CICM Basics

This document provides an overview of the Centrex IP Client Manager (CICM) node (gateway) and its element manager (CICM-EM). This document describes the hardware components, software components, and user interface of the CICM products.

Centrex is the Central Office exchange service. CICM uses Internet Protocol (IP) telephony to integrate voice and data capabilities. Voice over IP (VoIP) is the technology that enables voice to be carried over a data network. Analog voice signals are digitized, compressed, and transmitted as IP packets over an IP network.

The topics in this document are:

What's new for the CICM product

The feature changes provided by the SNxx release of this document are:

- Addition of active call failover
- Addition of additional tones and languages
- Addition of IP Conference Phone 2033
- Addition of UNIStim security - reset security
- Expansion of line capacities
- Expansion of CICM lines for P-Phones
- SDP parser improvements
- Support for CICM operating with the E911 feature
- Support for CICM operating with the GIC and GIAC features
- Support for CICM operating with the IW-SPM
- Support for CICM operating with the MRF feature
- Support for CICM operating with the SRG feature

Other changes to this version of the document include:

- added references to the new IP Phone user guides in Related documents
- added the section Other features and capabiltities for CICM
- added the section CICM cabinet
- in CICM chassis:
  - added the figure CICM chassis of a SAM16
  - added the figure CICM chassis of a SAM21
  - updated the description of hot-swapping
- updated the table IP addressing example

- updated the table CICM network interfaces
- updated the Call Server interaction with CICM in Restrictions to Centrex feature support
- updated the figure Using a GUI to associate a CICM
- renamed “CICM clients” to CICM clients with the IP Phones or m6350 SoftClient and updated the section
- updated Restrictions on CICM clients
- removed the XML method of associating a gateway with the gateway controller since this is no longer supported
- removed all occurrences of net6 since it is not supported in this release
- removed the Glossary since these are no longer supported for individual NTP documents

Addition of active call failover

Prior to SN08, IP terminals could connect to either node of a CICM for service. Should a node fail, all terminals hosted by the defunct node would experience an outage (possibly losing one or more calls) while they rebooted and reconnected to the mate node.

With SN08 and later, the Active Call Failover (ACF) functionality transitions the CICM from a load sharing model to a full takeover redundancy model. With ACF, all terminals connect to the master node of the CICM through single IP address. Should the master node fail, the mate assumes the role of master, takes over this floating IP address and begins the recovery of terminals (clients) while maintaining active calls.

Addition of additional tones and languages

CICM supports additional languages for terminals, as well as a number of country-specific tone sets. The new languages supported are Turkish and Portuguese. The new country-specific tone sets supported are Austria, Belgium, Bulgaria, Czech Republic, Ireland, Israel, Mexico, New Zealand, Portugal, Romania, Russia, Switzerland, Sweden, Turkey, and Venezuela. The complete list is in Tones and languages of CICM.

Addition of IP Conference Phone 2033

The IP Conference Phone 2033 is a conference terminal that can be deployed in locations where conferencing functionality is the main purpose of the terminal. It emulates the IP Phone 2001. The 2033 has been added throughout this document wherever IP Phones are mentioned.

Addition of UNIStim security - reset security

The UNIStim security feature provides the infrastructure required for secure communications between the CICM server and its clients. SN08 adds a function to reset security on CICM servers to facilitate moving multiple secure clients from one CICM server to another. For more details, refer to the UNIStim security section in *CICM Security and Administration*, NN10252-611.

Expansion of line capacities

The line capacity of the CPN5385 CICM nodes is expanded. Refer to the table CICM capacity attributes.

Expansion of CICM lines for P-Phones

Prior to SN08, the number of business sets that could be provisioned in table KSETINV was 31,743. With SN08 and later, the limit increases to 150,000.

> ***Note:*** This does not increase the number of equivalent directory number (DN) appearances or virtual lines that can be supported on these business sets provisioned in table KSETLINE.

SDP parser improvements

The CICM communicates with the Media Gateway Controller (MGC) using the H.248 (that is, Megaco) protocol. H.248 in turn uses the Session Description Protocol (SDP) to transmit and negotiate audio stream information. With SN08 and later, the CICM's SDP parser and generator have been replaced. This new and more efficient parser will improve the CICM's real-time performance.

Support for CICM operating with the E911 feature

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. For additional information, refer to CICM operating with the E911 feature (ECS Location Identification).

Support for CICM operating with the IW-SPM

The Inter-Working Spectrum Peripheral Module (IW-SPM) is a special gateway for Nortel's multi-core TDM switch (a DMS) to the IP network. For additional information, refer to CICM operating with the IW-SPM.

Support for CICM operating with the GIC and GIAC features

CICM clients support using the CS2K calling features Group Intercom (GIC) and Group Intercom All Calls (GIAC) on its clients. For additional information, refer to CICM operating with the GIC and GIAC features.

Support for CICM operating with the MRF feature

The MADN Ring Forward (MRF) feature provides the capability for MADN SCA appearances to ring on a delayed or abbreviated basis for various ringing options. For additional information, refer to CICM operating with the MRF feature.

Support for CICM operating with the SRG feature

The Survivable Remote Gateway (SRG) feature is located at the telco premises and offers a secondary fall-back for terminals on the network should the overall communication path to the CICM be lost. With an SRG on site, terminals that lose their connection to the CICM will restart and connect to the SRG. The SRG acts as a very basic call server, able to route calls between terminals on the local network.

For additional information on SRG, refer to CICM operating with the SRG feature.

Introduction to CICM

This section introduces the CICM products, which uses Voice over IP technology to deliver Centrex capabilities to users connected to an IP network.

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 provides the interface between the Centrex feature set and an IP network.

Fort SN08 and later, the CICM solution consists of these components:

- one Motorola SAM21 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 gateway controller (GWC) and distributed CICM IP clients on a managed IP network. It communicates with the GWC using the H.248 protocol (version 1).

> ***Note:*** H.248/MEGACO is a joint ITU-T / IETF protocol defined in ITU-T Recommendation H.248 and IETF RFC3525. It fully supports the same basic device or media control capabilities as protocols such

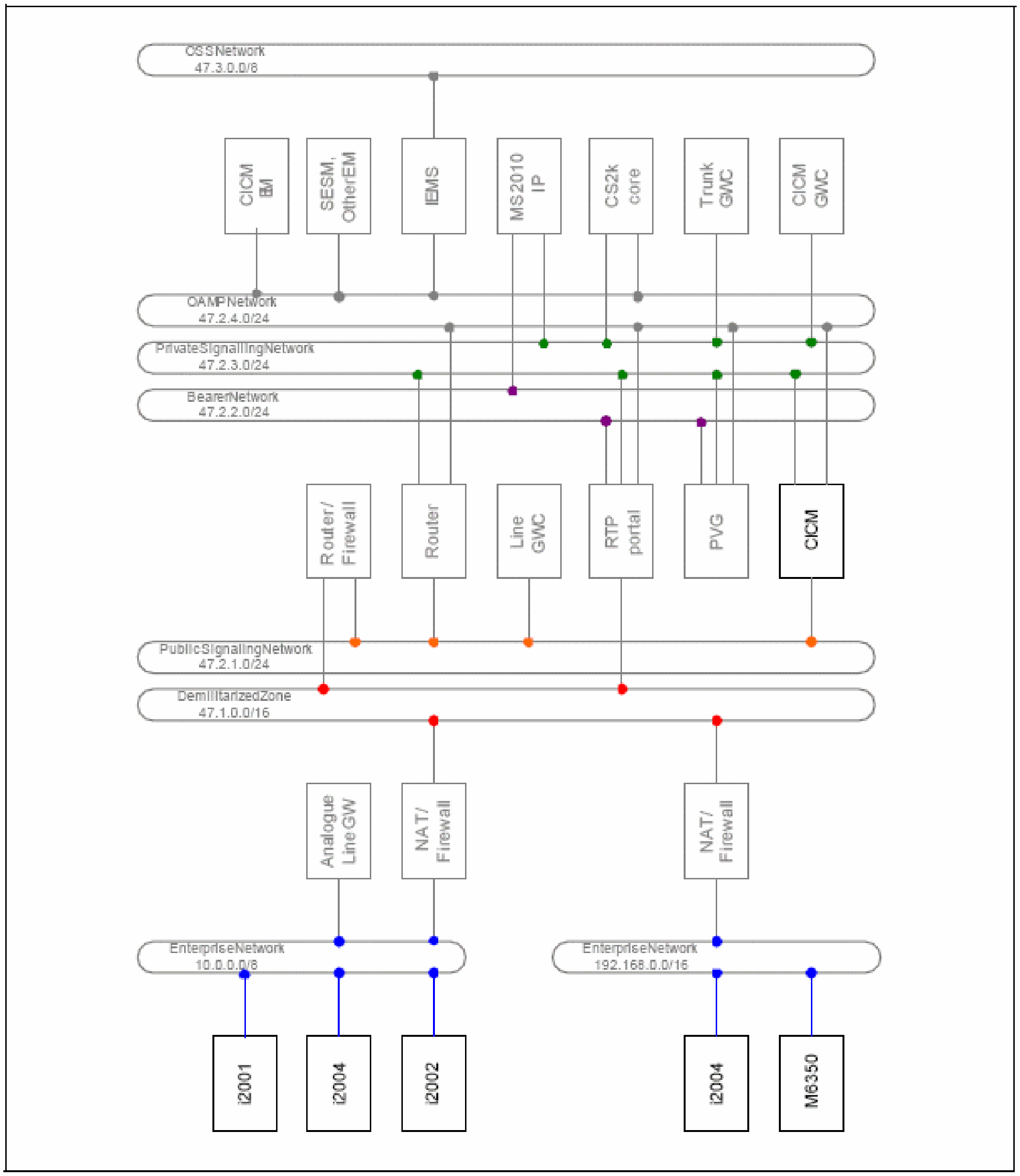
as ASPEN. More importantly, it is based on a more flexible functional mode that provides better support for multimedia and conference capabilities.

The CICM is not a media gateway. It is better described as a terminal proxy server or signaling gateway. Media streams in a Carrier Voice over IP (VoIP) solution are routed directly between media end-points. The CICM terminals (for example, IP Phone 200x) are media end-points. Other media end points in a Carrier Voice over IP (VoIP) network include:

- Time Divisiojn Multiplexed (TDM) trunk gateways (for example, MG 15000)
- analog line gateways (for example, MG9000, Mediatrix 1124)
- voice processing servers (for example, UAS or AMS)
- IP Terminals hosted off another CICM

The figure Role of the CICM and clients in Carrier VoIP shows a generic Carrier VoIP 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. Operations, Administration, Maintenance, and Provisioning (OAMP) devices and networks are also omitted from the figure.

Figure 1 Role of the CICM and clients in Carrier VoIP



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 (for example, 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 either:

- A PC equipped with suitable IP telephony client software (such as the m6350 SoftClient)
- A LAN-capable telephone (such as the Nortel IP Phones 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, CS2000 can support VoIP or VoATM (Voice over ATM), depending on the type of backbone packet network to be used.

Specific CS2000 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. CS2000 supports the following types of access through 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 analog subscriber lines only
    - Analog line access through a variety of gateway types, including CPE gateways attached to customer LANs or cable networks
    - ADSL access through 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 (for example, number portability).

A CS2000 can be regarded as a single node, but it is composed of separate components. The CS2000 capabilities listed above are provided by separate CS2000 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 through device/media control signalling based on packet network protocols
- to support communication between peer communication servers for the handling of networked calls (accomplished through inter-CS signalling, also based on packet network protocols)

For additional information, refer to the *CS2000 Product Description*, cs2000cPDISN07.

CS2000 Connectivity and network element control

CS2000 provides for control over the media gateways that provide the bearer connection interface between the packet network environment and other TDM or access networks. CS2000 supports the following types of access through 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 through a variety of gateway types, including CPE gateways attached to customer LANs or cable networks
- ADSL access through terminations on high-capacity line media gateways

CS2000 call processing

Call processing capabilities of CS2000 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

CS2000 service support

CS2000 service support capabilities include:

- support for specific sets of value-added features
- support for general-purpose service delivery platforms
- support for regulatory features (for example, number portability)

CS-LAN

For SN08 and later for the SAM21-based Carrier Voice over IP (VoIP) CICM, 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 VoIP Communication Server LAN (CS-LAN).

This standard VoIP CS-LAN consists of two high-density, high-throughput, high-resilience, NEBS-3 compliant Ethernet Routing Switch 8600 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.

For SN08 and later, the Public Signaling Interfaces (that is, the UNIStim-LAN interfaces) and the OAM/P Interfaces (that is, 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 CS-LAN of the standard Carrier Voice over IP (VoIP) Ethernet Routing Switch 8600. (Refer to the *Centrex IP Client Manager (CICM) Engineering Guide*, 297-5551-100 for details on the switch and the CS-LAN.)

Element Manager

The Element Manager (EM) 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.

Refer to Hardware of the CICM and CICM-EM for additional hardware-related details of the CICM-EM.

CICM clients

The CICM client is the component that allows a user to initiate and receive VoIP calls, and to receive Centrex features from CS2000. 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 IP Phone 200x and 2033 handsets, which connect directly to a client LAN or to a telephony switch module. The 200x includes 2001, 2002, and 2004 models.

CICM clients (except for 2033 in SN08) use the Nortel proprietary UNIStim (Unified Networks IP Stimulus) protocol to communicate with the CICM. This allows the clients to deliver the full range of CS2000 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 proprietary Unified Networks IP Stimulus (UNIStim) protocol. UNIStim security protects all signaling messages between a CICM node and its clients by encryption such that user id, password, and other call control information is unidentifiable.

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 (CICM) Engineering Guide*, 297-5551-100 for a detailed description of CICM network engineering.

Carrier VoIP and Carrier-based CICM

The (I)SN08 CICM supports the Carrier Voice over IP (VoIP) CS 2000 version of the product.

Related documents

The documents in the CICM document suite are:

- *CICM Basics*, NN10044-111
- *Upgrading CICM*, NN10230-461
- *CICM Fault Management*, NN10233-911
- *CICM Configuration Management*, NN10240-511
- *CICM Accounting*, NN10244-811
- *CICM Performance Management*, NN10248-711
- *CICM Security and Administration*, NN10252-611

For information about the m6350 SoftClient and TAPI service provider, refer to:

- *m6350 SoftClient Installation Guide*, NN10182-113
- *m6350 TAPI Service Provider Installation and Troubleshooting Guide*, 297-5551-901

For information about the Nortel IP Phone 200x and the IP Conference Phone 2033 clients, refer to:

- *CICM Configuration Management*, NN10240-511 for installing and configuring phone sets
- *Upgrading CICM*, NN10230-461 for phone set firmware
- *CS 2100 IP Phone 2001 User Guide*, NN10300-005
- *CS 2100 IP Phone 2002 User Guide*, NN10300-007
- *CS 2100 IP Phone 2004 User Guide*, NN10300-009
- *CS 2100 IP Phone Key Expansion Module User Guide*, NN10300-011

For information about the CICM provisioning that is handled by OSSGate, refer to the *OSSGate User's Guide*, NE10004512.

For information about the CS2000, refer to the *CS2000 Product Description*, cs2000cPDISN07.

For engineering information and specifications to support Voice over IP (VoIP), refer to the *Centrex IP Client Manager (CICM) Engineering Guide*, 297-5551-100.

For information on Microsoft Windows XP and XPe, refer to the Microsoft web sites:

- ***http://www.microsoft.com/windowsxp/default.asp/***
- ***http://www.microsoft.com/window/embedded/xp/default.asp/***

For information on Microsoft, refer to the Microsoft web site *http://www.microsoft.com/*

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

CPV5370:
http://mcg.motorola.com/cfm/templates/product.cfm?PageID=1841&ProductID=201&PageTypeID=1

CPN5385:
http://mcg.motorola.com/cfm/templates/product.cfm?PageID=2149&ProductID=249&PageTypeID=1

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

Terminology for CICM

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 CS-LAN in the carrier Central Office network. This subnet hosts the OAM/P interfaces of the CICM and the CICM-EM for such functions as CICM and client configuration and monitoring.

Centrex IP Client Manager (CICM)

The CICM refers to all the CICM resource cards (Motorola CPN5385 processor card) on a SAM21 chassis, associated with a single CS2000. 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 a terminal proxy server.

Chassis

The CICM is hosted on either a Motorola SAM16 or Motorola SAM21 chassis. A chassis may contain multiple CICM CPN5385 card pairs.

Chassis domains

For SAM16, a chassis consists of two CompactPCI domains, referred to as Domain A and Domain B (or node A and node B). The two domains of a single chassis provide a high availability (but not fault tolerant) host architecture for CICM software.

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

Client LAN

The Client LAN is the public signaling subnet in the CICM SN08 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, 2033, and SoftClient m5360) from the enterprise or CPE network, for communication of signaling messages (for example, 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.

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, the CICM-EM is a pair of Motorola CPN5385 resource cards, one active master and the other a hot standby slave 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 (nodes). The hot standby slave 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.

GWC
A gateway controller is the interface between the clients of a CICM node and the IP network.

H.248
The H.248 LAN refers to the Private Signaling Subnet in the CICM CS-LAN in the carrier Central Office network. In the carrier-hosted deployment, this signaling subnet serves to provide an H.248 communication path between CICM nodes and the Media Gateway Controller (MGC).

MBS
Meridian Business Set (MBS) is the Nortel brand name for the electronic keyset terminals (phones) used for delivering Centrex services (that is, M6320, M5216, etc).

Nodes
Each SAM21 chassis contains either one or two CPN5385 processor cards, and if only one, its mate is in another chassis for redundancy. Each SAM16 chassis contains two CPV5370 processor cards that cannot be slit into separate chassis. The SAM16 also contains other plug-in hardware, but CICM nodes essentially refer to a pair of cards configured to behave as master and slave.

North side
The gateway controller (GWC) side of the CICM.

South side
The terminal side of the CICM.

UNIStim LAN
The UNIStim LAN refers to the Public Signaling Subnet in the CICM CS-LAN in the carrier Central Office network. In the carrier-hosted deployment, this Public Signaling Subnet houses the public interface of the CICM. This public interface can be reached by Centrex IP clients (IP Phones 200x and m5360) from enterprise or CPE networks, for communication of signaling messages (for example, UNIStim registration, call processing, firmware download, etc).

