Carrier VoIP

CICM Basics

NN10044-111

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

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

Contents

New in this release

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

CICM Basics

The *CICM Basics* NTP 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.

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.

Navigation

Introduction to CICM

This section introduces Centrex IP Client manager (CICM) products and its interactive dependent products, which use Voice over IP (VoIP) technology to deliver central office exchange service (Centrex) capabilities to users connected to an IP network with a Call Server 2000 (CS2000).

The CICM products involve the following high-level network setup in an IP network:

- a pair of CICM nodes supporting clients (terminals) each of which is either a Nortel IP Phone or a PC running the m6350 SoftClient software
- a pair of CICM element managers (CICM-EM) to control, monitor, and maintain the CICM nodes
- a connection from each CICM-EM pair to the Integrated Element Management System (IEMS), which controls, monitors, and maintains nodes of the network
- a connection from each CICM node pair to the Call Server 2000

Navigation

CICM components and functionality

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

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

Beginning with release SN08, 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 CICM nodes and their clients
- client hardware and software

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 IP interface.

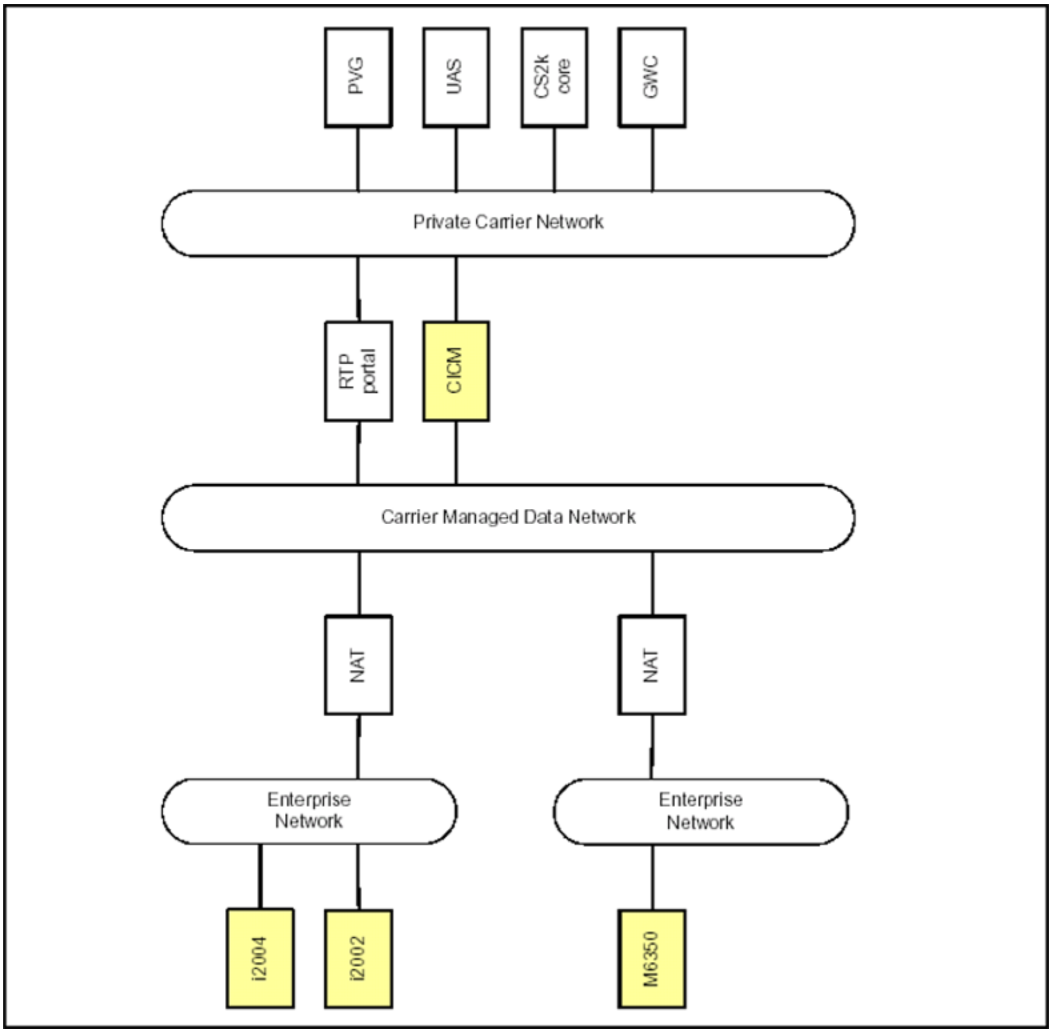
H.248 is a joint ITU-T and IETF protocol defined in ITU-T Recommendation H.248 and IETF RFC3015. It fully supports the same basic device/media control capabilities as protocols such as ASPEN. More importantly, it is based on a more flexible functional mode that provides better support for multimedia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

A CICM node 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. CICM IP Phones are media end-points. Examples of other media end points in a VoIP network are:

- Time Division Multiplexed (TDM) trunk gateways (for example, MG15000)
- analog line gateways (for example, MG9000, Mediatrix 1124)
- voice processing servers (for example, Universal Audio Server (UAS) or AMS)
- IP Terminals hosted off another CICM

The next figure 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.

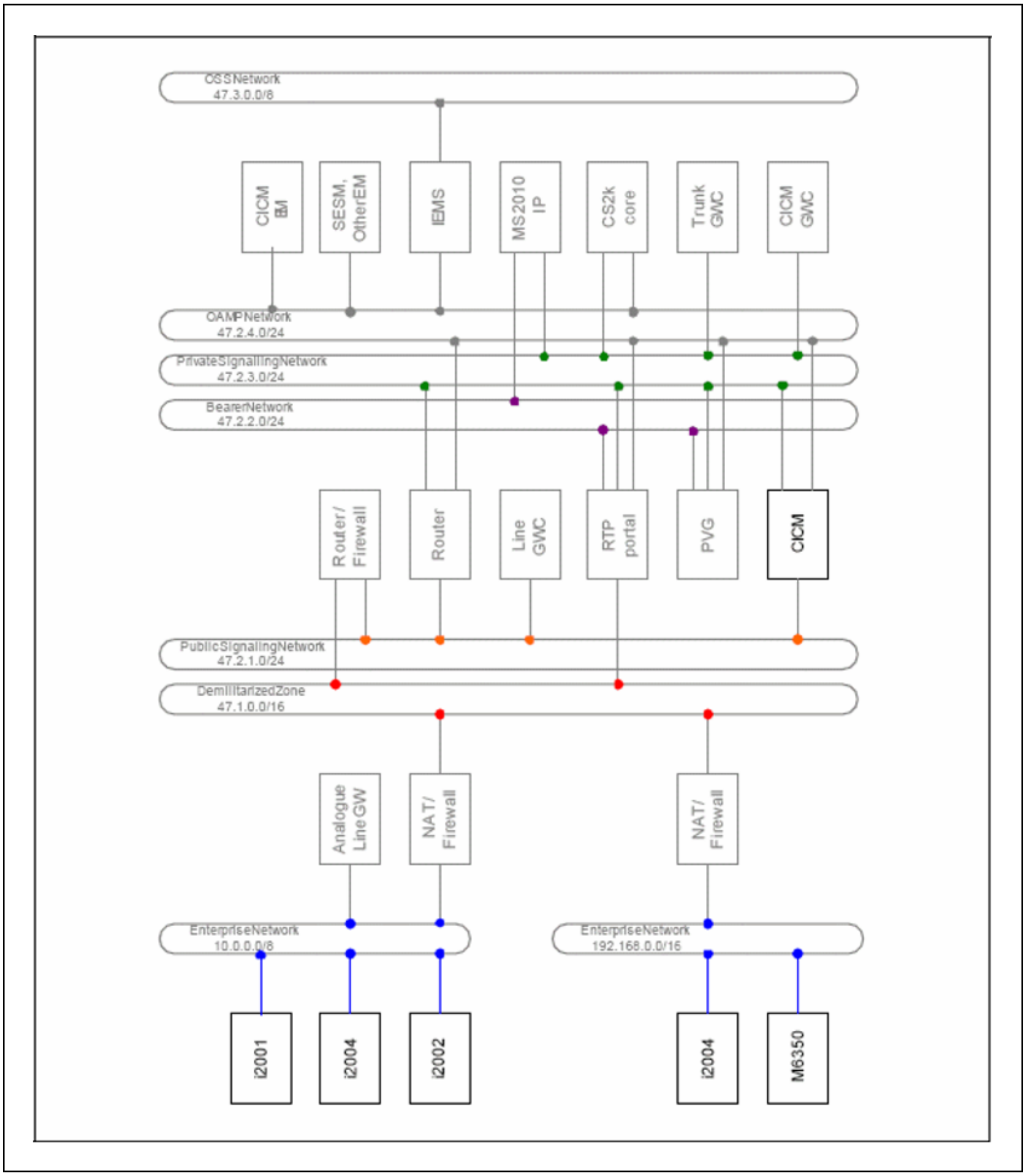
CICM and clients in the Carrier VoIP network



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

The next figure 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 figure; it shows general connectivity only. Operations, Administration, Maintenance, and Provisioning (OAM/P) devices and networks are also omitted from the figure.

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).

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

The central office exchange service (Centrex) is a set of capabilities that allows a Call Server 2000 (CS2000) 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

For a complete list of Centrex features, refer to the Nortel Web site, www.nortel.com.

