expansion Module (KEM) feature supports the implementation of a 24-key expansion module with an LCD that provides both icons and labels similar to those provided on the IP Phone 2002, applicable to 2002 and 2004 terminals.

- **EM Integration with PAM+ Proxy**
  Succession user authentication services have migrated to a single centralized third party server, which provide authentication services to succession management systems via a Pluggable Authentication Module (PAM) on the SSPSFS platform. This feature integrates the CICM-EM into this Succession strategy for user authentication, by interfacing CICM to PAM via the HTTPS PAM+ proxy on SSPFS.
- **CICM Unistim Security**
  The Clearing of Security Objects component of the Unistim Security feature is new for CICM 7.0 release. This is a new component of the Unistim Security feature that was added in CICM 2.5 MR6 release.
- **Inter-working of CICM and IW-SPM**
  The IP Inter-working Spectrum Peripheral Module (IW-SPM) provides a mechanism for bridging calls between the Nortel Networks existing DMS (TDM) switch and the public IP network.

  The Inter-working Spectrum Peripheral Module (IW-SPM) is a special gateway for the Nortel Networks' multi-core DMS switch (TDM) to the IP network, which acts as a bridge between the ENET of the TDM core and the ATM fabric.
- **Capacity Expansion**
  CICM 7.0 provides increased capacity and improved performance.

Feature: Support of the CPN5385 processor card

In 7.0, CICM runs on the Motorola 5385 card, which is a faster version of the older 5365 card.

Feature: SAM21 Integration (Inclusion in the SAM21 Chassis)

This feature supports the SAM21 Shelf Controller (SC) support for the CICM/CICM-EM application on the Motorola Intel CompactPCI card in the SAM21 shelf.

CICM no longer requires its own chassis. CICM can be incorporated into the same chassis as is used for GWC cards.

CICM no longer has need for TDM and DSP resource cards, so the existing SAM16 hardware arrangement is unnecessarily restrictive. To make CICM more economical and flexible to deploy, the application is now hosted on a slave processor board alongside the GWC processors (or any other applications) in the SAM21 chassis.

Insertion and removal processes

The insertion process for the GWC hardware is summarized as follows:

- The board is inserted into the chassis and detected by the event manager. Slots are automatically powered on when the shelf is

booted. A trap is sent to the SAM21 EM so it can be displayed to the user.

- Vterm (serial interface to MCPN750 firmware over the backplane) is used to connect to the board and perform the following:
  - — retrieve the firmware version
  - — retriever the MAC address(es) of the ethernet interfaces
  - — check if there were any power-on-self-test (POST) failures
  - — start the clock on the board
- If all the above occurred correctly, a trap is sent to the EM indicating the board is ready to be assigned service.

The removal process is:

- The latch pull occurs on the blade, which is detected by the event manager
- The event manager triggers execution of the **unconfigure** method, which in turn removes the device from its database and sends a trap to the SAM21 EM, indicating board removal.

Feature: Capacity Increase

The number of users and simultaneous calls has been increased substantially for (I)SN07 for 5385 platforms. The capacity of the CICM is:

- 3069 end users and 3000 terminations for 5385 platforms
- 1023 end users and 1023 terminations for 5370 platforms

Feature: E911 Support (ECS Location Identification)

The CICM ECS Location Identification solution allows location identification information to be configured at the network level and reported through the network, ultimately being reported to an ECS application. Each component can process the information as required, (e.g. the GWC uses the UNID in call processing for NAT traversal).

The Emergency Call Services (ECS) have been expanded in (I)SN07 to handle mobility of Internet Protocol (IP) telephony clients in a Voice over IP (VoIP) Enterprise environment. This functionality is applicable only to the Succession version of the CICM product, and not applicable to TDM CICM.

For fixed lines, either in a traditional TDM network or a line connected to an analogue line gateway, the location of the line, for Emergency Call Services (ECS), can be determined using the Calling Line Identity (CLI). Information from region telecommunications providers would be

required to associate a CLI with a location. Because the lines are of fixed location, the ECS call routing is statically configured as well.

For CICM telephony clients, the location of a user is not fixed. Unistim terminals in an Enterprise, connecting to the Call Server 2000 (CS2K) via the CICM, are not statically configured against a particular node in the network, and their physical location may be anywhere in the Enterprise.

This feature provides for the location information to be configured in, and provided by, the Dynamic Host Configuration Protocol (DHCP) server. The DHCP Server may have none or only some of the options configured. Only the configured Location Identification options will be returned by the DHCP Server to the CICM telephony client.

When the CICM telephony client registers with the DHCP server, it can request the location identification information options. If available, the DHCP server will return the location information to the set. The CICM gateway may then request the location information from the CICM telephony client at any time and report the location information, via H.248, to the GWC. If configured, an application running on the Gateway Controller (GWC) re-packages the information and reports it to a Location Recipient application.

This feature also supports the reporting of user-defined location identification. This is required for CICM telephony softclients on networks with DHCP servers that do not support the new location identification DHCP options.

This feature provides for reporting of the necessary information to support the Enterprise ECS solution. This solution uses a Location Information Server (LIS) to provide the physical location information. The ECS correlates the LIS information with the client information using IP addresses and MAC address.

The mechanism for reporting CICM telephony client location information can also be employed to report the client location's unique network id (unid) within the network topology.

In this Enterprise ECS feature, the Location Identification information is not configured as options in the DHCP servers. Instead, the Location Information Service (LIS) gathers etherswitch/port-to-IP/MAC address associations for all devices connected to the network. The LIS performs this function by gathering information from routers and etherswitches. The LIS forwards the information onto the Emergency Application/Data Manager (EADM).

The EADM determines how emergency calls from telephony clients should be handled, and sends this information to the Call Server. To accomplish this, the EADM correlates data from the LIS and the telephony client controller, and uses its own network topology data to determine what emergency call handling information to send to the Call Server. In addition, the EADM handles Emergency Response Location (ERL) management and Automatic Location Identification (ALI) entry updates to the ALI Database.

The CICM ECS Location Identification feature provides for the EADM to receive the Location Identification information from the GWC, not the telephony client controller (i.e. the CICM).

Included in the Location Identification information reported by the GWC to the EADM are the telephony client's public IP address, private IP address, MAC address and a way to uniquely identity the client on the Call Server. The EADM correlates this information with the information from the LIS. The EADM can then update the call server with emergency call routing for the telephony client and decide whether to use the Location Identification information reported by the GWC or use Location Identification information from it's own database.

IP Phone 200x Ethersets
The IP Phone 200x Etherset must be configured to use full or partial DHCP configuration to enable the CICM ECS Location Identification functionality.

m6350 Softclient
The CICM m6350 softclient has been modified to provide the user with an interface to specify their civil location description when logging in.

The CICM softclient has also been modified to allow the user to specify automatic server selection. If this is selected, the softclient retrieves the CICM and Location Identification options from the DHCP server, so the user is not required to specify the server address.

The CICM telephony softclient must be at release 7 to support this feature.

CICM Element Manager
The CICM ECS Location Identification functionality on the CICM is activated via the CICM Element Manager. The CICM-EM administrator configures a default civil location description and unique network ID against a network domain profile.

If a CICM telephony client registers with the CICM, but does not provide

either the civil location description or unique network ID, the default value is taken from the network domain profile.

GWC Element Manager
The CICM ECS Location Identification functionality on the GWC is activated via the GWC Element Manager Graphical User Interface (GUI).

The destination for the Location Identification information, (i.e. the Location Recipient) is configured in the GWC Element Manager. The Location Recipient is configured in the Location Recipient tab of the Network Devices section of the Network panel.

The GWC Element Manager enables Location Identification reporting on the GWC via the SNMP.

Feature: Enhanced FCAPS Interfaces and Integration into IEMS

CICM 7.0 provides enhanced interfaces for provisioning, fault reporting, performance measurements, and security. It provides capabilities to pass on fault and alarms to the overlaying OSS systems of the service provider.

Feature: Flow Through Provisioning

Flow Through Provisioning is a new (I)SN07 feature that is designed to minimize line provisioning time. It facilitates provisioning by providing for provisioning information datafilled at one time to be automatically available to other levels of the network, as needed.

The core portion of CICM preprovisioning has the following 2 parts:

- New slot and circuit ranges for CICM MGRP LGRP LENs have been defined.

  Note: CICMs use the existing LGRP GRPTYPE of M

- Disable Table LNINV autoprovisioning for SERVORD commands executed via CS2000 Management Server for MGRP LGRP lines. This restricts SERVORD from provisioning Table LNINV for CICM lines.

New NGRP LGRP LEN
The LEN for a line in an MGRP LGRP is comprised of the following 5 parts:

- **Site name**: CI<Shelf Slot>

  Example
  CI87 denotes a CICM node on shelf 87.

  Note: This nomenclature is suggested, but not enforced.

- **Frame**: 0 to 511
- **Logical Group**: 0
  There is only one logical group, denoted by **0**.
- **TT**: 00 to 10
  TT represents the upper value of the CICM circuit.
- **tt**: 0 to 99
  tt represents the lower value of the CICM circuit

  Note: For TT = 10, the range for tt is 00 to 23, because there is a limit of 1024 tids per LGRP.

  Example
  CI12 0 0 02 12

SERVORD restrictions
Flow through provisioning requires restricting SERVORD provisioning of Table LNINV for MGRP LGRPs. Disabling autoprovisioning of Table LNINV for certain SERVORD commands for MGRP LGRPs is required for flow through provisioning.

MG9K preprovisioning
The MG9K-EM part of the preprovisioning is required for the CICM flow through provisioning feature to work. The new office parameter RDT_SUCC_AUTOCREATE_LNINV enables autoprovisioning for non-MG9K line gateways.

The Flow Through Provisioning feature of (I)SN07 implements Media Gateway 9000 (MG9K) line provisioning throughput by preprovisioning. This flow through provisioning by preprovisioning is accomplished by the following three aspects:

- The format of an MG9K LEN now reflects a physical location.
  OLD FORMAT
  <SITE><0 to 511><0 to 9><subgroup, 0 to10><circuit, 0 to 99>
  NEW FORMAT

<SITE><frame, 0 to 511><shelf, 0 to 9><slot, 2 to 9, 14 to 21><circuit, 0 to 47>

- When the CS2000 Management Server provisions an MG9K node on shelves 0 to 3 and LGRP data, Table LNINV is automatically datafilled with the available circuits. Subsequent SERVORD+ commands issued by the CS2000 Management Server will not add or delete MG9K line datafill from Table LNINV. Essentially, autoprovisioning of Table LNINV will be disabled for MG9K lines.

  This new functionality will supersede the setting of office parameter RDT_SUCC AUTOCREATE_LNINV for determining the autoprovisioning of Table ININV. This feature does not restrict the MNO_DEFAULT value associated with RDT_SUCC_AUTOCREATE_LNIINV.

- Two new pad groups are defined for use by gateway lines.
  - — Pad group PKLNL has been created for use by gateway lines that have LGRP GRPTYPEset to S.
  - — Pad group PKNIL is for use by gateway lines during SERVORD provisioning and during CS2000 Management Server provisioning and preprovisioning. Changing the gateway line pad group from these two new groups is accomplished via changing the pad group in Table LNINV. Default pad levels are set for legacy interaction.

Logs

All LINE logs generated for MG9K lines will utilize the new LEN format. The administrator can use the log to identify the physical location of the reported MG9K circuit.

Tables

Two tables have been modified in support of this feature.

Table 2 Modified tables

Table	Changes	Comments
LGRPINV	The previously unused field GRPTYPE in table LGRPINV is used in this feature to denote a specific type of LGRP. The values for GRPTYPE are S, M, and C.	This feature disables SERVORD autoprovisioning for GRPTYPE S for groups on shelves 0 to 3. GRPTYPE S now denotes a set of LGRPs that now only includes MG9K LGRPs.
PADDATA	Two new pad groups added: • PKLNL • PKNIL	These 2 new pad groups are used by gateway lines as follows: • PKLNL is now used by gateways lines with LGRP GRPTYPE set to S. • [PKNIL will be used by gateway lines with LGRP GRPTYPE set to C.

Feature: H.248 compliancy Extensions

The H.248 compliancy extensions support additional H.248/SDP mechanisms.

Feature: H.248 Call Control Signalling

This feature upgrades the H.248 protocol stack software for the CICM product from the SN06 to (I)SN07 version. Generic H.248 signalling functionality has been enhanced with the following updates that have been developed on the MG9000 platform:

- ESA Entry
  Support for H.248 duration parameter in association with playing tones
- SDP Enhancements
  The maximum length of SDP string increased from 256 to 512 bytes.

No new logs are associated with this feature.

Feature: Multi-Timezone support

The Multi-Timezone feature provides the ability to store the local time of the user on the switch so that the features can be activated in terms of the local time of the user. This is a DMS/CS2K feature.

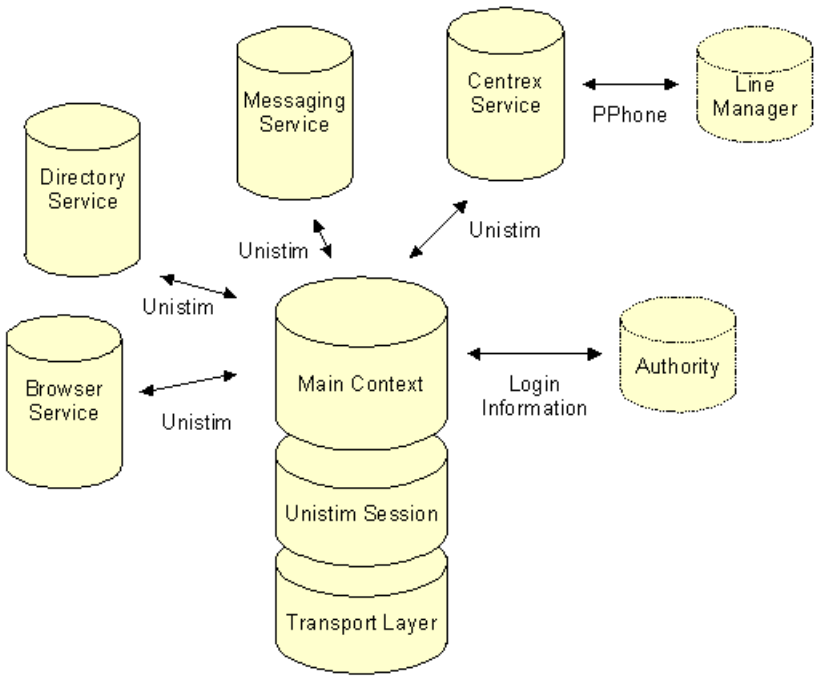
Feature: UNIStim Security

This feature provides the infrastructure for secure signalling communication (i.e. encryption/decryption) between the CICM Server and its clients.

The CICM session manager hosts sessions between end user terminals and the gateway. Terminals can be physical devices, such as the IP Phone 200x, or software applications running on a remote machine like the m6350 softclient. The terminals and the gateway communicate using a stimulus protocol called Unistim. By interacting with the terminal, an end user can use the services that are hosted by the gateway.

The following Figure 4 diagram demonstrates the components of a single session on the CICM Server. The **Unistim Session** and **Transport Layer** shown in the diagram encapsulates the signalling protocol/communication between the terminal clients and the CICM server.

Figure 4 Unistim security



Feature: Support for Interopt

This feature provides support for interopt with the Ambit line gateway.

Feature: Fault and Performance management

This section summarizes the Fault and Performance management changes for (I)SN07. It includes the changes for the alarms, logs, and performance features for the (I)SN07 release.

Note: These changes affect the Succession version of the CICM product only. The TDM version does not support these changes.

IEMS

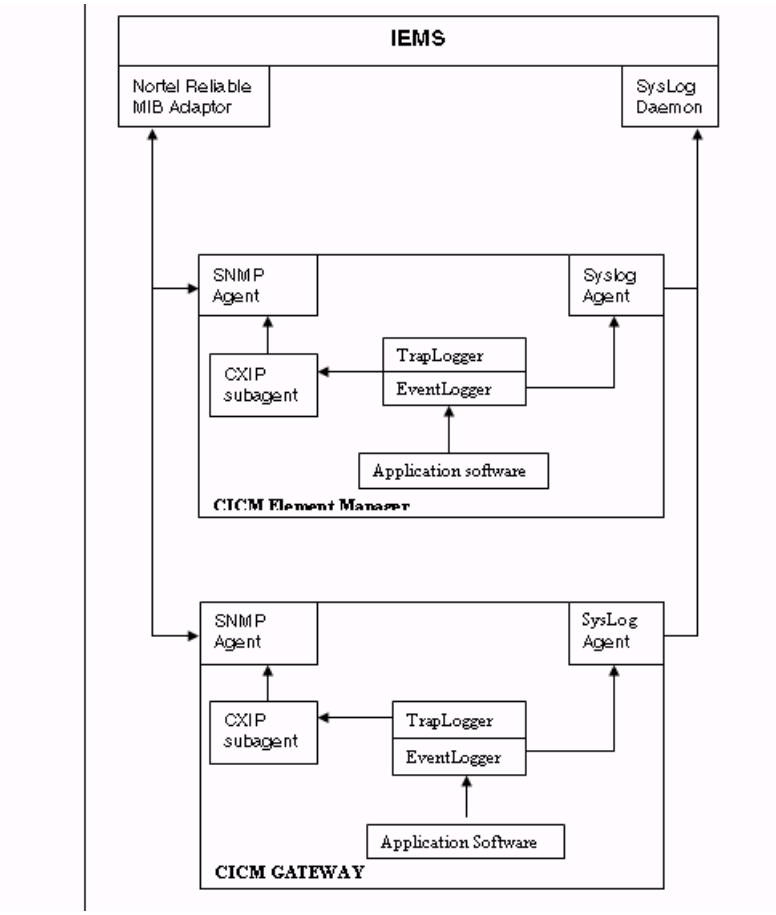
A new interface has been introduced to the Succession network that will manage the output used by external OSS to monitor the network element and detect alarm conditions. This new interface is the Integrated Element Manager System (IEMS). The IEMS is accessed using a Graphical User Interface (GUI), which will give access to the alarms and logs for a network element. This will also interact with the EM GUI.

The CICM must integrate with the IEMS. The CICM alarms, logs and performance metrics have all been formatted to be compatible with IEMS.

Both the CICM and the CICM-EM can raise alarms and faults to the IEMS. The EM will raise alarms associated with the EM Platform (e.g. memory shortage), and communication with the CICMs that it manages, but will not have knowledge of the alarms and faults generated by the CICM. The CICM sends alarms as SNMP traps directly to the IEMS.

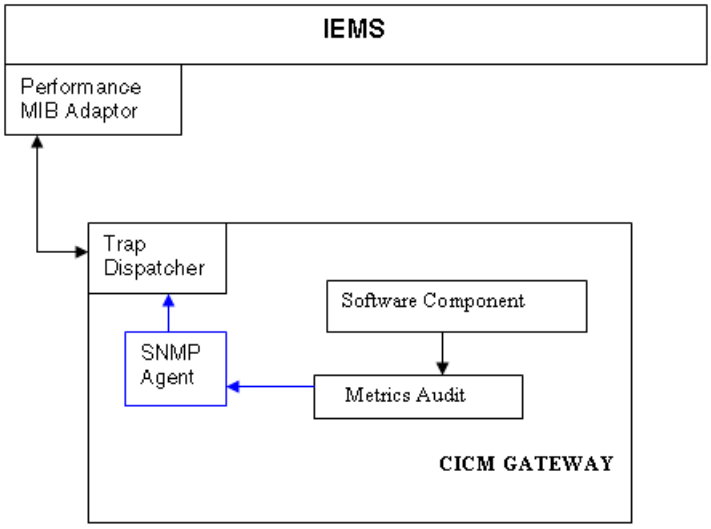
The following Figure 5 provides an overview of the CICM fault architecture.

Figure 5 CICM Fault Architecture



The following Figure 6 illustrates the CICM Performance architecture.

Figure 6 CICM Performance Architecture



Alarms

All alarms are sent to the IEMS as an SNMP trap, and as a log to SYSlog. Each trap sent from the gateway incorporates the following information:

- Sequence number
- Severity indicator
- Component ID
- Category of alarm
  - communications
  - quality of service
  - processing error
  - equipment
  - environment
- Notification ID
- Description
- Time stamp
- Probable cause
- Specific problem
- Correlation ID list

The alarm severity is classification is provided in the following table.

Figure 7 Alarm severity

	Critical	Major	Minor	Warning
Service Affecting	Yes	Yes	No (or few affected)	No
Action required	Yes	Yes	Yes	No
Recommended Timeliness of Action	Immediately – drop everything	Rapidly – in next work shift	Soon – could be delayed until next day	Later – investigate if reoccurance
Target Reporting time	Within 2 Sec	Within 30 Sec	Within 2 Min	Within 5 Min

Fields which are valid for alarm raises are:

- nortelNMIcurrentTxNotificationSequenceNum
- nortelNMIalarmComponentId
- nortelNMIalarmCategory
- nortelNMIalarmNotificationID
- nortelNMIalarmDescription
- nortelNMIalarmTimeStamp
- nortelNMIalarmProbableCause
- nortelNMIalarmSpecificProblem
- nortelNMIalarmCorrelationIdList
- nortelNMIalarmNeVendorSpecificInfo
- nortelNMIalarmTechnologySpecificInfo

Fields which are valid for alarm clears are:

- nortelNMIcurrentTxNotificationSequenceNum
- nortelNMIalarmComponentId
- nortelNMIalarmDescription
- nortelNMIalarmTimeStamp
- nortelNMIalarmCorrelationIdList

Component IDs

The CICM is divided into the following 3 objects for the purpose of reporting alarms:

- The CICM Element Manager
- A CICM node
- The platform which the EM and the CICM use.

These objects contain sub-objects which, appended together with the alarm type, form the Component ID. Component IDs are defined in Figure 8.