VMG
The CICM provides a single Virtual Media Gateway supporting up to 3,069 lines. The CS2000 thinks the CICM is a traditional media gateway. The CICM is virtual because it is an aggregation point for 3,069 individual gateways (that is, individual terminals) sitting in the customer network.

Tones and languages of CICM

CICM is designed for both International and North American 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:

- Austria
- Australia
- Belgium
- Bulgaria
- Czech Republic
- France
- Germany
- Ireland
- Israel
- Italy
- Mexico
- New Zealand
- North America
- Portugal
- Romania
- Russia
- Spain
- Sweden
- Switzerland
- Turkey
- United Kingdom
- Venezuela

The supported languages on the CICM are:

- English (UK)
- English (US)
- French
- Italian
- German
- Portuguese
- Spanish
- Turkish

Centrex features for CICM

This section describes:

- Centrex feature support
- Centrex IP enhancements over Centrex
- Restrictions to Centrex feature support

Centrex feature support

A client connected through the CICM appears to the CS2000 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 table Centrex feature support for CICM SN08 lists most key features and indicates whether each is supported or not for CICM SN08. The complete list of Centrex features is provided in the feature library, which is available at the web site **http://www.nortelnetworks.com/products/01/centrex/library/overview/** A search tool is available that will provide a feature description for each feature name entered.

Table 1 Centrex feature support for CICM SN08

Feature name	Support
Blind Transfer Recall	Y
Blind Transfer Recall Identification	Y
Call Disposal features	
Call Hold	Y
Call Park or Call Park for BS	Y
Call Waiting or Camp-On for Business Set (BS)	Y
Call Waiting Originating or Call Waiting Originating for BS	Y
Dial Call Waiting or Dial Call Waiting for BS	Y
Permanent Hold	Y
3-Way Calling or Call Transfer for BS	Y
Call Pickup features	
Call Pickup or Call Pickup for BS	Y
Directed Call Park	Y
Directed Call Pickup, No Barge-In	Y
Call Forwarding features	
Call Forward or Call Forward for BS (busy)	Y
Call Forward or Call Forward for BS (doesn’t answer)	Y
Call Forward or Call Forward for BS (station activation)	Y
(Sheet 1 of 4)	

Table 1 Centrex feature support for CICM SN08 (Continued)

Feature name	Support
Call Forward or Call Forward for BS (unconditional)	Y
Speed Calling features	
Speed Calling or Speed Calling for BS (individual long list)	Y
Speed Calling or Speed Calling for BS (individual short list)	Y
Business Set Display and Function Key features	
Six-Port Conference (MBS)	Y
Ring Again features	
Network Ring Again	Y
Ring Again or Ring Again for BS	Y
Single Digit Activation of RAG/CBWF	Y
Automatic Call Distribution (ACD) features	
ACD Not Ready (ACDNR)	Y
Answer Agent Key (AAK)	Y
Answer Emergency Key (AEMK)	N
Agent Status Lamp (ASL)	Y
Call Agent (CAG)	Y
Call Supervisor (CLSUP)	Y
Controlled Interflow (CIF)	Y
Display Agent Status (DASK)	Y
Display Queue Status (DQS)	N
Display Queue Threshold (DQT)	N
(Sheet 2 of 4)	

Table 1 Centrex feature support for CICM SN08 (Continued)

Feature name	Support
Extended Call Management (ECM / ICM)	N
Emergency Key (EMK)	N
Forced Agent Availability (FAA)	Y
Line of Business (LOB)	Y
Night Service (NGTSRVCE)	Y
Observe Agent (OBS)	N
Supervisor (SUPR)	Y
Uniform Call Distribution (UCD) features	
UCD Logged In Indication (UCDLI)	N
UCD Login (UCDLG)	Y
UCD Signal Distributor (UCDSD)	N
Miscellaneous features	
Automatic Recall (AR)	Y
Bridged Night Number (BNN)	Y
CLI with Flash/Malicious Call Hold/Malicious Call Hold for BS	Y
Directory Number Hunt (DNH)	Y
Distributed Line Hunt (DLH)	Y
Make Set Busy (MSB)	Y
Make Set Busy Intragroup (MSBI)	Y
Meet-Me Conference (MEETME)	Y
Message Waiting Indication (MWIDC)	Y
Multiple Appearance Directory Number (MADN)	Y
(Sheet 3 of 4)	

Table 1 Centrex feature support for CICM SN08 (Continued)

Feature name	Support
Multi-Line Hunt (MLH)	Y
Preset Conference (PRESET CONF)	N
(Sheet 4 of 4)	

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 these IP Phones: 2001, 2002, 2004, or 2033. An IP Phone 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

A third-party attendant console is 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.

When local ringing is configured for IP Phone 2004, distinctive ringing and ring back tones do not originate locally on the set itself, but may originate out-of-band.

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 Phones 2001 and 2033 do not have assignable feature keys. The 2001 can access features using the services key and star access codes.

While the Call Server can be configured with multiple features on a single key (for example, a primary DN and call forward busy), the CICM node is only concerned with the primary feature assigned to each key. For example, the DN is the significant feature and the key is labelled with the DN because the call forward busy has no user interactions.

The Key Expansion Module (KEM) support restriction is:

- Currently, 22 features on the KEM out of the 24 buttons for 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.

Other features and capabiltities for CICM

Other features and capabilitiers that are supported by CICM software include:

- CICM operating with the E911 feature (ECS Location Identification)
- CICM operating with the GIC and GIAC features
- CICM operating with the IW-SPM
- CICM operating with the MRF feature
- CICM operating with the SRG feature

CICM operating with the E911 feature (ECS Location Identification)

The CICM node must be at SN07 or later to support E911.

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

The Emergency Call Services (ECS) handle mobility of Internet Protocol (IP) telephony clients in a Voice over IP (VoIP) Enterprise environment. This functionality applies only to the VoIP version of the CICM product.

For fixed lines connected to an analog 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 clients, the location of a user is not fixed. UNIStim terminals in an Enterprise network that connect to the CS 2000 (CS2K) through the CICM are not statically configured against a particular node in the network, and their physical location may be anywhere in the Enterprise.

The E911 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 client.

When the CICM 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 node may then request the location information from the CICM client at any time and report the location information through H.248 to the GWC. If configured, an application running on the gateway controller re-packages the information and reports it to a Location Recipient application.

The E911 feature also supports the reporting of user-defined location identification. This is required for CICM softclients on networks with DHCP servers that do not support the new location identification DHCP options.

The E911 feature reports 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 client location information can also be employed to report the client location's unique network id (unid) within the network topology.

For the E911 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 CICM 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 E911 feature provides for the EADM to receive the Location Identification information from the gateway controller, not the CICM node.

Included in the Location Identification information reported by the gateway controller to the EADM are the CICM 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 gateway controller or use Location Identification information from it's own database.

IP Phones 200x

The IP Phone 200x 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.

CICM Element Manager

The CICM ECS Location Identification functionality on the CICM is activated through 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 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 gateway controller is activated through the CICM-EM Graphical User Interface (GUI).

The destination for the Location Identification information, (that is, the Location Recipient) is configured in the CICM-EM. The Location Recipient is configured in the Location Recipient tab of the Network Devices section of the Network panel.

The CICM-EM enables Location Identification reporting on the gateway controller through the SNMP.

CICM operating with the GIC and GIAC features

The GIC feature enables an originator to call other members of a pre-designated group using abbreviated dialing. The originator presses the GIC feature key and dials an abbreviated code or presses an id key (depending on the type of terminal) to page the called party. When the called party is on-hook, the loudspeaker is automatically activated for one-way speech path. When the called party is off-hook, the handset is automatically activated for two-way speech path. When the called party picks up the handset while the one-way call is activated, a two-way speech path is established.

The GIAC feature operates the same way as the GIC except that it can page and conference multiple GIC members simultaneously when pressing the GIC key.

Configuring the GIC and GIAC features and using them is briefly described in *PLN-08AT-OSS SN08 OSS Guide (ATM) Advance Feature Guide*.

CICM operating with the IW-SPM

The IW-SPM bridges the Enhanced Network (ENET) of the TDM core and the ATM fabric. It bridges calls between the TDM switch and the public IP network.

The IP IW-SPM accomplishes this by connecting to an ENET over the core side (C-side) DS512 fiber links and to the IP network over Gigabit Ethernet on the peripheral module side (P-side). Between these two connections are the common equipment module (CEM) and the IP resource module (IP RM) of the IW-SPM. The CEM connects to the DS512 links and performs the bridge management function. The IP RM connects to those bridges to the IP network over a Gigabit Ethernet.

CICM clients can interwork with the TDM clients either as an intra-group or an inter-group customer 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, and share the same dial plan and Centrex features. For example, MADN users can be split between TDM and CICM/IP transparently, or ACD agents on the TDM side share the same ACD groups or queues as on the CICM/IP side. This means features like Call Pick-up or Call Park span the IP-to-TDM bridge within the same customer 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 means features like Call Forward or 3-Way Call span the IP-to-TDM bridge within the different customer groups.

CICM interworks with IW-SPM independently of a specific hardware platform. For more information about IW-SPM, refer to the *IW-SPM IP Basics*, NN10015-111.

CICM operating with the MRF feature

The MADN Ring Forward (MRF) feature provides the capability for MADN SCA appearances to ring on a delayed or abbreviated basis for a total of four ringing options:

- Always ring
- Never ring
- Ring from call termination until MRF activation (abbreviated)
- Ring after MRF activation (delayed)

MRF also provides the capability for the user to manually “push” the ringing for an incoming call to the appearances of the MADN designated for delayed ringing by pressing a feature key provisioned with the MRF Manual (MRFM) feature.

MRF activation can be automatic or manual. Automatic ring forwarding is controlled by a timer, which is set on a per-MADN group basis. The automatic version of MRF can also be preempted manually by the user by activating a feature key on the terminal. The manual version of MRF is activated by a feature key on the terminal. That feature key is associated in datafill with one or more MADN appearances on the terminal, which have the MRF feature.

CICM operating with the SRG feature

The Survivable remote Gateway (SRG) feature is described in:

- Overview of SRG
- Hardware and software requirements for SRG
- Supported IP telephone sets for SRG
- Restrictions and limitations for SRG
- References for SRG

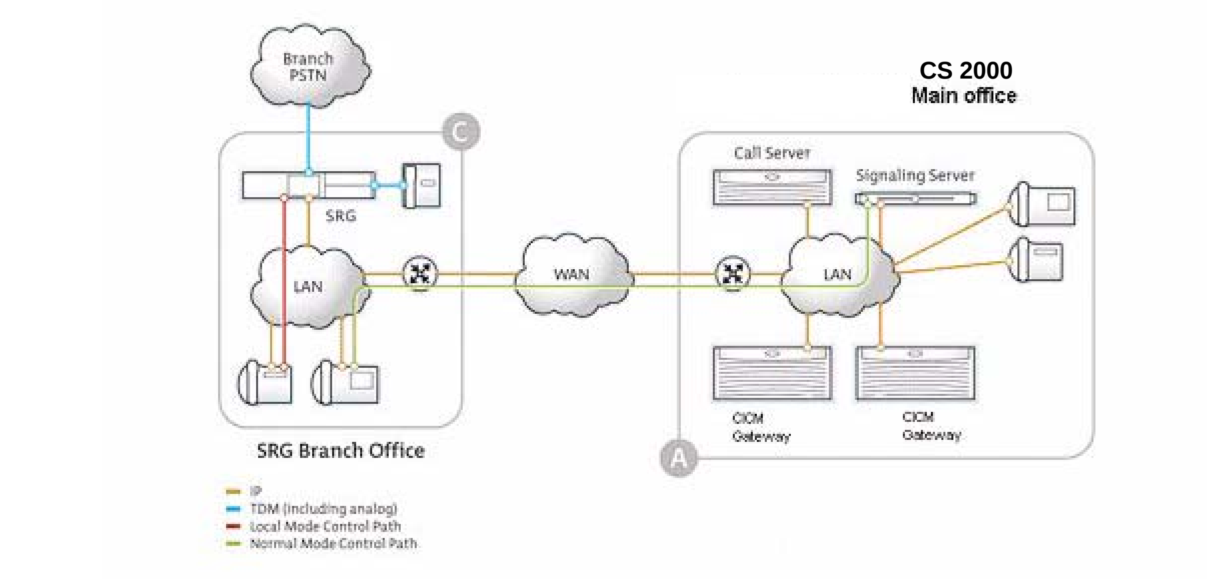
Overview of SRG

The Survivable Remote Gateway (SRG) extends Communication Server 2000 (CS 2000) features from a main office to a remote SRG location (branch office). The SRG50 operates with the Centrex IP Client Manager (CICM) gateway in a CS 2000 main office running SN08. The SRG50 is optimized for a branch office that has 5 to 32 users.

The SRG50 is a branch office of the CS 2000 main office and is part of the main office Local Area Network (LAN.) IP telephone sets are located at the SRG50 branch office, which connects to the main office using VoIP trunks across a Wide Area Network (WAN).

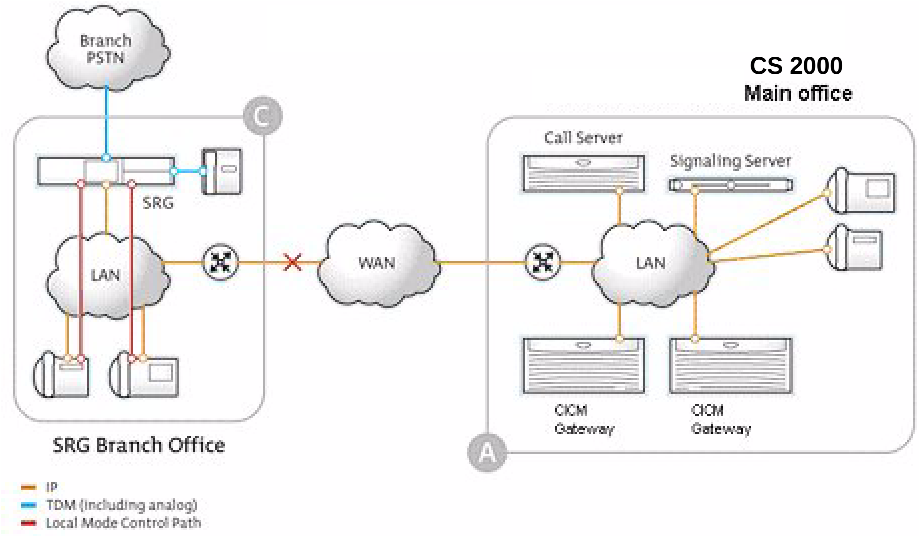
During normal mode of operation, the IP telephone sets located at the SRG50 branch office, are connected to the Centrex IP Client Manager (CICM) gateway located at the main office as shown in the figure that follows.

Figure 2 Normal mode of operation



If communication with the main office is lost either because the CICM gateway is out of service or there is a WAN failure, the IP telephone sets are redirected to the SRG50 branch office, which reverts to local mode of operation as shown in the figure that follows.

Figure 3 Local mode of operation



In local mode of operation, call processing is handled by the SRG50, and enables the IP telephones to survive the outage between the branch office and the main office. In local mode of operation, users have access to local extensions, Emergency Services and the local PSTN trunks (optional).

While in local mode of operation, the SRG50 monitors the connectivity to the CICM gateway in the main office. Once the connectivity is re-established, the SRG automatically redirects the IP telephone sets to the CICM gateway in the main office.

The sets will be held off from redirecting in the following situations:

- the set is busy on a call
- the Test Local mode timer has not expired

> ***Note:*** The Test Local mode timer can be cancelled by pressing the Stop key on the IP telephone set. The Test Local mode timer is configurable from the Main Office panel of the SRG Unified Manager.

Hardware and software requirements for SRG

For CICM interoperability with SRG, the following hardware and software are required:

- a fully configured CPV5370 or CPN5385 CICM node with Active Call Failover (ACF), and a CPV5370 or CPN5385 CICM-EM in the CS 2000 main office running the release SN08
- a fully configured BCM50 in the SRG branch office with the SRG50 keycode applied

Supported IP telephone sets for SRG

The following IP telephone sets are supported for CICM interoperability with SRG:

- Phase I IP Phones 2002 and 2004 with firmware 1.71 and above
- Phase II IP Phones 2001, 2002, and 2004 with firmware 2.49 and above

Restrictions and limitations for SRG

The following restrictions and limitations apply for CICM interoperability with SRG:

- H.323 communication between the SRG and the CS 2000 main office is not supported
- the m6350 softclient and IP Phone 2033 are not supported
- security is not available in local mode, which is when the IP telephone set is connected to the SRG
- registering IP telephone sets as redirected sets at the SRG must be done manually

References for SRG

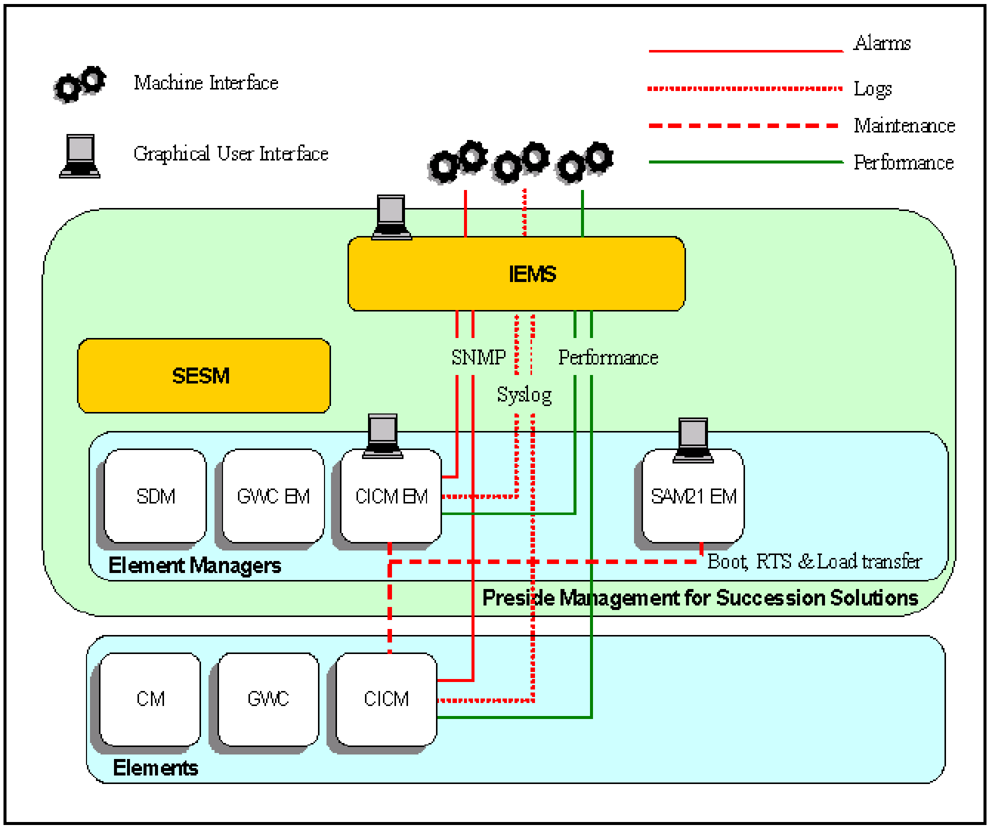
Details on how to configure the SRG branch office for CICM interoperability with SRG are provided in the document *BCM50 Configuration for Survivable Remote Gateway*, SRG50.