Call Server 2000

Call Server 2000 (CS2000) 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 gateways and servers, CS2000 supports VoIP or Voice over ATM (VoATM), depending on the type of backbone packet network to be used. The CS2000 capabilities that Centrex IP Client Manager (CICM) depends on are highlighted as follows.

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

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 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)

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

Beginning with release SN08, 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 are 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 8600s 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 wide area network (WAN) communication.

Beginning with release SN08, the Public Signaling Interfaces (that is, the UNIStim-LAN interfaces) and the Operations, Administration, Maintenance, and Provisioning (OAM/P) Interfaces (that is, the Admin-LAN interfaces) of the Centrex IP Client Manager (CICM) nodes and CICM-EMs 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.

CICM Element Manager

Centrex IP Client Manager Element Manager (CICM-EM) is the principal management platform for the CICM nodes. CICM-EM performs the following functions:

- hosts the Web pages that provide the Web-based interface for configuring and monitoring the CICM and its clients
- provides the database for CICM configuration data
- provides storage for user profiles and CICM software upgrades
- provides an open API for Integrated Element Management System (IEMS) and third-party Operations, Administration, and Maintenance (OAM) solutions

Refer to "Hardware of a CICM-EM and CICM node" (page 97) for additional hardware-related details of the CICM-EM.

CICM clients

CICM client is the component that allows a user to initiate and receive VoIP calls, and to receive Centrex features from Call Server 2000. CICM clients are also called terminals or client terminals. Two types of CICM client are supported, soft and hard clients:

- The m6350 SoftClient application, which is an IP telephony software client installed on a personal computer (PC) attached to a LAN. It works with a headset and adapter which plugs into a USB port on the PC. Attendant Console Softclients, which are soft clients developed externally using the m6350 Development SDK. Current ACs supported include: T-Metrics, Datapulse, and Conveyant.
- Supported Nortel IP Phone hard clients are:
  — IP Phone 2001

- — IP Phone 2002
- — IP Phone 2004
- — IP Phone 2007
- — IP Phone 1120E
- — IP Phone 1140E
- — IP Audio Conference Phone 2033
- — Wireless IP Phone 2210
- — Wireless IP Phone 2211
- — Wireless IP Phone 2212

CICM clients use the Nortel proprietary UNIStim (Unified Networks IP Stimulus) protocol to communicate with the CICM node. This allows the clients to deliver the full range of CS2000 Centrex services.

CICM nodes and the IP network

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

The CICM node controls client 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

In release (I)SN09, CICM supports the Carrier Voice over IP (VoIP) CS2000 version of the product.

Terminology

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

Administration LAN

The Administration (Admin) LAN is the Operations, Administration, Maintenance, and Provisioning (OAM/P) subnet in the Centrex IP Client Manager (CICM) CS-LAN in the carrier central office network. This subnet hosts the OAM/P interfaces for the CICM node and the CICM Element Manager (CICM-EM) for such functions as CICM and client configuration and monitoring.

Centrex IP Client Manager (CICM)

Centrex IP Client Manager (CICM) refers to all the CICM resource cards (Motorola CPN5385 processor card) on a SAM21 chassis, associated with a single CS2000. CICM resource cards are always in pairs. There is one active master card and one hot standby slave card in each pair providing redundancy. The term CICM is synonymous with a terminal proxy server.

Chassis

Centrex IP Client Manager (CICM) nodes and CICM Element Managers (CICM-EM) are 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 (Nortel IP Phones and m5360 SoftClient) from the enterprise or customer premises equipment (CPE) network, for communication of signaling messages (for example, UNIStim registration, call processing, firmware download, and so on).

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

EBS

Electronic Business Set. A 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

An element manager is the device used to configure, monitor, upgrade, and manage a group of components.

In a SAM21-based Centrex IP Client Manager (CICM), the CICM Element Manager (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.

GWC

A gateway controller (GWC) 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, and so on).

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 split 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 client (terminal) side of the CICM.

Terminals

Terminals in context of CICM are the IP Phones that connect to the CICM nodes. Terminals are also referred to as clients. Throughout this document the terms are synonymous unless otherwise specified.

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 (Nortel IP Phones and m5360 SoftClient) from enterprise or CPE networks, for communication of signaling messages, for example, UNIStim registration, call processing, and firmware download.

VMG

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

CICM document suite and related documents

The documents in the Centrex IP Client Manager (CICM) document suite are:

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

Documents for m6350 SoftClient software

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

- *m6350 SoftClient Installation Guide* (NN10182-113)

Documents for IP Phones

For additional information about Nortel IP Phones, refer to:

- *CICM Configuration Management* (NN10240-511) for installing and configuring phone sets
- *Upgrading CICM* (NN10230-461) for phone set firmware
- *Nortel IP Phone 2001 User Guide* (NN10300-005)
- *Nortel IP Phone 2002 User Guide*(NN10300-007)
- *Nortel IP Phone 2004 User Guide* (NN10300-009)
- *Nortel IP Phone 2007 User Guide* (NN10300-020)
- *Nortel IP Phone 1120E User Guide* (NN10300-022)
- *Nortel IP Phone 1140E User Guide* (NN10300-023)
- *Nortel IP Phones 2210, 2211, 2212 User Guide* (NN10042-116)

- *Nortel IP Audio Conference Phone 2033 User Guide* (NN10300-013)
- *Nortel IP Phone Key Expansion Module User Guide* (NN10300-011)
- *IP Phones Description, Installation, and Operation* (553-3001-368), the Appendix on IP Phone diagnostic utilities

Documents associated with CICM products

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

For information about the Call Server 2000, refer to the *CS2000 Product Description* (cs2000cPDISN07) and later.

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, Microsoft Windows XP and XPe, go to the Microsoft Web site, http://www.microsoft.com/.

For information about the CICM chassis and processor card, go to the Motorola Web site at http://www.motorola.com/and refer to SAM16, SAM21, CPV5370, and CPN5385.

CICM-specific features and capabilities

Navigation

Active call failover

Prior to release 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.

Beginning with release SN08, the Active Call Failover (ACF) functionality transitions the CICM node pair 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 clients (terminals) while maintaining active calls.

CICM line capacities

The line capacities of the CPN5385 CICM nodes are listed in "CICM capacity attributes" (page 175).

CICM lines for P-Phones

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

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

Key expansion modules

Nortel IP Phone Key Expansion Modules (KEM) are optional add-on units, which expand the capabilities of some of the Nortel IP Phone models. Refer to "Key Expansion Module for Nortel IP Phones" (page 135).

The limits to the mobility of a subscriber is determined by the boundaries of the Enterprise profile to which the user belongs, because the user names are now defined within the scope of a particular Enterprise. In particular, this means:

- Improved flexibility in assigning belong to more than one Enterprise name can be assigned to different separate Enterprise profile.
- Increased security because the home CICM authenticates the user's login details within the scope of the associated Enterprise profile. The CICM rejects any attempt to obtain service unless the request comes from an Enterprise profile to which the user belongs.
- Greater consistency, in situations where a single Enterprise profile is hosted across multiple CICMs. A user name/Enterprise profile association can be used to identify a single subscriber across all CICMs hosting the Enterprise profile.
- Reduced ambiguity because user names are unique within the boundaries of their Enterprise profile, rather than to a single or multple CICMs.

Nortel IP Phone emulation

The function and operation of a Nortel IP Phone is emulated by the m6350 SoftClient software that runs a personal computer (PC) connected to a CICM node pair. The SoftClient is also referred to as a soft phone. Refer to "CICM clients with the IP Phones or m6350 SoftClient" (page 125).

Nortel IP Phones

Each Nortel IP Phone model connects to a CICM node pair and operates using Centrex features. Refer to "CICM clients with the IP Phones or m6350 SoftClient" (page 125).

Ring tones and language options 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.

Beginning with release SN09, the supported tone sets on the CICM nodes 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

Beginning with release SN09, the supported languages on the CICM nodes are:

- English (UK)
- English (US)
- French

- Italian
- German
- Spanish

Session Description Protocol

The Centrex IP Client Manager (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. Beginning with SN08, the CICM's SDP parser and generator have been replaced. This new and more efficient parser will improve the CICM's real-time performance.

Pre-answer and mid-call SDP renegotiation

Pre-answer occurs prior to the destination answering. Mid-call occurs while there is an active voice path, as in two-way speech.