Figure 8 Component IDs

Object	Sub Object	Component Id
CICM element manager	Node (CICM)	CICMEM<NN>;CICMEM.NODE.<cicmID+node>
	General	CICMEM<NN>;CICMEM.GENERAL.<cicmID+node>
CICM node	User	CICM<NN>;CICM.USER.<user id>.<event>
	Terminal	CICM<NN>;CICM.TERMINAL.<Terminal id>.<event>
	Endpoints	CICM<NN>;CICM.EP.<Endpoint Number>.<event>
	Network Transport	CICM<NN>;CICM.NET.<event>
	VMG	CICM<NN>;CICM.VMG.<VMG id>.<event>
	General	CICM<NN>;CICM.GENERAL.<event>
CICM platform	User	CICM[EM]<NN>;CICMP.USER.<event>
	Console	CICM[EM]<NN>;CICMP.CON.<event>
	Network connections	CICM[EM]<NN>;CICMP.NET.<event>
	Mate node	CICM[EM]<NN>;CICMP.MATE.<event>
	Chassis	CICM[EM]<NN>;CICMP.CHAS.<event>
	Cards	CICM[EM]<NN>;CICMP.CARD.<card number>.<event>
	Logs	CICM[EM]<NN>;CICMP.LOGS.<event>
	Software Component	CICM[EM]<NN>;CICMP.SW.COMP<component number>
	Configuration database	CICM[EM]<NN>;CICMP.CONF.<event>

Logs

Both the CICM and the CICM-EM are responsible for sending their logs to the IEMS. Logs are not exchanged between the CICM and CICM-EM.

Logs are sent to the IEMS using CUSTLOG or security log formats via a syslog agent. Three log streams are used to send logs to up to three different syslog daemons (i.e. IEMS). This is a change from previous CICM releases, where all logs were stored on the CICM. In (I)SN07, logs are still stored on the CICM, but the CICM also sends logs to CUSTLOG, Audit Log, and Security Log streams.

> ***Note:*** Each log is formatted specifically for each of the three streams.

The CICM will use the syslog protocol to send logs to the IEMS. The CICM and CICM-EM both act as log senders. They are only able to send syslog messages; they are not able to receive or relay syslog messages. UDP port 514 (the syslog port) is used to send the syslog messages to the IEMS. The log packet must be no greater than 1024 bytes.

Custlog
the CICM will log the following events using the custlog format, and output the logs to the custlog stream.

- Service affecting state changes
- Specific customer/blm requested events
- Data corruptions/data mismatches
- Shutdown and restart of processes

Security logs
Security Logs are generated from the CICM gateway as follows:

- upon successful/unsuccessful login from an etherset (IP Phone 200x) or m6350 Softclient
- logout from an etherset (IP Phone 200x) or m6350

Security Logs are generated from a CICM-EM as follows:

- upon launching CICM-EM from IEMS

The CICM will log the following events using the security log format and output the logs to the security log stream.

- Unsuccessful terminal logins
- Successful terminal logins

Audit logs
Audit logs are generated from the CICM Gateway on executing flow-through commands at OSSGATE (e.g. ado, deo, etc.).

The audit logs are in the same format as the security logs. The following actions will be logged to the audit stream:

- All configuration changes made by the CICM-EM administrator. (e.g. adding CICM nodes)
- All mtc actions performed by the device (e.g. restarts)

Debug logs
Debug logs are used by Nortel Networks support personnel only; not the service provider. Debug logs are not changed in (I)SN07, but they can now be viewed using the EM Web page interface. Debug logs will not be sent via syslog to the IEMS.

Performance
The new interface introduced to the Succession network that manages the output used by external OSS' to monitor CICM network elements is the IEMS. Performance metrics have been re-formatted in (I)SN07 to

be compatible with IEMS.

The following performance metrics are supported in CICM 7.0:

- Percentage Memory Usage
- Number of Active Connections
- Percentage CPU Usage
- Number of logs
- Number of Active Sessions
- Number of Busy Hour Call Attempts
- Transmitted Bytes/Sec
- Received Bytes/Sec
- Number of Logged in Users

The metrics will be stored in the performance MIB and will be collected at intervals by the IEMS.

Feature: GWC-EM VCAC Support for CICM gateways

This feature introduces Virtual Connections Admission Control (VCAC) for (I)SN07. It provides GWC-EM Internet Transparency VCAC provisioning support for CentrexIP gateways.

VCAC introduces Limited Bandwidth Links (LBLs) to the CS2000 Management Server (network panel), and a topological hierarchy that links LBLs and NATs to form a tree of internet transparency middleboxes. These devices are sent to the small lines GWCs via the:

- **GWC-MIDDLE-BOX-MIB**, and
- **GWC-MIDDLEBOX-RSRCUSAGE-MIB**
  The resource usage of the LBL

The model for this download of data has been designed for the fixed-lines IAD deployment, and occurs when the gateway is associated to an adjacent middlebox.

This feature allows VCAC to function for CICM gateways because unlike the small-lines IAD solution the CICM gateways resides in the TSP (Succession) domain.

When CICM users login to the CICM terminals, a message is sent to the GWC. In (I)SN07 this message will contain the “discovered” adjacent middlebox of the terminal/endpoint. The CallP ITA function will then “look-up” this middlebox in the GWC static tables. For a more

comprehensive problem definition please refer to the DID for this activity.

This solution allows the user to provision a set of root (top-level) middleboxes, allowing the GWCEM to send all the underlying middleboxes to the GWC. Ensuring that when a CICM user logs in, the middlebox will be available on the GWC.

This feature provides the following functionality:

- Provision (from the OSS and GWC-EM GUI) a set of root middleboxes (a maximum of 5) against CICM gateways.
- Change the current provisioning of root middleboxes against provisioned CICM gateways.
- Display/Query the root middleboxes that are provisioned against a CICM gateway.

This feature executes as part of the CS2000 Management Server.

User interfaces
The following GUIs have been modified for this feature:

- Associate Media Gateway Dialog
- Change Gateway Dialog
- Gateway Provisioning Panel

The following XML commands have been modified for this feature:

- AssocMG
- ChangeRootMiddleBoxes
- QueryMG

The on-line help facility has been updated to provide information on the use, syntax, and valid values for these user GUI modifications.

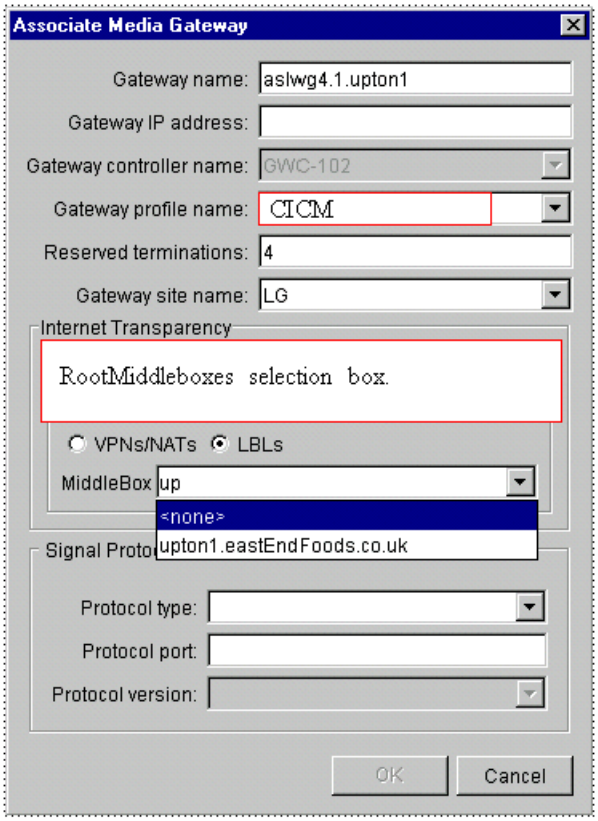
Gateway provisioning changes
The association of a CICM gateway to a GWC has been modified to allow the user to provision a set of root middleboxes. Already provisioned gateways can also be changed to have a different set of root middleboxes (or none).

Associate gateway GUI
The Associate gateway dialogue has been modified to display a new Internet transparency panel. This is displayed when a CICM gateway has been selected. The user may select up to 5 root middleboxes to

associate with the CICM gateway. These are selected to define the roaming area where VCAC will function for the CICM users/endpoints.

Figure 9 illustrates the Associate gateway dialogue GUI.

Figure 9 Associate gateway dialogue



Change gateway GUI

The change gateway Root Middleboxes dialogue has been created to allow the user to modify (or remove) the Root Middleboxes associated with an already provisioned CICM gateway.

Root middleboxes selection

The root middlebox selection process is controlled from within the root middlebox selection area. This is the same for either the **Associate Gateway** or the **Change Gateway** commands.

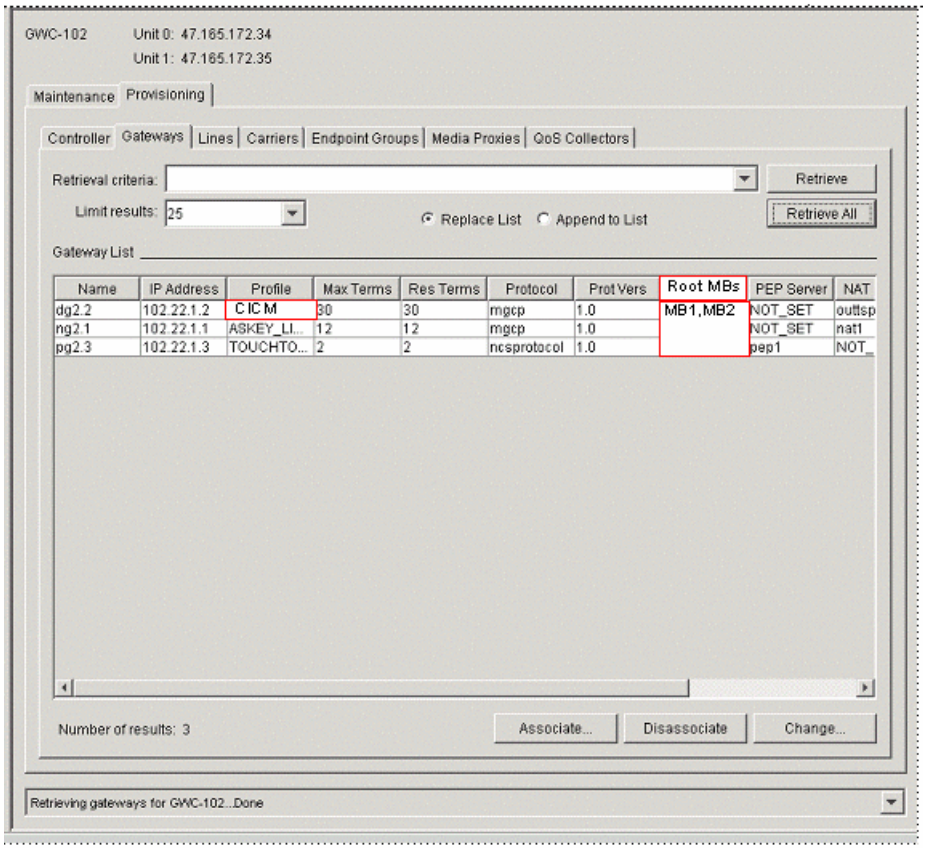
XML Interface

The AssocMG and QueryMG interface has been modified to allow/display root middleboxes. A new interface **ChangeRootMiddleboxes** has been added. If any request is unsuccessful, an error message is returned.

GWC-EM GWC provisioning

The GWC-EM has been modified to display the rootMiddleboxes that are provisioned against the CICM gateways. This is illustrated in the Figure 10.

Figure 10 The GWC-EM gateways panel



Authorization for commands

The security for the GUI Client and OSSgate interface includes support for permission/authorization levels for commands. Each command is associated with one or more user groups. In order to execute a command, a user must belong to at least one of the associated user groups. The user groups associated with the new commands are specified in the table below.

Figure 11 New Internet transparency commands authorization

Command	User Group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
ChangeRootMiddleboxes	X	X			

Limitations

The limitations of this feature are:

- The GWC has a limit of 2000 middleboxes.
- Internal counting limits the provisioning of gateways onto the same GWC as the associated chain of LBLs, which must be provisioned onto one GWC.
- The CentrexIP users cannot roam outside of their provisioned “enterprise” area, and expect VCAC to function.

Feature: Present Conference on Succession

The Preset Conference on Succession feature addresses the functionality of the Preset Conference in the Succession environment. For a detailed description of the Preset Conference, please refer to the Nortel Technical Publication (NTP) *297-8001-350 DMS 100 Family NA100 Translation Guide, Volume 13 of 20*.

This feature provides support for the following types of line on both North American and International markets:

- CICM lines: IP Phones 2001, 2002, and 2004; and m6350 softclients
- MG9K Pphones and IBN lines

Preset conference feature limitations

In the Succession domain, the following are limitations to the Preset Conference functionality:

- The maximum supported conferences in Preset Conference is 25. Larger conference sizes are not supported.
- Preset Conference is implemented in non-hybrid scenarios only. In the hybrid environment, the support remains the same.
- The ADDON functionality for Preset Conference is not supported on Succession. The subfield **ADDON** in Table **PRECONF** shall be set to **N**.

Figure 12 Table PRECONF, subfield ADDON

```
0 0 9192461888 D IBN POTSDATA 0 N N N N N Y $
```

- The Audio Tone Detector is an MTM component and the functionality is not available through UAS. Hence, this activity does not support the ATD functionality of the Preset Conference. The **ATD** subfield in Table **PRECONF** should be set to **N**.

Figure 13 Table PRECONF, subfield ATD

```
0 0 9192461888 D IBN POTSDATA 0 N N N N N Y $
```

- The support of Tones or Announcements for Preset Conference on Succession is not implemented through this activity. The **IMMSTART** subfield in Table **PRECONF** should be set to **Y**.

Figure 14 Table PRECONF, subfield IMMSTART

```
0 0 9192461888 D IBN POTSDATA 0 N N N N N Y $
```

- The **Conferee Class P** and **D** are supported by this feature. The **Conferee Class A** and **C** are not supported.
- The Preset Conference options **MADNOPT** and **NARS** is not supported through this activity and should not be datafilled.

Figure 15 Table PRECONF, Options

```
0 0 9192461888 D IBN POTSDATA 0 N N N N N Y $
```

- This feature makes use of conference tones (e.g. conference entry tone, conference exit tone). The Preconference tones PCNOR (Preset Conference NotificatiOn Tone) and PCALR (Preset Conference Precedence Notification Tone) is not supported through this activity.

Feature: Support of IP Phone 2001 Etherset

The IP Phone 2001 Etherset has been introduced to the terminal portfolio in (I)SN07 release. It is the most economical version of the IP Phone 200x terminal series. In addition, the IP Phone 2001 is the first phase II Unistim terminal.

Phase II terminals have a new bootstrap and require some incremental work on the CICM for support. Phase I terminals will be Manufacture Discontinued (MD) when Phase II terminals become more generally available. The Phase II terminals can be configured as “emulations” of the existing Phase I terminals.

Feature: IP Phone 2002/2004 Key Expansion Module

The Key Expansion Module (KEM) feature supports the implementation of a 24-key expansion module with an LCD that provides both icons and labels similar to those provided on the IP Phone 2002, applicable to 2002 and 2004 terminals.

Of the 24 keys on the KEM, 22 are available for use in (I)SN07. Up to two KEMs can be utilized with a single terminal, providing up to 44 additional keys.

The KEM is provisioned through both the DMS and the Element Manager. Before any features can be assigned to the keys on the KEM, the M522 line option must be assigned to the associated terminal on the DMS. The M522 line option includes the specification of one or two expansion modules.

Within the Element Manager, on the IP Phone 2002 and 2004 **Terminal Configuration** pages, the following Feature Key Attributes should be provided:

- Number of extension modules supported
- Number of features available on each extension modules

Additionally, if user profiles are used, the following User Setting should also be provided on the **User Profile Edit** page:

- Number of Extension Modules

Both the M522 line option and the Element Manager information must be provisioned. The M522 line option on the DMS enables the provisioning of features on the additional keys, while the Element Manager data controls the use of any KEMs connected to a terminal.

More specifically, with regard to the Element Manager data, the Gateway will use the information in the Element Manager to either support or block KEM usage. For example, if there are two KEM units attached to a terminal, but the terminal configuration and/or the User Profile specifies only one extension module, then the user at that terminal will only be able to utilize the first KEM unit. The other will be unavailable, having been blocked (based on the Element Manager data).

The display, particularly the icons, is very similar to that provided on the IP Phone 2002 terminal. Icons and labels will operate on the KEM just as they do on an IP Phone 2002 terminal. However, no paging capability is provided for the KEM. 22 of the 24 keys are available for use in (I)SN07.

Feature: CICM EM Integration with PAM+ Proxy

Succession user authentication services have migrated to a single centralized third party server, which provide authentication services to succession management systems via a PAM on the SSPSFS platform.

This feature integrates the CICM-EM into this Succession strategy for user authentication, by interfacing CICM to PAM via the HTTPS PAM+ proxy on SSPFS.

By using PAM, Succession management systems can interact with any pluggable authentication technology without having to make any changes to succession management applications. The use of a centralized authorization database via PAM also provides the advantage of having a single account management interface for use by all succession management tools.

The CICM-EM User Interface requires a username/password login. Prior to this feature, only a single user level was supported – which provided full access to all the provisioning, maintenance and admin functions of the CICM-EM. With the introduction of this feature, the CICM-EM can be configured to access the HTTPS PAM+ proxy, passing it the username and password, and the SSPFS then returns a user authentication level to the CICM-EM, or rejects the username and password if they are not a valid combination. This user authentication level is then used by the CICM-EM to restrict access to functions that are not appropriate for particular user groups.

Note: Authentication using the SSPFS will only occur when the user is accessing the CICM-EM via the Web interface. This feature will not change the method used for authenticating users who are logging in using a Telnet session.

Login

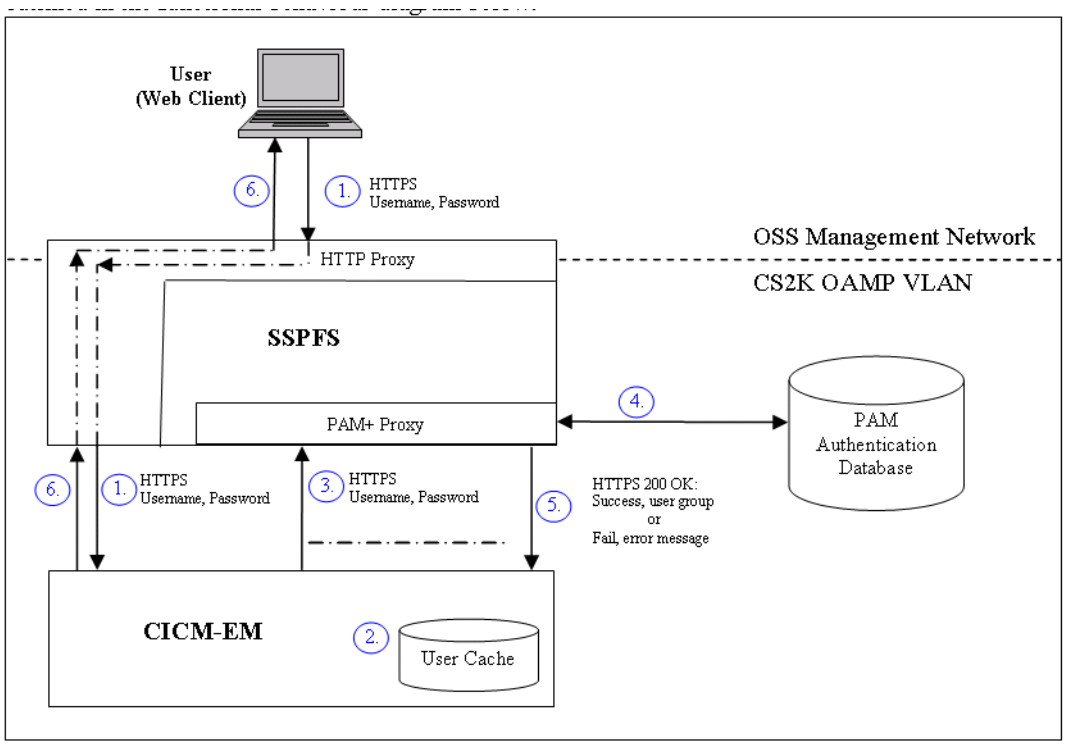
In SN06 and prior releases, the username and password supplied when logging into the element manager corresponded to local user accounts on the CICM-EM. For (I)SN07 Succession deployments, username and password can be configured as a global Succession account managed on a centralized authentication database. This database interfaces to Succession management tools via the PAM+ proxy located on the SSPFS.

Local user account management and user authentication on the CICM-EM is preserved for TDM deployments, where the SSPFS platform is not used. For Succession deployments, a method of local user authentication is also provided for use when connectivity is lost to the SSPFS platform.

User authentication via SSPFS PAM proxy

The behavior provided by CICM-EM user authentication via the PAM proxy running on the SSPFS is outlined in the functional diagram below.

Figure 16 HTTPS PAM+ proxy and CICM-EM integration



The numbers in Figure 16 refer to the following steps in the user authentication process:

1. Using a web client, the user attempts to log into the CICM-EM through the HTTP proxy located on the SSPFS. The supplied username and password are for a global Succession user account, which is managed on a centralized authentication database. The Web Client sends an HTTPS request to the CICM-EM with the username and password built into the HTTP authentication header.

2. The CICM-EM uses the supplied username and password as a key to search a cache of recently authenticated users. Each user entry in

the cache contains a corresponding username and password for a temporary local user account assigned to that user. If the user is present in the cache, the mapped local username and password is passed back to the PAM and the process proceeds to step 5 (with successful authentication).