Integrated Element Management System

The Integrated Element Management System (IEMS) product provides Operations, Administration, Maintenance, and Provisioning (OAM&P) capabilities, particularly when it comes to interfacing with the service provider's OSS equipment. The CICM-EM and CICM nodes are compatible with Carrier Voice over IP (VoIP)'s IEMS.

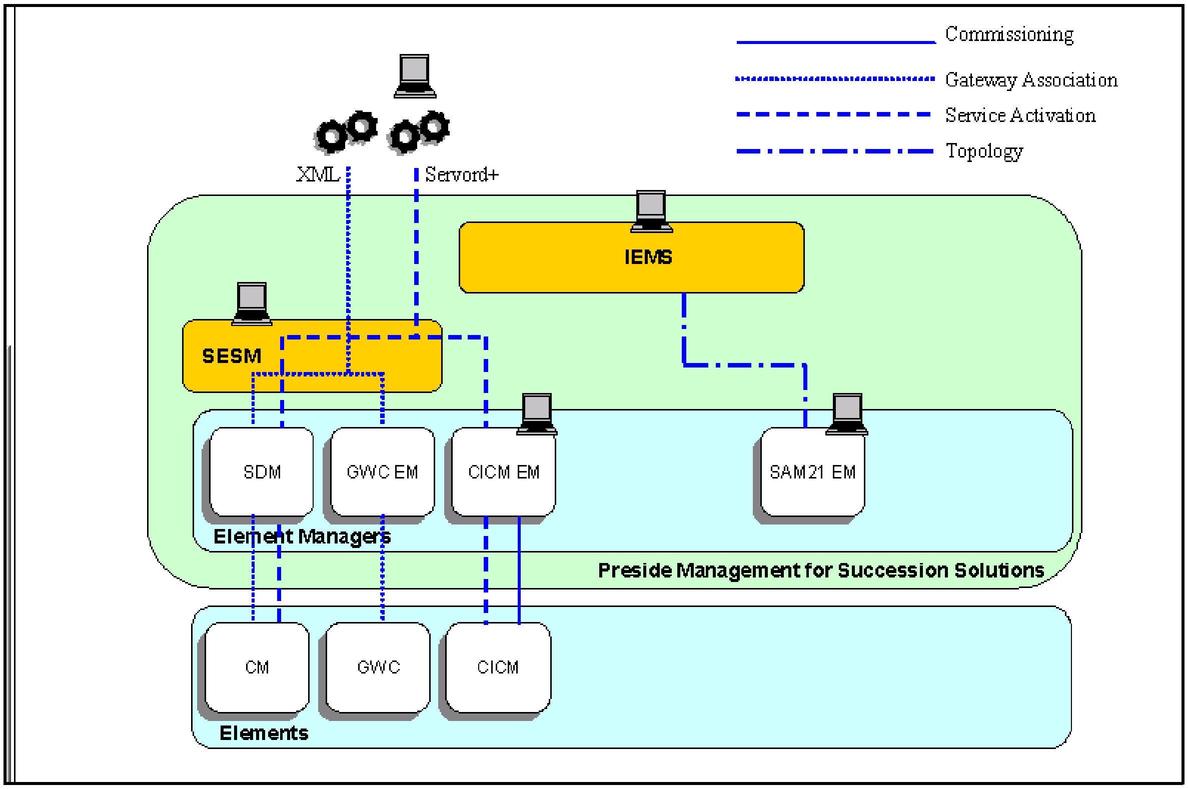
As shown in the figure Carrier VoIP CICM fault and performance overview, the IEMS takes the alarms, logs, and performance monitoring data produced by CICM and passes it to the OSS systems in a choice of industry standard formats.

Figure 4 Carrier VoIP CICM fault and performance overview



A flow-through provisioning system is implemented, as shown in the figure Carrier VoIP CICM configuration overview. It is possible in CICM SN08 to use the CS2000 Management Server OSSGate or web interface to associate a CICM with a GWC. Data is automatically propagated to all elements (in order to remove the risk of inconsistent data). Servord is no longer used to configure CICM users.

Figure 5 Carrier VoIP CICM configuration overview



Engineering information

This section provides general engineering information, including the Carrier Voice over IP (VoIP) platform, the telco central office (CO) requirements, and the Admin and Client LANs. For detailed engineering information, refer to the *Centrex IP Client Manager (CICM) Engineering Guide*, 297-5551-100.

Carrier VoIP platform

For CICM, SN08 is a combined hardware and software release based on Carrier Voice over IP (VoIP) release (I)SN08. It applies to both International and North American customers.

Central Office requirements

CS2000 platform software dependencies

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

The software dependencies of CICM SN08 are listed in the table Software load configuration.

Table 2 Software load configuration

System	Minimum software load	Recommended software load
CICM	8.0	8.0
CICM-EM	8.0	8.0
CS2000	(I)SN08	(I)SN08
CS2M (SDM)	CS2M0080	CS2M0080
GWC	GC080	GC080
IEMS	(I)SN08 IEMS	(I)SN08 IEMS
IP Phones 2002, 2004 (Phase I)	1.57	1.74
IP Phones 2001, 2002, & 2004 (Phase II)	3.45	3.91
IP Phone 2033	8.0	10.0
M6350	7.0	8.0

Hybrid CS2000 platform

For SN08 CICM is not supported when connected on the hybrid side of an SN08 XACore.

Interworking limitations

The CICM does not support mid-call Session Description Protocol (SDP) renegotiation, and therefore does not interwork to the following services which rely on mid-call SDP renegotiation:

- Multimedia Communication Server (MCS) Click to Call
- Multimedia Communication Server (MCS) Auto Announcement

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 master Element Manager (EM) and the slave CICM-EM. 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's Administration LAN must provide the following resources:

- direct connection to the master and the slave
- a PC for performing configuration, administration, and monitoring
- isolation of the Administration LAN from the Client LAN
- secured remote access to the CICM-EMs for Nortel 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 connection 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. The media end points in a Carrier Voice over IP (VoIP) IP network include:

- CICM terminals (IP Phone 200x and 2033)
  - — hosted by the same CICM
  - — hosted on another CICM
- TDM trunk gateways (for example, MG 15000)
- analog line gateways (for example, MG9000, Mediatrix 1124)
- voice processing servers (for example, 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.

Ping 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 CICM-EM node through the Admin network is password protected. Access to the administration web pages on the

CICM-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 through 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 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 (through 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 (CICM) Engineering Guide*, 297-5551-100.

NAT traversal

Nortel's 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 RTP Portal usage summary provide a summary of the RTP portal usage.

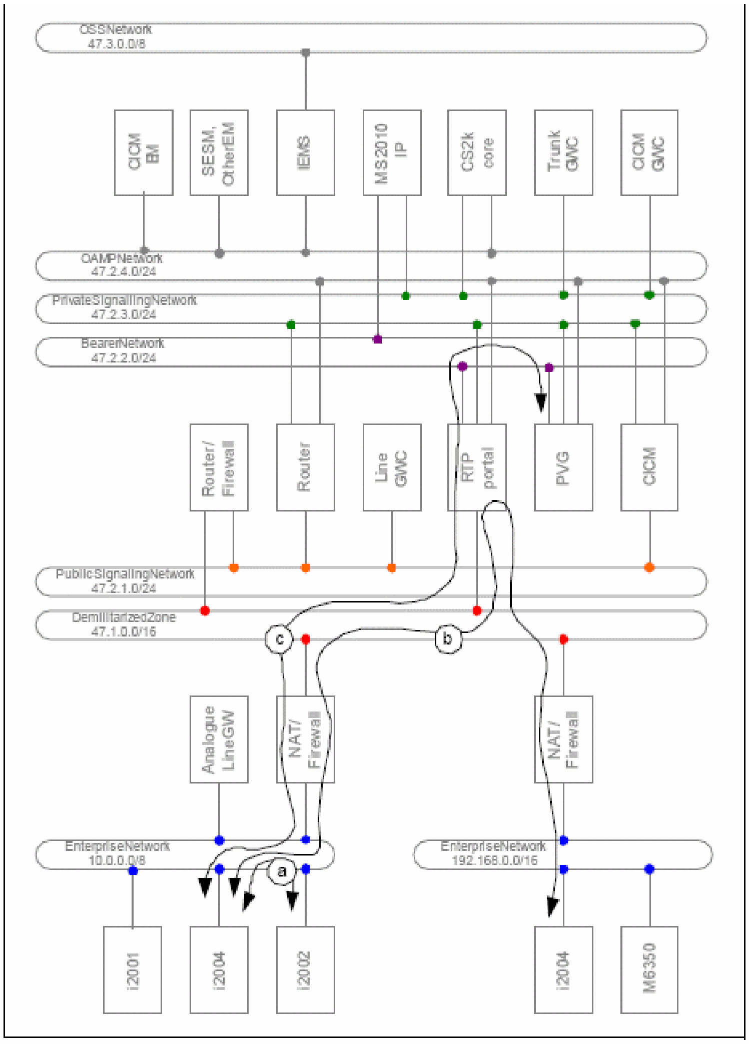
Table 3 RTP Portal usage summary

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 CS2000	Does not matter	Yes

The 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 Public Switching Telephone Network (PSTN) trunk (hosted from a MG 15000)

Figure 6 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 (CICM) Engineering Guide*, 297-5551-100.

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 wants to test whether a client PC or IP Phone 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 through 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*, NN10248-711. For related engineering details, refer to the *Centrex IP Client Manager (CICM) Engineering Guide*, 297-5551-100.

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*, NN10233-911. For additional details, refer to the *Centrex IP Client Manager (CICM) Engineering Guide*, 297-5551-100.

Architectural resiliency

In the SAM21-based CICM, the two CICM nodes operate in an active and hot standby mode with 1+1 redundancy. The two nodes act as a single entity towards the core GWC for H.248 private call signaling, towards IEMS and other related OAM/P interfaces, and towards clients for public signaling interfaces through UNIStim. Failure of one node won't have any service impact (that is, no impact to any of the communications towards GWC, towards OAM/P systems, and towards clients), and no impact on any active (stable) calls.

Software resiliency

The CICM uses Microsoft Windows XP as its operating system (OS).

Only the core components of the OS are used, for which reliability has been tested and proved over a decade of use in millions of installations. No graphical user interface is provided, thus reducing the likelihood of unexpected conditions as well as the number and complexity of the components running on the system.

To provide a highly stable platform for the CICM software, third party drivers on the CICM are limited to those required to manage the resource cards and chassis, and they are strictly controlled and tested.

Additionally, the CICM software constantly performs sanity checks on software operations for unexpected or rare conditions. Failures generate Informational, Warning, or Error logs, which can help resolve any reported problems.

System availability

The SAM21-based CICM is designed to meet the 99.999% system availability requirement, with the Call Path Downtime Performance Measure (DPM) less than 1.5 minutes per year.

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 Ethernet Routing Switch 8600s. In addition to supporting the CS2000 and other CS2000 components, the dual-Ethernet Routing Switch 8600s provide the LAN connections between the CICM and:

- The telco's administrative LAN, which includes the master and slave CICM-EM pair.
- The client LAN.

The CentrexIP Client Manager can be collocated with or sited remotely from the CS2000 GWC. Nortel recommends collocating the CICM with the CS2000.

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, electromagnetic compliance (EMC) standards, and telecom center installation standards including Neywork Equipment Building System (NEBS) and European TTI Standards Institue (ETSI).

For additional information on engineering standards, compliances and non-compliances, and compliance testing, refer to the *Centrex IP Client Manager (CICM) Engineering Guide*, 297-5551-100.

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

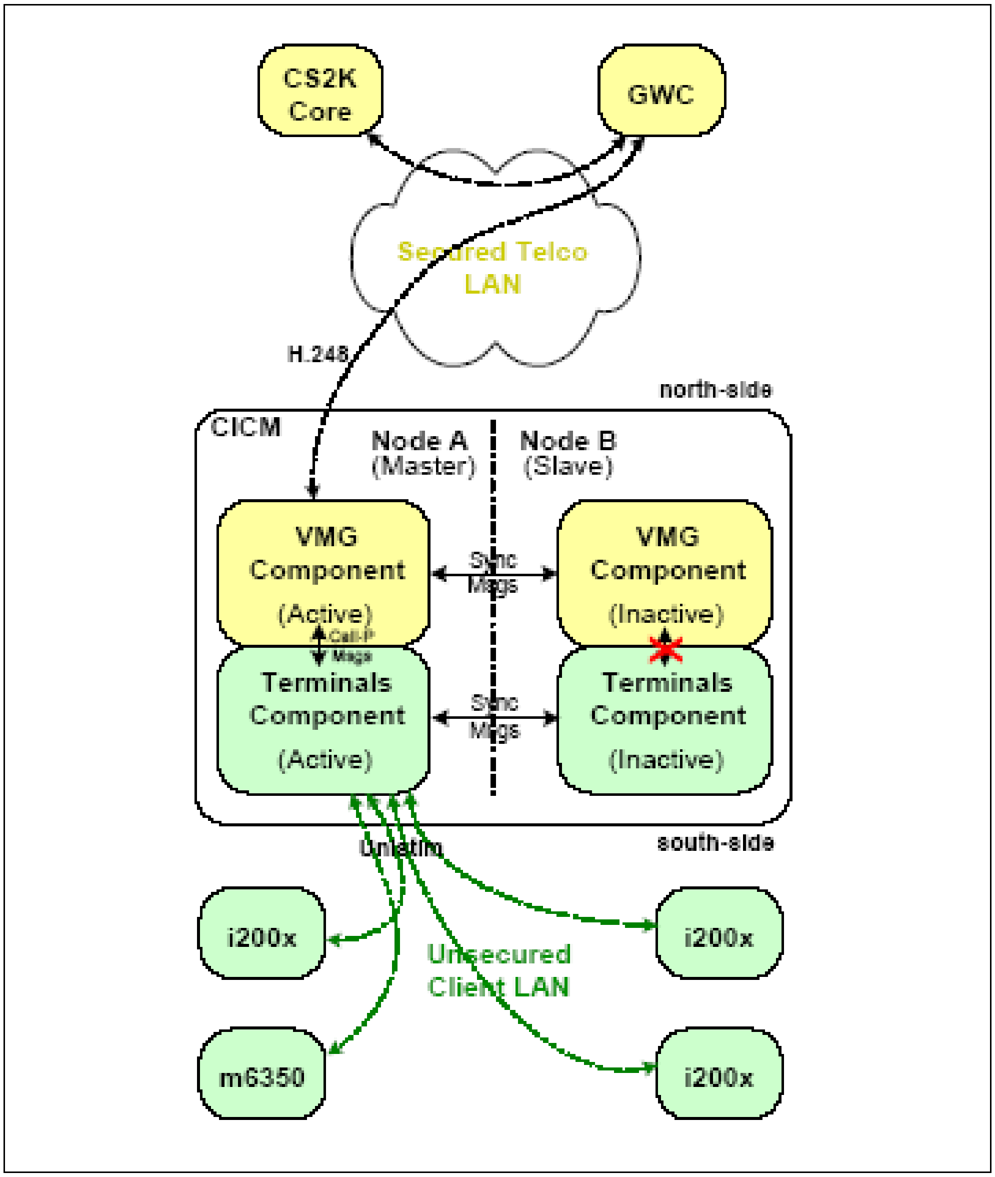
Carrier VoIP and Carrier CICM

The release (I)SN08 supports the Carrier Voice over IP (VoIP) (CS2000) version of CICM.

Redundancy

The redundancy provided by the CICM is best understood in terms of the software components that make up the CICM, as shown in the figure CICM redundancy model.

Figure 7 CICM redundancy model



This figure shows that each CICM node (that is, each half of the gateway) executes an identical software load.

The GWC facing side of the CICM (or north side) communicates with the GWC using the H.248 protocol through a single interface. Likewise, the south side communicates with all terminals hosted by the CICM using the UNIStim protocol through a single interface.