During each call setup, a CICM node negotiates:

- which compression/decompression algorithms (CODEC) to use
- the duration of the paketization times
- the destination IP informatiuon through exchanging SDP messages with the far end of the connection

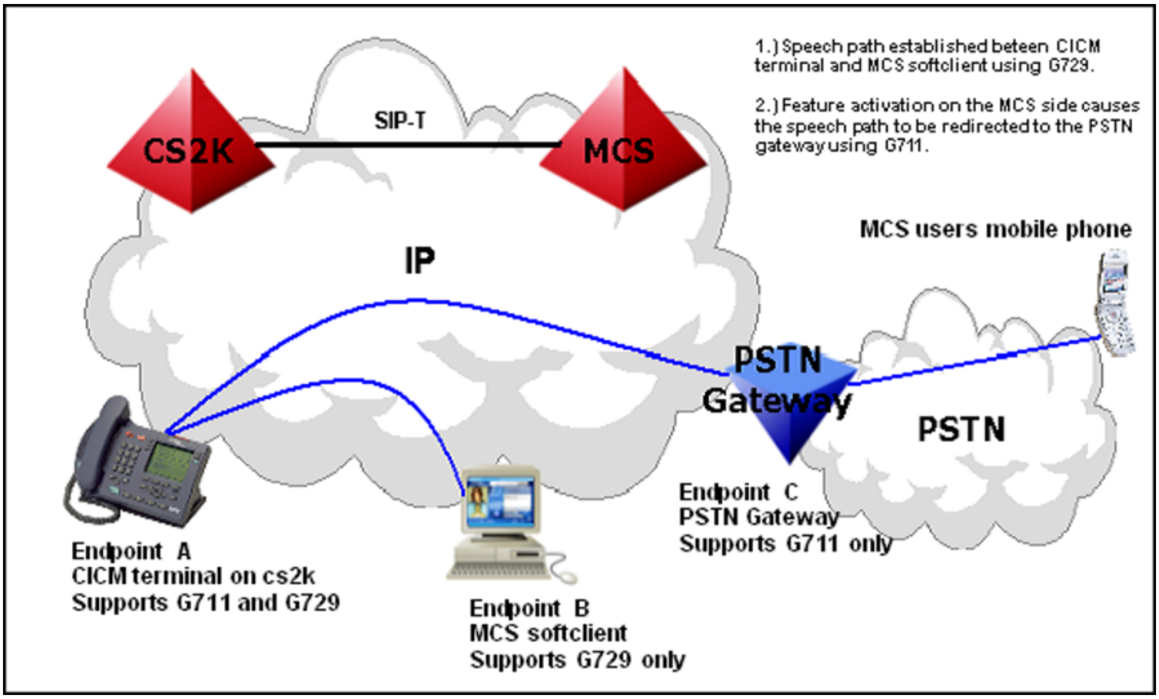
A Centrex IP Client Manager (CICM) node is unable to process SDP renegotiation attempts from the peer gateway. This causes problems when interworking with gateways which rely on SDP renegotiation to change or destination IP address pre-answer or mid-call.

Prior to release SN09, the lack of support for SDP renegotiation on the CICM node caused problems when interworking with a Multimedia Call Server (MCS). An SDP renegotiation attempt can be triggered when MCS features are activated. Beginning with release SN09, when interworking with an MCS a CICM node is supported for pre-answer and mid-call IP address and CODEC renegotiation.

The following figure shows an example of how activating a feature on MCS can trigger changes in the destination IP address and CODECs. The example shows:

- a single CICM client hosted on a CS2000 (CS2K)
- a SoftClient and a Public Switching Telephone Network (PSTN) gateway hosted on an MCS
- the CS2000 connected to MCS

CICM interworking with MCS


1.) Speech path established beteen CICM terminal and MCS softclient using G729.
2.) Feature activation on the MCS side causes the speech path to be redirected to the PSTN gateway using G711.
CS2K
SIP-T
MCS
IP
MCS users mobile phone
PSTN Gateway
PSTN
Endpoint A
CICM terminal on cs2k
Supports G711 and G729
Endpoint B
MCS softclient
Supports G729 only
Endpoint C
PSTN Gateway
Supports G711 only

From the example in the figure, the pre-answer IP address and CODEC renegotiation means:

- the CICM terminal (IP Phone) calls the SoftClient on the MCS
- the speech path is negotiated to use CODEC G.729 and to terminate at the MCS SoftClient
- the MCS user does not answer so the MCS SoftClient re-directs the call to the MCS mobile user through the PSTN gateway
- the speech path is renegotiated to use CODEC G.711 and to terminate at the PSTN gateway

In the same scenario, the post-answer and CODEC renegotiation means:

- the CICM terminal (IP Phone) calls the SoftClient on the MCS (or vice versa)
- the speech path is negotiated to use CODEC G.729 and to terminate at the MCS SoftClient
- the MCS user answers but has to leave, so the user re-directs the call from the MCS SoftClient to the MCS mobile user
- the speech path is renegotiated to use CODEC G.711 and to terminate at the PSTN gateway

When a CICM node is interworking with an MCS, it is expected that only the CODEC is renegotiated since the MCS inserts the media portal, and the destination address through that portal will not change during the call. Refer to "Border Control Point for CICM" (page 73) for the relationship between a CICM node and the portal.

For calls that terminate to a CICM user who is not logged on, the CICM node does not know of the CODECs supported by the CICM terminal (IP Phone) until the user logs on and while the user is being alerted. The CICM node indicates in the SDP negotiation that CODECs G.711 and G.729 are supported.

When a CODEC, for example G.711, is selected during a pre-answer SDP negotiation by the peer gateway, and a call requires a different CODEC, for example a G.729 that was configured for an m6350 SoftClient, the call cannot be established. Beginning with release SN09, the CODEC is determined by the CICM node. In this scenario, the m6350 call would be established.

For additional information, see *CODEC negotiation rules* in *CICM Configuration Management* (NN10240-511).

UNIStim security—reset security

The UNIStim security feature provides the infrastructure required for secure communications between the CICM server and its clients. Beginning with release SN08, a function to reset security on CICM servers and clients was added, which facilitated the transfer of multiple secure clients from on CICM server to another. For more details, refer to the UNIStim security section in *CICM Administration and Security* (NN10252-611).

Centrex features for CICM

Navigation

- "Centrex feature support" (page 35)
- "Centrex IP enhancements over Centrex" (page 37)
- "Restrictions to Centrex feature support" (page 38)

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 following table lists most key features and indicates if the feature is supported CICM release SN08. The complete list of Centrex features is provided in the feature library, which is available at www.nortel.com/products. A search tool there provides a feature description for each feature name entered.

Centrex feature support for CICM

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

Feature name	Support
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
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)	Y
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
Extended Call Management (ECM / ICM)	N
Emergency Key (EMK)	Y
Forced Agent Availability (FAA)	Y
Line of Business (LOB)	Y

Feature name	Support
Night Service (NGTSRVCE)	Y
Observe Agent (OBS)	Y
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
Multi-Line Hunt (MLH)	Y
Preset Conference (PRESET CONF)	N

Centrex IP enhancements over Centrex

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

- **geographical freedom**

  A user can log on and access their Centrex services from any location that has IP connectivity with the CICM node.

- **choice of client**

  Users can choose between the m6350 SoftClient or the Nortel IP Phones, see "IP Phone models" (page 127). 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 on to any terminal connected to the CICM node. 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 on to a selected CICM node from a group of CICMs, and log on to any terminal connected to the selected node. Enterprise Profiles allow the administrator to define groupings of CICM nodes 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 node on a per-line basis. When a previously disconnected client is reconnected, the lamp status for features such as call forwarding, message waiting, and so on, 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 to Centrex IP Client Manager (CICM).

When local ringing is configured for IP Phone 2004, distinctive ringing and ring back tones originate locally (that is, out-of-band) on the set itself. The set does the ringing based on an out-of-band request.

The IP Phone 2004 has six feature keys. Up to 11 features are available by using the navigation keys. The IP Phone 2002 has four 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 Nortel IP Phone Key Expansion Module (KEM) supports 22 features on the KEM out of the 24 buttons.

CICM operating with the E911 feature (ECS Location Identification)

Navigation

E911 overview

Beginning with release SN07, the Centrex IP Client Manager (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.

To support E911, the firmware load on the CICM node must be release SN07 or later.

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 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 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 CS2000 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 gateway controller (GWC). If configured, an application running on the gateway controller repackages 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 its own database.

E911 for Nortel IP Phones

Nortel IP Phone models, identified in "IP Phone models" (page 127), must be configured to use full or partial DHCP configuration to enable the CICM ECS Location Identification functionality.

E911 for the m6350 SoftClient

Centrex IP Client Manager (CICM) m6350 SoftClient provides the user with an interface to specify their civil location description when logging on.

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.

E911 for the CICM-EM

The Centrex IP Client Manager (CICM) ECS Location Identification functionality on the CICM is activated through the CICM Element Manager (CICM-EM). 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 Centrex IP Client Manager (CICM) ECS Location Identification functionality on the gateway controller (GWC) is activated through the CICM Element Manager (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.

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

CICM operating with the GIC and GIAC features

Beginning with SN08, Centrex IP Client Manager (CICM) clients support using the Call Server 2000 (CS2000) calling features Group Intercom (GIC) and Group Intercom All Calls (GIAC) on its clients. 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

Beginning with release SN07, 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. 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

Beginning with release SN07, 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

Beginning with SN08, 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.

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

Navigation

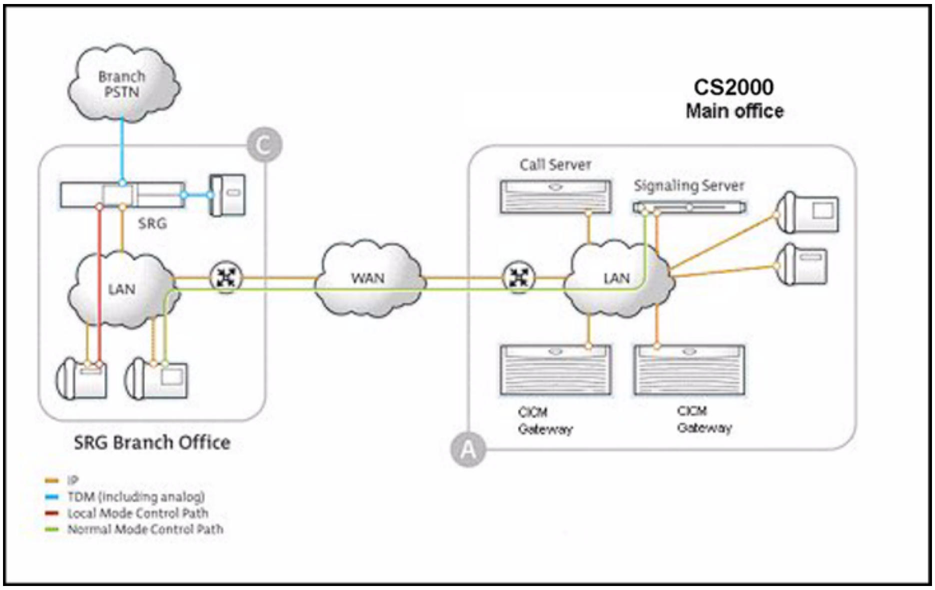
SRG operation overview

The Survivable Remote Gateway (SRG) extends Call Server 2000 (CS2000) 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 CS2000 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 CS2000 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).