3. The CICM-EM sends an authentication request to the HTTPS PAM+ proxy located on the SSPFS platform.

4. The PAM+ proxy authenticates the user on a centralized authentication database via the PAM.

5. If the authentication is successful, the PAM+ proxy responds with a list of succession user groups to which the user belongs. The CICM-EM has a list of pre-defined local user groups that are equivalent to the user groups returned by the PAM proxy. The CICM-EM creates a temporary local user account on the CICM-EM when a response to a user authentication request is successful. The temporary local user account is added to the pre-defined local user groups that are equivalent to the Succession user groups returned by the PAM proxy.

Additionally, the CICM-EM adds the authenticated username/password and the corresponding temporary local username/password to the user cache. This entry is held in the local cache for a pre-determined amount of time. While this entry is present in the cache, subsequent authorization requests for this user do not need to be processed through the PAM proxy. This reduces the processing load on both the CICM-EM and PAM proxy.

The CICM-EM also replaces the global Succession username/password in the HTTPS authentication request with the username/password of the temporary local user account. The temporary local username and password combination is then authenticated locally by standard user authentication.

If the authentication is unsuccessful, then the CICM-EM rejects the user's attempt to log in.

6. If the authentication is successful, then the CICM-EM provides the user with access to the requested webpage. If the authentication is unsuccessful, then the CICM-EM denies access to the requested webpage.

User authentication levels

Succession User authentication levels on the PAM+ proxy are organized into five separate domains, with each domain containing 5

separate levels of user authentication. This provides a total of 25 user authentication levels, as shown below in the following table.

Access Level	USER DOMAIN				
	Trunks	**Lines**	**MGC**	**MG**	**EMS**
Administrator	trkadm	lnadm	mgcadm	mgadm	emsadm
Read-Write	trkrw	lnrw	mgcrw	mgrw	emsrw
Provisioning	trkprov	lnsprov	mgcprov	mgprov	emsprov
Maintenance	trkmtc	lnmtc	mgcmtc	mgmtc	emsmtc
Read-Only	trkro	lnro	mgcro	mgro	emsro

The PAM proxy returns a list of groups for which the user has been successfully authenticated. The user domains relevant to the CICM Element Manager are Lines, MG and EMS. All CICM-EM web pages are configured with access control levels that are appropriate to their functionality.

Local user authentication

Centralized user authentication via the SSPFS PAM proxy is not available to TDM deployments of CICM. In addition, it is important to provide access to the CICM-EM if connectivity is lost between the CICM EM and the SSPFS.

The CICM-EM checks to determine if it is running in a TDM or Succession CICM deployment before it attempts to process the authentication via the PAM proxy. For TDM deployments, the authentication functionality will immediately pass control of the authentication back to the standard mechanism used for CICM.

For Succession deployments, users are able to select local authentication by prefixing their username with a period (“.”). This allows users to access the CICM-EM when the PAM proxy is out of service, provided they have a local user account on the CICM-EM. Therefore, to access the CICM-EM when the SSPFS is not accessible, the user can log in using local user authentication.

Configuration for the SSPFS PAM+ proxy

The configuration of the IP address to use for the SSPFS PAM+ proxy is configured by Nortel Networks Installers during the EM preboot stage. The user can select to use HTTP or HTTPS (secure HTTP) to communicate with the PAM proxy. If HTTPS is selected, the user will be

prompted to enter the Fully Qualified Domain Name (FQDN) of the PAM server. HTTPS requires that a certificate from a valid signing authority is installed on the SSPFS.

Logs
This feature logs the following events on the IEMS:

- User successfully authenticated through PAM
- User authentication through PAM failed
- Request Timeout on PAM proxy

The CICM-EM will also raise an alarm on the IEMS when a request to the PAM proxy times out. This alarm is cleared the next time an authentication request is successfully processed through the PAM server.

Feature: Inter-working of CICM and IW-SPM

The Inter-working Spectrum Peripheral Module (IW-SPM) is a special gateway for the Nortel Networks' multi-core DMS switch (TDM) to the IP network, which acts as a bridge between the ENET of the TDM core and the ATM fabric. This product is built upon the SPM platform.

The IP IW-SPM has two components:

- Common Equipment Module (CEM)
- Resource Module (IP RM)

The IP Inter-working Spectrum Peripheral Module (IW-SPM) provides a mechanism for bridging calls between the Nortel Networks existing DMS (TDM) switch and the public IP network.

The IP IW-SPM accomplishes this by connecting to an Enhanced Network (ENET) over C-side DS-512 fiber links and to the IP network over Gigabit Ethernet on the P-side. Between these two connections are the CEM and the IP RM. The CEM connects to the DS-512 links and performs the bridge management function. The IP RM provides the means to connect those bridges to the IP network over a Gigabit Ethernet.

There are two scenarios in which CICM clients may inter-operate with the TDM clients:

- **Intra-group**
  Intra-group refers to clients in the same customer group. Centrex users on the TDM side and on the CICM/IP side are in the same Centrex group, share the same dial plan and Centrex features, etc. For example, MADN users can be split between TDM and CICM/IP

transparently. Similarly, ACD agents on the TDM side and on the CICM/IP side are in the same ACD groups or queues. This affects services which could potentially span the IP to TDM bridge by the fact that they belong to the same customer group (Both TDM and IP based clients reside in the same customer group, for example, Call Pick-up or Call Park)

- **Inter-group**
  Inter-group refers to clients in different customer groups. TDM users and CICM/IP users are not in the same Centrex group, or they are in different enterprise networks, or they are not part of the same ACD group. This affects services that can potentially bridge across from the TDM to IP, or from IP to the TDM side (For example, Call Forward or 3WC).

Inter-working of CICM and IW-SPM does not depend on a specific CICM hardware platform.

Feature: Capacity Expansion

CICM 7.0 supports one or more pairs of CPN5385 CPU card per shelf. Each card pair's capacity limits are detailed in the following Table, and the definitions of attributes follow the table.

Table 3 CICM 7.0 Capacity and Performance Limits

Capacity Attribute (Maximum)	SAM16 Platform (Motorolla 5370)	SAM21 Platform (Motorolla 5385)
Lines that can be provisioned	1023	3069
Simultaneous terminal sessions	2500	4096
Simultaneous Active Half-Calls	512	3069
BHHCA	7200	21600
RUDP Messages/Sec	500	500
H.248 Messages/Sec	100	250

Provisionable lines

This number represents the maximum number of lines, and therefore

users, that a CICM can accommodate. (A CICM line corresponds to a LEN on the CS2K core.)

Simultaneous terminal sessions
The maximum number of terminals that may be connected and therefore presented with a login prompt by a CICM at any given time. Note that a user that logs in to a joint session uses two session resources on the CICM.

Simultaneous Active Half-Calls
Because of the client-focussed nature of the CICM in the Succession network, the CICM only recognizes half-calls. Even if the second half of a call is also hosted by the same CICM, the CICM treats them as independent call halves. The number of simultaneous half-calls represents the maximum number of half-calls that can be established at any one time by the CICM. Once the maximum is reached, new call attempts, both incoming or outgoing, are denied.

> ***Note:*** Any single terminal can support up to eight simultaneous active call halves, using various features such as multiple DNs, call hold, etc.

BHHCA
Busy Hour Half Call Attempts represents the maximum rate at which half call attempts can be made per hour. Once the BHHCA reaches 80% of the state value, a minor alarm is raised. At 100%, a major alarm is raised, and at 150% a critical alarm is raised. Calls above the 150% threshold are throttled. The count of throttled calls can be viewed from the EM.

RUDP Messages/Sec
Reliable User Datagram Protocol (RUDP) is the transport mechanism for the Unistim protocol. Unistim is the protocol used for all messaging between the CICM and its terminals. The incoming message rate is throttled to prevent the CICM from becoming overloaded.

H.248 Messages/Sec
H.248 is the messaging protocol used between the CICM and the GWC. Similarly, the incoming message rate from the GWC is throttled to prevent the CICM from becoming overloaded.

Feature: CICM Unistim Security

The Unistim Security feature was added in CICM 2.5 MR6 release. For this CICM 7.0 release, there are three new enhancements to CICM Unistim Security:

- The Clearing of Security Objects component
- Securing the UFTP stream component
- Support for Phase 2 sets component

The securing of the UFTP stream and the support for Phase 2 sets are enhancements that are not user visible and require no Telco administrator action.

The Clearing of Security Objects component provides the functionality to move a secured terminal from one CICM to another.

In the initial CICM 2.5 MR6 Implementation of Unistim Security, once a terminal has been connected securely to a CICM, it is tied to that particular CICM. Once in this state, the client is not capable of connecting to a different CICM without manual intervention. This feature enhancement adds an automated procedure to replace the manual intervention. This functionality is administered from the Security webpage of the CICM-EM web pages. Refer to the *Security Configuration* Procedure in the *NN10252-611 CICM Administration and Security* document.

Element Manager Web site enhancements

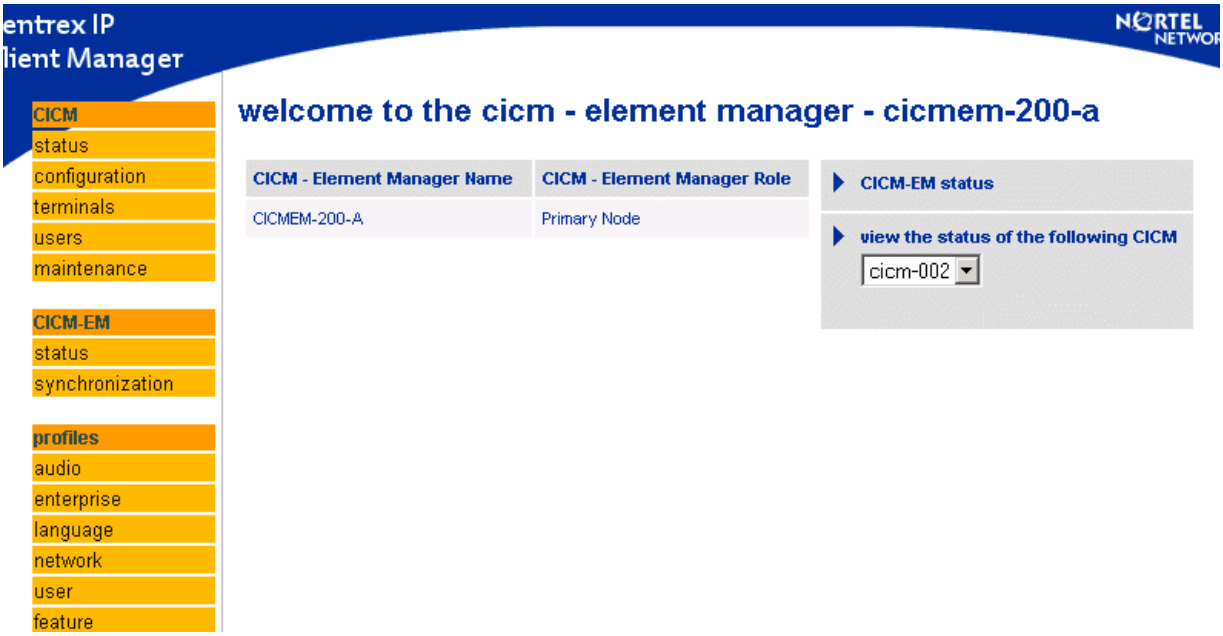
The CICM EM Web interface has been enhanced to support the new features. It has also been reorganized to improve userability. This section provides a brief overview of the enhanced Web interface.

Main menu

The main menu on the left side of each webpage has been organized into four sections: **CICM, CICM–EM, Profiles**, and **Diagnostics**.

CICM - element manager

The **welcome to the cicm - element manager - <cicmem_name>** page is the first page presented after entering the CICM-EM URL into the Web browser and logging on to the Web site.



CICM home

The **cicm home** page is accessed by selecting **status** from the **CICM** section of the main menu bar.

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

Figure 17 CICM Home

Configuration Wizard home

The **Configuration Wizard home** page is accessed by selecting the **configuration** option from the **CICM** section of the main menu bar.

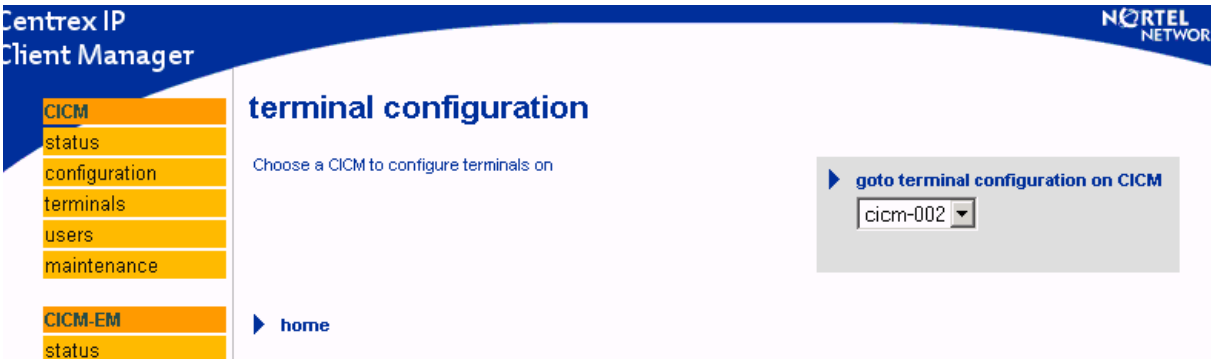
Figure 18 Configuration Wizard home

Terminal configuration

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

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

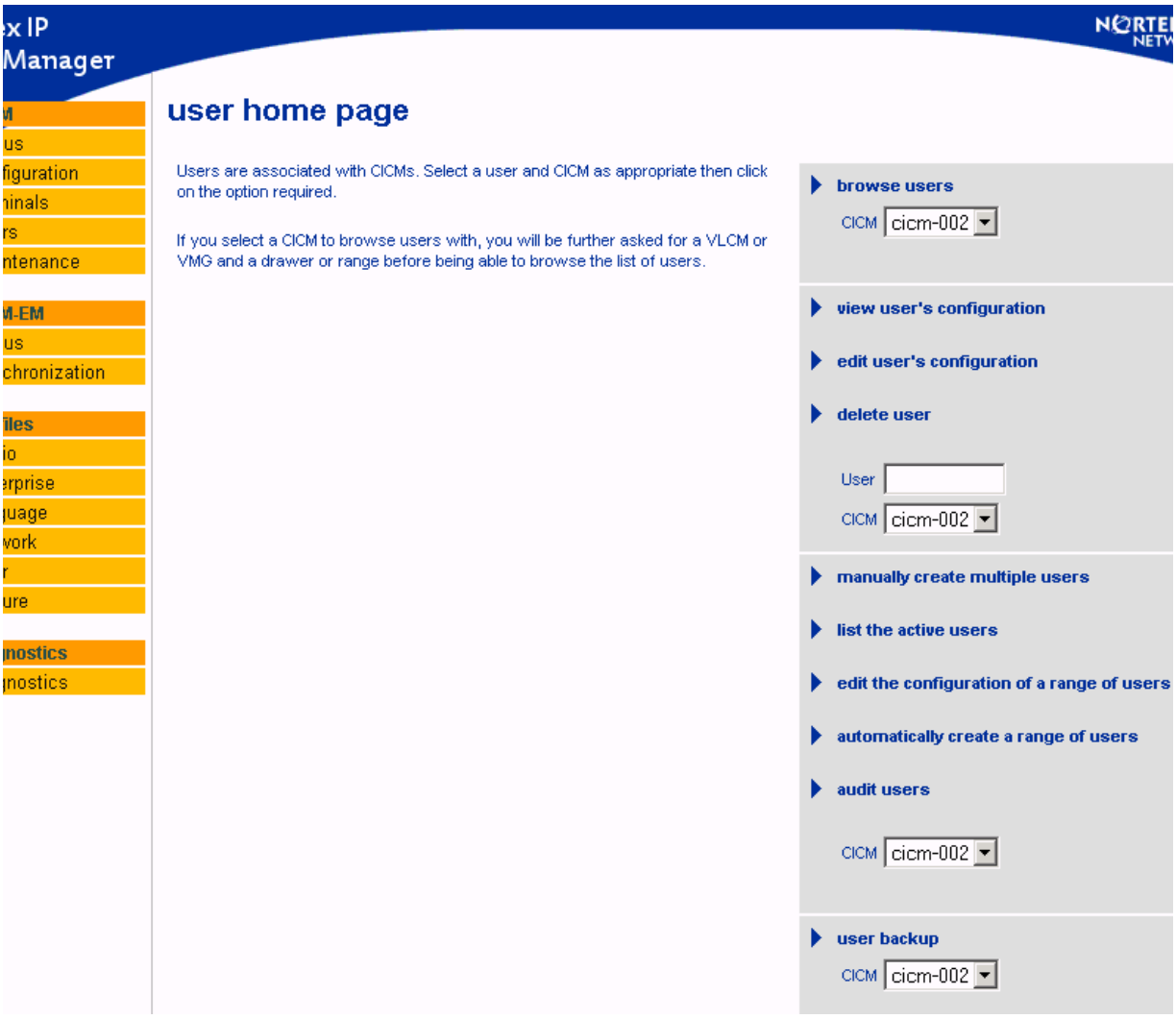
Figure 19 Terminal configuration



User home page

The **User home page** is accessed by selecting the **Users** option of the **CICM** section of the main 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.

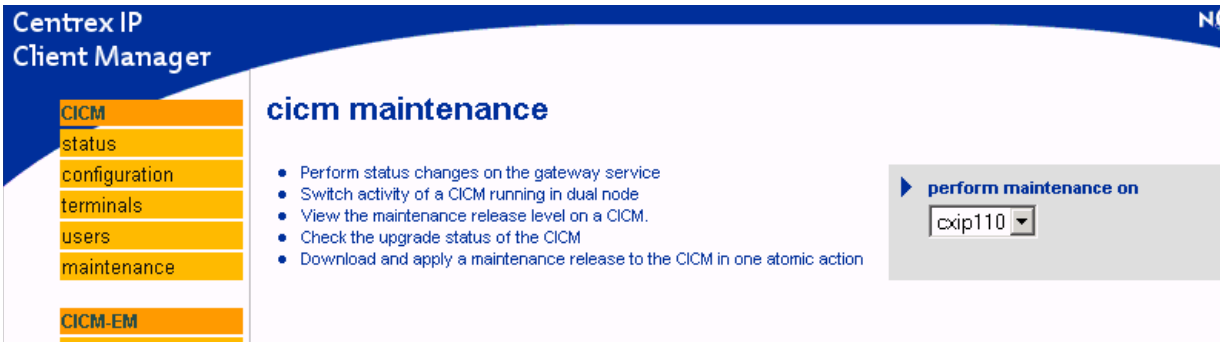
Figure 20 User home page



CICM maintenance

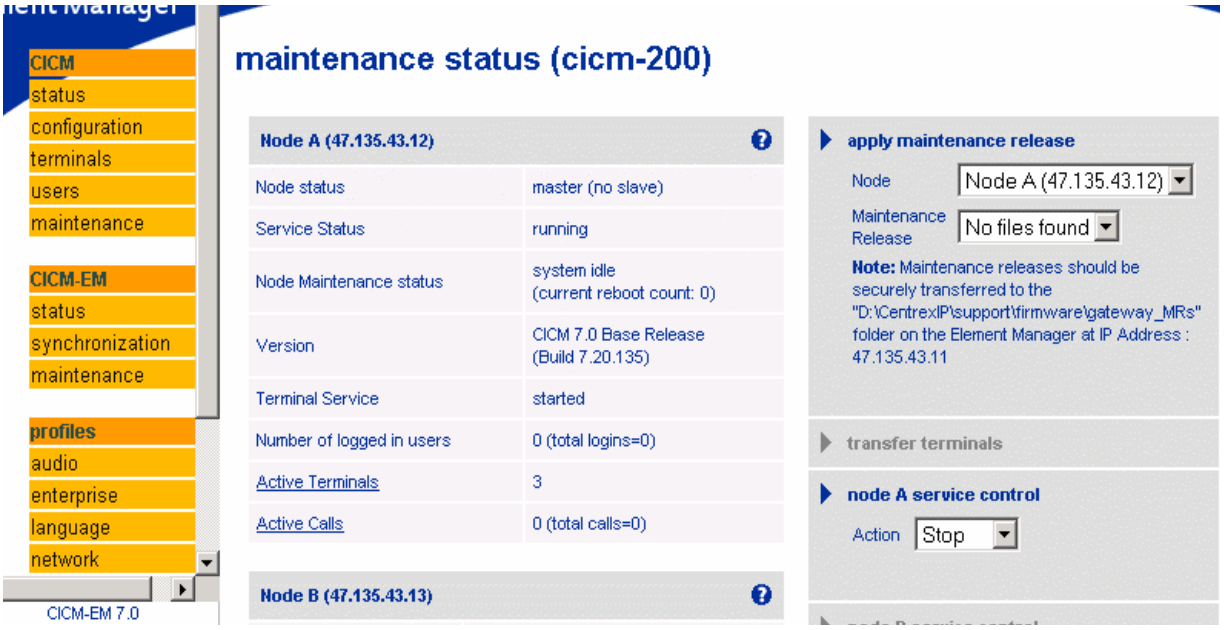
The **CICM maintenance** page is accessed by selecting the **maintenance** option from the **CICM** section of the main menu bar. It is illustrated in the following figure.

Figure 21 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 (transfer terminals), a maintenance release upgrade, and a status change on the gateway. This **maintenance status <cicm_name>** page is illustrated below.