Thus, both the H.248 and UNIStim interfaces each make use of their own floating IP address that is bound dynamically to the master node's interface. Each component shown in the figure *CICM Redundancy*

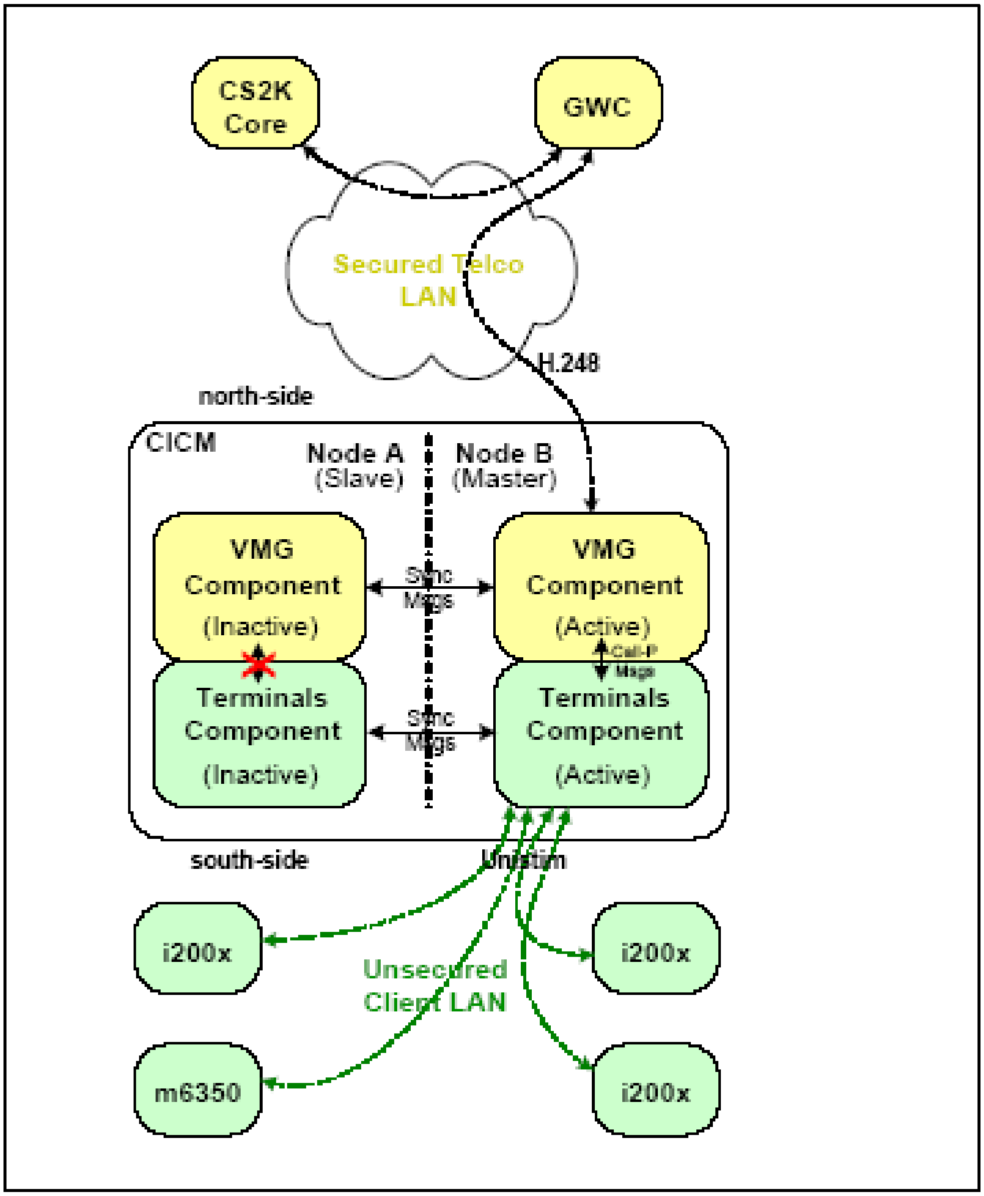
Model is responsible for managing its floating address and ensuring it is swapped to the mate on a switch of activity (SWACT).

The inactive VMG component keeps in constant near-full synchronization with the active side (shown by the double-headed arrow in the figure *CICM Redundancy Model* above). This ensures that both nodes know the state of call processing at any time, and that the inactive side can take control of all functions on a switch of activity.

SWACT

A switch of activity (SWACT) occurs when the role of the master node is transferred 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 shown in the figure CICM following a switch of activity.

Figure 8 CICM following a switch of activity



A platform switch of activity is carried out internally one component at a time. The process begins with the VMG and ends with the Terminals component. It is therefore possible that as the switch of activity is in progress, one node may find itself hosting the active VMG component while simultaneously hosting the inactive Terminals component. This is a transient state, and carried out automatically over the entire platform such that once completed, both nodes will have entirely exchanged roles. It is not under the direct control of the operator to select individual components and their order of switching.

As part of the SWACT, it is the responsibility of the CICM to ensure that the floating H.248 and UNIStim IP addresses are moved to the newly promoted master. This is necessary in order to ensure continued communication with both the GWC and terminals.

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 in such a circumstance.

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 lose 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 mis-dialled call.

Hardware of the CICM and CICM-EM

This section describes the hardware components of CICM and CICM-EM.

Hardware overview

For SN08 the 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 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 CS 2000.

The CS2000 deployment can use dual-Ethernet Routing Switch 8600s. It is recommended that the CICM also uses these switches to provide network connectivity.

Hardware frame

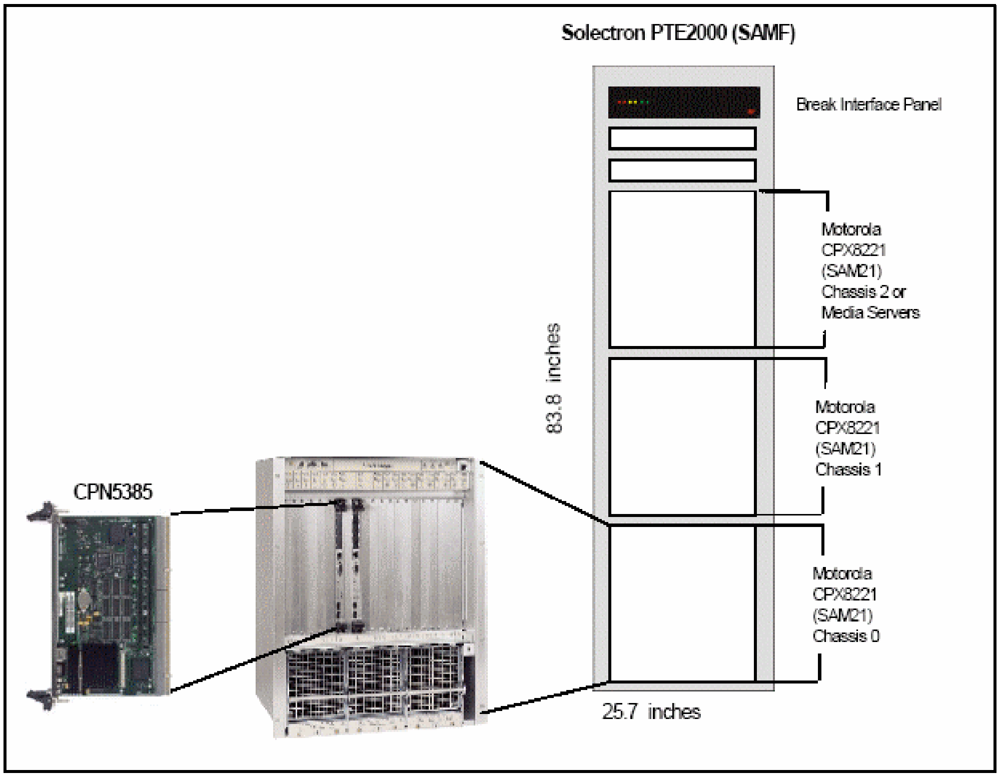
The CICM is shipped as a set of components fitted into a standard NEBS3 compliant frame (also called a cabinet). CICM release SN08 uses the SAMF and CCS frames.

SAMF Frame

The SAMF frame is shown in the figure SAMF Frame. The characteristics of the SAMF frame are:

- NEBS3 compliant
- Configurations supported:
    - up to 3 SAM21 Chassis
    - 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:
    - one CICM-EM card (Motorola CPN5385 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 9 SAMF Frame


Solectron PTE2000 (SAMF)
Break Interface Panel
Motorola CPX8221 (SAM21) Chassis 2 or Media Servers
Motorola CPX8221 (SAM21) Chassis 1
Motorola CPX8221 (SAM21) Chassis 0
83.8 inches
25.7 inches
CPN5385

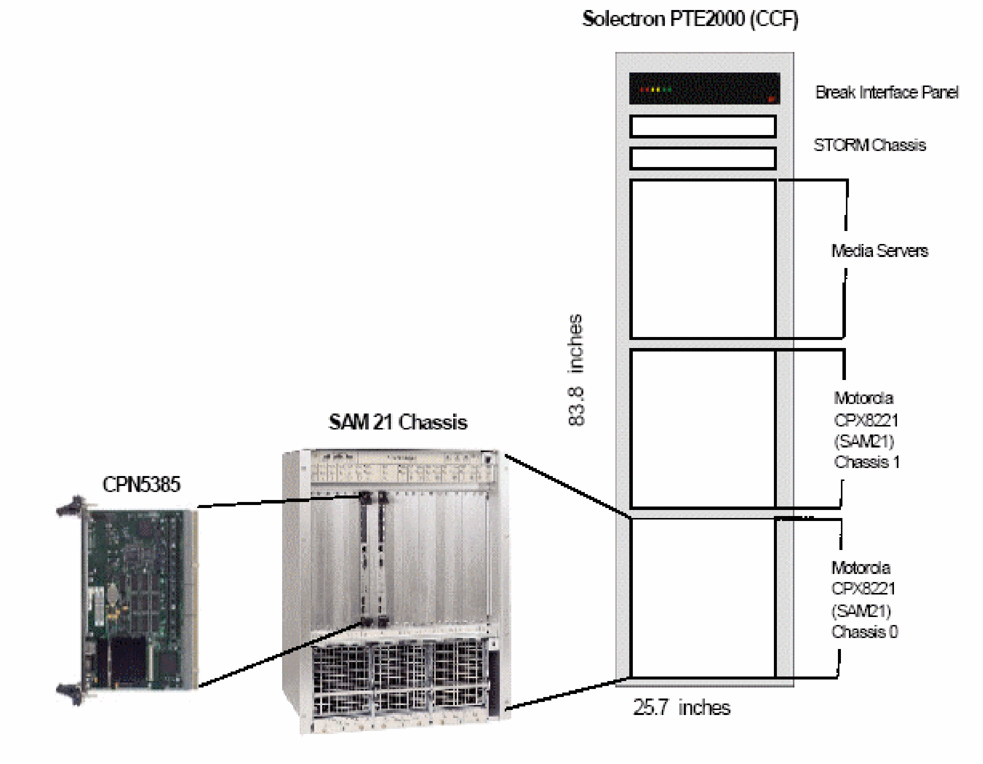
CCF Frame

The CCF frame is shown in the figure CFF 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.
  - — one CICM-EM card (Motorola CPN5385 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.

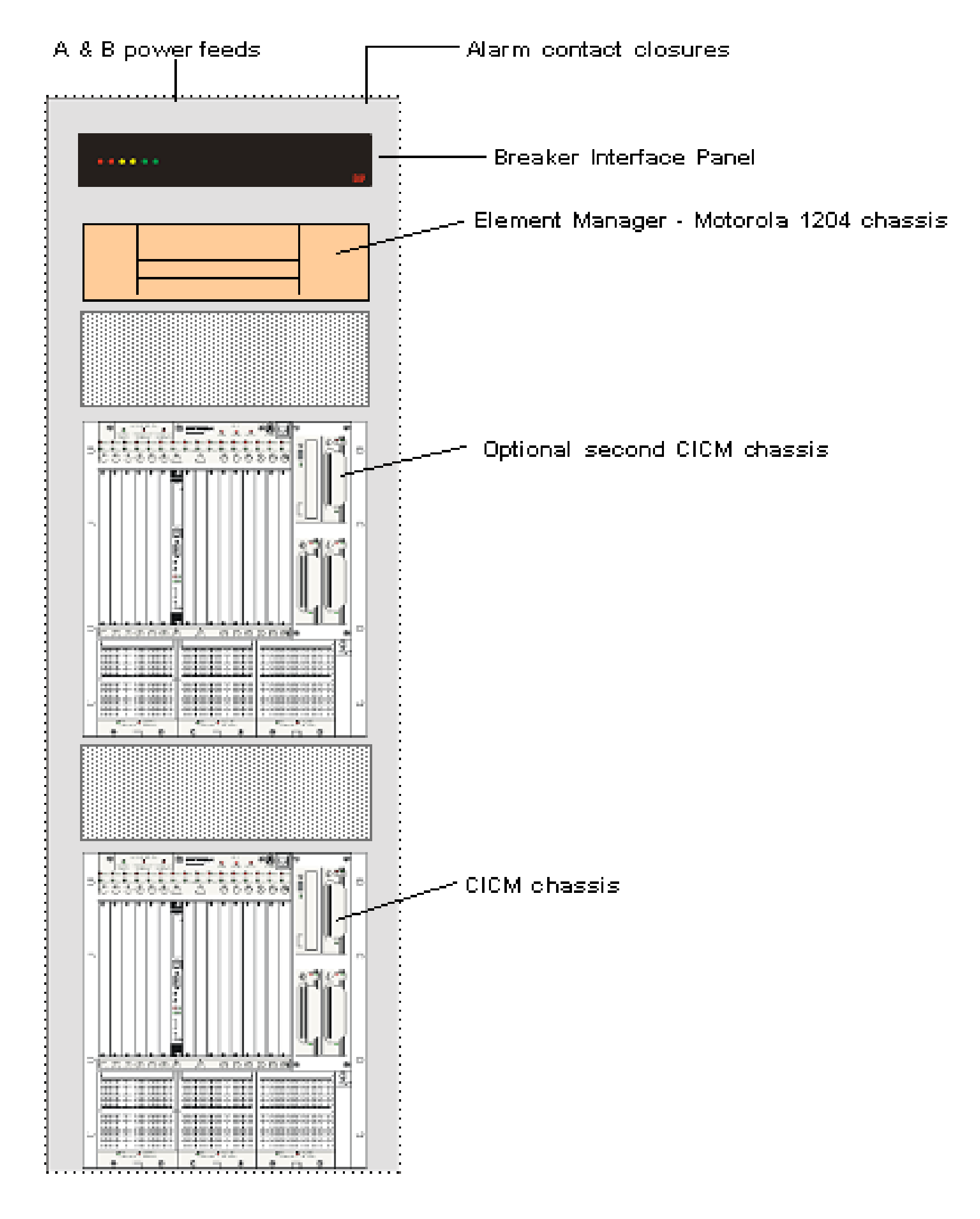
Figure 10 CFF Frame



CICM cabinet

The CICM hardware for a SAM16 platform is shipped in a NEBS-compliant 19-inch wide PTE 2000 frame, as shown in the figure Two SAM16 chassis with hardware in PTE 2000. The frame includes a power unit (BIP), element manager in a Motorola 1204 chassis, and one or two SAM16 chassis.

Figure 11 Two SAM16 chassis with hardware in PTE 2000



Element Manager

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

The functions of the CICM-EM include:

- operating in a redundant pair where one EM is the master and the other is a slave
- 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 in-service backup process
- providing storage for user profiles and CICM software upgrades
- storing the firmware upgrade files for the IP Phones 2001, 2002, 2004, and 2033, plus 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 CICM-EM supplies the absolute time and each CICM applies local timezone corrections.

In the SAM21-based CICM release SN08, the CICM-EM is a pair of Motorola CPN5385 resource cards; one active and the other hot standby for redundancy. Although a CICM node requires only one CICM-EM, Nortel configures EMs in pairs to provide redundancy and to avoid a single point of failure.

In the SAM16-based CICM release SN08, the CICM-EM is the whole chassis with all cards plugged into it (the CPU, hot swap controller, disks, etc).

Only one pair of the CICM-EM resource cards is required per CS2000, which is capable of supporting up to 100 pairs of CICM resource cards (nodes). The slave (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 CICM Element Manager (CICM-EM) is supplied with a Backup and Restore Tool (BRT) that allows the administrator to take offline disk images of both the CICM and CICM-EM. Since this tool requires a shutdown of the EM, its use temporarily prevents access to the web-based administration interface to the slave EM.

The CICM-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 CICM Element Manager (CICM-EM) 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 through 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 OS machine with the appropriate access rights on the service provider's Admin LAN, using a combination of Windows OS remote management functions, and the Nortel CICM management tools accessed through the CICM-EM web pages. refer to the *CICM Configuration Management*, NN10240-511 and *CICM Administration and Security*, NN10252-611 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 CS2000.

<u>Admin LAN redundancy</u>

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.

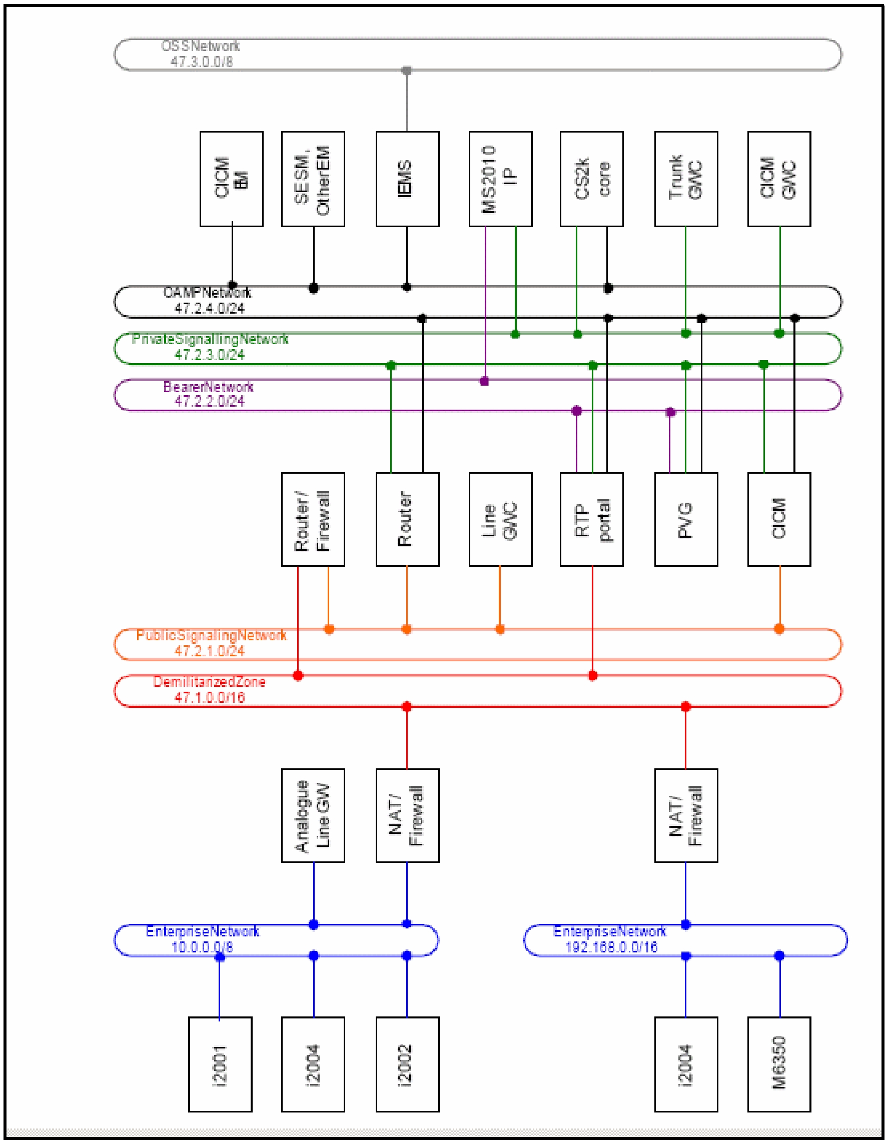
If all the CICM Ethernet ports are connected to a single Ethernet switch, this switch becomes a potential single point of failure. If the switch fails for any reason, or a cable or adapter becomes faulty, the two nodes of the CICM would no longer be able to communicate with each other. In this situation, 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.