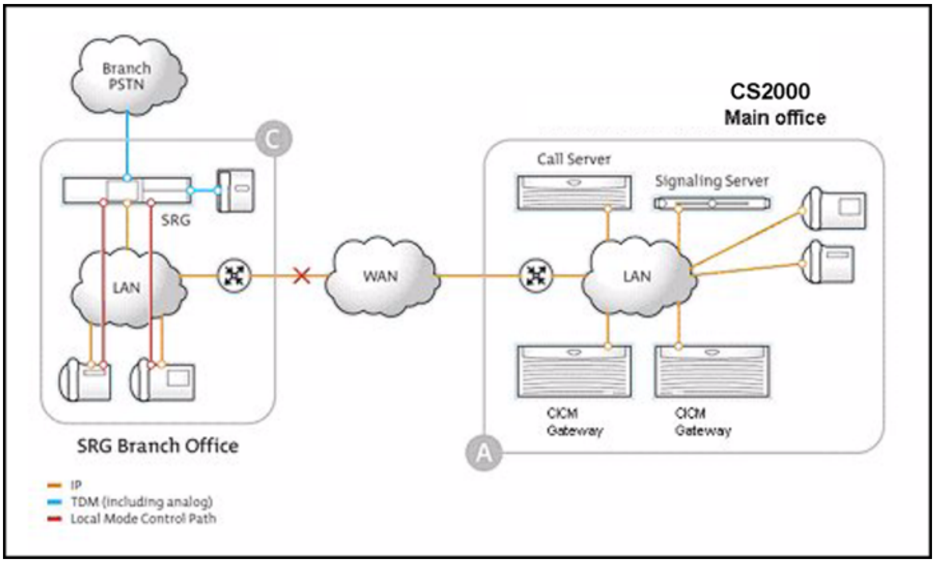
During normal mode of operation, the IP telephone sets located at the SRG50 branch office, are connected to the Centrex IP Client Manager (CICM) gateway located at the main office as shown in this figure.

Normal mode of operation in SRG



If communication with the main office is lost 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 this figure.

Local mode of operation in SRG



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. After 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

The Test Local mode timer can be cancelled by pressing the Stop key on the IP telephone set. The Test Local mode timer can be configured from the Main Office panel of the SRG Unified Manager.

Hardware and software requirements for SRG

For Centrex IP Client Manager (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 Element Manager (CICM-EM) in the CS2000 main office running the SN08
- a fully configured BCM50 in the SRG branch office with the SRG50 keycode applied

Supported IP Phone sets for SRG

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

- Phase 1 IP Phones 2002 and 2004 with firmware B76 (1.76) and later
- Phase 2 IP Phones 2001, 2002, and 2004 with firmware D98 (3.98) and later
- with release SN09, IP Phones 2210, 2211, and 2212 with firmware 97.061 and later
- Beginning with release SN09, IP Phone 2007 with firmware C23 (2.23) and later
- Beginning with release SN09, Nortel IP Phones 1120E and 1140E with firmware C16 and later

Restrictions and limitations for SRG

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

- H.323 communication between the SRG and the CS2000 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.

Ambit line gateway

Centrerx IP Client Manager supports interworking with the Ambit line gateway.

Flow-through provisioning

Beginning with release SN07, flow-through provisioning supports the passage of line and user provisioning data between the Call Server 2000 (CS2000) Management Tools server OOSGate interface, and the Centrex IP Client Manager (CICM) setup. Line provisioning involves the location of the card (blade) in a slot and circuit ranges for CICM MGRP LGRP LENs. When datafilling LGRP GRPTYPE, use M for CICM. Table LNINV automatically handles CICM when the table is datafilled from the CS2000 Management Tools server.

Datafilling the NGRP LGRP LEN

The line equipment number (LEN) for a line in an MGRP LGRP tuple (and LINE logs) is comprised of the following:

- CI<shelf_slot> denotes a CICM node on a shelf, for example, CI87
- <frame_number> is 0 to 511 for the number of the hardware frame
- <logical_group> is 0 (zero) for the logical group
- <TT> is 00 to 10 for the upper value of the CICM circuit
- <tt> is 0 to 99 for the lower value of the CICM circuit. When TT is 10, the range for tt is 00 to 23 because of the limit of 1024 tids per LGRP

H.248 signaling

Beginning with release SN07, the H.248 compliancy extensions support additional H.248 and SDP mechanisms.

Beginning with release SN07, the H.248 call control signaling supports the CICM product from release SN07 and later. Generic H.248 signaling has been enhanced for the MG9000 platform, especially for:

- ESA (Emergency Stand-Alone) Entry in association with playing tones.
- Session Descriptior Protocol (SDP), which is used to negotiate audio session information between two or more parties, for example, compression/decompression algorithm (CODEC) types and parameters.

Pluggable Authentication Module for CICM-EMs

Navigation

PAM overview

Beginning with release SN07, the Pluggable Authentication Module (PAM) of the SSPFS platform has migrated to a single centralized server that provides authentication services to VoIP management systems. The user authentication for the Centrex IP Client Manager Element Managers (CICM-EM) occurs through the HTTPS PAM and apache proxy on the SSPFS.

The CICM-EM User Interface requires a user name and password to log on. Prior to release SN07, only a single user level was supported, which provided full access to all the provisioning, maintenance and admin functions of the CICM-EM. With the introduction of PAM, the CICM-EM can be configured to access the HTTPS PAM+ proxy, passing it the username and password, and the SSPFS then returns a user authentication level to the CICM-EM, or rejects the username and password if they are not a valid combination. This user authentication level is then used by the CICM-EM to restrict access to functions that are not appropriate for particular user groups.

Authentication using the SSPFS only occurs when the user is accessing the CICM-EM through the Web interface. PAM does not change the method to authenticate users who are logging on using a Telnet session.

The procedures to configure PAM and the apache proxy server for CICM-EMs are in *CICM Configuration Management* (NN10240-511).

Login

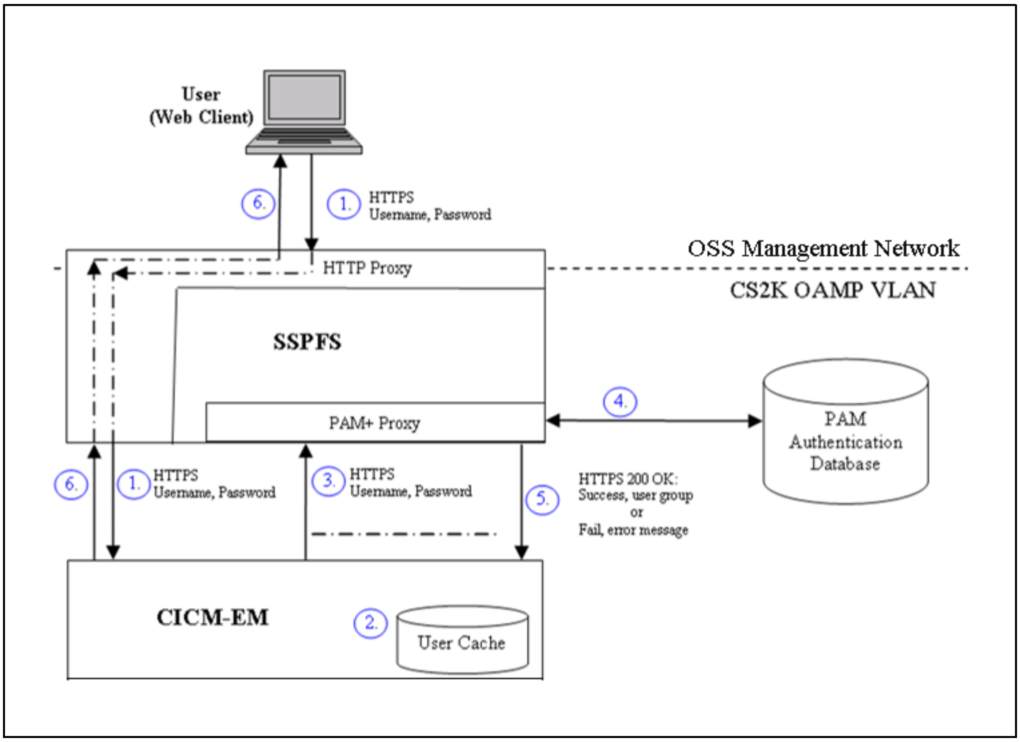
In releases prior to SN07, the user name and password supplied when logging on to the Centrex IP Client Manager Element Manager (CICM-EM) corresponded to local user accounts on the EM. Beginning with release SN07, user name and password can be configured as a global VoIP account managed on a centralized authentication database. This database interfaces to VoIP management tools through the PAM proxy located on the SSPFS.