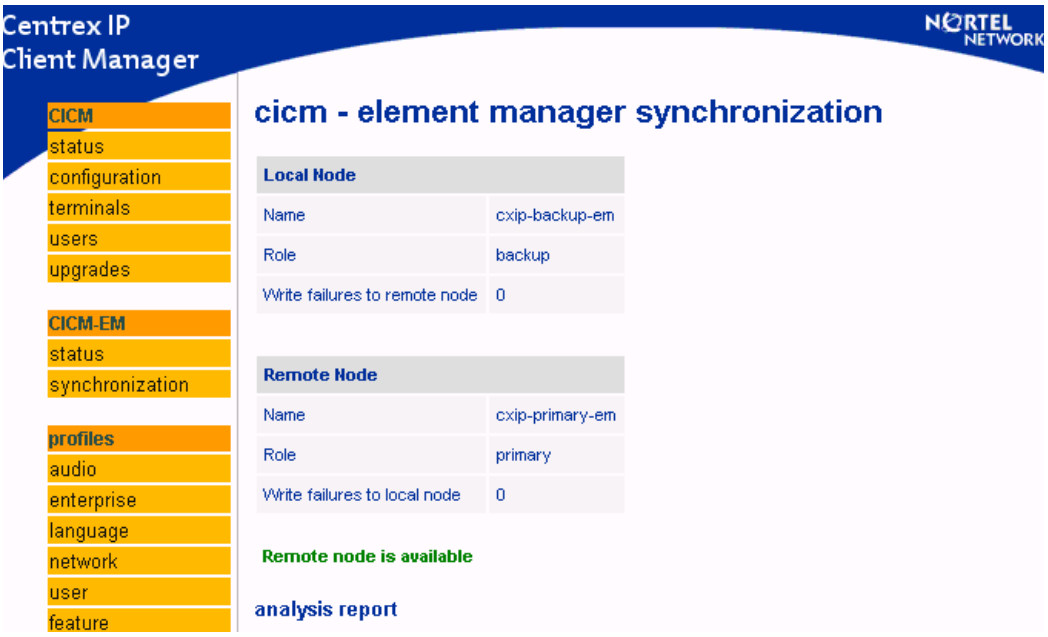
Figure 22 Maintenance status <cicm_name>



CICM – Element Manager synchronization

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

Figure 23 CICM – Element Manager synchronization

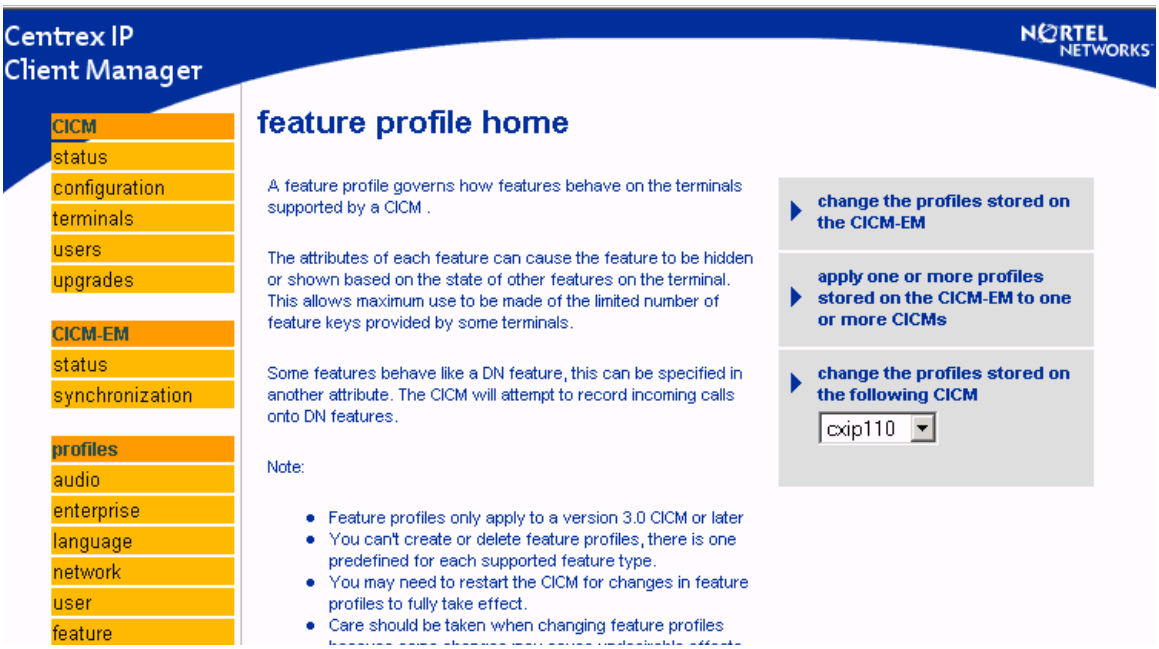


Feature Profile home

The **Feature Profile home** page is accessed by selecting the **feature** option of the **Profiles** section of the main menu. 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 24 Feature Profile home

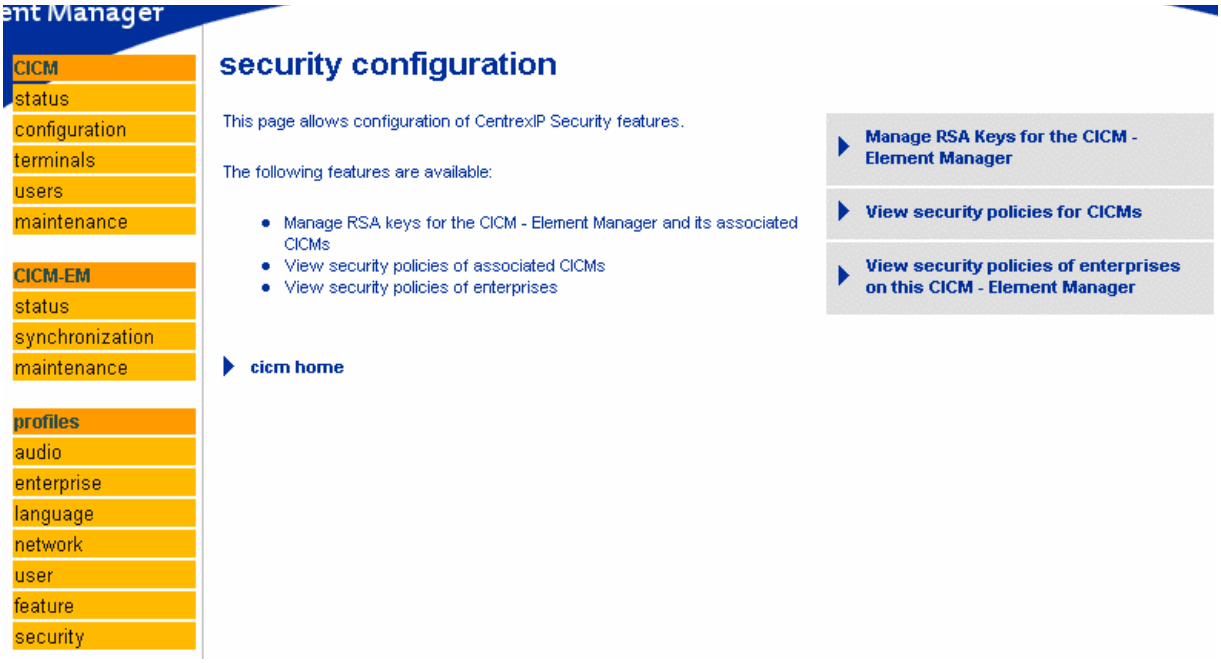


Security configuration

The Security Configuration webpage is new for the CICM 7.0 release. It is illustrated in Figure 25. From this page the administrator can:

- Manage RSA keys for the CICM-EM and its associated CICMs
- View the security policy of the associated CICMs
- View the security policies of enterprises

Figure 25 Security configuration



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 7.0 release of the CICM is a combined hardware and software release based on Succession release (I)SN07. It is applicable to both International and North American customers.

Central Office requirements

CS2000 platform software dependencies

The CICM uses the Microsoft Windows XP Embedded Operating System. The CICM-EM uses Microsoft Windows 2000 Server Operating System.

The software dependencies of CICM 7.0 are listed in the following Table.

Table 4 Software load configuration

System	Minimum Software Load	Comments
CS2000	(I)SN07	
GWC	GC070	New naming convention for this release
CICM	7.0	
CICM-EM	7.0	
IEMS	(I)SN07 IEMS	
CS2M (SDM)	CS2M0070	
IP Phones 2002, 2004	1.57	Older releases are supported (1.38 on) without support for RFC2833. Firmware level version required for DTMF and RFC2833 tone generation in Succession.
IP Phones 2001, 2002, 2004 (Phase II)	1.00	
M6350	7.0	

Administration Data Network Infrastructure (Admin LAN)
The Telco 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. It is also commonly referred to as the Operations, Administration, Maintenance, and Provisioning (OAM&P) Network.

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

The Admin LAN connects directly to the Primary Element Manager (PEM) and the (optional) Backup Element Manager (BEM). It allows the two nodes of the CICM to communicate with each other.

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

Traffic Data Network Infrastructure (Client LAN)
The Traffic Data Network, or Client LAN, is the network that supports communication between Centrex IP clients and the CICM. This network extends from the carrier's Central Office network (CO-LAN) to the enterprise network, through carrier and enterprise data transport networks.

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.

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:

- CICM terminals (IP Phone 200x)
  - — hosted by the same CICM
  - — hosted on another CICM
- TDM trunk gateways (e.g. PVG)
- Analogue line gateways (e.g. MG9000, Mediatrix 1124
- Voice processing servers (e.g. MS 2010)

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 IP Phone 200x 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 enterprise customers, the CICM is located in the Private Signalling Network in the Carrier's managed IP network, as part of the Carrier's IP address space. The 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 firewall 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 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. This will allow a UDP packet (via a 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 the 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.

The table below provide a summary of the RTP portal usage.

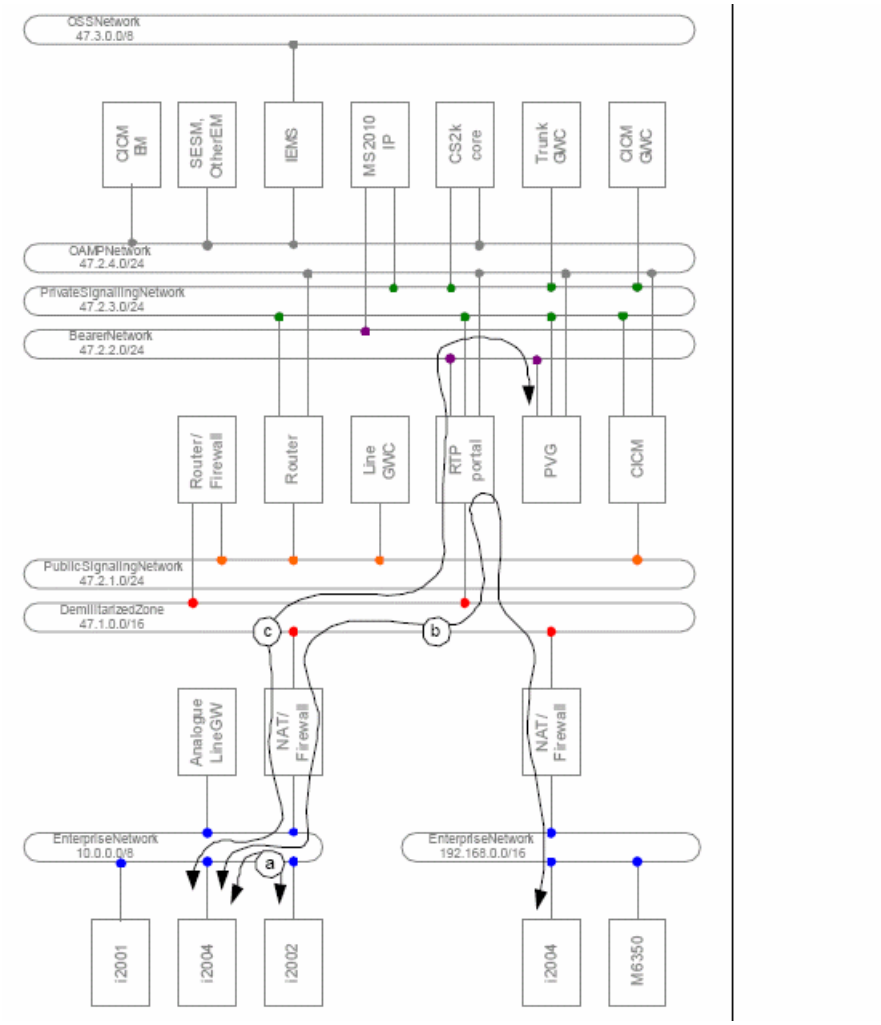
Table 5 RTP portal usage summary

Terminating GW	Originator and Terminator in the same enterprise network?	RTP portal inserted?
Same CICM as originator	Yes	No
	No	Yes
Another media gateway or CICM on the same GWC	Yes	No
	No	Yes
A media gateway or CICM on a different GWC	Yes	No
	No	Yes
A media gateway or CICM on a different CS2K	Does not matter	Yes

The following figure, *RTP portal usage in the CS2000 network*, shows the flow of RTP packets between end-points for the following call scenarios:

- A call between two CICM clients on the same enterprise network
- A call between two CICM clients in different enterprise networks
- A call from a CICM client terminating on a PSTN trunk (hosted from a PVG)

Figure 26 RTP portal usage in the CS2000 network



For the correct operation of the CICM when using the RTP portal, the NAT must be provisioned on both the CS2000 Management Server and the CICM Element Manager. Additionally, if an RTP portal is not available, then all calls made to a user who is not logged in will be routed to treatment.

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

Security of the OAM&P and Public Signalling Subnets

To prevent disruption of the OAM&P subnet by the Public Signaling Subnet, or vice versa, the two subnets are physically isolated from each other. Routing directly between the two subnets is disabled in the CICM. If, for example, an administrator wishes to test whether a client

PC or IP Phone 2004 is visible on the Public Signaling Subnet they would have to:

- Use Telnet to log into the CICM on which the user is registered, or
- Use **Ping** or **Tracert** from the Telnet command line to try to reach the IP address of the client

Note: **Ping** and **Tracert** commands may not be used for deployment 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.

Ping and **Tracert** are the only commands that have any effect on the Public Signaling Subnet. 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 Public Signaling Subnet interface. Only a strictly limited set of UDP ports are allowed on the Public Signaling Subnet. Other ports are blocked by the CICM CPU card.

Access to the CICM and Element Manager via the OAM&P network is password protected. Access to the administration web pages on the Element Manager is also password protected. Login to terminals on the Public Signaling Subnet is protected by user names and passwords.

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 to the *CICM Fault Management* document. For additional details, refer to the *CICM Engineering Guide*.

Situating the CICM

The CICM should be collocated with the CS2000. When collocated, the CICM 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 collocated with or sited remotely from the CS2K GWC. Nortel recommends collocating the CICM with the CS2K.

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

NEBS compliance, 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).

For additional information on engineering standards, compliances and non-compliances, and compliance testing, refer to the *CICM Engineering Guide*.

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

Succession and Carrier grade CICM

The (I)SN07 release is the first release that supports both TDM and Succession versions of the CICM product.

Dual Node Redundancy

Dual Node Redundancy (DNR) is a key feature of the CICM 7.0 architecture, designed to provide fault tolerance for both the Succession and the TDM versions of the CICM product.

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.

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 was made for (I)SN07 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 for Succession. 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 7.0

The key aspects of the DNR feature are:

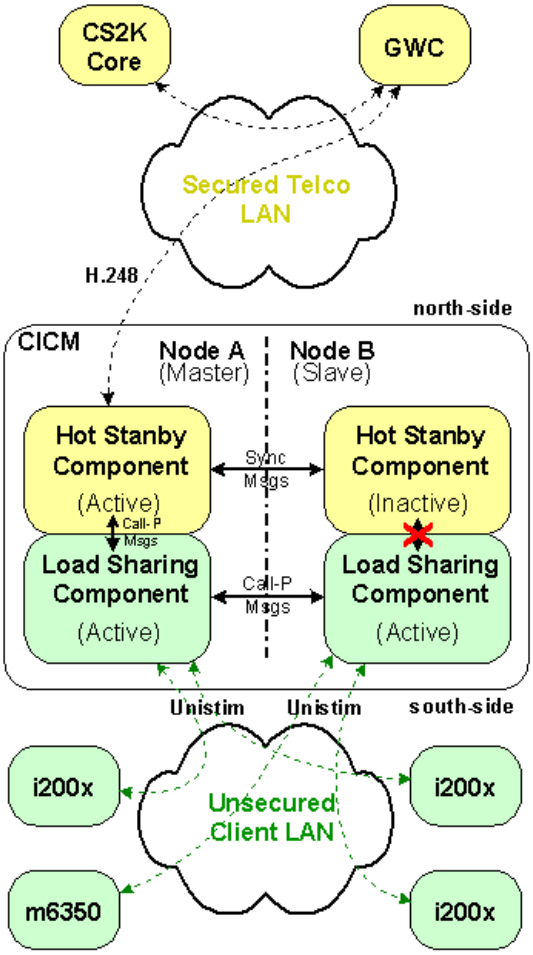
- Only a single node, the master, can communicate with the CICM gateway controller (GWC) at any time. The CICM will ensure the IP and port are moved to the appropriate interface as needed.
- In a failure scenario on the active node, the CICM will automatically initiate a switch of activity in order to 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 in the 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 includes the capability for an administrator to monitor and control SWACT activity.

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 *CICM redundancy model in Succession*.

Figure 27 CICM redundancy model in Succession



This figure 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.

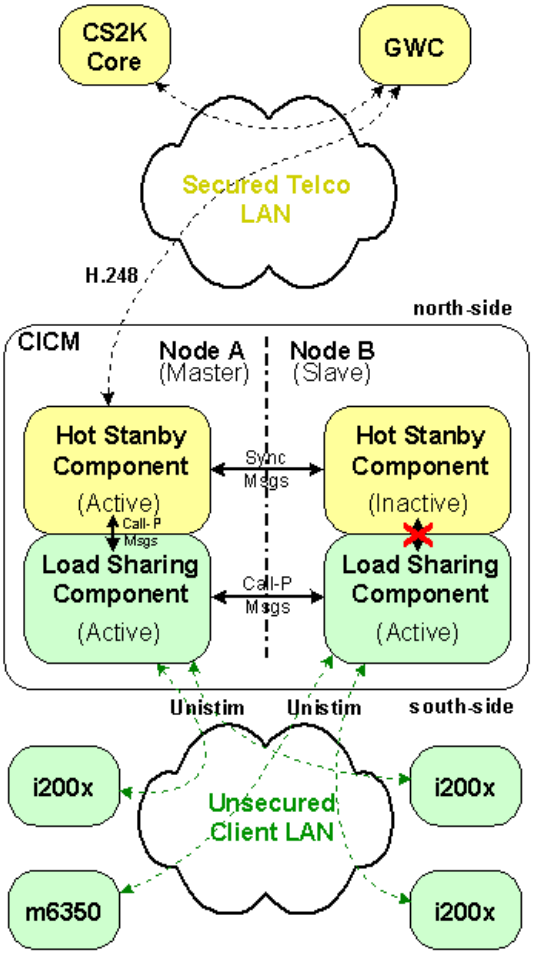
The illustration also shows that although both load sharing components host terminals, the message path ensures that all terminal events from either side are routed to the master hot standby component as only it may communicate with the GWC.

Note that the south side's role and functionality remain effectively the same as in the TDM variant of the CICM. 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 the figure below, *CICM following a SWACT*.

Figure 28 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 the figure *CICM following a SWACT* 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.

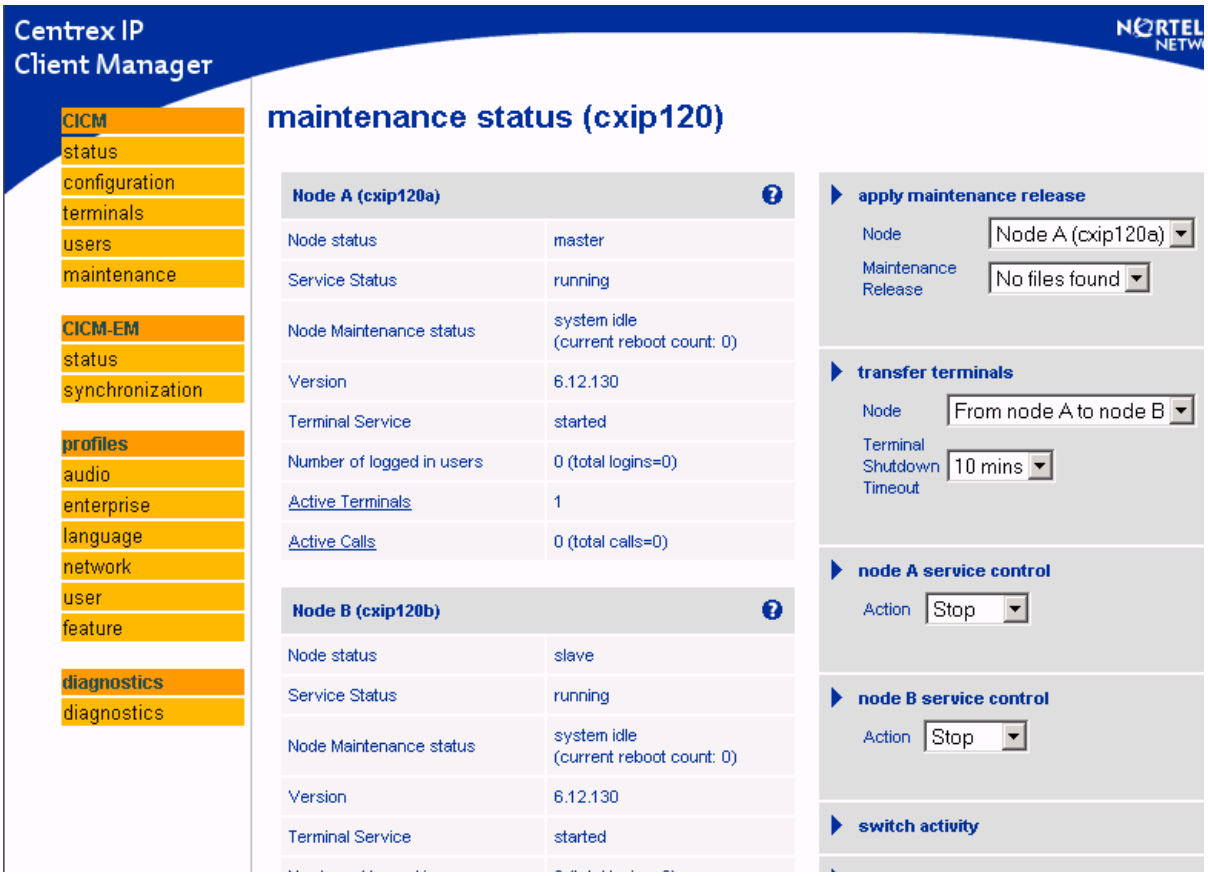
The following list provides a few examples of possible effects that could occur during a SWACT:

- 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.