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 Ethernet Routing Switch 8600s rather than one. These switches can then be connected to the rest of the telco’s network. The figure CICM in the CS2000 network provides a reference network for CICM in the CS2000 environment.

Figure 12 CICM in the CS2000 network



The sub-networks shown in the figure *CICM in the CS2000 Network* 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 (for example, CS2000 core to trunk GWC), except those that require connectivity to devices outside the Central Office (for example, GWC serving remote analog 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 Carrier Voice over IP (VoIP) 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 CICM in the CS2000 network 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 MG9000. Therefore a CICM can share a GWC with another CICM, or an MG9000, 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 through the OSS Network. The Northbound CICM-EM interface is accessed through Secure Proxy through the IEMS.

Refer to the *Centrex IP Client Manager (CICM) Engineering Guide*, 297-5551-100 for further details.

Network interfaces

CICM interfaces

Each CICM node uses a CPN5385 processor card with three physical network interfaces. The table CICM interface summary provides a mapping of the physical characteristics of the CPN5385 to a set of logical interfaces used by the CICM.

Table 4 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 Carrier Voice over IP (VoIP) CICM exposes four IP addresses to the rest of the Carrier VoIP network. One address on each node is 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 CICM IP Addresses provides additional details.

Table 5 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

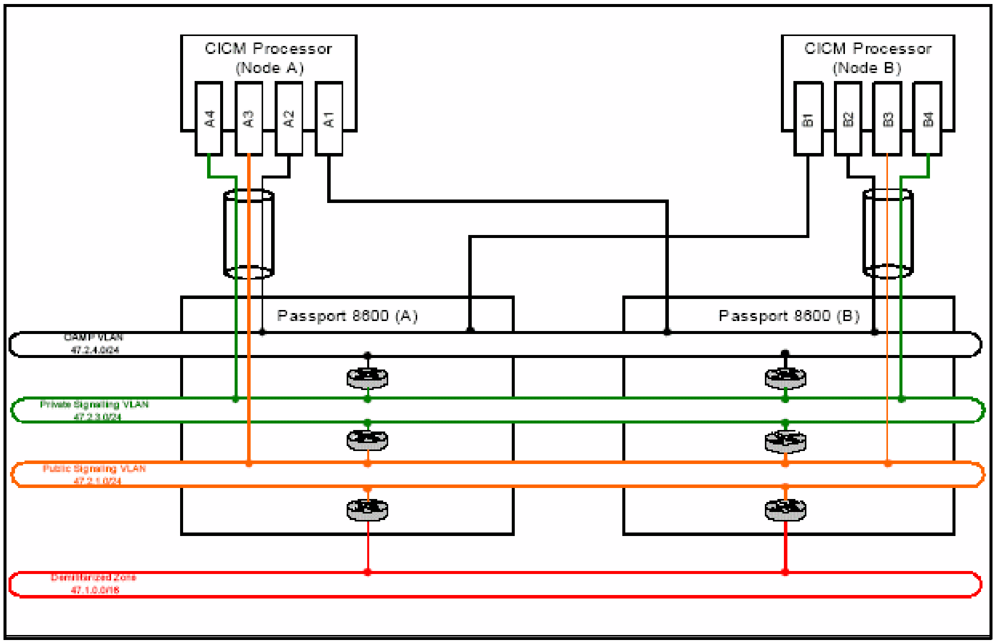
The CICM requires eight system IP addresses: one for each of the logical adapters on each of the CICM nodes (SA1-SA4 and SB1-SB4 on nodes A and B, respectively).

The 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 Carrier VoIP 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 (for example, 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 Ethernet Routing Switch 8600, as shown in the figure 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 13 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) through 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 Carrier Voice over IP (VoIP) 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 CICM-EM interfaces.

Table 6 CICM-EM interfaces

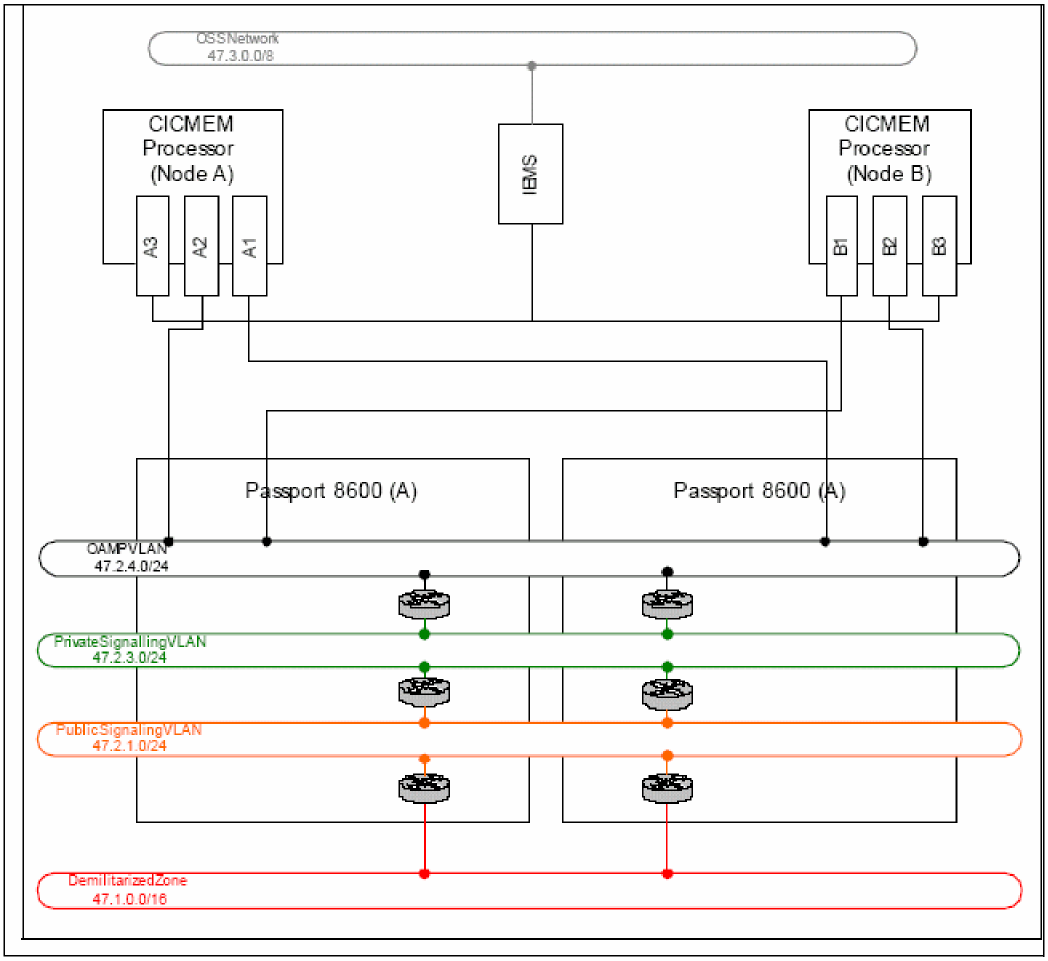
Network	IP addresses	Logical interface	Purpose
O (OSS)	O	Adapter 3 on Node A or Node B	OSS machine and GUI interfaces ***Note:*** This access is through secure proxy through the IEMS.
P (CICM Administration)	PA	Adapter 1 or Adapter 2 on Node A	Node A OAMP and inter-node signalling
	PB	Adapter 1 or Adapter 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 Graphical User Interface (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 CICM-EM Network Connectivity.

Figure 14 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 CS2000 management platform; therefore with a single SC2K node. Even if the CS2000 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 Carrier Voice over IP (VoIP) 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.

UNIStim Interface

The Carrier Voice over IP (VoIP) variant of the CICM exposes a single UNIStim (Client) LAN IP address. This address is used for all signalling to and from terminals managed by the CICM. This floating address is also dynamically managed and is always bound to the master’s UNIStim interface.

The CICM also supports an independent VLAN specifically intended for all UNIStim traffic. Each node therefore implements a virtual network interface to host this VLAN.

CS-LAN Routing Switches

The SAM21-based CICM release SN08 must be collocated with the CS2000. As such, the CICM can leverage on the CS2000 CS-LAN infrastructure, which consists of two Ethernet Routing Switch 8600. In addition to supporting the CS2000 Core and other CS2000 components, the dual 8600s 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 Ethernet Routing Switch 8600 being used in Carrier Voice over IP (VoIP) CS2000 CS-LAN deployment is:

- 10-slot Multiservice Switch 8010CO chassis on a Multiservice Switch 7480 Universal Frame
- One Multiservice Switch 8691SF CPU Module
- Two Multiservice Switch 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:

- Multiservice Switch 8632TXE Routing Switch Module supporting 32 Fast Ethernet ports
- Multiservice Switch 8648TXE Routing Switch Module supporting 48 Fast Ethernet ports
- Multiservice Switch 8608GBIC Routing Switch Module supporting 8 Gigabit Ethernet ports (mostly for WAN interface)
- Multiservice Switch 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 CS2000 CS-LAN in dual-Ethernet Routing Switch 8600s are:

- NEBS-3 compliance
- superior reliability with 99% availability
- up to 128 Gbit/s 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 CS2000 as a VMG unit. A client can initially log on to the master CICM node through a floating UNIStim IP address and receive service. With the master and a slave node operation, the CS2000 send messages only to the master CICM node.

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, while the other is a hot-standby slave).

If one of the CICM nodes becomes unusable (for example, due to a hardware failure or during an upgrade), the hot-standby node can still be used to provide service. During the switch of activity, calls are maintained and actively recovered by the mate.

The figure CICM redundancy model shows the model used for dual node operation.

CICM chassis

The CICM is housed in a Motorola CPX8216T chassis (SAM16) or in a PTE 2000 frame (SAM21). Examples of the chassis are shown in the figures CICM chassis of a SAM16 and CICM chassis of a SAM21.

> ***Note:*** These figures are exemplary, which means the position, number, and version of each card in the chassis may be different.

Figure 15 CICM chassis of a SAM16

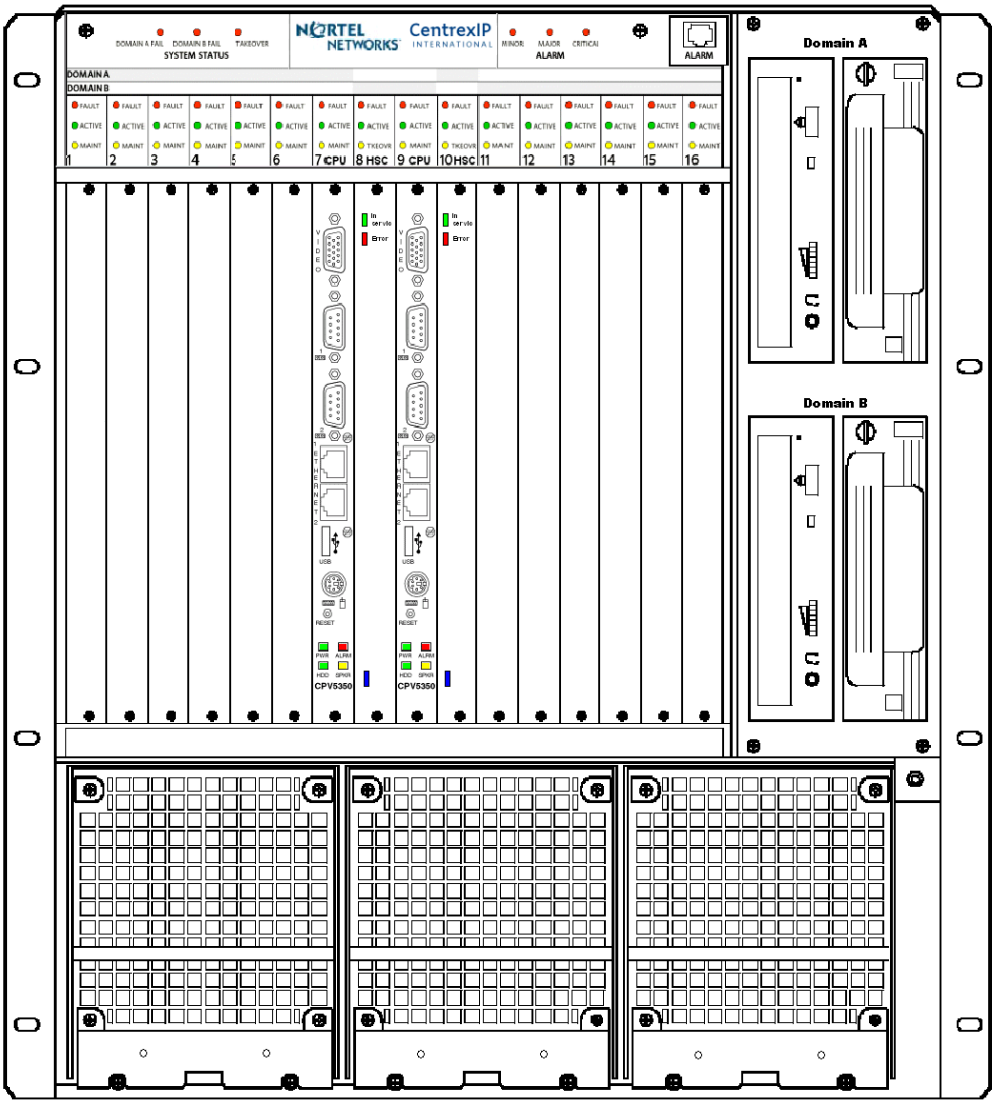
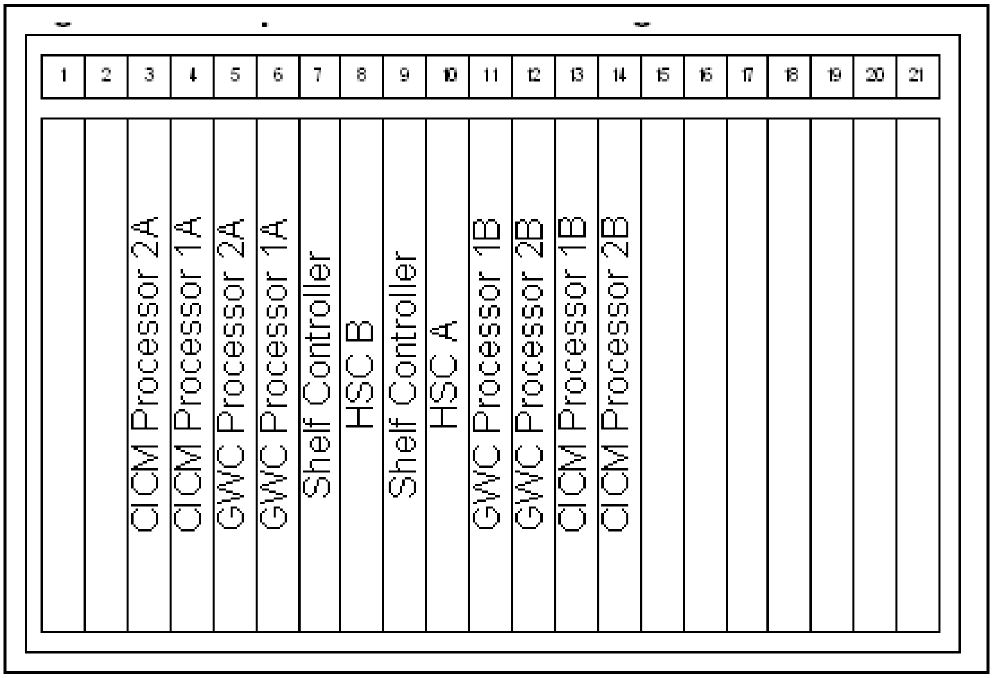


Figure 16 CICM chassis of a SAM21



The 8.0 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 node-pair for a SAM16 is split into two domains: Domain A and Domain B. Each domain is controlled by its own processor card running the Windows XP operating system and CICM software. From the software perspective, each domain is regarded as a separate CICM node.

Any 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 procedure “Restart (soft reboot) the node” in *CICM Fault Management*, NN10233-911.

All major hardware components of the CICM can safely be inserted or removed while powered up (hot-swapped), although a restart is required before an inserted card is available for use by the CICM software.

Telephony bus

The Motorola CPX8216T chassis for a SAM16 includes an integrated H.110 telephony bus. (The SAM21 has cPCI instead of H.110.)

CPU cards

For release SN08, the single backplane chassis contains two separate PCI bus domains (A and B), each with its own CPV5370 Intel processor card running the Windows XP operating system.

Each Central Processor Unit (CPU) card in a SAM16 has an Intel Pentium III BGA2 MMX processor at 700 Mz 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).

Each CPU card in a SAM21 has an Intel Pentium III processor at 1200 MHz with 512 MB ECC protected DDR SDRAM (266 MHz).

The CPV5370 processor card has provision for supporting a single PMC daughter card, which can be used to provide additional processing power.