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

User authentication through the SSPFS PAM proxy

The behavior provided by Centrex IP Client Manager Element Manager (CICM-EM) user authentication through the PAM proxy running on the SSPFS is illustrated in the following figure.

HTTPS PAM proxy and CICM-EM integration



The numbers in the figure refer to these steps in the user authentication process:

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

2. CICM-EM uses the supplied username and password as a key to search a cache of recently authenticated users. Each user entry in the cache contains a corresponding username and password for a temporary local user account assigned to that user. If the user is present in the cache, the mapped local username and password is passed back to the PAM and the process proceeds to step 5 (with successful authentication).

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

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

5. If an authentication is successful, the PAM proxy responds with a list of VoIP user groups to which the user belongs. CICM-EM has a list of pre-defined local user groups that are equivalent to the user groups

returned by the PAM proxy. CICM-EM creates a temporary local user account on the CICM-EM when a response to a user authentication request is successful. The temporary local user account is added to the pre-defined local user groups that are equivalent to the VoIP user groups returned by the PAM proxy.

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

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

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

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

User authentication levels

VoIP User authentication levels on the PAM proxy are organized into five separate domains, with each domain containing 5 separate levels of user authentication. This provides a total of 25 user authentication levels, as shown in the following table.

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

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

Local user authentication

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

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

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

Configuration for the SSPFS PAM proxy

The configuration of the IP address to use for the SSPFS PAM proxy is configured by Nortel installers during the initial software configuration of the CICM setup (using the preboot command). The user can select to use HTTP or HTTPS (secure HTTP) to communicate with the PAM proxy. If HTTPS is selected, the user is prompted to enter the Fully Qualified Domain Name (FQDN) of the PAM server. HTTPS requires that a certificate from a valid signing authority is installed on the SSPFS.

Logs for PAM

This feature logs the following events on the Integrated Element Management System (IEMS):

- a user was successfully authenticated through PAM
- a user was unsuccessfully authenticated through PAM
- a Request Timeout occurs on the PAM proxy, which cleared the next time an authentication request is successfully processed through the PAM server

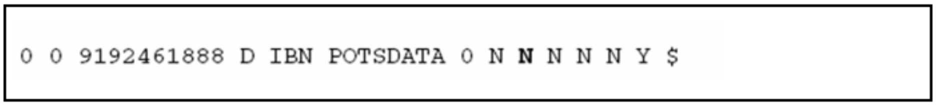
Preset Conference for VoIP

The Preset Conference feature of Voice over IP (VoIP) supports CICM using it. This feature supports the following types of line on both North American and International markets:

- CICM lines for Nortel IP Phones and m6350 SoftClients
- MG9000 P-phones and IBN lines

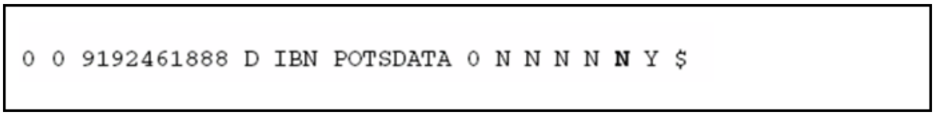
For VoIP, these limitations apply to the Preset Conference functionality.

- Up to 25 conferences are supported in Preset Conference.
- Preset Conference is implemented in non-hybrid scenarios only. In the hybrid environment, the support remains the same.
- The ADDON functionality for Preset Conference is not supported for VoIP. The subfield ADDON in the table PRECONF is set to N.



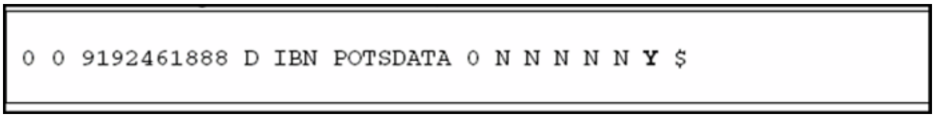
```
0 0 9192461888 D IBN POTSDATA 0 N N N N N Y $
```

- The Audio Tone Detector is a component of a DMS maintenance trunk module (MTM) and the functionality is not available through the Universal Audio Server (UAS). This activity does not support the ATD functionality of the Preset Conference. The subfield ATD in the table PRECONF should be set to N.



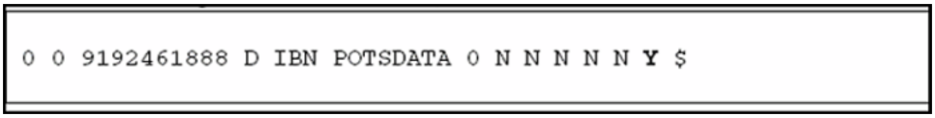
```
0 0 9192461888 D IBN POTSDATA 0 N N N N N Y $
```

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



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

- The options Conferee Class P and D are supported for CICM, but not Conferee Class A and C.
- The Preset Conference options MADNOPT and NARS is not supported through this activity. Omit datafilling it.



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

- The Preset Conference uses conference tones (for example, the conference entry or exit tone). The Preconference tones PCNOR (Preset Conference NotificatiOn Tone) and PCALR (Preset Conference Precedence Notification Tone) are not supported through this activity.

For a detailed description of the Preset Conference, refer to *DMS 100 Family NA100 Translation Guide, Volume 13 of 20*, 297-8001-350.

Quality of Service reporting for CICM node calls

In Voice over IP (VoIP) networks, the Quality of Service (QoS) of calls can be adversely affected by the components in the network. Unlike Time Division Multiplexed (TDM) networks where the voice quality is consistent for all calls, VoIP networks can experience a different voice quality on each call.

QoS statistics can be used for:

- network engineering
- trend analysis
- troubleshooting network problems
- service-level agreement (SLA) validation

When enabled, QoS statistics are accumulated on active calls on Nortel IP Phones. When a call is placed on hold, the QoS statistics are suspended until the call is resumed. When a compression/decompression algorithm (CODEC) is renegotiated for a call, the QoS statistics report only from the start of the new CODEC. The reporting of QoS statistics is enabled or disabled through:

- the element manager of the gateway controller (GWC) for regular QoS statistics
- the CICM Element Manager (CICM-EM) for the extended QoS statistics

Refer to the procedure *Enabling or disabling QoS reporting for a CICM node*, in *CICM Configuration Management* (NN10240-511).

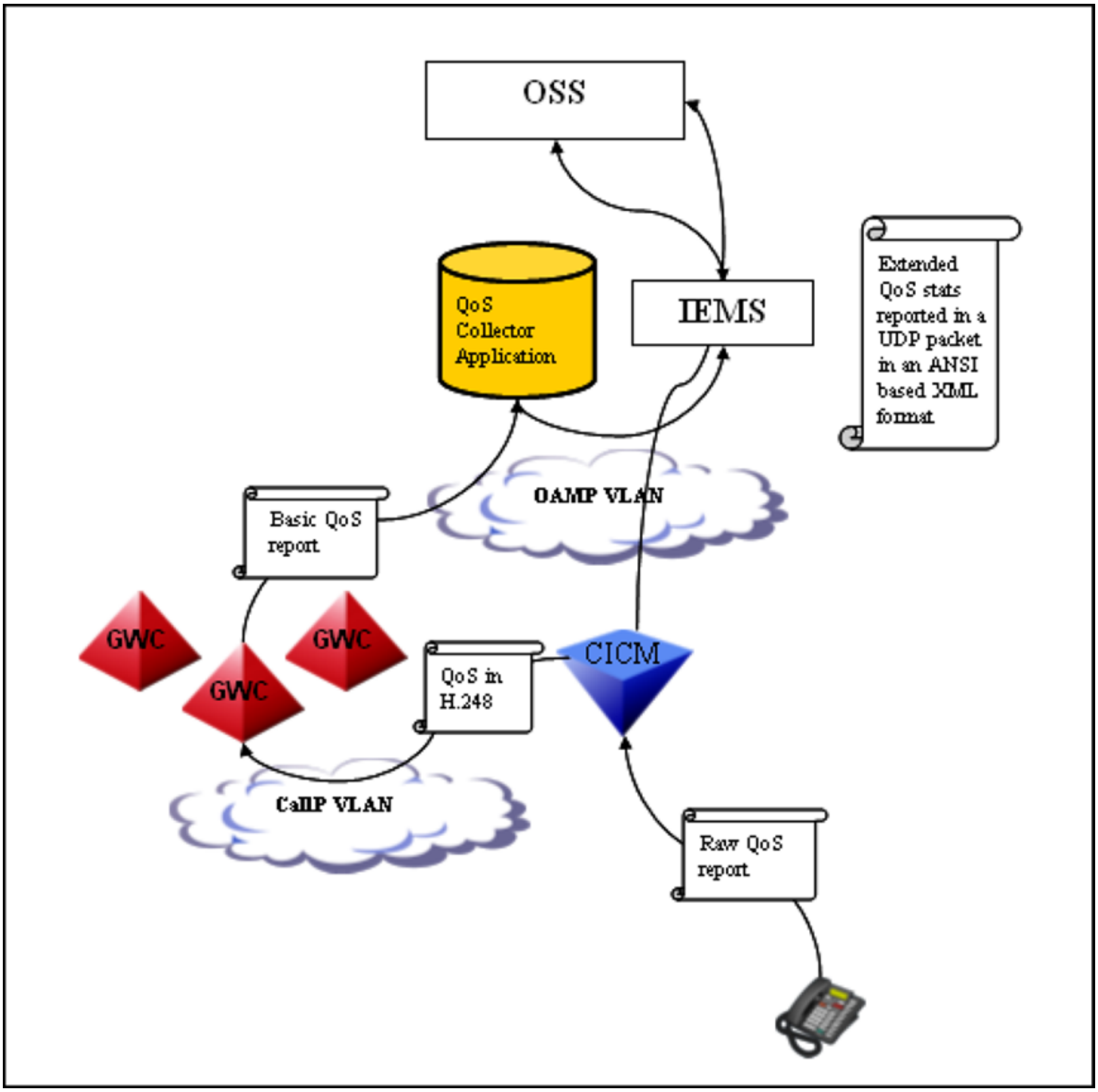
The QoS reporting involves different statistics parameters for the phase 1 and phase 2 Nortel IP Phones. The phase 1 phones have basic QoS statistics while the phase 2 phones have extended QoS statistics. The extended QoS statistics are sent to a configured destination by UDP in an ANSI-based .xml file format. The destination becomes the extended call server. Each statistic that cannot be obtained from an IP phone is reported upwards to the GWC or the extended QoS server with value of 0 (zero). All

QoS statistics are descibed in QoS and extended QoS statistics for a CICM node, and the procedure to view them is *Viewing QoS statistics of a CICM node*, in *CICM Performance Management* (NN10248-711).