DNR user interface

All controllable aspects of the DNR functionality can be accessed from the **Maintenance Status** Web page of the EM, illustrated in the following figure, *Maintenance Status Web page*.

Figure 29 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 26, *CICM following a SWACT*) 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 26) 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 alarms

The following alarms are most significant and specific to the dual node functionality of CICM 7.0:

- The CICM alarm behavior of the VLCM also applies to the CICM 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.

DNR systems engineering

The table below, *Timing of DNR related maintenance activities*, summarizes the lengths of times various maintenance activities related to DNR may require to complete.

Table 6 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
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 (I)SN07 Succession CICM load. In order to make such a conversion, it is necessary to re-install and datafill both nodes.

Hardware

This section describes the hardware components of the Series 7.0 CICM.

Hardware overview

The Series 7.0 CICM hardware platform provides the functionality that allows CICM clients to access the full range of 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.

The CS2K deployment can use dual Passport 8600 Ethernet switches. It is recommended that the CICM also utilizes these switches to provide network connectivity.

Hardware frame

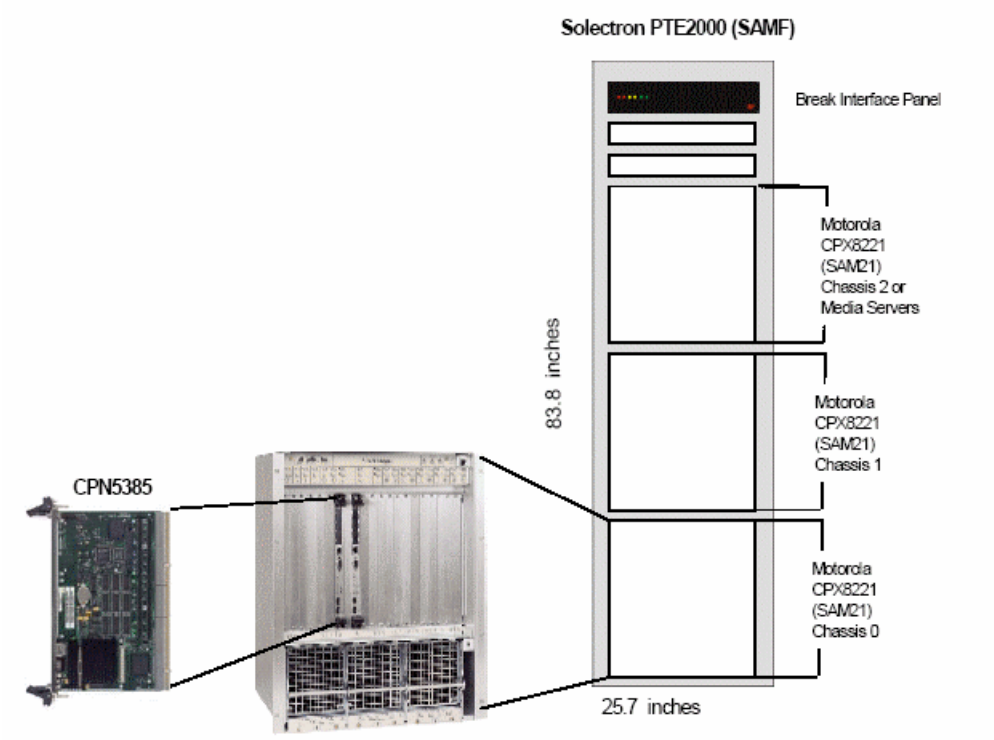
The CICM is shipped as a series of components fitted into a standard NEBS3 compliant frame (also called a cabinet). CICM 7.0 uses the SAMF and CCS frames.

SAMF Frame

The SAMF frame is illustrated in the figure below, *SAMF frame*. The characteristics of the SAMF frame are:

- NEBS3 compliant
- Configurations supported:
  - — Up to 3 SAM21 Chassis, or
  - — Up to 2 SAM21 Chassis + Media Server Applications (up to 6 MS2010 IP Chassis if Media Servers are included in the Solution)
- 4 System slots already occupied (2 HSC and 2 shelf controllers)
- 17 application slots:
  - — 1 CICM-EM card (Motorola CPN 5385 processor board, NTRX51HJ, along with its transition module on the rear shelf, NTRX51HK). Its mate will be on another chassis for redundancy.
  - — Up to 10 CICM cards (Motorola CPN5385 processor board, NTRX51HJ, along with its transition module on the rear shelf, NTRX51HK). Their mates are on another chassis.
  - — Up to 6 GWC cards (Motorola N750, no rear transition module needed): 5 for CICM control and 1 for RTP Media Portal control (if Portals are used). Their mates are on another chassis. ONe GWC pair supports 6400 CICM lines, or roughly 2 CICM card pairs.
  - — Application slots 15 and 16 do not support rear I/O because their rear slots are already occupied by the Extension Bridge circuit packs. These cards are required in the chassis and can not be removed.

Figure 30 SAMF Frame



CCF Frame

The CCF frame is illustrated in the figure below, *CCF Frame*. The characteristics of the CCF frame are:

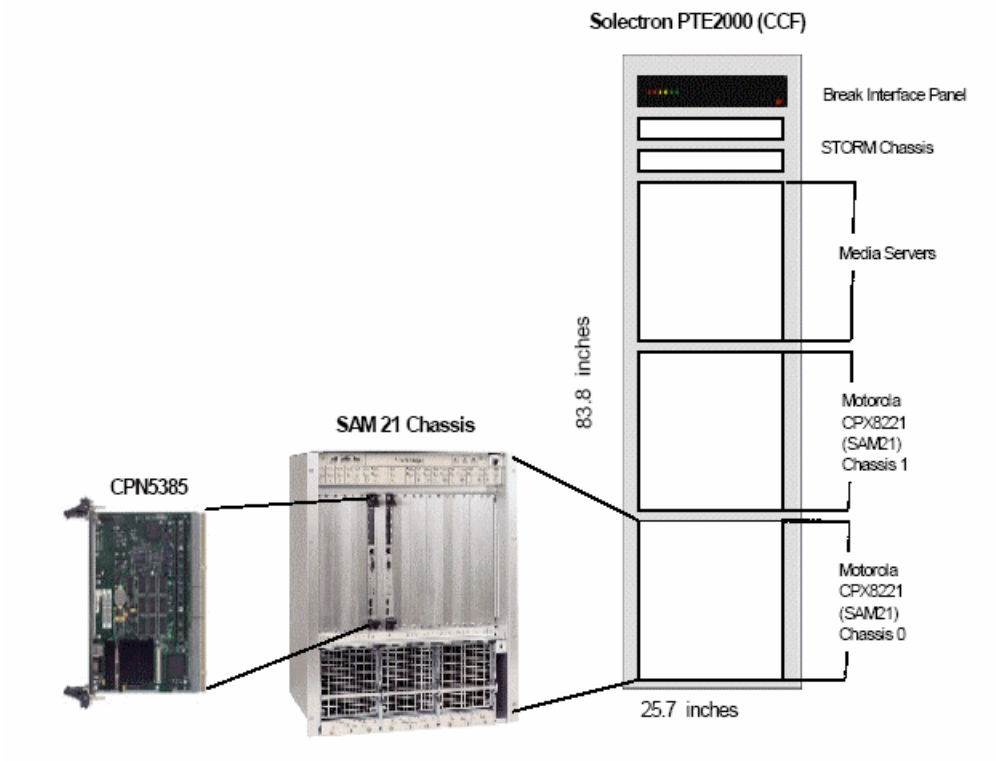
- NEBS3 compliant
- Configurations supported:
  - — Up to 2 SAM21 Chassis, or
  - — Up to 2 SAM21 Chassis + Media Server Applications (up to 6 MS2010 IP Chassis)
  - — STORM storage systems
- 4 System slots already occupied (2 HSC and 2 shelf controllers)
- 2 Slots are reserved, leaving a maximum of 13 slots available. The two reserved slots are:
  - — One slot for the Call Agent Card
  - — One slot for the USPc card
- There are 15 usable application slots: up to 13 of these slots are usable for CICM and the rest usable for GWC cards.
  - — 1 CICM-EM card (Motorola CPN 5385 processor board, NTRX51HJ, along with its transition module on the rear shelf,

NTRX51HK). It is an active card, and its mate will be on another chassis for redundancy.

— Up to 8 CICM cards (Motorola CPN5385 processor board, NTRX51HJ, along with its transition module on the rear shelf, NTRX51HK). These are active GWC cards and their hot stand-by mates are on another chassis.

— Up to 6 GWC cards (Motorola N750): 4 for CICM control, and 2 for RTP Media Portal control (if portals are used). These GWC cards are active cards. Their hot standby mates are on another chassis.

Figure 31 CFF Frame



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 IP Phone 2004/2002 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.

In the SAM21-based CICM 7.0, the CICM-EM is a pair of Motorola CPN5385 resource cards; one active and the other hot standby for redundancy. 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.

Only one pair of the CICM-EM resource cards is required per CS2K, which is capable of supporting up to 100 pairs of CICM resource cards. The hot standby CICM-EM resource card is equivalent to the Secondary Element Manager (SEM) chassis in the SAM16-based CICM releases.

Element Manager Backup and Restore Tool

The Element Manager is supplied with a Backup and Restore Tool (BRT) 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.

The EM is also provided with the ability to perform automatic in-service backups of CICM configuration data. CICM has its own synchronization tool, which allows the nodes to synchronize themselves.

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

Processors

The single backplane chassis contains two separate cPCI bus domains (A and B), each with its own CPN5385 processor card running the Windows XPe operating system. Each CPN5385 card has a Pentium Mobile III processor at 1.2 GHz with 512 Mb of RAM. The CPN5385 also has a PMC daughterboard attached to it, containing a 40 GB PMC243 Ramix hard drive.

The processor handles the following tasks:

- UNIStim session management
- Client interfacing
- Media stream control
- Remote configuration of the CICM
- H.248 Signalling

Administration 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 from:

- Any platform running Microsoft Internet Explorer (IE), version 6.0 or later. Note that other Web browsers may use the Web-based management interface, but only Internet Explorer is supported.
- Any Microsoft Windows Embedded OS machine with the appropriate access rights on the service provider's Admin LAN,

using a combination of Windows Embedded OS remote management functions, and the Nortel CICM management tools accessed via the Element Manager Web pages. Refer to the *CICM Configuration* and *CICM Administration and Security* documents for additional details.

The Administration interface can also be used to gain access using SSH (Secure Telnet) to the base operating system from which tools can be run and various logs can be viewed. The CICM must be collocated with the CS2K.

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:

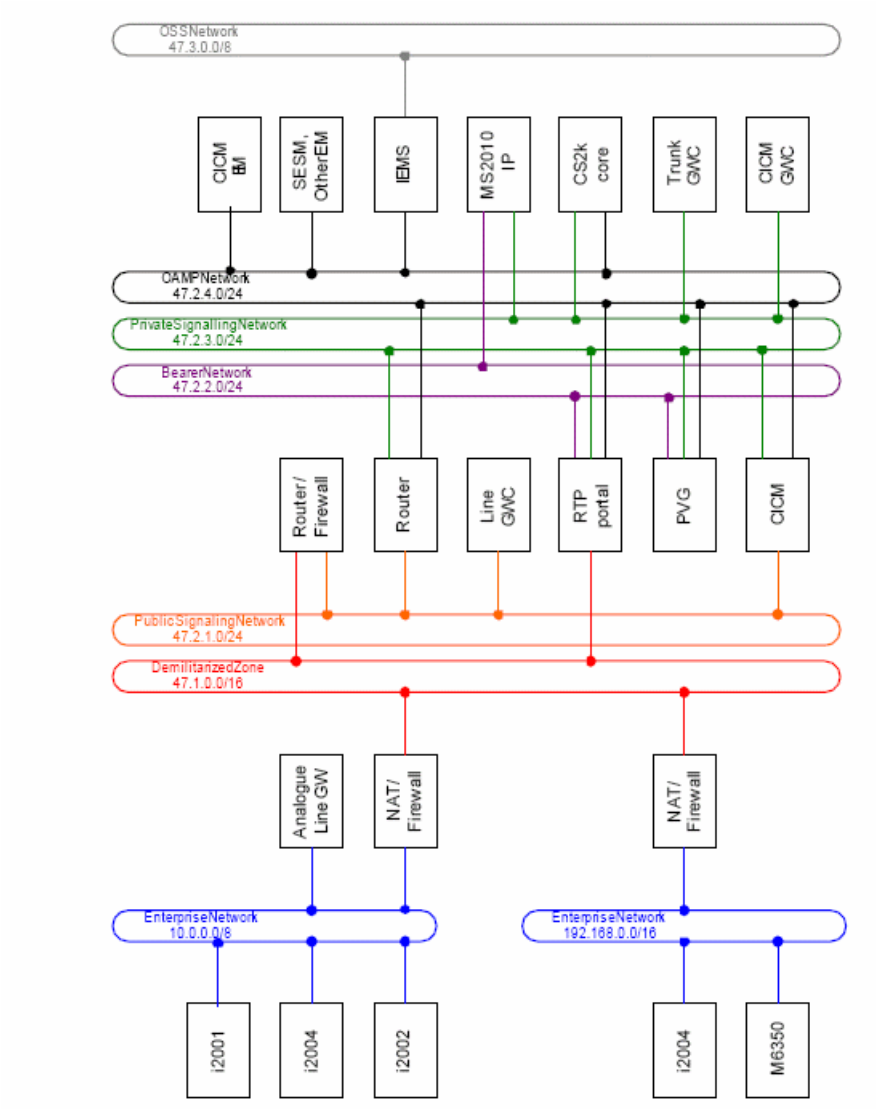
- The **CICM Admin LAN** is a private network for inter-node and Element Manager communications. The traffic on this LAN is not secured, so the Admin LAN is isolated to provide security.
- The **CICM Client LAN** is the network on which all media and call signalling is carried. This network extends to 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.

Network engineering

Protection against a single point of failure in the Ethernet network is achieved by connecting the CICM to two PP8600 routing switches rather than one. These switches can then be connected to the rest of the Telco network. The figure below, *CICM in the CS2000 Network*, provides a reference network for CICM in the CS2000 environment.

Figure 32 CICM in the CS2000 network



The sub-networks shown in Figure 30 above 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 and other interconnected service providers networks to the Succession Core Network.
- Two enterprise networks are shown in the Figure 30 above. Each network uses a private addressing scheme, and is isolated from the DMZ by a NAT device and firewall.

Figure 30 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).

Note: 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. 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 stateful 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.

The CICM EM is not directly accessed via the OSS Network. The Northbound CICM EM interface is accessed via Secure Proxy through the IEMS.

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

Network interfaces

CICM interfaces

Each CICM node uses a CPN5385 processor card with three physical network interfaces. The table below, *CICM Interface Summary*, provides a mapping of the physical characteristics of the CPN5385 to a set of logical interfaces used by the CICM.

Table 7 CICM Interface Summary

Node	Logical Interfaces	Physical Interface Assignment
A	A1	Adapter 1
	A2	Adapter 2
	A3	Adapter 2 (VLAN3)
	A4	Adapter 2 (VLAN4)
B	B1	Adapter 1
	B2	Adapter 2
	B3	Adapter 2 (VLAN3)
	B4	Adapter 2 (VLAN4)

Because the CICM connects to more logical networks than it has physical network adapters, the CICM multiplexes some functions onto one of the adapters using VLAN tagging. Table 8 provides details of the

VLAN assignments. Alternative VLAN identifiers can be specified when the CICM is provisioned.

Using these logical interfaces, the Succession CICM exposes four IP addresses to the rest of the Succession network. One address on each node s used for inter-node signaling and OAMP access from the CICM-EM (PA and PB). The other two addresses are used for each of the call signaling interfaces (R and Q for UNIStim and H.248 respectively). All four addresses are dynamically bound to one of two adapters based on the current state of the CICM network connectivity. The table below, *CICM IP Addresses*, provides additional details.

Table 8 CICM IP Addresses

Network	IP Addresses	Logical Interface	Purpose
P (CICM Administration)	PA	A1 or A2	Node A OAMP and inter-node signalling
	PB	B1 or B2	Node B OAMP and inter-node signalling
Q (Public call signalling)	Q	A3 or B3	UNIStim signalling
R (Private call signalling)	R	A4 or B4	H.248 signalling
S (System)	SA1	A1	Inter-node keep-alive
	SA2	A2	
	SA3	A3	Reserved
	SA4	A4	Reserved
	SB1	B1	Inter-node keep-alive
	SB2	B2	
	SB3	B3	Reserved
	SB4	B4	Reserved

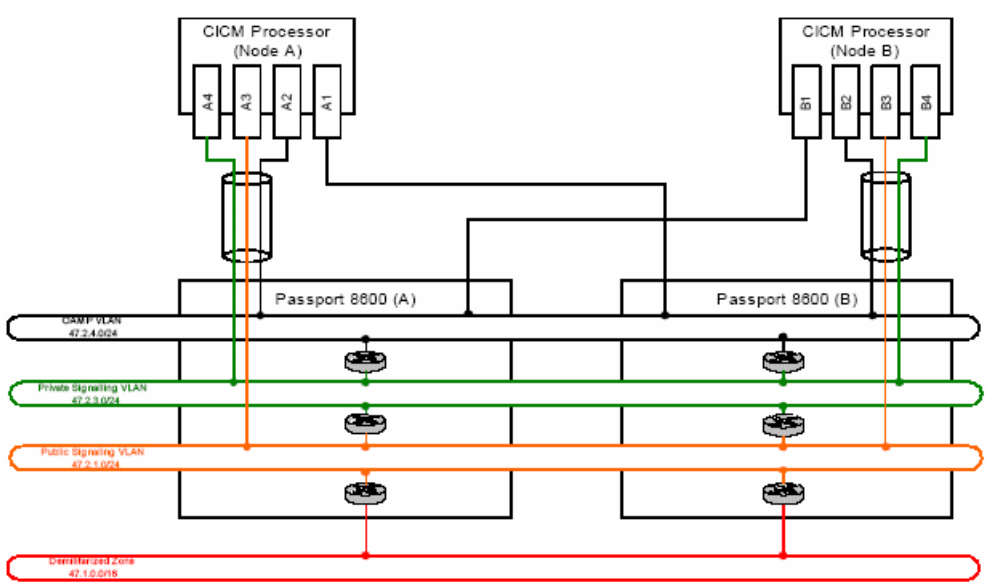
The CICM requires eight system IP addresses: one for each of the logical adapters on each of the CICM nodes (SA1-SA4 and SB1-SB4 on nodes A and B, respectively). The TDM CICM requires six system IP addresses (SA1-SA3and SB1-SB3), one for each of its interfaces.

The system IP network runs directly on top of the VLAN provided for IP network P. Two of these on each node (SA1, SA2, SB1, and SB2) are used for sending heartbeat messages to the mate CICM. The master CICM node interprets these messages and it controls the binding of the PA, PB, R, and S addresses to ensure that they are always available to other Succession network elements. The other two or four addresses (SA3, SA4, SB3, and SB4) are required for OS initialization and are not used by the CICM. These address bindings use a restricted subnet mask to ensure they cannot be misused.

The system IP addresses can be allocated from any range that does not overlap with addresses used in IP networks P, Q, and R. It is recommended that a sub-network in one of the private address ranges 10/8, 17.16/12,192.168/16 or 169.254/16 should be used. Other public IP address ranges (e.g. 20/8) can also be used if they do not overlap with addresses used in IP networks P, Q, and R and if the CICM does not need to route to devices in the chosen range through IP networks P, Q, and R. Each CICM connected to a single Ethernet network should have a unique IP address range reserved for its system addresses.

The two CICM nodes must be cross-connected to a pair of redundant Ethernet switches (by default this will be Passport 8600, as shown in the figure below, *CICM Network connectivity*. By forming these cross-connections, the two CICM nodes can transparently survive a failure of any single device connecting the two nodes. The CICM will loose sanity if the two nodes loose connectivity at any point. Both nodes will attempt to become the master node. When connectivity is restored, the CICM will resolve the problem by demoting Node B to be a slave.

Figure 33 CICM Network connectivity



Address redundancy is implemented by moving the IP address from one Ethernet adapter to another. The CICM broadcasts a gratuitous ARP message to inform other devices of the change in address binding.

CICM-EM Interfaces

Although the CICM-EM interfaces connect to different network segments, they behave in a similar manner to those on the CICM. The CPN5385 processor card has three physical network interfaces. Two of these interfaces connected to the CICM administration network (P), the other is connected to the OSS network (O) via a secure proxy through the IEMS. Like the CICM, the CICM-EM also uses a private system IP network for inter-node heartbeat messaging (S). This IP network is multiplexed onto the Ethernet fabric provided for the CICM administration IP network (P).

The CICM-EM exposes three IP addresses to the other Succession network elements. One address on each node (PA and PB) is used for inter-node ICM-EM signaling and communications between the CICM-EM and the CICM (note that it is always the CICM-EM that initiates communications with the CICM). The other address (O) is shared between the two nodes in a redundant configuration and is

connected to the IEMS. The addresses and interfaces are summarized in the table below, *CICM-EM Interfaces*.