The CPU tasks in either a SAM16 or a SAM21 shelf 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 master CICM-EM

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:*** With one switch, if there is failure, the two CPU cards will not be able to communicate with each other through the Admin LAN. Each CPU card will then tell Carrier Voice over IP (VoIP) that its mate node is missing, and Carrier VoIP will take both nodes out of service.

The CICM release SN08 should be collocated with the CS2000. As such, the release can use the CS2000 CS-LAN infrastructure, which consists of two Ethernet Routing Switch 8600s. In addition to supporting the CS2000 Core and other CS2000 components, the dual-8600s provide the LAN connections between the CICM and:

- the service provider’s Admin LAN, which includes the master and slave CICM-EM
- the client LAN

The base configuration of the Ethernet Routing Switch 8600 being used in Carrier VoIP CS2000 CS-LAN deployment is:

- a 10-slot Multiservice Switch 8010CO chassis on a Multiservice Switch 7480 Universal Frame
- one Multiservice Switch 8691SF CPU Module
- two (2) Multiservice Switch 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:

- Multiservice Switch 8632TXE Routing Switch Module supporting 32 Fast Ethernet ports
- Multiservice Switch 8648TXE Routing Switch Module supporting 48 Fast Ethernet ports
- Multiservice Switch 8608GBE GBIC Routing Switch Module supporting eight (8) Gigabit Ethernet ports (mostly for WAN interface)
- Multiservice Switch 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 CS2000 CSLAN in dual-Ethernet Routing Switch 8600s are:

- NEBS-3 compliance
- superior reliability with 99.99999% availability
- up to 128 Gbit/s 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. The Ethernet switches must provide support for 802.1Q VLANs. The CS2000 deployment uses dual Ethernet Routing Switch 8600s, and Nortel recommends that the CICM release SN08 also use 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.

Refer to the *Centrex IP Client Manager (CICM) Engineering Guide*, 297-5551-100 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 access networks. CS2000 supports the following types of access through 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 analog subscriber lines only
    - analog line access through a variety of gateway types, including CPE gateways attached to customer LANs or cable networks
    - ADSL access through 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 (for example, 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 through 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 through inter-CS signalling, also based on packet network protocols

For additional information on the CS2000, refer to the *CS2000 Product Description*, cs2000cPDISN07.

CICM node in the Carrier Voice over IP network
The CICM node provides the control interface between the gateway controller (GWC) and distributed CICM IP clients on a managed IP network. It communicates with the GWC using the H.248 IP interface.

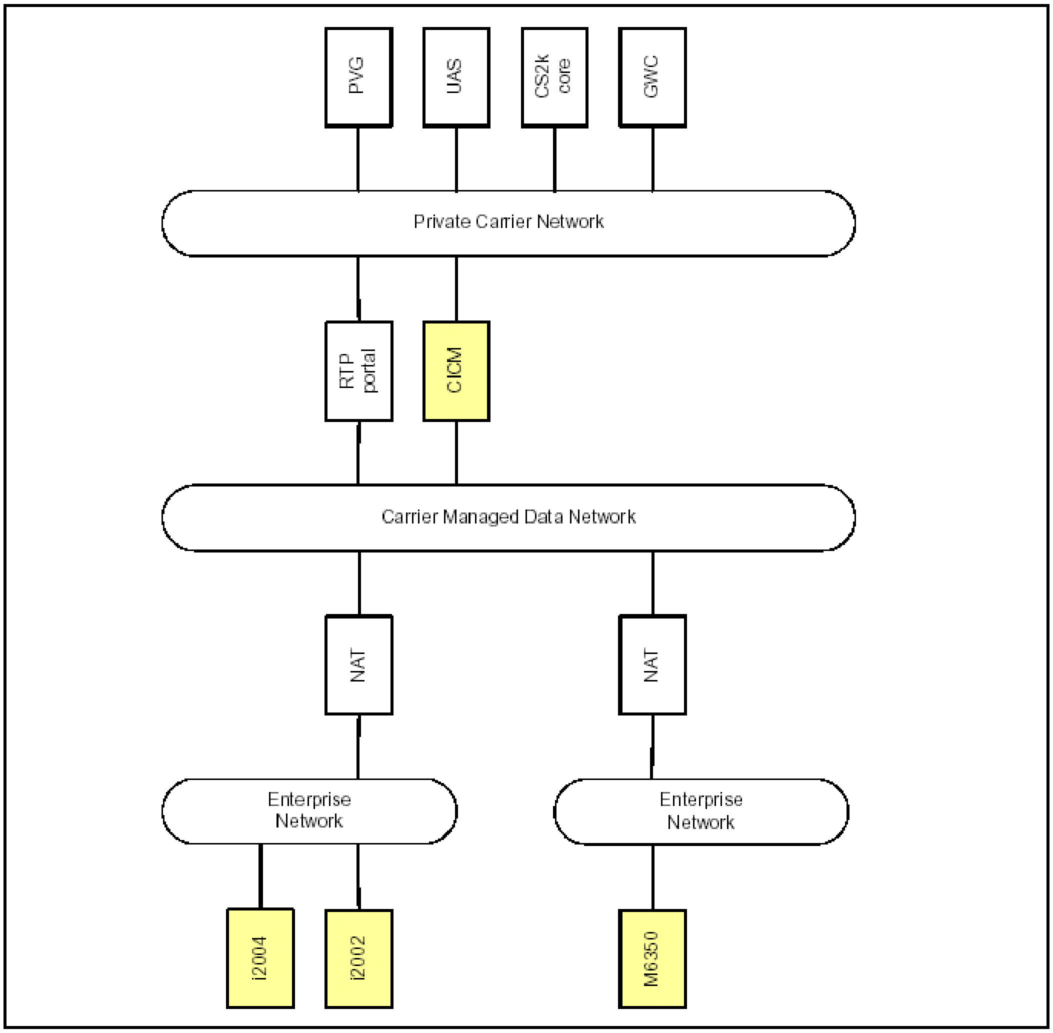
H.248 is a joint ITU-T and IETF protocol defined in ITU-T Recommendation H.248 and IETF RFC3015. It fully supports the same basic device/media control capabilities as protocols such as ASPEN. More importantly, it is based on a more flexible functional mode that provides better support for multimedia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

The CICM node is not a media gateway. It is better described as a terminal server or signaling gateway. Media streams in a Carrier VoIP solution are routed directly between media end-points. The CICM terminals (for example, IP Phone 2004) are media end-points. Other media end points in a Carrier VoIP network include:

- TDM trunk gateways (for example, MG 15000)
- analog Line gateways (for example, MG9000, Mediatrix 1124)
- voice processing servers (for example, UAS)
- IP Terminals hosted off another CICM

The figure CICM and clients in the Carrier VoIP network shows a generic Carrier VoIP network with a CICM serving IP terminals in two enterprise customer networks. The figure shows general connectivity only, and not the details of network engineering.

Figure 17 CICM and clients in the Carrier VoIP 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 through 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

Ethernet Routing Switch 8600 routers provides the connectivity and routing capabilities of the CS-LAN.

The CICM release SN08 should be collocated with the CS2000. When it is collocated, the CICM release can use the CS2000 CS-LAN infrastructure, which consists of two Ethernet Routing Switch 8600s. In addition to supporting the CS2000 Core and other CS2000 components, the dual-8600s provide the LAN connections between the CICM and:

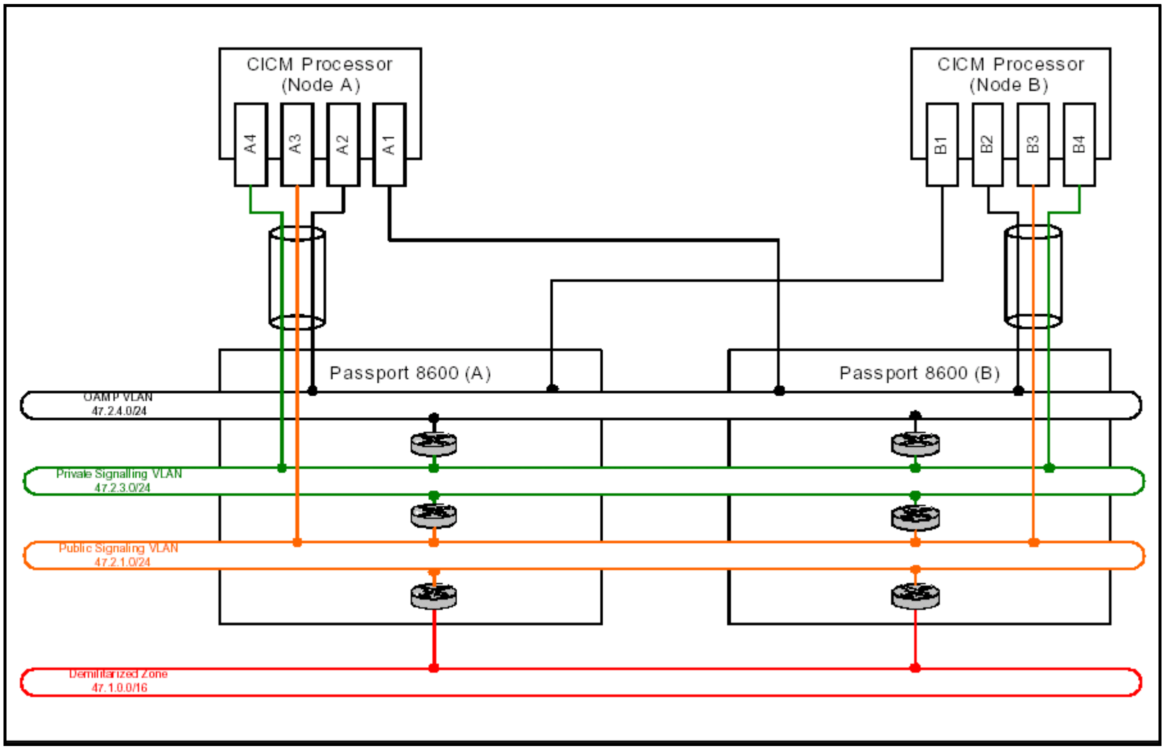
- the telco's administrative LAN, which includes the master and slave Element Managers
- the client LAN

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 Multiservice Switch restricts the routing capabilities to achieve the highest available level of security.

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

The figure Network connectivity for LAN redundancy shows a typical deployment scenario for the Carrier Voice over IP (VoIP) CICM in a central office. The figure is associated 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 18 Network connectivity for LAN redundancy



IP Addressing

Assuming the network configuration provided in the figure *Network connectivity for LAN redundancy*, the table IP addressing example, provides an example of the IP addresses required by a pair of CICM processing nodes.

Table 7 IP addressing example

Network	IP address	Interface	Description	DHCP support
OAMP	47.2.4.100	A1	Node A OAMP address	No
	47.2.4.102	B1	Node B OAMP address	No
Private Call Signaling	47.2.3.100	A4 or B4	H.248 signaling address	No
Public Call Signaling	47.2.1.100	A3 or B3	UNIStim signaling address	No
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 table CICM network interfaces summarizes the redundancy model used for each network interface on the CICM.

Table 8 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.	N/A
UNIStim signaling	terminals	The dual node architecture of the CICM is hidden to the terminals because a single address is shared across the pair of nodes. The state of the public signaling interfaces (A3 and B3) 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 and the terminals are recovered on the new master node.	up to 5 minutes, depending on the number of connected terminals and the current BHHCA of CICM.
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 to 2 seconds
Inter-node communications	mate CICM processor	A virtual private network between the two nodes is maintained across adapters A1, A2, B1, and B2.	1 to 2 seconds

Hardware configuration

The SN08 hardware configuration includes:

- 2 Motorola CPV5370 Intel CPU cards for SAM16
- 2 Motorola CPN5385 Intel CPU cards for SAM21

CICM software

This section defines the software loads, delivery, upgrades and maintenance releases applicable to CICM SN08.

Software loads

The base load for CICM is release (I)SN08.0.

A release SN08 CICM-EM can manage releases SN07 or SN08 in CICM nodes provided both nodes of the configured pair have the same software version.

Software upgrades

The types of software upgrades are either a product release upgrades or a Maintenance Release (MR) upgrade. A product release upgrade increments the release number. An MR upgrade increments the build number within the same release. The software upgrade versions and the procedures to do an upgrade are identified in “Preparing to upgrade CICM” in *Upgrading CICM*, NN10230-461.

CICM clients with the IP Phones or m6350 SoftClient

This section provides an overview of the CICM clients and the Nortel IP Phones or the m6350 SoftClient software they use. A VoIP call can be initiated from either a software client or a hardware client. Nortel’s software client is called the m6350 SoftClient, which is set up and run from a personal computer (PC). The hardware clients include IP Phone models, which are connected directly to a client LAN or to a telephony switch module.

For installing or using CICM clients, refer to the documents for IP Phones and the m6350 SoftClient in Related documents.

An administrator can prevent clients from logging into the CICM node if they do not have the required level of software (in the m6350) or firmware (in the IP Phones 200x and 2033). The CICM administrator may also configure the CICM to upgrade the terminals automatically, in a controlled manner. The procedure to upgrade IP Phone firmware is in *Upgrading CICM*, NN10230-461.

The topics in this section are:

- Datafilling to use IP Phones and m6350 SoftClient
- UNIStim with IP Phones and m6350 SoftClient
- Codec with IP Phones
- IP Phone models
- Functional components of IP Phones
- User interface of IP Phones
- Hardware feature comparison of IP Phones
- m6350 SoftClient

Datafilling to use IP Phones and m6350 SoftClient

CICM lines are datafilled on the CS2000 as standard MBS lines, using the M5216 template. There is no distinction between a normal MBS line and one connected to a CICM node.

UNIStim with IP Phones and m6350 SoftClient

CICM clients use the Nortel proprietary Unified Networks IP Stimulus (UNIStim) protocol to deliver the full range of CS2K Centrex service set which would not be possible to deliver with standardized protocols and terminals.

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.

Codec with IP Phones

Clients support the following codecs:

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

A codec is assigned to a terminal through an Audio Profile by the CICM-EM web-based interface. The profile (and therefore the codec used) can be overridden from the client's interface.

IP Phone models

The CICM hardware clients include these models:

- IP Phone 2001
- IP Phone 2002
- IP Phone 2004
- IP Conference Phone 2033

The capabilities and distinctions of each IP Phone model are described in the user guides identified in Related documents. The physical appearances of the phones are shown in the figures:

- IP Phones 200x, where 2002 is above left, 2001 is above right, and 2004 is at the bottom
- IP Conference Phone 2033

Figure 19 IP Phones 200x

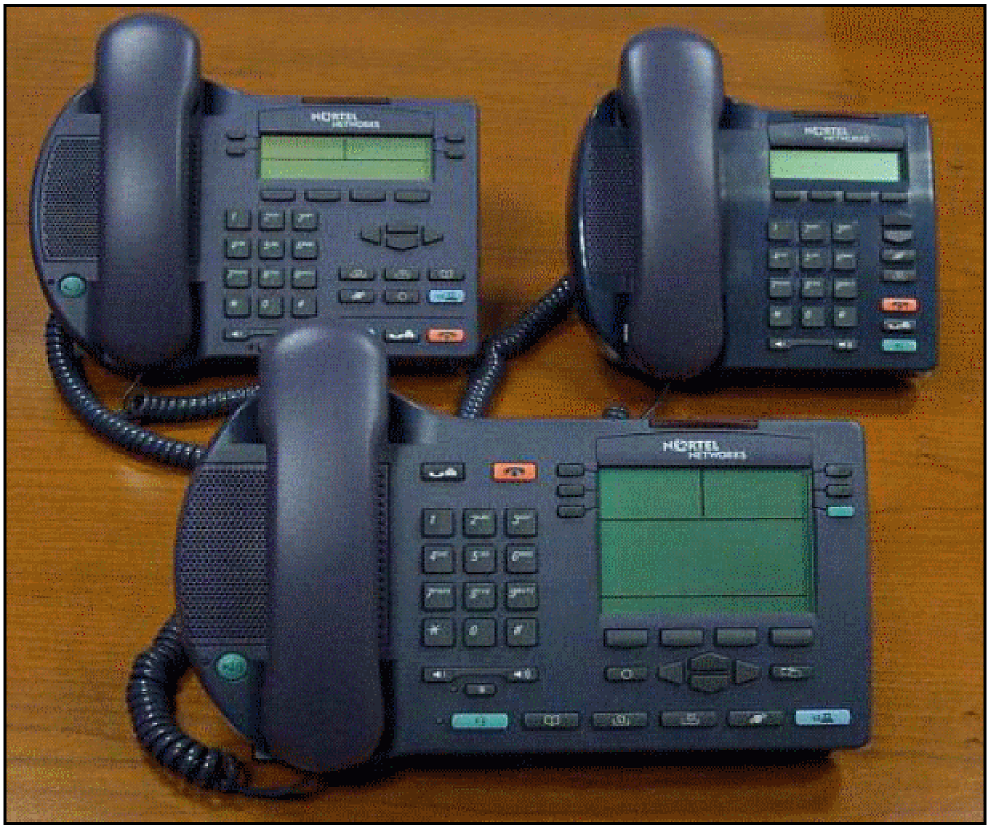
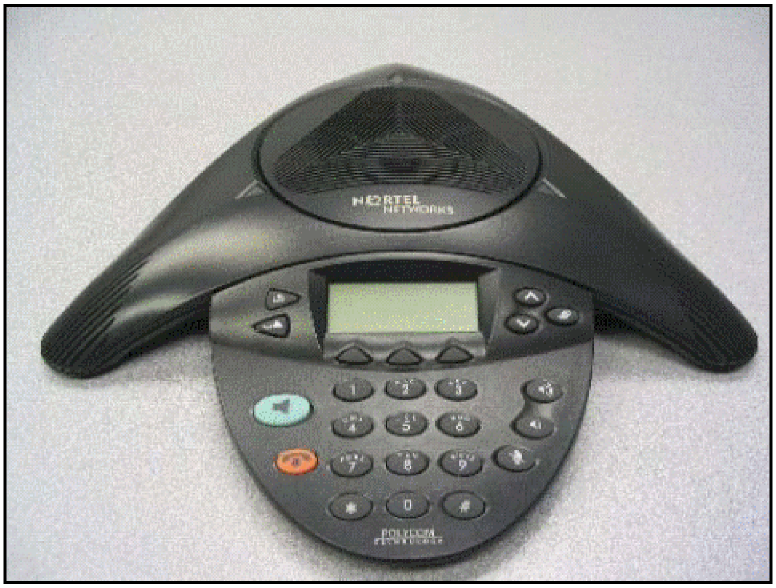


Figure 20 IP Conference Phone 2033



Functional components of IP Phones

Feature key assignments can be made either through the CICM-EM administration web interface, or directly through the client interface. Feature assignments on a client must be labeled to match the features provisioned through CS2000 line provisioning. Refer to the CS2000 provisioning documentation for provisioning procedures.