QoS statistics, as shown in "A CICM node reporting QoS statistics" (page 71), are reported in this manner:

- At the end of a call, the Centrex IP Client Manager (CICM) node reports the QoS statistics. Each ephemeral associated with a call reports the QoS statistics separately. When the GWC instructs the CICM node to subtract the QoS statistics of the ephemeral termination, the statistics are sent to:
  - — the GWC over H.248
  - — the server for extended QoS statistics over a User Datagram Protocol (UDP) in an ANSI-based .xml file format
- The GWC reformats the statistics from the CICM node into a binary format and sends the QoS report to the QoS Collector Application (QCA)
- The QCA manages QoS streams from multiple GWCs by reformatting the data to an IDPR (Inter-Domain Policy Routing) format and stores the data on a disk.

A CICM node reporting QoS statistics


OSS
IEMS
QoS Collector Application
Extended QoS stats reported in a UDP packet in an ANSI based XML format
OAMP VLAN
Basic QoS report
GWC
GWC
GWC
QoS in H.248
CICM
CallP VLAN
Raw QoS report

Nortel IP Phone models depend on minimum firmware releases to enable QoS reporting, as listed in the following table. For information on upgrading firmware, see *Upgrading firmware on IP phone sets* in *Upgrading CICM* (NN10230-461).

Minimum firmware per IP Phone for QoS basic and extended reporting

Nortel IP Phone model	Minimum firmware for basic QoS	Minimum firmware for extended QoS
1120E	C16	C16
1140E	C16	C16
2007	not applicable	not applicable
2001	3.98	3.98
2002 phase 1	1.76	not applicable
2002 phase 2	3.98	3.98
2004 phase 1	1.76	not applicable
2004 phase 2	3.98	3.98
2033	not applicable	not applicable
2210	not applicable	not applicable
2211	not applicable	not applicable
2212	not applicable	not applicable
M6350	not applicable	not applicable

Border Control Point for CICM

Beginning with release SN09, a call terminating to a Centrex IP Client Manager (CICM) line is allowed to complete even when the user associated with the directory number (DN) is not logged on to a CICM client (IP Phone or m6350 SoftClient) at the time of the call. This allows interactions with features such as call forwarding and voice mail while the user is not logged on. Also, the user can log on to the CICM client while receiving the call, be alerted to the call, and answer it.

Prior to release SN09, the feature interactions are achieved by inserting a real-time transport protocol (RTP) media portal for calls terminating to a logged CICM user. This provides the originating point with a real network location to send its pre-answer audio stream to, and automatically discovers the media address of a terminal that logs on and starts transmitting its audio stream. This establishes a two-way speech path when the user logs on and answers the call.

Prior to release SN09, an RTP media portal is required between a CICM node and its gateway into the network. The portal terminates calls made to CICM users who are not logged on so that features such as call forwarding or voice mail can be used. The portal also enables users who log on while being called to be alerted and to respond to the call.

Beginning with release SN09, the requirement for the RTP media portal no longer applies to CICM calls that do not use the NAT traversal capability. This is achieved by delaying the Session Description Protocol (SDP) for terminating CICM users until the user logs on, which reveals the media address of the CICM client. Refer to "Pre-answer and mid-call SDP renegotiation" (page 32). An RTP media portal is still required when a CICM user wants carrier-hosted Centrex IP feature interactions enabled, or to fulfill media NAT traversal and media anchoring for Lawful Intercept (LI).

For the description of the portal, see also "Border Control Point" (page 88) 6in context of firewalls and NAT traversals.

Time zones

Beginning with release SN07, the Multi time Zone (MTZ) feature of DMS and CS2000 enables Centrex IP Client Manager (CICM) to store the local time of the user on the switch. CICM features can be activated relative to local time.

Virtual Connections Admission Control for CICM

Navigation

VCAC overview

Beginning with release SN07, Virtual Connections Admission Control (VCAC) provisioning supports Centrex IP gateways such as Centrex IP Client Managers (CICM). It provides Gateway element manager (GWC-EM) Internet transparency, that is, an auto-discovery by the network.

The model for this download of data has been designed for the fixed-lines IAD deployment, and occurs when the gateway is associated to an adjacent middlebox. This feature allows VCAC to function for CICM gateways because unlike the small-lines IAD solution, the CICM gateways reside in the TSP (VoIP) domain.

When CICM users log on to the CICM terminals (Nortel IP Phones or m6350 SoftClients), a message is sent to the gateway controller (GWC). This message contains the discovered adjacent middlebox of the terminal or endpoint. The CallP ITA function then looks-up this middlebox in the GWC static tables.

This capability allows a user to provision a set of root (top-level) middleboxes, allowing the GWC-EM to send all the underlying middleboxes to the GWC thereby ensuring that when a CICM user logs on, the middlebox is available on the GWC.

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

- **GWC-MIDDLE-BOX-MIB**
- **GWC-MIDDLEBOX-RSRCUSAGE-MIB** (the resource usage of the LBL)

VCAC provides the following functionality:

- provision (from the OSS and GWC-EM GUI) a set of root middleboxes (up to 5) against CICM nodes
- change the current provisioning of root middleboxes against provisioned CICM nodes
- display or query the root middleboxes that are provisioned against a CICM node

VCAC executes as part of the CS2000 Management Server.

VCAC user interfaces

The following GUIs are used to interface VCAC:

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

In the context of VCAC, the gateway is synonymous with a Centrex IP Client Manager (CICM) node.

Refer to the procedure Updating Auto-discovery networks, in *CICM Configuration Management* (NN10240-511).

The following XML commands are available for VCAC:

- **AssocMG**
- **ChangeRootMiddleBoxes**
- **QueryMG**

The on-line help facility provides information on the use, syntax, and valid values for these user GUI modifications.

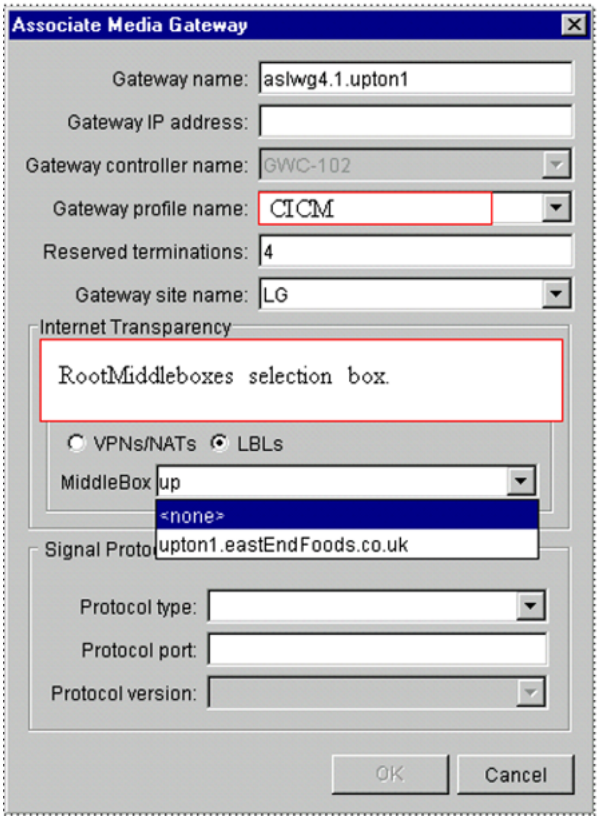
CICM node provisioning changes

The association of a Centrex IP Client Manager (CICM) node to a GWC allows the user to provision a set of root middleboxes. Nodes that are already provisioned can also be changed to have a different set of root middleboxes (or none).

Associate Media Gateway GUI

The Associate Media Gateway dialog GUI, shown in the next figure, displays an Internet transparency panel. The panel is displayed when a Centrex IP Client Manager (CICM) gateway (node) has been selected. The user may select up to 5 root middleboxes to associate with the CICM gateway. These are selected to define the roaming area where VCAC functions for the CICM users or endpoints.