Table 9 CICM-EM Interfaces

Network	IP Addresses	Logical Interface	Purpose
O (OSS)	O	Adapter 3 on Node A or Node B	OSS machine and GUI interfaces ***Note:*** This access is via secure proxy through the IEMS.
P (CICM Administration)	PA	Adapter 1 or Adapter 2 on Node A	Node A OAMP and inter-node signalling
	PB	Adapter 1 or Adapter 2 on Node B	Node B OAMP and inter-node signalling
S (System)	SA1	Adapter 1, Node A	Inter-node keep-alive
	SA2	Adapter 2, Node A	
	SA3	Adapter 3, Node A	Reserved
	SB1	Adapter 1, Node B	Inter-node keep-alive
	SB2	Adapter 2, Node B	
	SB3	Adapter 3, Node B	Reserved

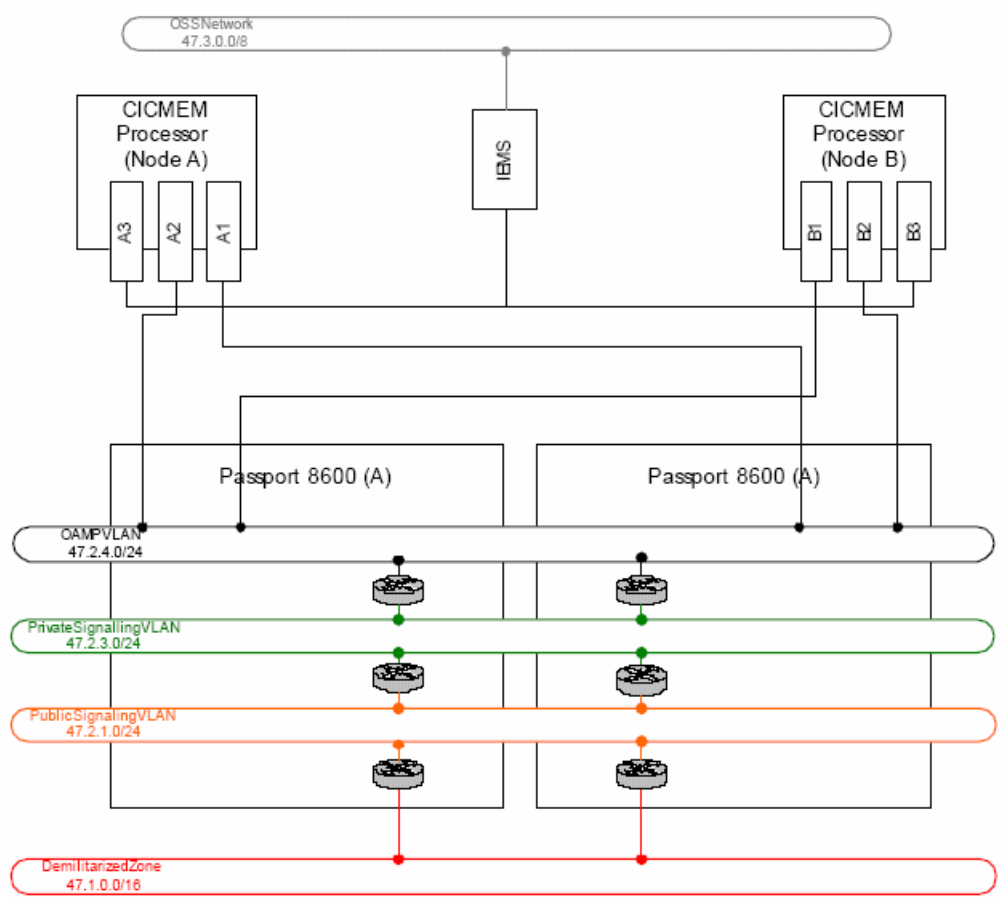
Address O is intended for use by end-users in the OSS (proxied through the IEMS). Browsers can be pointed to this address to receive the CICM-EM GUI. If a node or network link on the CICM-EM fails, the browser will automatically be redirected to the mate node. The CICM-EM GUI is generally stateless, but when the browser fails over to the mate node, some context of the operations being performed by the end-user may be lost. The end-user will generally be required to re-authenticate themselves when activity fails over from one node to the other. If a third-path provisioning application is being used, it may also use the CICM-EM automated provisioning interface, using address O.

Addresses PA and PB are used by the CICM-EM to communicate with the CICM, and for the CICM-EM nodes to communicate with each other. These addresses can also be used to access the CICM-EM GUI and automated provisioning interface. If the PA or PB addresses are

used for provisioning tasks, it should be noted that they are redundant against a single point of failure in the network but do not provide redundancy across the two CICM-EM nodes. The other significant difference with addresses O and PA or PB is that the PA and PB addresses have DCOM enabled for communications to the CICM. Powerful functionality is available through the DCOM interface and access to this protocol should be restricted (by securing network P).

The CICM-EM network connectivity to the central office LAN is provided in the figure below, CICM-EM Network Connectivity.

Figure 34 CICM-EM Network Connectivity



Each adapter on the CICM-EM sends, by default, two heartbeat messages every few hundred seconds. The CICM-EM interprets the heartbeat messages received from the mate node and ensures that network redundancy converges within two seconds of any network failure.

A CICM-EM has affinity with a single CS2K management platform; therefore with a single SC2K node. Even if the CS2K is split across different geographic locations, the two CICM-EM nodes are likely to be connected by a dedicated high speed Ethernet network.

H.248 Interface

The Succession variant of the CICM requires an H.248 IP address to enable communication between it and the GWC. This floating address is dynamically managed by the CICM, and is always bound to the master node's H.248 interface.

That is, the CICM supports an independent VLAN specifically intended for H.248 traffic. In order to make use of this VLAN, each CICM node implements an additional virtual network interface.

The CICM also supports making use of the Client VLAN for H.248 communication with the GWC. However, in the interest of improved security, the default and strongly recommended option is to use the separate H.248 VLAN option.

CS-LAN Routing Switches

The SAM21-based CICM 7.0 must be collocated with the CS2K. As such, the CICM can leverage on the CS2K CS-LAN infrastructure, which consists of two Passport 8600 routing switches. In addition to supporting the CS2K Core and other CS2K components, the dual PP8600s provide the Ethernet connectivity to the CICM and the CICM-EM resource cards, support various CICM and CICM-EM VLANs, and also function as the default gateway routers for WAN communications.

The base configuration of the PP8600 being used in Succession CS2K CS-LAN deployment is:

- 10-slot Passport 8010CO chassis on Passport 7480 Universal Frame
- One Passport 8691SF CPU Module
- Two 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 8608GBIC Routing Switch Module supporting 8 Gigabit Ethernet ports (mostly for WAN interface)
- Passport 8672 ATME 2-slot MDA Baseboard, supporting up to 8 OC-3 or two OC-12 ports for ATM WAN interface

The key features of the dual-PP8600-based CS2K CS-LAN are:

- NEBs-3 compliance
- Superior reliability with 99% 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)

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.

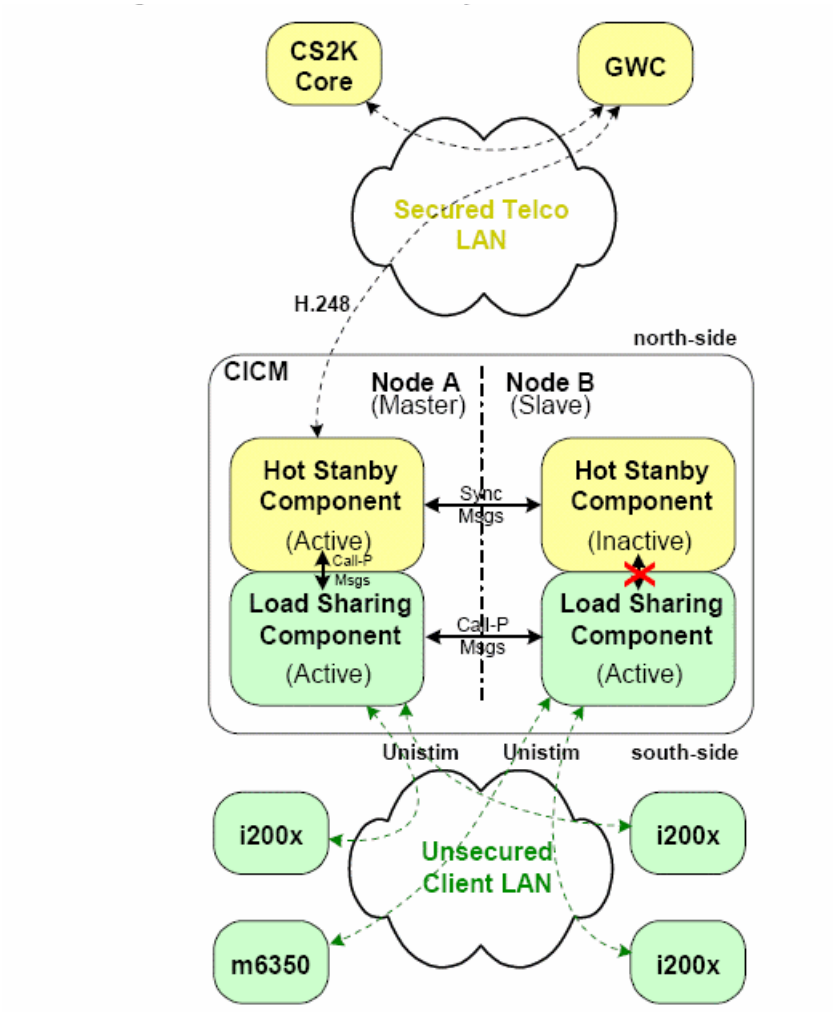
Pairs of CPU cards provide hardware redundancy for the CICM applications. The two CPU cards present themselves to the GWC as a

single network entity (one CPU is the master, the other is a warm-standby slave).

If one of the CICM nodes becomes unusable (e.g. due to a hardware failure or during an upgrade), the hot-standby node can still be used to provide service. With the new Active Call Failover feature in (I)SN07, when one node becomes unusable, all current calls on the failed node will be transferred over to the hot-standby mate node.

The following figure, *Dual Node Redundancy Model*, shows the model used for Dual Node Redundancy.

Figure 35 Dual Node Redundancy model

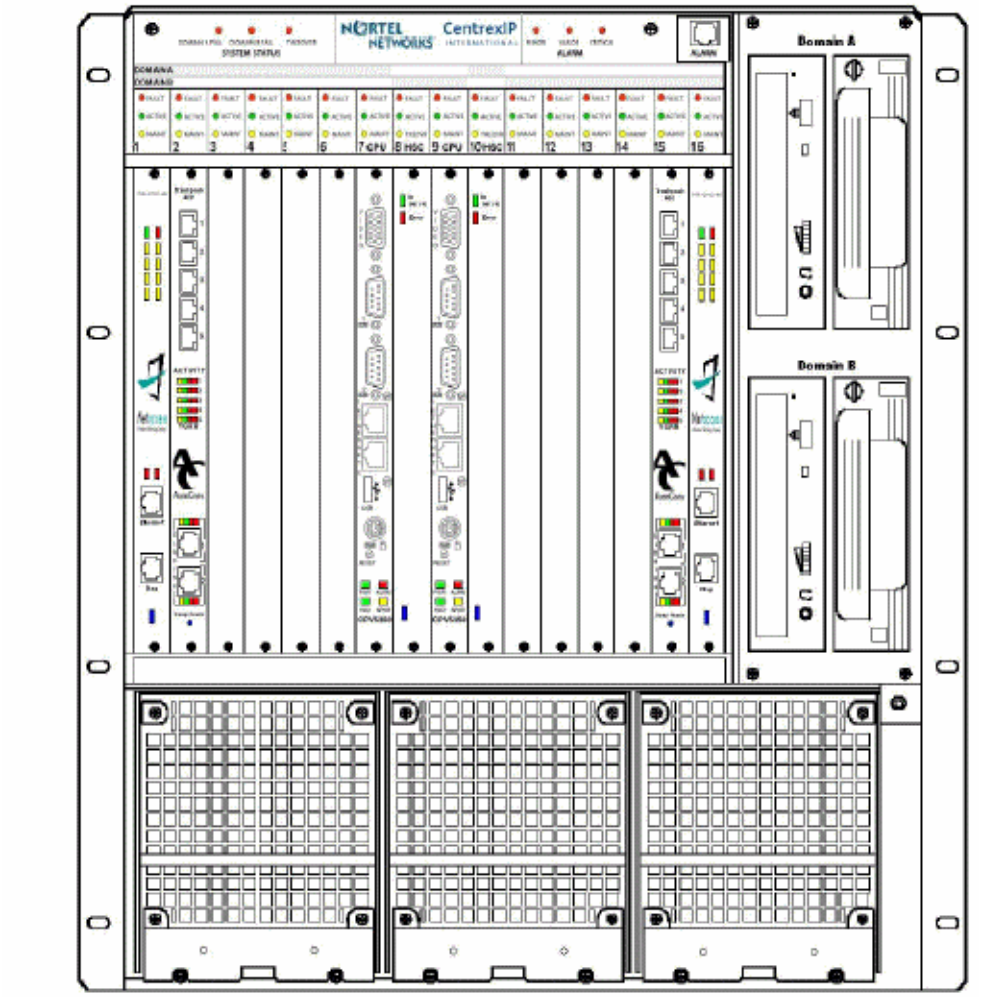


CICM chassis

The CICM is housed in a Motorola CPX8216T chassis. An example of the chassis is shown in the following figure, *CICM chassis*.

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 36 CICM chassis



The 7.0 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.

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

CPU cards
For Series 7.0, 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

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 7.0 should be collocated with the CS2000. As such, the CICM 7.0 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 7.0 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.

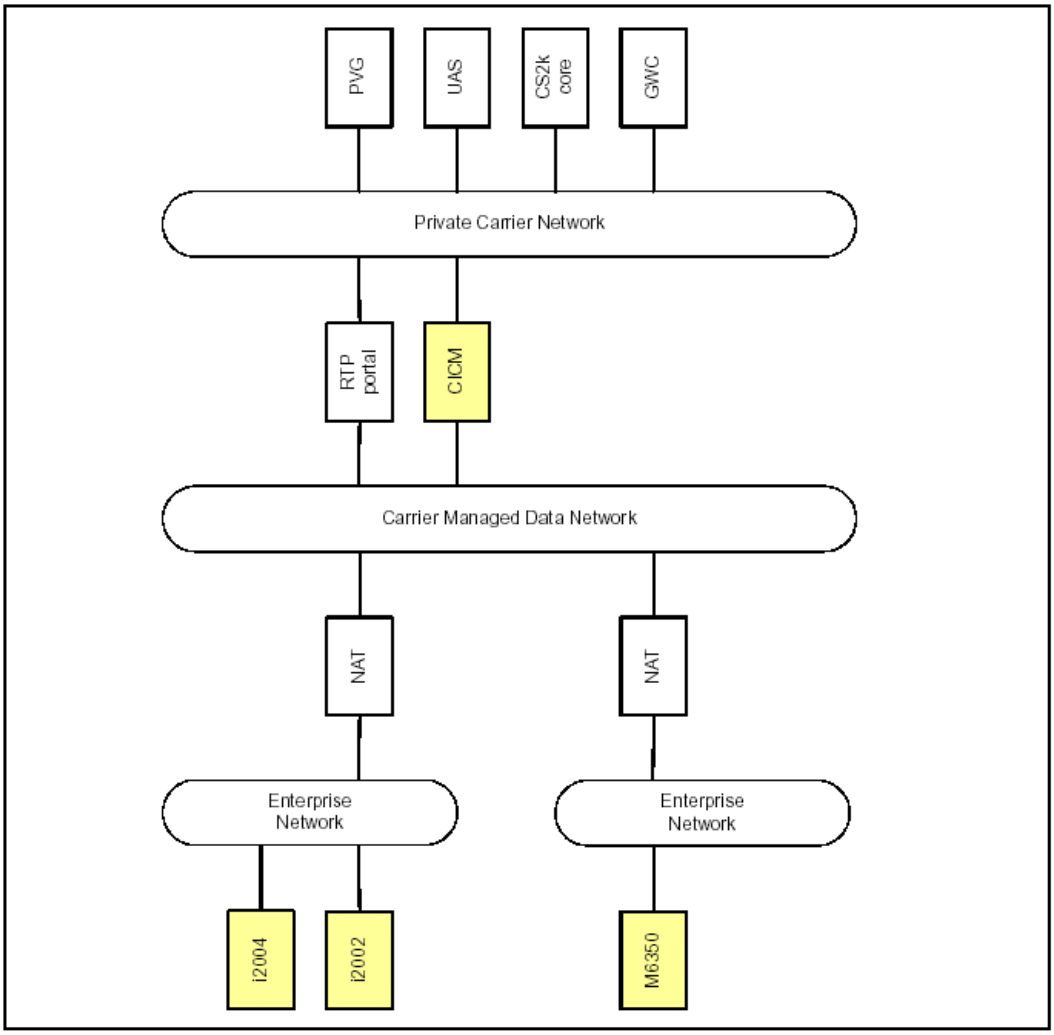
H.248 is a joint ITU-T / IETF protocol defined in ITU-T Recommendation H.248 and IETF RFC3015. It fully supports the same basic device/media control capabilities as protocols such as ASPEN. More importantly, it is based on a more flexible functional mode that provides better support for multimedia and 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. IP Phone 2004) 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 figure below, *CICM and clients in the Succession network*, 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 37 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 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 7.0 should be collocated with the CS2000. When it is collocated, the CICM 7.0 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:

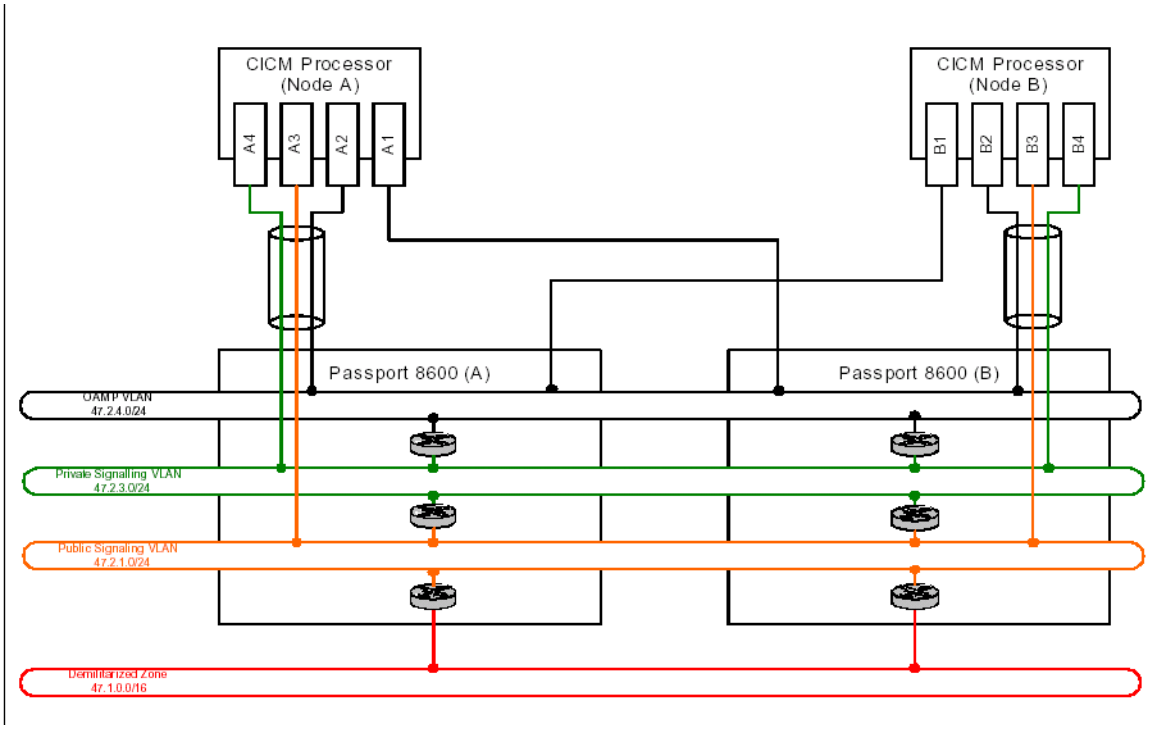
- The Telco's administrative LAN, which includes the Primary and Backup Element Managers.
- The client LAN.

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.

The figure below, *Network Connectivity for LAN redundancy*, shows a typical deployment scenario for the Succession CICM in a central office. Figure 37 should be considered in conjunction with the figure *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 38 Network connectivity for LAN redundancy



IP Addressing

Assuming the network configuration provided in Figure 38, Table 10 provides an example of the IP addresses required by a pair of CICM processing nodes.

Table 10 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 10 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 11 summarizes the redundancy model used for each network interface on the CICM.

Table 11 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

Hardware configurations

The series 7.0 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 7.0 CICM.

Software loads

The base load for Series 7.0 CICM is (I)SN07.0.

A Series 7.0 CICM EM can manage Succession Series 6.1 and 7.0 CICMs.

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.

Upgrades

There are two types of software upgrades: product upgrades and Maintenance Release (MR) upgrades. Product upgrades involve upgrading the release number. Maintenance Release upgrades involve build number upgrades, within the same release. Refer to the *CICM Upgrade* document for additional information and upgrade procedures.

Supported upgrades

CICM 7.0 supports the following software upgrades:

- Succession upgrade from release 6.0 to 7.0 on SAM21 Platform
- Conversion from TDM release 2.4 or 2.5 on SAM 21 Platform

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.