The table Comparison of IP Phone functional components summarizes distinctions between phone models.

Table 9 Comparison of IP Phone functional components

Component	2033	2004	2002	2001
Handset	N	Y	Y	Y
Speaker	Y	Y	Y	Y
Microphone	Y	Y	Y	N
Headset connector for hands-free operation	N	Y	Y	N
Standard keypad	Y	Y	Y	Y
Release key	Y	Y	Y	Y
Hold key	Y	Y	Y	Y
Volume control	Y	Y	Y	Y
Mute button	Y	Y	Y	N
Number of navigation keys	2 (Up or Down)	4 (Up or Down, Left or Right)	4 (Up or Down, Left or Right)	2 (Up or Down)
Function/display LCD	Y	Y	Y	Y
Number of soft keys	3	4	4	4
Number of line or dn keys	0 or 1	6	4	0 or 1
Transducer control	0	2 (HF or HS)	2 (HF or HS)	0
Other keys	0	2 (Stop or Copy)	2 (Stop or Copy)	0
Power over Ethernet capable	N	Y	Y	Y
Audio capabilities	High end audio. Full duplex speaker phone only	High end audio. Full duplex speaker phone with wideband transducers (Wideband transducer is only available in handsfree mode)	Standard audio. Full duplex speaker phone with narrowband transducers	Basic audio. On-hook dial or listen with narrowband handset and no handsfree capability

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

User interface of IP Phones

To use an IP Phone, log into the CICM node, supplying a user name and password. Once logged in, the handset and standard keypad of an IP Phone behave in the same way as a standard MBS telephone.

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

The table Comparison of IP Phones user interfaces summarizes distinctions between phone models.

Table 10 Comparison of IP Phones user interfaces

Option	2033	2004	2002	2001
Display contrast	Y	Y	Y	Y
Feature key configuration	Y	Y	Y	Y
Language selection	Y	Y	Y	Y
Time and date format selection	Y	Y	Y	Y
Audio configuration	Y	Y	Y	Y
Firmware upgrades at the phone	Y	Y	Y	Y
A user-created 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 automatically dials the number associated with the entry.	N (Contacts available but lack of feature keys restricts the functionality)	Y	Y	N (Contacts available but lack of feature keys restricts the functionality)
Call history feature, providing access to CICM-hosted inboxes (incoming calls) and outboxes (outgoing calls).	Y	Y	Y	Y

Hardware feature comparison of IP Phones

The IP Phone clients support IEEE 802.1p and IETF DiffServ Code Point (DSCP) marking through firmware. The table Comparison of IP Phones 200x and 2033 hardware features summarizes physical distinctions between phone models.

Table 11 Comparison of IP Phones 200x and 2033 hardware features

2033	2004	2002	2001
Sits flat on desk	Adjustable-angle stand	Fixed-angle stand	Fixed-angle stand
For desk only	Wall mount	Wall mount	Wall mount
1 RJ-45 jack (no Ethernet switch)	Plug-in Ethernet switch (on older models), plus built-in Ethernet switch (2 RJ-45 jacks) in newer models.	2 RJ-45 jacks with built-in Ethernet switch	1 RJ-45 jack (no Ethernet switch)
0 or 1 line key	6 line keys	4 line keys	0 or 1 line key
2-line display area	4-line display area	2-line display area	2-line display area
High quality speaker suited to conferencing	Extended low-frequency speaker	Standard Stetron LS19 speaker (no tuned cavity)	Basic audio
No AEM or ACM	AEM accessory port for key expansion modules (KEMs) and ACM accessory port	AEM accessory port for key expansion modules (KEMs)	No AEM or ACM
Handsfree microphone for wide-band audio	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. The supported versions are identified in *m6350 SoftClient Installation Guide*, NN10182-113.

The m6350 SoftClient communicates with the CICM over the IP LAN using the Nortel proprietary 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:*** It is not possible to guarantee the voice quality provided by the m6350 client, since it is significantly influenced by:
>
> - the characteristics of the operating system on which the client is installed
> - the mix of other computing tasks in progress during the call.

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 the chapter on branding in *m6350 SoftClient Installation Guide*, NN10182-113.

M6350 users can view, and in some cases modify, option data on the CICM node 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.

For an m6350 SoftClient 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 ring splash are implemented by a simultaneous pop-up dialog box and an audio prompt from the client PC speaker.

SoftClient platform requirements

The platform requirements to run the m6350 SoftClient are identified in *m6350 SoftClient Installation Guide*, NN10182-113.

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 Nortel headset equipment (all options are identified in NN10182-113).

The Nortel headsets, 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 is not possible to meet these requirements if you mix third-party sound cards, headsets, handsets, or speakers and microphones with the setup.

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.

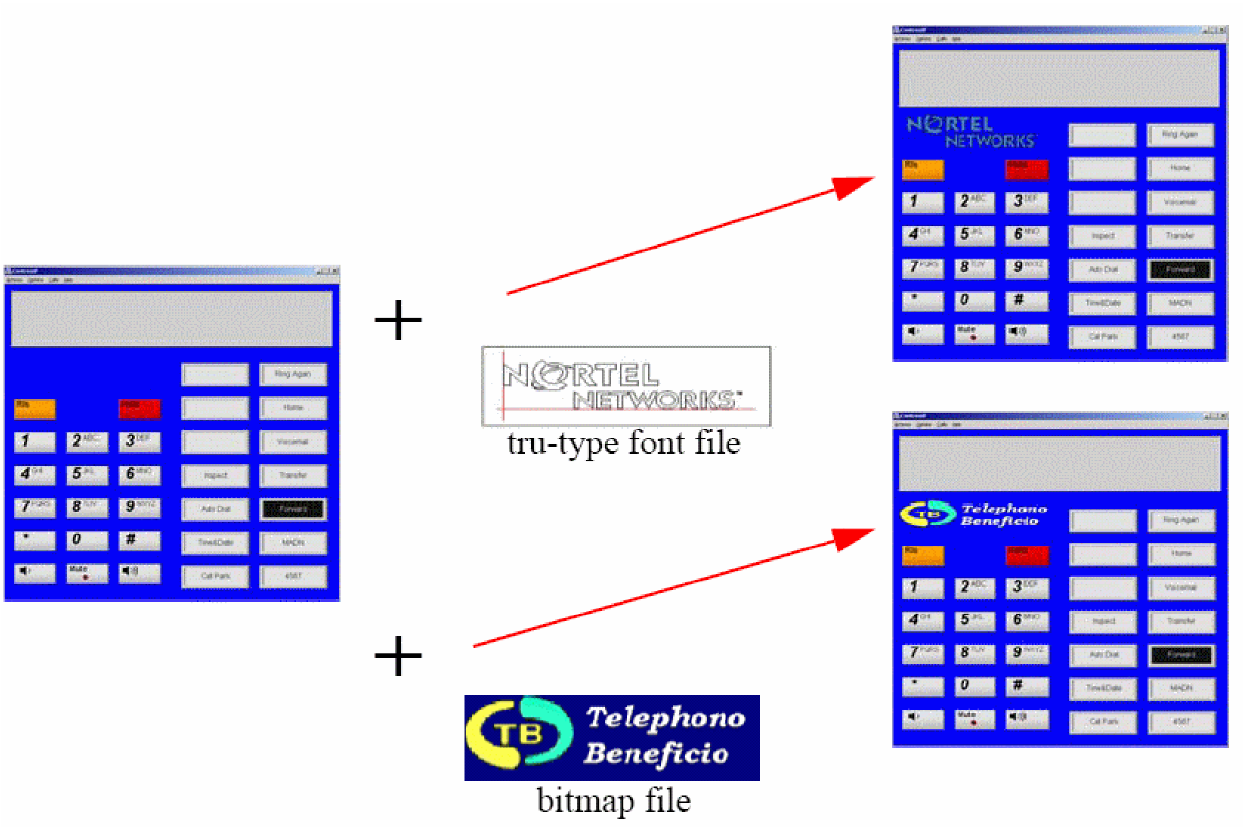
m6350 user interface

You start the m6350 just like any Microsoft Windows program and the m6350 client behaves as a standard Windows program, which means that simultaneously running CPU-intensive applications may degrade the audio quality of the m6350 client.

After logging into m6350, the you then log into the CICM node with a user name and password.

After login to the CICM, you are provided with a GUI that mimics the appearance of an MBS set, as shown in the figure m6350 SoftClient user interface with 2 additional banks of feature keys. 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 21 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 through a pop-up dialogue)
- Customizable appearance

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

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 *m6350 TAPI Service Provider Installation and Troubleshooting Guide*, 297-5551-901 provided on the CICM documentation CD.

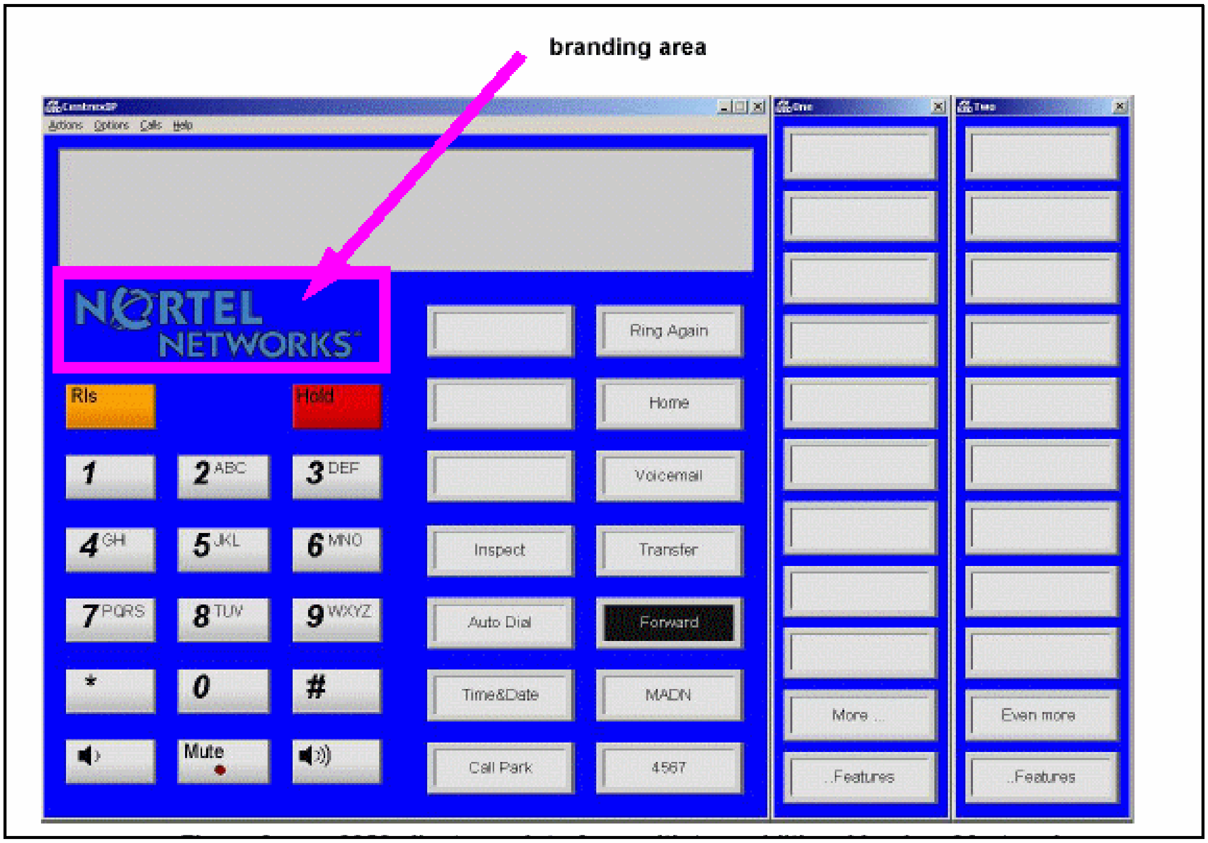
Client branding

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, as shown in the figure m6350 SoftClient Branding. 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 22 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.

Configuring CICM resident options

The 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 the *m6350 SoftClient Installation Guide*, NN10182-113.

Call History and Contacts Directory features

The IP Phones and m6350 clients support a Call History feature, which enables users to display a history of recent incoming and outgoing calls. The feature makes use of inboxes and outboxes hosted by the CICM.

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

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

The contacts directory allows the user to maintain a quick-dial address book (of up to 16 names and numbers). Entries can be copied to the contacts directory directly from the Inbox or Outbox, or can be added to the directory through an edit dialog. Contacts can be dialed from the directory, on the IP Phone 2002 or 2004 through an assigned feature key, and on the m6350 from a drop-down list on the main menu.

Interworking between m6350s and IP Phones

A user can be logged in from both an m6350 and an IP Phone 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 (for example, 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 IP Phone 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 IP Phone 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), the user is presented with the following options:

- Join the currently logged-in client in a cooperative session.

  Note: A cooperative session can only be established between an m6350 and an IP Phone, not between two clients of the same type. This option is therefore not available if the user is already logged in on a client of the same type (or if the user is already in a cooperative session with two clients).

- Take over the session by forcibly logging out the currently logged in client (or clients, if the user is already in a cooperative session with two clients). 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 IP Phone will receive audio.
- A cooperative session can only be established on the master CICM node.

For detailed procedures, refer to *m6350 SoftClient Installation Guide*, NN10182-113.

DHCP and Centrex IP Clients

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

For m6350 clients, standard Microsoft 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 (for example, 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 Phone clients support two modes of DHCP operation:

- Full DHCP, in which the IP Phone obtains all its configuration data from the DHCP server, including the CICM addresses and ports.
- Partial DHCP, in which the IP Phone obtains only its IP address, subnet mask, and default router address from the DHCP server. Other data must be configured manually.

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.

Using full DHCP mode

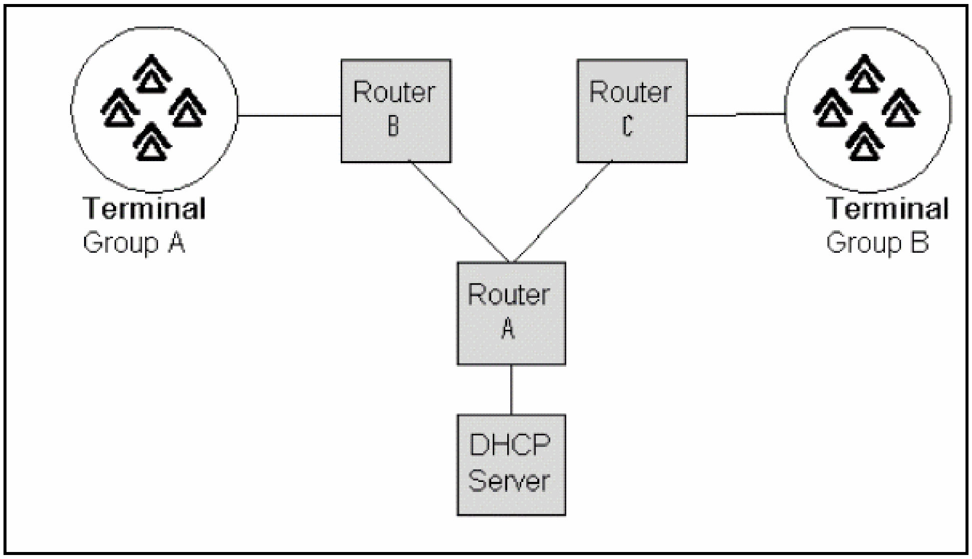
There is a potential issue with using full DHCP mode. The DHCP server can only return one set of details to any one terminal. This means that should a terminal hard reboot, it will always return to one particular

(DHCP server decreed) CICM. This CICM may not be the CICM the terminal was previously connected to.

There are two solutions to overcome this issue:

- Switch off full DHCP and choose partial or no DHCP. In this case, only the terminal's IP address, netmask, and default CICM will be assigned by the DHCP server.
- Group the terminals, and separate and contain them within DHCP scopes. This solution requires routers that support DHCP. The DHCP server can be set to give different information to different groups of DHCP clients (such as CICM IP addresses). These groups are determined by checking which routers the connection between the DHCP server and DHCP client passes through. In the figure DHCP scoping diagram, a terminal in Terminal Group A would have Router B and Router A between it and the DHCP server. When the terminal connects to the network it will broadcast a DHCP request. DHCP enabled routers will add information to the request to tell the DHCP server which part of the network the broadcast originated. In this manner the DHCP server in the figure would be able to distinguish between Terminal Group A and Terminal Group B, and, if configured to do so, assign terminals in the two different groups different CICM IP addresses.

Figure 23 DHCP scoping diagram



Other client-related features

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

Auto firmware upgrade

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 (for example, 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 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.

- The Call Server can support multiple feature assignments to each feature key, but the CICM shows only one label per key.

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 through 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.

- *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 although this is not supported for phase 2 terminals)
- G.729A and G.729A annex B

User interfaces for CICM

The normal mode of access to the CICM-EM is through a PC connected to the Administration LAN. The procedures in the CICM document suite are 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**
  The CICM Element Manager interface uses a web browser to access the Element Manager web pages. Refer to the *Element Manager Web pages procedures* in *CICM Security and Administration*, NN10252-611.
- **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 *CICM Security and Administration*, NN10252-611.
- **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.

CICM-EM web interface

The web-based CICM Element Manager (CICM-EM) interface is a web site (that is, collection of web pages) hosted on the EM. 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 EM web site provides the user interface for most of the functionality necessary for configuring and monitoring a CICM and its clients.