Associate Media Gateway dialog



Associate Media Gateway

Gateway name: aslwg4.1.upton1

Gateway IP address:

Gateway controller name: GWC-102

Gateway profile name: CICM

Reserved terminations: 4

Gateway site name: LG

Internet Transparency

RootMiddleboxes selection box.

○ VPNs/NATs ● LBLs

MiddleBox up

<none>

upton1.eastEndFoods.co.uk

Signal Proto

Protocol type:

Protocol port:

Protocol version:

Change gateway GUI

The change gateway Root Middleboxes dialog was created to allow users to modify, or remove, the Root Middleboxes associated with provisioned Centrex IP Client Manager (CICM) gateway (node).

Root middleboxes selection

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

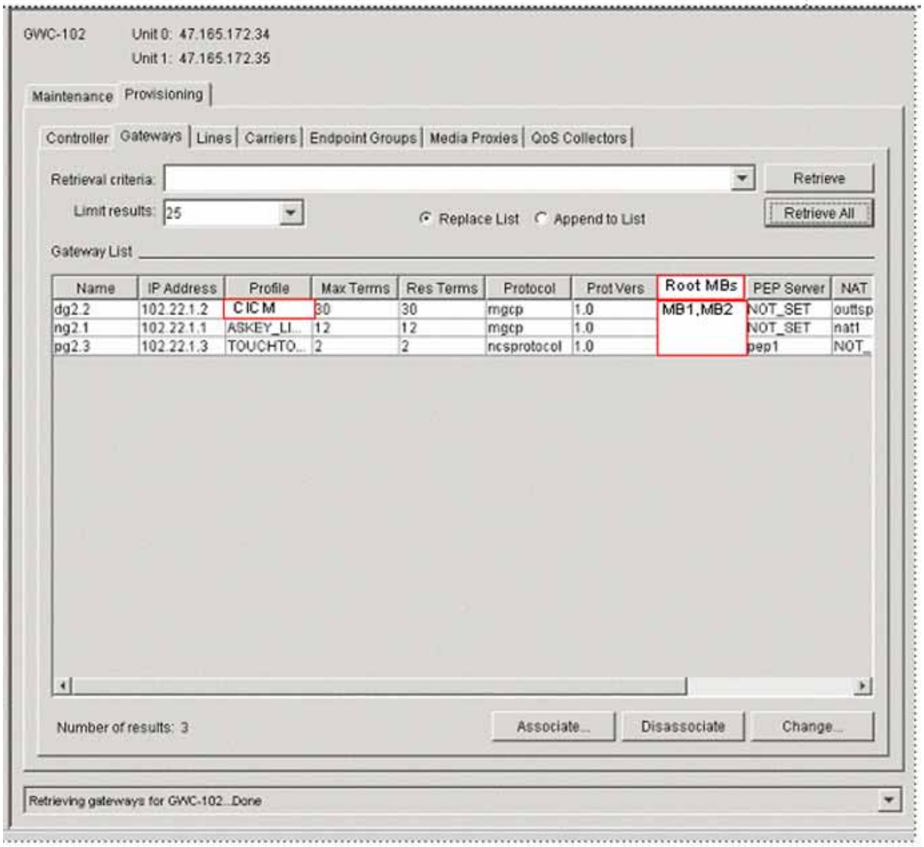
XML interface

The AssocMG and QueryMG interface allows or displays root middleboxes. The interface **ChangeRootMiddleboxes** has been added. If any request is unsuccessful, an error message is returned.

GWC-EM provisioning

The Gateway element manager (GWC-EM) was modified to display the root middleboxes that are provisioned against the Centrex IP Client Manager (CICM) gateways (nodes), as shown in this figure.

The GWC-EM gateways panel



GWC-102 Unit 0: 47.165.172.34
Unit 1: 47.165.172.35

Retrieval criteria:

Limit results: 25

● Replace List ○ Append to List

Gateway List

Name	IP Address	Profile	Max Terms	Res Terms	Protocol	Prot Vers	Root MBs	PEP Server	NAT
dg2.2	102.22.1.2	CICM	30	30	mgcp	1.0	MB1,MB2	NOT_SET	outtsp
ng2.1	102.22.1.1	ASKEY_LI...	12	12	mgcp	1.0		NOT_SET	nat1
pg2.3	102.22.1.3	TOUCHTO...	2	2	ncsprotocol	1.0		pep1	NOT_

Number of results: 3

Retrieving gateways for GWC-102...Done

Authorization for commands

The security for the GUI Client and OSSgate interface includes support for permission (authorization) levels for commands. Each command is associated with one or more user groups. To execute a command, a user must belong to at least one of the associated user groups. This table lists user groups associated with the new commands.

New Internet transparency commands authorization

Command	User Group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
ChangeRootMiddleboxes	X	X			

Limitations of VCAC

The limitations of VCAC are:

- The gateway controller (GWC) has a maximum limit of 2000 middleboxes.
- Internal counting limits the provisioning of gateways (Centrex IP Client Manager (CICM) nodes) onto the same GWC as the associated chain of LBLs, which must be provisioned onto one GWC.
- The CentrexIP users cannot roam outside of their provisioned enterprise area, and expect VCAC to function.

Engineering information for CICM

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).

Navigation

Carrier VoIP platform

Centrex IP Client Manager (CICM) release SN09 is a combined hardware and software release. It applies to both International and North American customers.

Central office requirements

Central office requirements to accommodate having Centrex IP Client Manager (CICM) in the network include:

- "Call Server 2000 platform software dependencies" (page 84)
- "Administration Data Network Infrastructure—Admin LAN" (page 84)
- "Traffic Data Network Infrastructure—Client LAN" (page 85)

Call Server 2000 platform software dependencies

The Centrex IP Client Manager (CICM) nodes use the Microsoft Windows XP Operating System (OS). The CICM Element Managers (CICM-EM) use Microsoft Windows 2000 Server OS.

The software dependencies of CICM, beginning with release SN09, are listed in this table.

Software load configuration

System	Minimum software load	Recommended software load
CICM node	9.0	9.0
CICM-EM	9.0	9.0
CS2000	(I)SN09	(I)SN09
CS2M (SDM)	CS2M0090	CS2M0090
GWC	GC090	GC090
IEMS	(I)SN09 IEMS	(I)SN09 IEMS
IP Phones 2002, 2004 (Phase I)	1.57	1.76
IP Phones 2001, 2002, & 2004 (Phase II)	3.45	3.98
IP Phone 2033	S13	S18
IP Phones 2210, 2211, 2212 (wireless)	97.065	97.065
M6350	9.0	9.0
IP Phone 1120E	C1B	C1B
IP Phone 1140E	C1B	C1B
IP Phone 2007	C27	C27

Administration Data Network Infrastructure—Admin LAN

The telco private network infrastructure is used for all administrative functions of the Centrex IP Client Manager (CICM) that are not related to Voice over IP (VoIP) traffic. It is referred to as the Administration (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, so it must be physically separate from the Client LAN.

The Admin LAN connects directly to the master and slave CICM Element Manager (CICM-EM) pair and allows the two CICM nodes to communicate with each other.

The Admin LAN connects PCs or workstations for remote access to the CICM-EMs. It is used for all administrative and access functions of the CICM nodes. The Admin LAN does not carry call signaling (UNIStim messages) or voice traffic.

The telco's Admin LAN must provide the following resources:

- direct connection to the master and slave
- a PC for performing configuration, administration, upgrades, and monitoring
- isolation of the Admin LAN from the Client LAN
- secured remote access to the CICM-EMs by Nortel support personnel

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 Centrex IP Client Manager (CICM) nodes. 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 the 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 over IP and UDP over 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 a CICM node 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) network include:

- CICM terminals (Nortel IP Phones)
  - — hosted by the same CICM node

  - — hosted on another CICM node

- TDM trunk gateways (for example, MG15000)
- analog line gateways (for example, MG9000, Mediatrix 1124)
- voice processing servers (for example, MS2010)

Detailed traffic capacity information is provided in the *Centrex IP Client Manager (CICM) Engineering Guide*, 297-5551-100.

Security of the Admin and Client LANs

Access to the Administration (Admin) LAN is separated from the Client LAN by a user ID and password.

Routing directly between the Admin and Client LAN is disabled in the active Centrex IP Client Manager (CICM) node. To test whether a client PC or Nortel IP Phone is visible on the Client LAN, you must:

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

The commands **`ping`** and **`tracert`** may not be used for deployments where the CICM node and its clients are separated by firewalls and NATs. Messages from **`ping`** and **`tracert`** are not able to traverse firewalls and NATs.

The commands **`ping`** and **`tracert`** are the only ones to affect the Client LAN. No other commands are installed on the CICM nodes, 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 Element Manager (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 user names and passwords.

Firewall and NAT traversal

Firewalls and Network Address Translators (NAT) 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 Centrex IP Client Manager (CICM) node pair is located in the Private Signalling Network in the Carrier's managed IP network as part of the Carrier's IP address space. The Nortel 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 node through the Demilitarized 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 use Carrier Centrex IP services should activate the minimally restricted UDP policy on their firewalls that normally perform dynamic stateful packet filtering. This allows a User Datagram protocol (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; see also "Border Control Point" (page 88)
  - RTCP (RTP Control Protocol) for periodic network performance monitoring
  - UNIStim FTP packets for Nortel IP Phone firmware downloads 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

The Nortel Centrex IP supports all types of Network Address Translation (NAT). NAT is also referred to as a Network Address and Port Translator (NAPT), regardless whether it is a:

- full cone NAT
- restricted cone NAT
- port-restricted NAT
- symmetric NAT

Every NAT must have at least a two-minute UDP lease period.