The following 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 attached to a LAN. It works with a headset and adapter which plugs into a USB port on the PC. The Windows XP and 2000 operating systems are supported for the m6350.
- The Nortel Networks IP Phone 200x, which connect directly to a client LAN or to a telephony switch module. The IP Phone 2001, 2002, and 2004 models are supported.

CICM lines are datafilled on the CS2K as standard MBS lines, using the M5216 or M5316 template. There is no distinction between a normal MBS line and one connected to a CICM. However, if the M5316 template is used, intraswitching will not work.

Feature key assignments can be made either through the EM administration Web interface, or directly via the client interface. Feature assignments on a client must be labeled to match the features provisioned through CS2K line provisioning. Refer to the CS2K provisioning documentation for provisioning procedures.

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 Centrex services.

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.

An administrator can prevent clients from logging in to the CICM if they do not have the required level of software (in the m6350) or firmware (in the IP Phone 200x). The CICM administrator may also configure the CICM to upgrade the terminals automatically, in a controlled manner.

Nortel Networks IP Phone 200x Etherset client

Three versions of the Nortel Networks Etherset client are supported for the 7.0 CICM: the IP Phone 2001, 2002, and 2004. All three Ethersets are MBS-like handsets that connect directly to a LAN. The Ethersets are shown in Figure 39.

Figure 39 IP Phone 2001 (above right), 2002 (above left), and 2004 Etherset (bottom)

Functional components

Table 12 lists the functional components of the three versions of the Etherset.

Table 12 Etherset physical functionality comparison

Component	2004	2002	2001
Handset	Y	Y	Y
Speaker	Y	Y	Y
Microphone	Y	Y	N
Headset connector for hands-free operation	Y	Y	N
Standard keypad	Y	Y	Y
Release key	Y	Y	Y
Hold key	Y	Y	Y
Volume control	Y	Y	Y
Mute button	Y	Y	N
Number of navigation keys	4 (Up/Down/ Left/Right)	4 (Up/Down/ Left/Right)	2 (Up/Down)
Function/Display LCD area	Y	Y	Y
No. of soft keys	4	4	4
Number of line/dn keys	6	4	0/1
Transducer control	2 (HF/HS)	2 (HF/HS)	0
Other keys	2 (Stop/Copy)	2 (Stop/Copy)	0

Table 12 Etherset physical functionality comparison

Component	2004	2002	2001
Power over Ethernet capable	Y	Y	Y
Audio capabilities	High end audio. Full duplex speakerphone with wideband transducers (Wideband transducer is only available in handsfree mode).	Standard audio. Full duplex speakerphone with narrowband transducers.	Basic audio. On Hook dial/listen with narrowband handset and no handsfree capability

The IP Phone 200x family is designed as multi-service access devices. The keys beneath the function/display areas are used to switch between one service context and another.

Etherset user interface

To use the IP Phone 200x, the user logs in to the CICM, supplying a user name and password. Once logged in, the handset and standard keypad of the IP Phone 200x 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.

Table 13 provides a comparison of the IP Phone 2002 and 2004 user interfaces.

Table 13 IP Phones 2004, 2002, and 2001 User Interface Comparison

Option	2004	2002	2001
Display contrast	Y	Y	Y
Feature key configuration	Y	Y	Y
Language selection	Y	Y	Y
Time and date format selection	Y	Y	Y
Audio configuration	Y	Y	Y
Firmware Upgrades	Y	Y	Y

Table 13 IP Phones 2004, 2002, and 2001 User Interface Comparison

Option	2004	2002	2001
A user can create a simple editable contacts list of up to 16 entries. An entry in the contacts list can be associated with a feature key so that pressing the feature key so that pressing the feature key automatically dials the number associated with the entry.	Y	Y	N (Contacts key available, but lack of feature keys restricts the functionality)
Call history feature, providing access to CICM-hosted inboxes and outboxes.	Y	Y	Y

Etherset hardware feature comparison

The IP Phones 200x clients support IEEE 802.1p and IETF DiffServ Code Point (DSCP) marking, with Phase I Unistim IP phone firmware 1.57. Phase II Unistim IP phone firmware will also be supported. Table 14 provides an IP Phone 200x hardware feature comparison.

Table 14 IP Phone 200x Hardware Feature Comparison

2004	2002	2001
Adjustable-angle stand	Fixed-angle stand	Fixed-angle stand
Wall mount	Wall mount	Wall mount
Plug in Ethernet switch available (on older models), plus built-in Ethernet switch (2 RJ-45 jacks) in more recent version.	2 RJ-45 jacks with built-in Ethernet switch	1 RJ-45 jack (no Ethernet switch)
6 line keys	4 line keys	0/1 line keys
4 line display area	2 line display area	2 line display area
Extended low-frequency speaker	Standard Stetron LS19 speaker (no tuned cavity)	Basic audio
AEM and ACM accessory port (ports for key expansion modules)	AEM accessory port (for key expansion modules)	No AEM or ACM
Handsfree microphone for wideband audio	Standard Primo EM-80 handsfree microphone	No active speakerphone; on-hook listen only

m6350 SoftClient

The m6350 software client (SoftClient) is accessed through a Windows interface and uses Microsoft Internet Explorer, version 6 and above. For

this release the m6350 is supported only on Windows platforms; other operating systems are not supported.

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.

Note 1: 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.

Note 2: 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 IP Phones 2004 and 2002 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 Professional is the minimum operating system requirement. Windows XP is also supported for the m6350.

- 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 XP
- 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.

Using a headset with the m6350 can result in an echo. If the volume is turned up too far on the earphone(s), the sound may be picked up by

the microphone. The end result could be a noticeable echo to all other participants in the call.

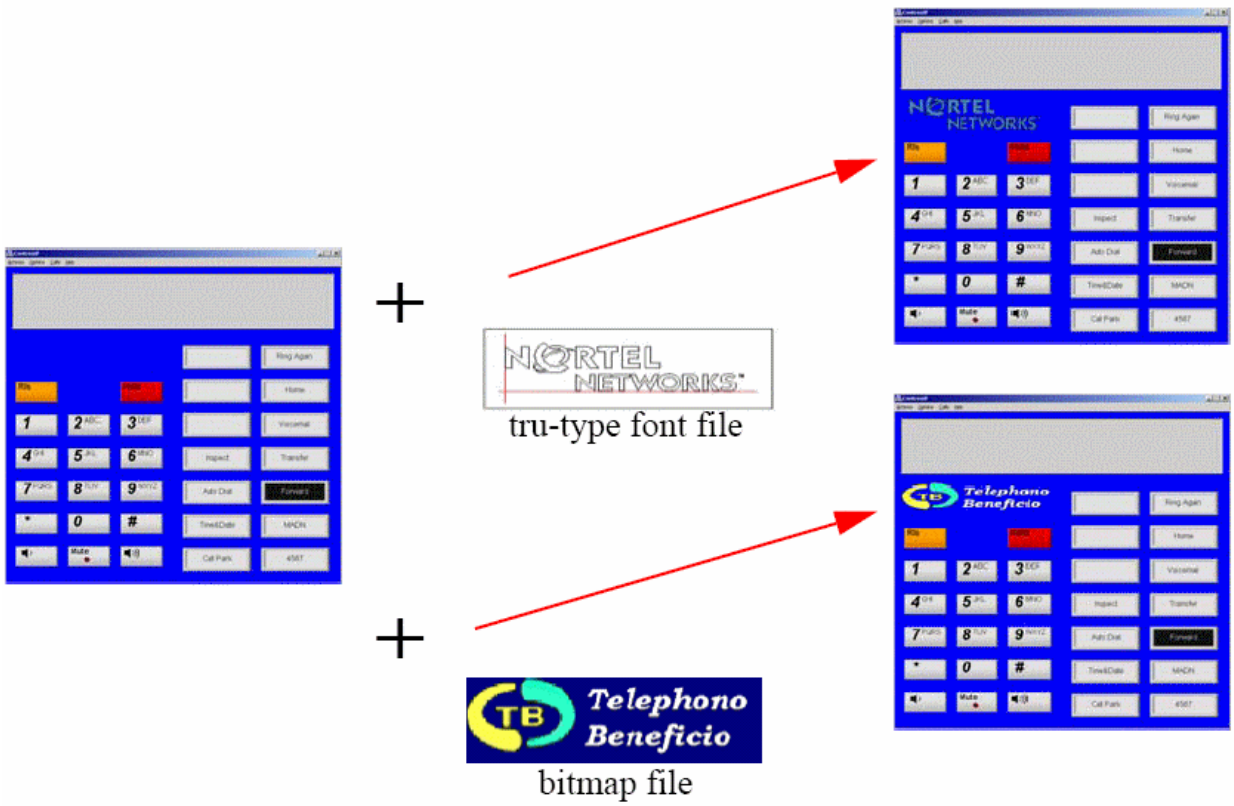
m6350 user interface

The user starts the m6350 just like any Windows program, and the m6350 client behaves as a standard Windows program. It can therefore be run in parallel with many other programs on the PC. However, simultaneously running CPU-intensive applications may degrade the audio quality of the m6350 client.

After login to m6350, the user then logs in to the CICM with a user name and password.

After login to the CICM, the user is provided with a GUI that mimics the appearance of an MBS set (as illustrated by Figure 40). The m6350 behaves exactly like an M5216 or 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 40 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.

Refer to the *NN10182-113 CICM 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,* provided on the CICM 7.0 documentation CD.

Client branding

An OEM customizer is available to allow a service provider 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 41 below). A service provider 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

Figure 41 m6350 Softclient branding

The branding facility allows the server provider to brand the m6350 GUI and produce an installable kit where the company/product information and default software placement details have been tailored to represent the service provider, 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 6 or later) to display HTML pages served by the CICM. If the user's PC does not have IE 6 or later installed, the m6350 will continue to function normally, but will not provide access to this new functionality.

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

Call History and Contacts Directory features

Both m6350 and IP Phone 2004 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.

Note: The call history feature is not available on the IP Phones 2002 or 2001.

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 IP Phones 200x

A user can be logged in from both an m6350 and an IP Phones 200x at the same time, in a cooperative session. The user can dial or answer from either the m6350 or the IP Phones 200x 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 IP Phone 200x 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 IP Phone will ring.

If a user is currently logged in and attempts to log in from another client (m6350 or IP Phone 200x), 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 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.

  Example
  If a user logs into Node 1 from client A, and then attempts to log in from client B, which is connected to Node 0, the user cannot join the other client, but can force out the existing client.
- If a logged in client is making a call, and an attempt is made to either establish a cooperative session with the client or to force out the client, the result is that the call will be cleared.

For detailed procedures, refer to *NN10182-113 CICM m6350 SoftClient Installation and User Guide* and the *NN10027-113 CICM IP Phone 2000x 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 IP Phones 200x clients support two modes of DHCP operation:

- Partial DHCP, in which the IP Phones 200x 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.
- Full DHCP, in which the IP Phones 200x obtains all its configuration data from the DHCP server, including the CICM addresses and ports.

  Note: The DHCP server can only return one set of details to any one terminal. This means that should a terminal hard reboot, it will always return to one particular (DHCP server decreed) CICM. This CICM may not be the CICM the terminal was previously connected to.

  To resolve this issue, it is recommended to switch off full DHCP and choose partial or no DHCP. In this case, only the terminals IP address, netmask, and default CICM will be assigned by the 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.

Other client-related features

There are two other features related to the clients, regardless of whether they are softclient or Etherset.

Auto firmware upgrade

The firmware automatic update feature has been upgraded for (I)SN07.

If the firmware auto-update feature is enabled, and the time criteria is currently met, the user is offered an upgrade (if they are currently logged into a terminal). An on-screen prompt indicates that an upgrade is available, and gives the user an option to “Upgrade Now,” or to “Cancel” the upgrade at this time.

If the user is actively using the terminal, they may cancel the upgrade and their current activity continues unhindered. Accepting the upgrade offer initiates the usual upgrade procedure, which renders the terminal unavailable for a short time, typically a minute, while the upgrade is performed. The user is automatically logged back in after the upgrade is completed.

If the user ignores the prompt, or is not aware of the prompt (e.g. if the user is away from their terminal at the time), then approximately one

minute later the CICM will automatically initiate a firmware upgrade for that terminal. On completion of an automatic upgrade, the user will be logged back in.

If no user is logged into the terminal when the upgrade becomes available, the upgrade will proceed without any notification to the end user.

Emergency Call Services Location Identification Support
The CICM Emergency Call Services (ECS) location identification feature provides functionality to report the location of a user from the CICM telephony client to an ECS system.

The usual operation for CICM telephony clients is to retrieve the location information from the Dynamic Host Configuration Protocol (DHCP) server. However it is also possible for the user to manually enter their location when using a CICM telephony softclient.

It is the responsibility of the network administrator to configure and maintain the CICM telephony client location information in the DHCP Server. If configured, the CICM requests the location information from the telephony client when the user logs in, and reports the information to the call server. The call server reports the location information in XML format over a TCP/IP connection to the ECS system.

Restrictions on CICM clients

The following restrictions exist for CICM 7.0 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 IP Phones 2004 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 IP Phones 200x and m6350 clients.

- The IP Phone 2004 has 6 feature keys and up to 11 features are available from these keys by using the page up/page down keys. The IP Phone 2002 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.

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

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.

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

- **CICM-EM Web 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.
- **Integrated Element Management System**
  The IEMS provides the capability for a user to browse alarms, logs and performance metrics for all CICMs and CICM-EMs. The IEMS can also launch the CICM-EM Web interface for the CICM that has been selected on the IEMS.
- **CICM-EM Web interface launched from the IEMS**
  The IEMS can launch the CICM-EM Web interface for the CICM that has been selected on the IEMS.
- **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.
- **SNMP**
  A standard Simple Network Management Protocol (SNMP) interface for remote status monitoring is available.

For all procedures that use 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 6.0 or later.

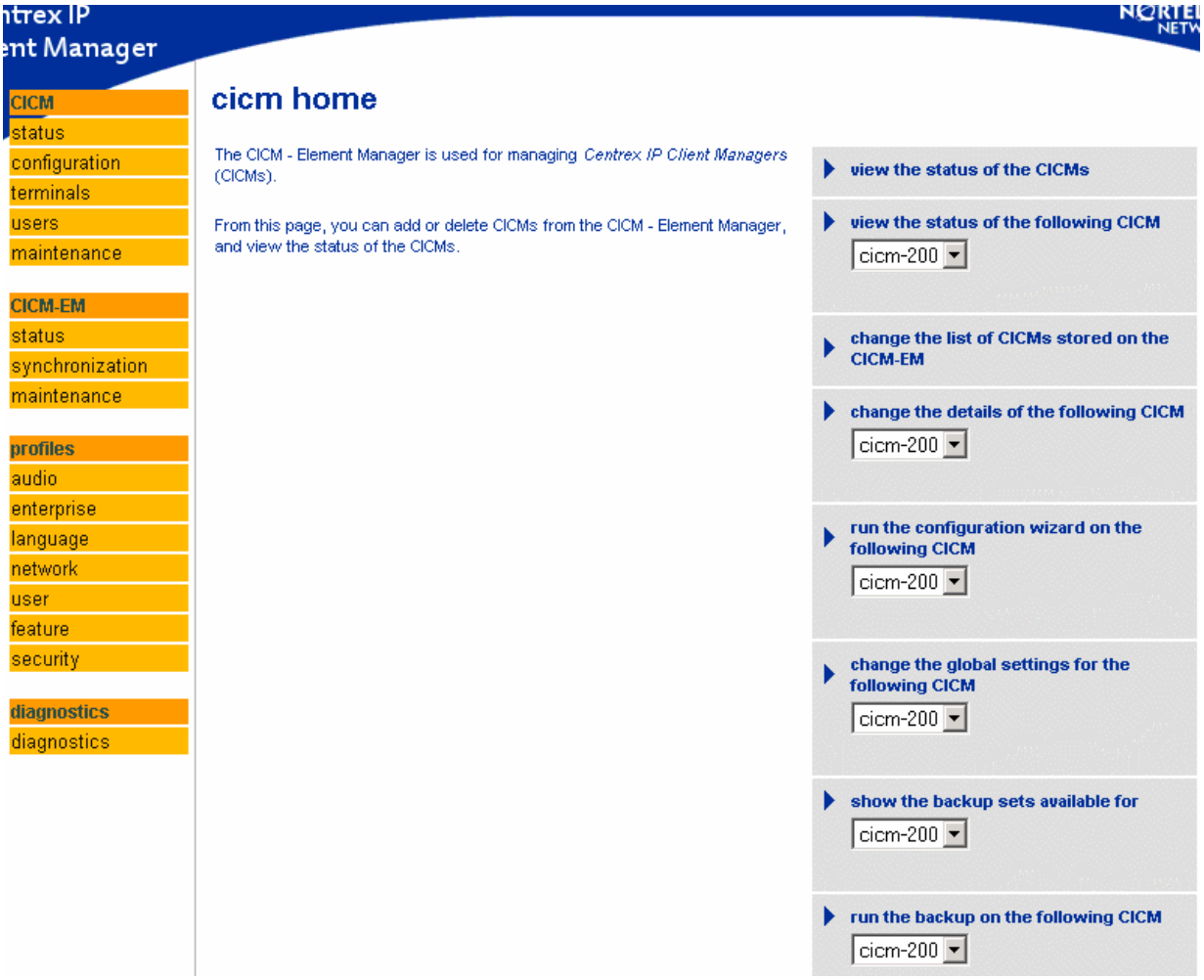
The Element Manager Web site provides the user interface for most of the functionality necessary for configuring and monitoring a CICM and its clients.

The CICM Element Manager Web-based interface consists 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 viewing and configuring the following types of profiles: (, network, audio, language, feature, and enterprise profiles)
  - audio
  - enterprise
  - language
  - network
  - user
  - feature
  - security
- Pages for configuring users
- Pages for configuring client terminals

The following Figure 42 shows the CICM home page. For detailed description of the EM Web page interface and procedures, refer to the *NN10240-511 CICM Configuration Management* and *NN10252-611 CICM Security and Administration* documents.

Figure 42 CICM home page



IEMS interface

The Integrated Element Manager System (IEMS) provides an interface to CICM to perform the following tasks:

- View and monitor faults.
- View system configuration information, including:
  - Instances of CICMs and CICM-EMs
  - Where CICMs are configured in each SAM21 shelf
  - Which GWC manages each CICM
- Launch the CICM-EM Web Interface for a selected CICM

Telnet interface

Telnet is a terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on a PC and connects the PC to a server on the network.

Telnet is a common way to remotely control Web servers. Commands can be entered through the Telnet interface, which will be executed as if they were entered directly on a server console. This enables the control of the server and communication with other servers on the network.

In the CICM environment, Telnet is secured via SSH and provides a basic command line interface for remote emergency or administrative access 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.

CICM SNMP interface

The CICM provides a standard Simple Network Management Protocol (SNMP) interface for remote status monitoring. Each CICM node sends SNMP traps to a set of management systems when specific events occur.

An SNMP browser can be used to view the standard MIB-2 MIBs as well as the Nortel Networks enterprise-specific CICM MIB. New in (I)SN07 for CICM is support of the Nortel Reliable MIB format, which is a standard across the Nortel Succession product range.

Network interfaces

CICM and the IP network

The CICM connects to clients using the IP protocol on its client side network interface.

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.

CICM Logs

The CICM software generates Windows NT event logs for various cases such as client session events and initializations. 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)

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 15.

Table 15 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

Commissioning

Commissioning is the process whereby a CICM is provided with sufficient initial configuration so that it can be subsequently provisioned with service. For example, this initial configuration information would include an IP address of the CICM.

This is a two-stage process, both of which can be run from the Element Manager. The first stage, Preboot, provides the CICM with sufficient information so that it can fully boot and be configured. This stage can be simplified through the use of common configuration files.

Once a node has the basic configuration, the second stage of the process is to configure the remaining datafill, as required, through the Configuration Wizard, which is accessed through the CICM-EM Web Interface. In (I)Sn07, the entire configuration is done in the Preboot stage.

Once commissioned, the service provider may use standard Windows backup tools to ensure that critical configuration data is archived externally to the CICM.

Configuration data

Configuration data (e.g. EM IP addresses, maximum number of concurrent sessions) resides within the Windows Server system registry. Previously backed-up configuration data may be restored to the Window's registry in the event of data loss or corruption due to a hardware or software failure, so that service may be resumed on a replacement or repaired system with minimal loss of service.

Previously backed up configuration data may be restored to the Windows 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).

Back-up and Restore

Data can be backed up in two ways:

- As part of a regularly scheduled task
- On demand from the Element Manager client.

When a node is backed up, the relevant non-volatile data is read from the Window's registry and written to an XML file and stored on the Element Manager.

Typical data that is backed up is:

- User information (e.g. Passwords, Locality Preferences, Contacts)
- Terminal information (e.g. Locality Preferences and Sticky Login)
- Line information (e.g Features)
- Profiles (e.g. Global Profile Overrides)

The Element Manager itself can be backed up, including the Global Profiles, which are maintained on the EM.

Data may be restored as part of the PREBOOT sequence. It is possible to select a particular image to restore, and to select either a full or partial restoration.

GWC Association

For both GWC Association and Subscriber provisioning, the CS2000 Management Tools provide flow-through to the different elements which require this data. In order to keep this data synchronized, it is important to not make modifications directly at the elements themselves.

Before subscribers can be added to a CICM, it is necessary to assign the CICM to a GWC. This process is called Gateway Association.