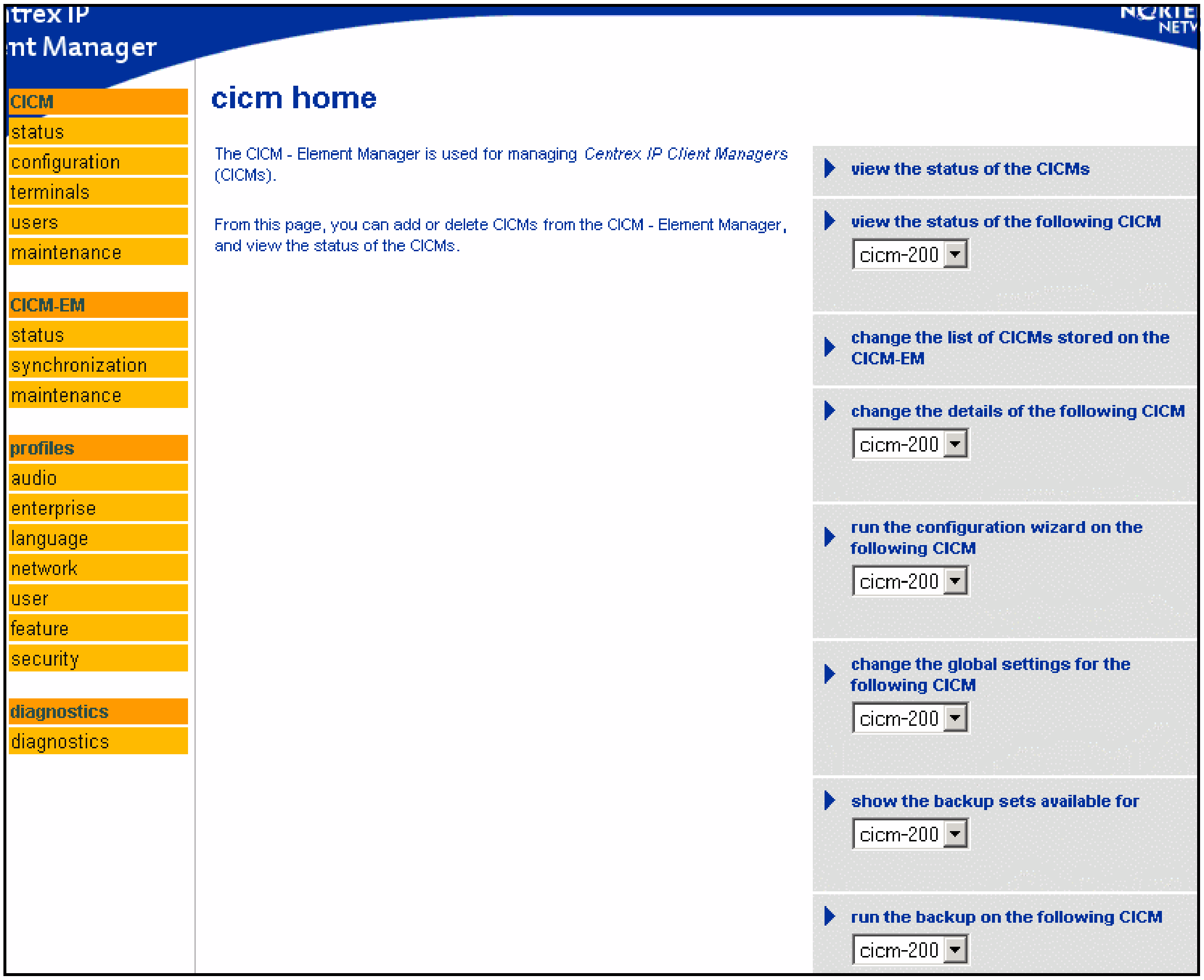
The CICM-EM web-based interface consists of:

- An EM home page, which provides links to:
  - a CICM Status Overview page, which provides a summary of the status of the CICM and its components
  - detailed status pages for each CICM node
- A collection of read-only status pages, which present the current CICM-EM node status.
- Pages for viewing and configuring the following types of profiles:
  - audio
  - enterprise
  - language
  - network
  - user
  - feature
  - security
- Pages for configuring users
- Pages for configuring client terminals

The figure CICM home page shows the home page of the CICM-EM web site, and the main menu that can be accessed from every page on the site. For the CICM-EM web page interface and procedures, refer to the:

- *CICM Configuration Management*, NN10240-511
- *CICM Security and Administration*, NN10252-611

Figure 24 CICM home page



cicm home

The CICM - Element Manager is used for managing *Centrex IP Client Managers* (CICMs).

From this page, you can add or delete CICMs from the CICM - Element Manager, and view the status of the CICMs.

- view the status of the CICMs
- view the status of the following CICM: cicm-200
- change the list of CICMs stored on the CICM-EM
- change the details of the following CICM: cicm-200
- run the configuration wizard on the following CICM: cicm-200
- change the global settings for the following CICM: cicm-200
- show the backup sets available for: cicm-200
- run the backup on the following CICM: cicm-200

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 SAM16 or SAM21 shelf
  - — which gateway controller (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. It 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 through 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*, NN10252-611.

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 enterprise-specific CICM MIB. New in (I)SN08 for CICM is support of the Nortel Reliable MIB format, which is a standard across the Nortel Carrier Voice over IP (VoIP) product range.

Network interfaces for CICM

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 Networks IP Stimulus (UNIStim) protocol. The UNIStim protocol carries information about client key presses between the client and the CICM, and is secure. Gateway 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 according to the standards G.711 or G.729. The rate of transmission for voice packets is 10 ms or 20 ms.

Protocols for CICM

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 table Protocols relevant to VoIP.

Table 12 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 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. This initial configuration information includes, for example, an IP address of the CICM, and the maximum number of concurrent sessions.

Commissioning is a two-stage process. Preboot provides the CICM with sufficient information so that it can fully boot and be configured. The second stage is provisioning the CICM nodes through the CICM-EM.

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 (for example, CICM-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.

CICM-EMs can be configured to automatically back up the configuration data of all CICM nodes once per 24-hour period (for example, the default is 2:00 am when enabled).

Back-up and Restore

Data can be backed up in two ways:

- as part of a regularly scheduled task
- on demand from the CICM-EM 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 CICM-EM.

Typical data that is backed up is:

- User information (for example, Passwords, Locality Preferences, Contacts)
- Terminal information (for example, Locality Preferences and Auto Login)
- Line information (for example, Features)
- Profiles (for example, Global Profile Overrides)

The CICM-EM 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.

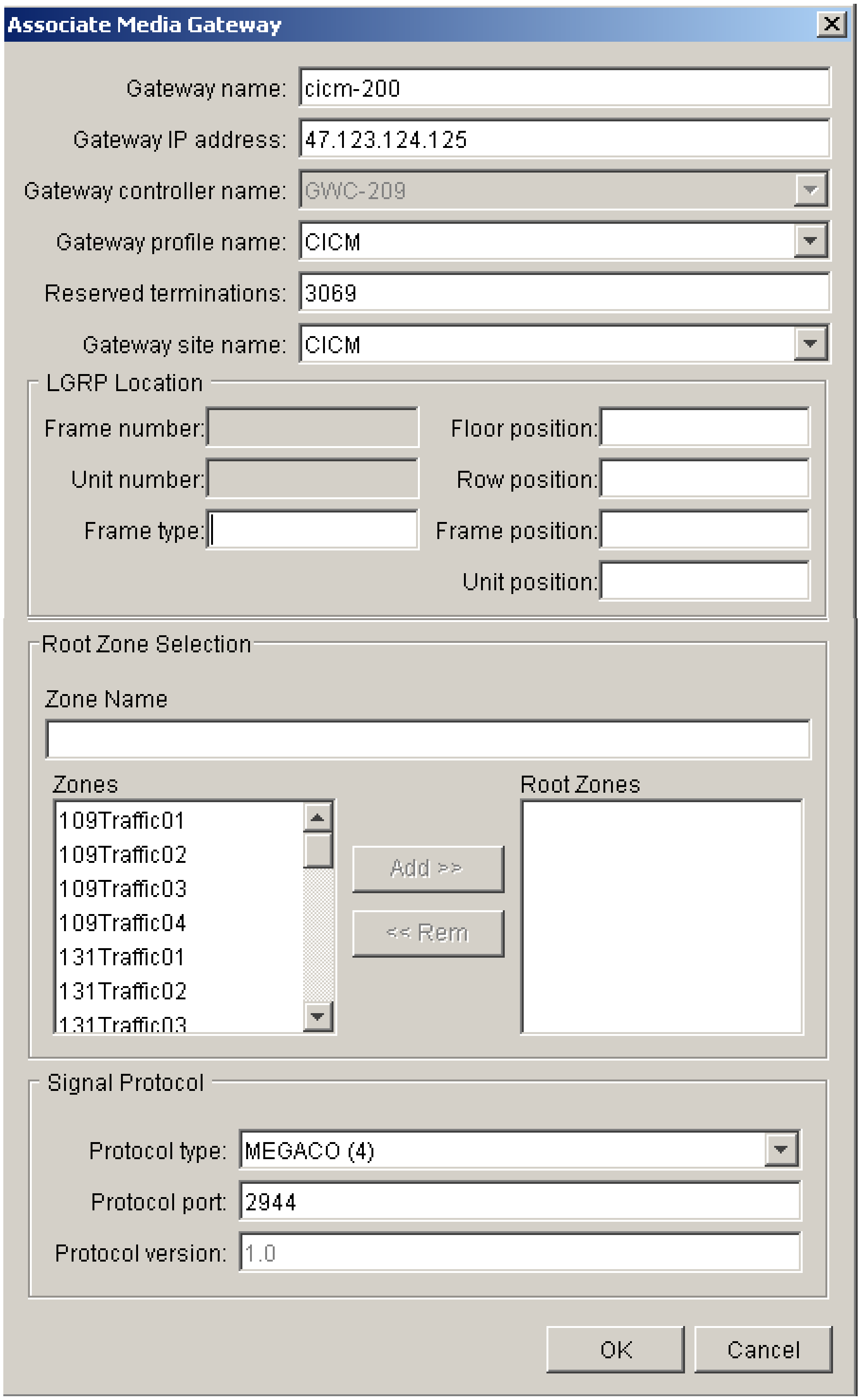
A generic gateway may be associated with a GWC either through the XML interface on OSSGate, or through the CS2000 Management Tools GUI. Whichever interface is used, the following information is required:

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

- the site name, for example, LG
- the signalling protocol, which must be MEGACO

The figure Using a GUI to associate a CICM is an example of the CICM being associated using the GUI.

Figure 25 Using a GUI to associate a CICM



Associate Media Gateway

Gateway name:	cicm-200
Gateway IP address:	47.123.124.125
Gateway controller name:	GWC-209
Gateway profile name:	CICM
Reserved terminations:	3069
Gateway site name:	CICM

LGRP Location

Frame number:		Floor position:	
Unit number:		Row position:	
Frame type:		Frame position:	
		Unit position:	

Root Zone Selection

Zone Name

Zones

109Traffic01
109Traffic02
109Traffic03
109Traffic04
131Traffic01
131Traffic02
131Traffic03

Root Zones

Signal Protocol

Protocol type:	MEGACO (4)
Protocol port:	2944
Protocol version:	1.0

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 OSSGate.

To configure subscribers, an authorized user must connect to OSSGate in CI mode. Any commands which contain a line equipment number (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 the gateway controller (GWC).

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

- user ID
- user profile
- key mappings
- enterprise zone

CICM supports all OSSGate 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 only returns data from the XA-Core

The OSSGate commands for handling a CICM are in *OSSGate User’s Guide, version 08.01 for SN08*, NE10004512.

In addition to changing user details through OSSGate, they may also be changed from the CICM-EM.

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 procedure “Perform line provisioning for CICM clients” in *CICM Configuration Management*, NN10240-511.

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

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.

Security and administration for CICM

Element Manager security

CICM Element Manager (CICM-EM) operator authentication and authorization is tied into the Carrier Voice over IP (VoIP) SSPFS authorization database.

Logon from and to the CICM-EM is performed over HTTPS. CICM does not administer users locally; it delegates the authentication to the SSPFS Authentication Database through 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 Carrier VoIP elements, a user can have a single account to access different VoIP components.

Telnet security

The Telnet connection is secured by SSH.

UFTP security

The UFTP connection between a CICM node and its clients with IP Phone firmware has a secure download. The protection is provided by the UNIStim security feature. UFTP is supported on the UNIStim signaling port (UDP port 5000) of phase 1 IP Phones (formerly referred to as Ethersets). All m6350 soft phones support UFTP phone firmware download over the secured UDP 5000 UNIStim connection. Secure UFTP is not supported on the phase 2 IP Phones.

UNIStim security

All signaling messages between a CICM node and its clients (IP Phones 200x or m6350 sets) are encrypted if the UNIStim security feature is being used. Userid, password, and other call control information are not identifiable on the system. UNIStim is a Nortel proprietary stimulus protocol. Each CICM node as an application server uses the UNIStim commands to control client resources such as displays, handsets, keypads, microphones, and speakers.

Security is by the AES 128-bit encryption for confidentiality and AES-based message authentication code (MAC) for authentication and data integrity. A reliable user datagram protocol (RUDP) layer provides a reliable transport of UNIStim messages by using a go-back-n windowing protocol.

Administration

refer to the administrative procedures in *CICM Security and Administration*, NN10252-611.

Performance management for CICM

Capacity and performance limits

CICM supports up to 8 pairs of CPN5385 CPU cards per SAM21 shelf or one pair of CPV5370 CPU cards per SAM16 shelf. Each pair's maximum capacity is identified in the table CICM capacity attributes.

Table 13 CICM capacity attributes

Capacity attribute (maximum)	SAM16 platform (CPV5370)	SAM21 platform (CPN5385)
Provisionable Lines	1,023	3,069
Simultaneous Terminal Sessions	2,500	4,096
Historical Terminal Entries	10,000	10,000
Simultaneous Active Half-Calls	512	3,069
BHHCA	7,200	21,600
RUDP Messages/Sec	500	500
H.248 Messages/Sec	100	250

The definitions of these attributes are:

- **Provisionable Lines**
  The maximum number of lines (a CICM line corresponds to a LEN on the CS2000). This represents the number of users that a CICM can accommodate.
- **Simultaneous Terminal Sessions**
  The maximum number of terminals that may be connected and presented with a login prompt by the CICM at any given time. A user that logs into a joint session uses 2 session resources on the CICM. Therefore, on a CPN5385-based CICM, the value 4,096 could be interpreted as allowing all provisioned users (lines) to connect at least one terminal, but allowing 1,000 of these users to login as a joint session. However, the system does not enforce this, so it is possible that 1,000 + n (number of users) could have 2 of their terminals connected to the CICM, thus preventing N users connection to a terminal.
- **Historical Terminal Entries**
  As a new terminal connects to the CICM, information about the terminal is automatically added to the CICM MIB (that is, firmware load, etc). As each terminal identifies itself uniquely to the CICM, it is possible to ensure that the same entry is re-used when this terminal connects again.

  Each new terminal that has never connected to a CICM will generate a new entry in the MIB. However, since this configuration data uses memory resources, there is a limit to the amount of historical information that is saved on the CICM. When this maximum is reached, additional new connections will be denied access until other entries are cleared manually using the CICM-EM. When this maximum is reached, an alarm is raised.

  This limit also represents the maximum number of terminals that can be serviced by a single enterprise profile.
- **Simultaneous Active Half-Calls**
  The CICM knows only about half-calls. Even if the second half of a call is also hosted by the same CICM, the CICM has no knowledge of this and 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 (incoming or outgoing) are denied.

Any single terminals 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 (BHHCA) represents the maximum rate at which half call attempts can be made per hour. Once the BHHCA reaches 80%, a minor alarm is raised. At 100%, a major alarm is raised, and at 150% a critical alarm is raised and no additional calls are permitted. The critical alarm clears automatically once the BHHCA drops to below 100% for more than 5 minutes. The major alarm is cleared once the BHHCA drops to below 80% for 5 minutes. The minor alarm clears once BHHCA drops below 80% for 15 minutes.
- **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 becoming overloaded.

CICM-EM card pairs

One pair of CICM-EM cards is needed per CS2000. The CS2000 is able to support up to 100 CICM resource card pairs.

GWC resource card pairs

Each GWC resource card pair supports:

- 6,400 subscriber line provisioning capacity
- 38,000 BHHCA

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 Carrier Voice over IP (VoIP) performance MIB. Each metric contains the following information:

- The instance of the object (for example, SAM21 x blade y)
- The property of the object being reported (for example, processor occupancy)
- The type of the property (for example, gauge)
- The value (for example, 22%)

Fault management

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

SNMP alarms

Alarms are raised by each CICM and CICM-EM node 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.

All CICM or CICM-EM software alarm identifiers have CICM-nnn, where nnn denotes a unique sequence number for the event that occurred.

Alarms can be viewed on the IEMS, and are aggregated with alarms from other components into a single machine feed from the IEMS. For Carrier Voice over IP (VoIP) 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)

System busy CICM nodes and the PM banner display

When a CICM or CICM-EM node is system busy (SysB), a status display for it will appear under the PM banner of MAPCI of a DMS. Since the CICM hardware is not a true peripheral module (PM), the number of SysB CICM nodes is not included in the total count of SysB

PMs shown in the display. There is no CICMxxx alarm when a CICM or CICM-EM becomes system busy.

LEDs

The following details on LEDs relate 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

CICM logs

The CICM software generates Windows XP 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 (for example, 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)

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 Carrier Voice over IP (VoIP) 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
```

Upgrades for CICM

The supported software upgrades are identified in *Upgrading CICM*, NN10230-461. The telco administrator or Nortel support can perform the upgrade on site for Sam 16 or remotely for SAM21.

Accounting for CICM

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 customer support

For customer support information, contact your Nortel account prime.

Customer documentation

Nortel 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, contact your Nortel Training and Documentation representative. For enrollment assistance, contact Training Registration at 1-800-4-NORTEL (1-800-466-7853).

www.nortelnetworks.com

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

Operations support services

Nortel 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.