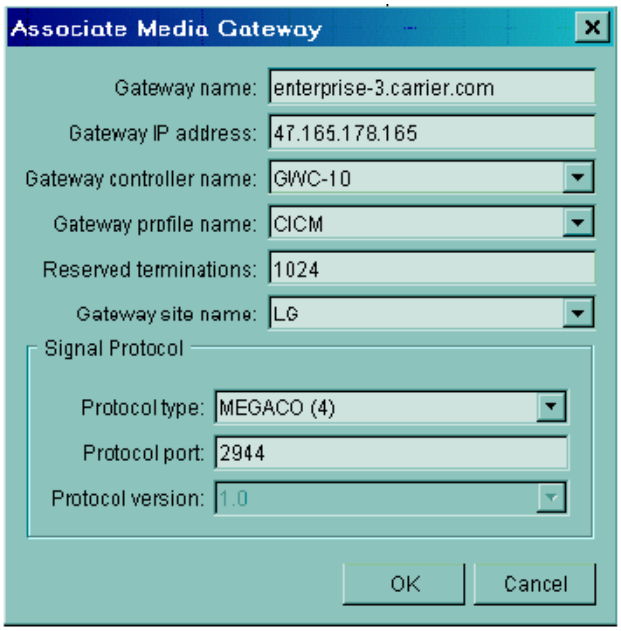
A generic gateway may be associated with a GWC either through the XML interface on OSSGate, or via the CS2000 Management Tools GUI. Whichever interface is used, the following information is required:

- The Gateway Name, e.g. enterprise-3.carrier.com
- The Gateway IP address e.g. 47.165.178.165
- The GWC to be associated with, e.g. GWC-10
- The Gateway profile, which must be CICM
- The number of terminations, if less than the maximum is required

- The site name, e.g. LG
- The signalling protocol, which must be MEGACO

The following Figure 43 is an example of the CICM being associated using the GUI.

Figure 43 Using GUI to Associate a CICM



The following Figure 44 shows an example of the CICM being associated using XML

Figure 44 Using XML to Associate a CICM

```
<assocMG usn="1" version="1.0">

    <Parameters>

      <mgUIName>enterprise-3.carrier.com</mgUIName>
      <mgProfileName>CICM</mgProfileName>
      <mgIpAddr>47.165.178.165</mgIpAddr>
      <gwcUIName>GWC-10</gwcUIName>
    </Parameters>

</assocMG>
```

In addition to creating the association between the CICM and a GWC, this GWC association command automatically provisions the CM tables LGRPINV and LNINV.

Subscriber provisioning

CICM subscribers and their features are added, changed, and deleted through Servord+. The (I)SN07 provisioning feature removes the need to separately provision a subscriber, both on the CS2000 Management Tool and the CICM-EM.

To provision subscribers, an authorized user must connect to OSSGate in CI mode. Any commands which contain a LEN of the format “CICM nnn n nn nn” are intercepted on the CS2000 Management Tool. The command is passed onto the Line Provisioning application so that the line can be datafilled on the CM and GWC.

In addition, the following data, if present, is passed onto the CICM EM:

- User ID
- User profile
- Key mappings
- Enterprise zone

Figure 45 provides an example of a line being added with the Servord+ NEW command:

Figure 45 Example of Servord+ NEW command

NEW $ 8906917 M5216 CSLINES 0 0 125 1 Y CICM 142 2 00 01 3 3WC 4 ACB 1 $ 1 USERID 9999 SRV 1 PASSWD 1234 $

RESULT: features 3WC, ACB, USERID, PASSWD added to CICM LEN

OSSGate example:

```
> NEW $ 8906917 M5216 CSLINES 0 0 125 1 Y CICM 142 2 00 01 3 3WC 4 ACB 1
$ 1 1 USERID 9999 SRV 1 PASSWD 1234

COMMAND AS ENTERED:
NEW NOW 3 10 27 PM 8906917 M5216 CSLINES 0 0 125 1 Y CICM 142 2 00 01 ( 3
3WC ) ( 4 ACB ( 1 ) $ ) $
JOURNAL FILE IS INACTIVE, SERVICE ORDERS NOT ALLOWED
WARNING - MNO (MANUAL OVERRIDE) FIELD HAS BEEN SET TO Y
>
```

CICM supports all Servord+ commands containing a CICM LEN with the exception of:

- Hunt group commands
- CDN - Change Directory Number
- EXBADD - Add MADN Extension Group LEN
- EXBDELG - Delete Primary and Secondary EXB LEN
- QLEN will only return data from the XA-Core

In addition to changing user details via Servord+, they may also be changed from the CICM-EM.

Status

The IEMS provides an overall fault status for each CICM node. This information is updated in real-time. More detailed status information specific to the CICM can be obtained from the CICM-EM itself.

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

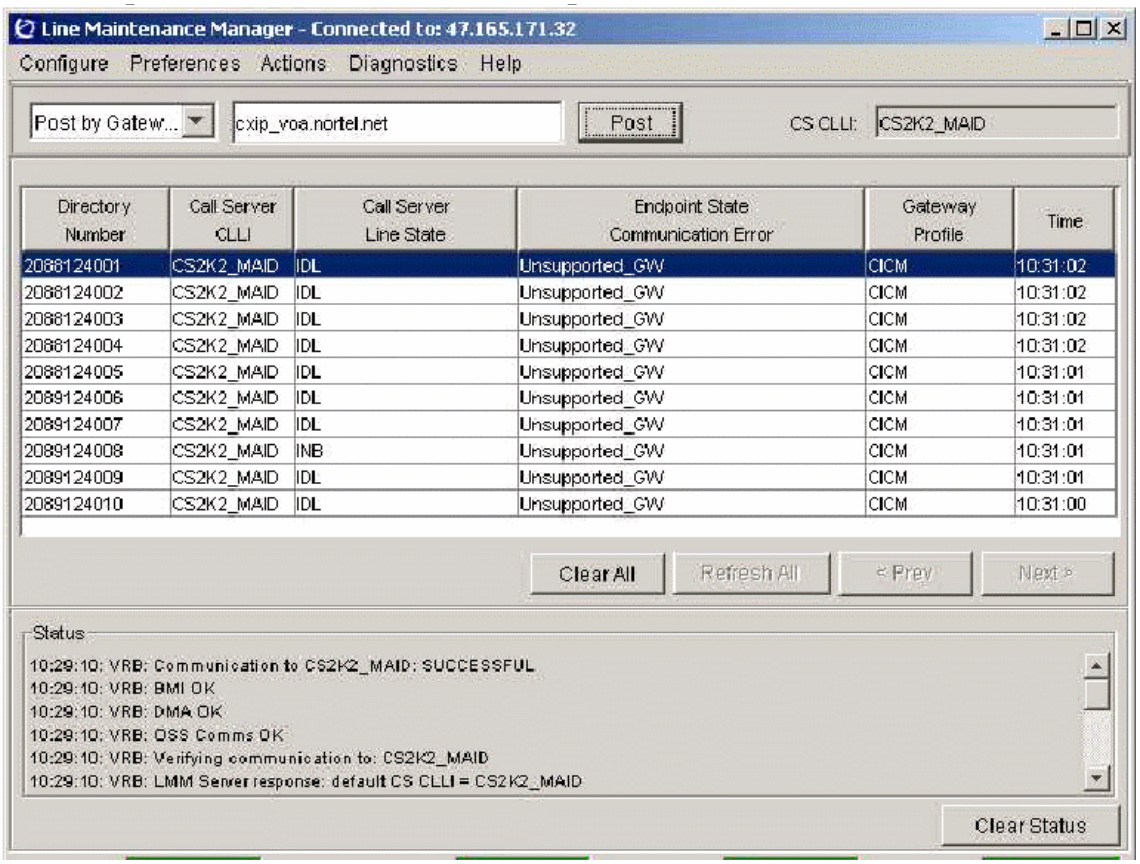
The Line Maintenance Manager (LMM) is a GUI provided by the CS2000 Management Server to replace and emulate the functionality provided by the MAPCI tool on the CS2000 Core. The LMM provides the functionality to post individual lines as well as to post a gateway.

Note: Currently the LMM does not support H.248 gateways, so it is not possible to view the endpoint state.

The LMM main dialog window is illustrated in the following Figure 46. The LMM provides the following commands:

- BSY
- RTS
- FLRS
- INB

Figure 46 Line Maintenance Manager



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

Security and administration

Security

Element Manager security

Element Manager operator authentication and authorization is tied into the Succession SSPFS authorization database.

Logon from and to the EM is performed over HTTPS. CICM does not administer users locally; it delegates the authentication to the SSPFS Authentication Database via the HTTPS PAM Proxy on the SSPFS platform.

If the authentication succeeds on SSPFS, then a local Window's account is created for the user with the appropriate authorization levels from the authentication database. This account is cached so that if the same user logs on again, they can be authenticated without having to consult SSPFS.

The CICM-EM functionality will be partitioned by the type of authentication required to perform an action. For example, a user with read-only access will not be able to modify nodal configuration.

By using the same database as other Succession elements, a user can have a single account to access different Succession components.

Telnet security
The Telnet connection is secured by SSH.

Administration

Refer to (I)SN07 *NN10252-611 CICM Security and Administration* for administrative procedures.

Performance management

Metrics

Performance metrics are generated by both the CICM and the CICM-EM. They are passed northbound into the IEMS, where they are available for display and are aggregated with other IEMS southbound feeds into a single OSS feed.

The CICM and CICM-EM gather the following metrics:

- Percentage Memory usage
- Percentage Disk C Usage
- Percentage Disk D Usage
- Number of Active Users
- Number of Active connections
- Percentage CPU Usage
- Number of Busy hour call attempts
- Number of logged in users
- Number of failed call attempts
- Messaging throughput

Each of these metrics is collected, averaged over a specified time interval, and stored in the MIB. Measurements relating to call traffic are taken every 5 minutes. Other measurements are collected and averaged over either 15 or 30 minute intervals. This 15 or 30 minute period is configurable.

The metrics are transferred in the standard Succession performance MIB. Each metric contains the following information:

- The instance of the object (e.g. SAM21 x blade y)
- The property of the object being reported (e.g. processor occupancy)
- The type of the property (e.g. gauge)
- The value (e.g. 22%)

Traffic loading

Series 7.0 supports one or more pairs of CPN5385 CPU cards per shelf.

Series 7.0 CICM has the following capacity limits:

- Per CICM resource card pair:
  - 3,069 subscriber line provisioning capacity
  - 21,600 BHHCA for 5385 platforms and 7,200 BHHCA for 5370 platforms
  - 3,069 active calls
- Scalable solution by adding more CICM resource cards
- One pair of CICM-EM cards is needed for CS 2000
  - Able to support up to 100 CICM resource card pairs
- Per GWC resource card pair:
  - 8,200 subscriber line provisioning capacity
  - 38,000 BHHCA

For more capacity information refer to:
http://livelink-ott.ca.nortel.com/livelink/livelink.exe?func=ll&objId=8715441&objAction=browse&sort=name

Any single terminal can support up to eight simultaneous active call halves, using functionality such as multiple DNs and call hold. Acting as a slave processor to the core and GWC in the CS2k network, the CICM performance cannot accurately be measured in BHCA. The CICM only has knowledge about half calls, the other half of the call, even if it is hosted from the same CICM, is made anonymous by the CS2k and GWC.

TDM capabilities

The TDM capabilities of the 7.0 product are based on those of the 2.5 CICM version. For a detailed summary of the 2.5 product, please consult the *Series 2.5 CICM Product Specification*.

The TDM product is deployable to both North American and International markets. It continues to support both T1 and E1 interfaces, communicating with the DMS via the DMS-X protocol.

TDM hardware

The TDM product continues to be based around the SAM16 hardware chassis. The SAM21/5385 hardware configuration is not supported for the TDM configuration.

The hardware line-up for (I)SN07 is:

- MCG SAM16 chassis
- MCG 5370 processor card
- Brooktrout NS301 TDM card
- Audiocodes TP610 DSP card

Due to the size of the CICM load, the MCG 5350 processor card is not supported in CICM 7.0.

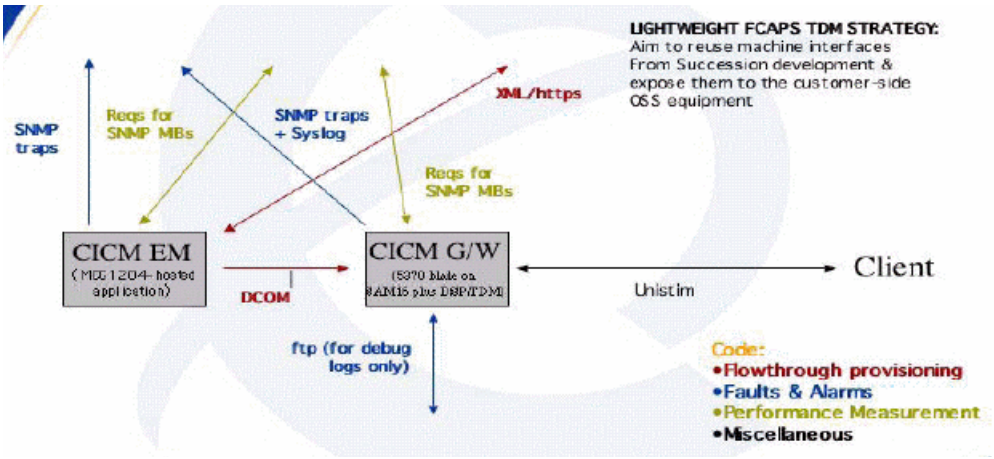
TDM-related features

The following 7.0 features are applicable to the TDM version of CICM:

- **Support of the IP Phone 2001 and other 200x Phase 2 IP Phones**
  The 7.0 TDM product supports exactly the same set of clients (both softclient and physical Etherset) as the CS2K version of CICM.
- **Improved OAM&P interfaces**
  Although the CS2000 Management Server and IEMS are not approved parts of the DMS configuration, the machine interfaces that CICM presents to them are available for TDM customers to interface with other third party products.

Figure 47 provides a TDM high level overview of CICM.

Figure 47 TDM High Level Overview



Fault management

For detailed information on fault management for the CICM, refer to *NN10233-911, CICM Fault Management*.

SNMP alarms

Alarms are raised by both the CICM and the CICM-EM through SNMP, using the Nortel Reliable MIB. Alarms are generated as SNMP Traps when the event causing the Trap occurs. If a Trap is lost, or if the SNMP manager needs to examine historical alarms, they can be retrieved through SNMP Gets.

Alarms can be viewed on the IEMS, and are aggregated with alarms from other components into a single machine feed from the IEMS. For TDM systems and Succession nodes hosted in a SAM16, it is possible to route alarms to a generic SNMP manager.

Each alarm contains the following information:

- Sequence number
- Severity indicator
- Component ID - The distinguishing name ID of the component in the Network element that the alarm was raised against
- Category - The category of the Alarm (Communications, Quality of Service, Processing Error, Equipment, or Environment)
- Notification ID - Unique ID generated from the process number and sequence number combined
- Description - The textual description of the particular alarm

- Time Stamp - The time the alarm was raised, in UTC (Universal Time Code) time
- Probable Cause - An enum representing one of the most likely causes of the fault, as defined in ITU-T X733 & X736
- Specific problem - A refinement of the probable cause
- Correlation ID list - A list of related alarms

The following is an example of an alarm:

Example
Critical Alarm Notification on node B:

Component Id: CICM100B;CICMP.CHAS.FAN1

Category: 5 (equipment)

Notification ID: nnnn:nnnn

Description: Fan Overheating

Probable cause:21– heatingOrCoolingOrVentilationProblem

Specific Problem:

CorrelationId list: (none)

LEDs

The following details on LEDs relates only to a CICM hosted in a SAM16. When run in a SAM21 the LEDs are controlled by the SAM21 Shelf Controller.

Problems with the CICM hardware will be indicated on the physical CICM chassis through a series of lights on the front panel. These alarms are also reflected on the Element Manager.

During runtime, the CICM alarm panel will be directly updated from the software controlling each CompactPCI card. Any status changes which occur in the physical hardware state will be reported as a FAULT alarm above the corresponding CompactPCI card.

Domain A controls the chassis. Only Domain A has the ability to access the alarm panel LED settings and update both the chassis and system alarm states for both sides of the chassis. Domain B does not have the ability to update any system of chassis alarms on its own. Domain A, as the controlling domain, is responsible for showing the state of both itself and Domain B.

If Domain A is unable to determine the state of Domain B, it will make a pessimistic assumption and show a Domain B failure. In this case, the

"Component out of Service" LED will be illuminated along with a "Major" Telecom alarm.

Telco alarm LEDs

Telco alarm LEDs are used to signify faults on the CICM cards and components. Minor, Major and Critical alarms are consistent with CS2000 alarms, and are defined as:

- **Minor chassis alarm LED**
  A minor chassis alarm is an occurrence when one, but not both, domains are reporting a minor alarm.
- **Major chassis alarm LED**
  A major chassis alarm is defined as an occurrence when both domains are reporting a minor alarm, or one (but not both) domains are reporting a major alarm.
- **Critical LED**
  A critical chassis alarm is defined as an occurrence when both domains are reporting a major alarm.

System Status LEDs

The System Status LEDs signify the following:

- **System In Service LED**
  No alarms are raised on the CICM.
- **Component Out of Service LED**
  One or more minor or major chassis alarms have been reported.
- **System Out of Service LED**
  One or more critical alarms have been reported.

Logs

Northbound logs

CICM and the CICM-EM provides a northbound fault stream over Syslog. There are three different logical streams which each use a different Syslog facility:

- A Fault stream carrying details of events such as state changes, data mismatches, and shutdown and restart of processes. This stream uses the standard Nortel Custlog format.
- A Security stream, which contains information about logon attempts and suspected security violations. The format follows the standard Succession security log format.
- An Audit log, which carries details of configuration changes and maintenance actions. The log uses the same format as the security log.

The following shows an example of how the Custlog fields will be populated for a CICM log:

Example

Date, time, hostname, & Application	Generated by Syslog
NODE id	CICM-100
Hostname	CICM100A
Application Name	CICM
Sequence Number	nnn
Report name	PLAT
Report no	301
Alarm value	Major
Event Type	TBL
Label	Software Error Report
Source ID	CICM100A
Text Format	Message Text

Following is an example of a log entry:

Example

V2_~I=CICM~H=cicm100~A=CICM/GW ~S=0001~~CICM 675 MINOR TBL CICM/GW 34400 CWin32Service Constructor called with 0 instances

Accounting

CICM does not affect the way that billing is implemented on the CS2000. All calls, regardless of destination, generate AMA records on the CS2000 in line with existing rules.

All existing CS2000 hosted billing functions appropriate to the MBS terminal are also available for CICM clients.

If specific call rates are required for CICM calls, this would have to be implemented in the downstream billing system to charge for these calls at a different rate.

Billing information generated for CICM calls does not contain IP-specific information, such as the codec type used.

The CICM uses the following policies for billing:

- When a terminal is disconnected from the CICM, the call is billed. This policy prevents customers deliberately disconnecting their terminal from the CICM at the end of a call to avoid being billed.
- When a call is cleared because a component of the CICM fails, the call is not billed.

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 Table 16.

Table 16 Glossary

ACRONYM	DEFINITION
ACD	Automatic Call Distribution
ALI	Automatic Location Identification
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.
CICM-EM	CICM Element Manager
COM	Common connection
cPCI	Compact Peripheral Component Interconnect
CS	Call Server
CS-LAN	Communication Server LAN
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.

Table 16 Glossary

ACRONYM	DEFINITION
DSCP	Differentiated Services Code Point
DSP	Digital Signal Processing
EADM	Emergency Application/Data Manager
EBS	Electronic Business Set.
ECS	Emergency Call Service
EM	Element Manager
EMC	Electromagnetic Compliance
ENET	Enhanced Network
ERL	Emergency Response Location
GUI	Graphical User Interface
GW	Gateway
GWC	Gateway Controller. Interfaces between the CS2K CM and the various supported gateways.
GWC-EM	Gateway Controller Element Manager
HSC	Hot Swap Controller
HTTP(S)	Hypertext Transfer Protocol (Secure)
IEMS	Integrated Element Management System
IETF	Internet Engineering Task Force
IMS	Interactive Media Server
IIS	Internet Information Server
IP	Internet Protocol
LAN	Local Area Network
LBL	Limited Bandwidth Links
LCM	Line Concentrating Module

Table 16 Glossary

ACRONYM	DEFINITION
LEN	Line Equipment Number
LGC	Line Group Controller
LGRP	Logical Group (of lines)
LIS	Location Information Server
LMM	Line Maintenance Manager
LM(D)	Line Module
LTC	Line/Trunk Controller
LNINV	Line Inventory (table)
MAP	Maintenance and Administration Position
MBS	Meridian Business Set.
MCDN	Meridian Customer Defined Network
MCS	Multimedia Communications Server
MG9K	Media Gateway 9000
MGC	Media Gateway Controller.
MIB	Management Information Block, Managed Information Base
MIDCOM	IETF Middle-box Communications Working Group
MMP	Multi-Market Platform
MR	Maintenance Release
MTM	Maintenance Trunk Module
NA	North America
NAPT	Network Address and Port Translator
NAT	Network Address Translation
NEBS	Network Equipment-Building System

Table 16 Glossary

ACRONYM	DEFINITION
OA&M	Operations, Administration, and Maintenance
OAMP	Operations, Administration, Maintenance, and Provisioning
OM	Operational Measurement
OSS	Operations Support System
PAM	Pluggable Authentication Module
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
PVG	Passport Voice Gateway
QoS	Quality of Service
RCC	Remote Communications Controller
RLCM	Remote Line Concentrating Module
RMM	Remote Maintenance Module
RTCP	RTP Control Protocol
RTP	Real-Time Transport Protocol
SAM	Service Application Module
SC	Shelf Controller

Table 16 Glossary

ACRONYM	DEFINITION
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.
SDM	Succession Data Manager
SIP	Session Initiation Protocol
SLU	Subscriber line usage
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SSL	Secure Sockets Layer
SSPFS	Succession Server Platform Foundation Software
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 Multiplexed
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
UNID	Unique Network ID
UNIStim	Unified Networks IP Stimulus protocol. Nortel signalling protocol used for the IP Phone 200x

Table 16 Glossary

ACRONYM	DEFINITION
VCAC	Virtual Connections Admission Control
VLAN	Virtual Local Area Network (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