Border Control Point

The Border Control Point (formerly the RTP Media Portal) provides secure inter-working for calls between end points in different enterprise networks, and provides NAT traversal capabilities for these end points.

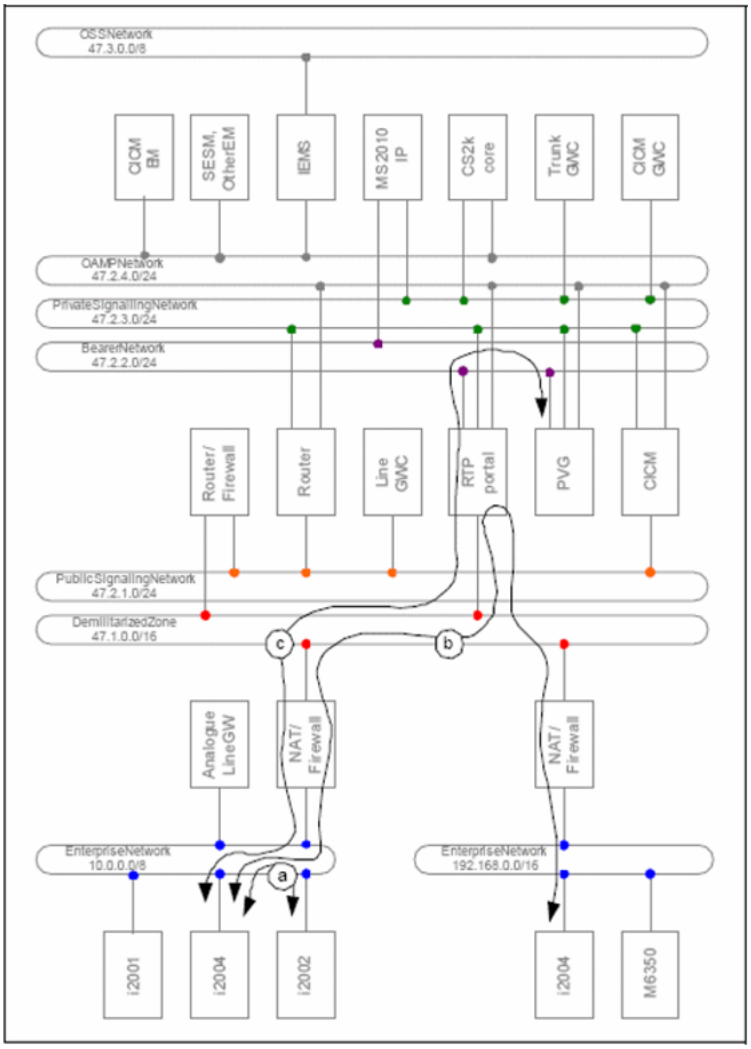
Border Control Point usage summary

Terminating GW	Originator and terminator in the same enterprise network?	RTP portal inserted?
Same CICM as originator	Y	N
	N	Y
Another media gateway or CICM on the same GWC	Y	N
	N	Y
A media gateway or CICM on a different GWC	Y	N
	N	Y
A media gateway or CICM on a different CS2000	Does not matter	Y

"Border Control Point usage in the Call Server 2000 network" (page 89) shows the flow of RTP packets between end-points for the following call scenarios:

- A call between two Centrex IP Client Manager (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 an MG15000)

Border Control Point usage in the Call Server 2000 network



For the correct operation of the CICM node when using the Border Control Point, the NAT must be provisioned on both the CS2000 Management Server and the CICM-EM. Additionally, if Border Control Point is not available, then all calls made to a user who is not logged on will be routed to treatment.

For additional information, see also "Border Control Point for CICM" (page 73).

For details of Border Control Point usage and how NAT traversal works, refer to the *Centrex IP Client Manager (CICM) Engineering Guide*, 297-5551-100.

Security of the OAMP and Public Signalling Subnets

The disruption of the Operations, Administration, Maintenance, and Provisioning (OAM/P) subnet by the Public Signaling Subnet is handled the same way as described in "Security of the Admin and Client LANs" (page 86).

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 of CICM

The Centrex IP Client Manager (CICM) setup minimizes 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 with SAM21

In the SAM21-based Centrex IP Client Manager (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 Integrated Element Management System (IEMS) and other related Operations, Administration, Maintenance, and Provisioning (OAM/P) interfaces, and towards clients for public signaling interfaces through UNIStim. Failure of one node does not impact service (that is, no impact occurs to any of the communications towards the GWC, OAM/P systems, or clients), and no impact on any stable active stable calls.

Software resiliency

Only the core components of the operating system (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 Centrex IP Client Manager (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 with SAM21

The SAM21-based Centrex IP Client Manager (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.

Positioning the CICM hardware

The Centrex IP Client Manager (CICM) nodes and CICM Element Managers (CICM-EM) are collocated with the CS2000 to use 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 nodes and:

- the telco’s administration LAN, which includes the master and slave CICM-EM pair
- the client LAN

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

Carrier VoIP and Carrier CICM

Centrex IP Client Manager (CICM) release (I)SN09 supports the Carrier Voice over IP (VoIP) (CS2000) version of CICM.

Redundancy of the CICM nodes and CICM-EMs

Beginning with SN08, Centrex IP Client Manager (CICM) design is 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.

Any CICM node or element manger (EM) 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).

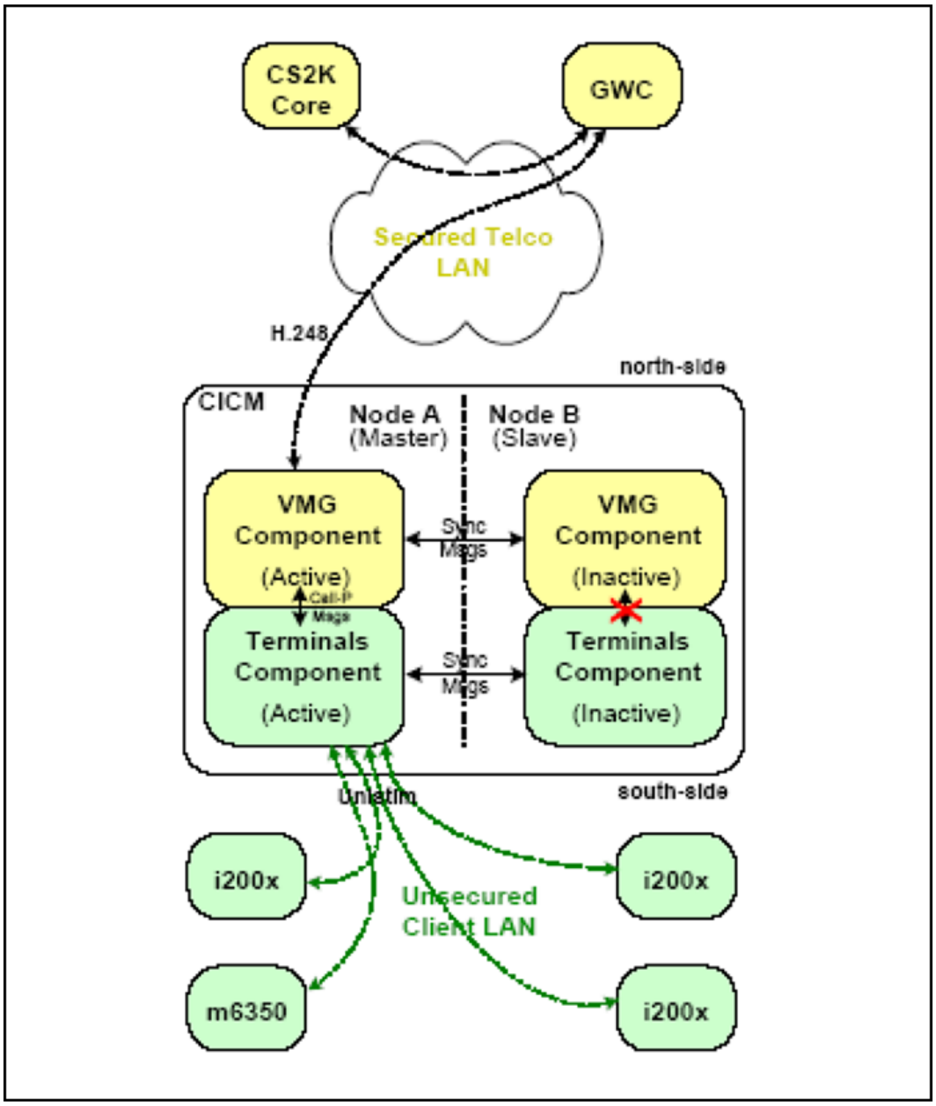
Under normal operation, each CICM node appears to the CS2000 as a VMG unit. A client can initially log on to the master CICM node through a floating UNIStim IP address and receive service. With the master and a slave node operation, the CS2000 sends messages only to the master CICM node.

Pairs of CPU cards provide hardware redundancy for the CICM applications. The two CPU cards present themselves to the gateway controller (GWC) as a single network entity. One CPU is the maste, while the other is a hot-standby slave.

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 Microsoft Windows XP operating system and CICM software. From the software perspective, each domain is regarded as a separate CICM node.

The redundancy provided by the software and hardware components of the CICM nodes and the CICM-EMs is shown in the next figure. The figure shows that each CICM node (that is, each half of the gateway) executes an identical software load.

CICM redundancy model



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

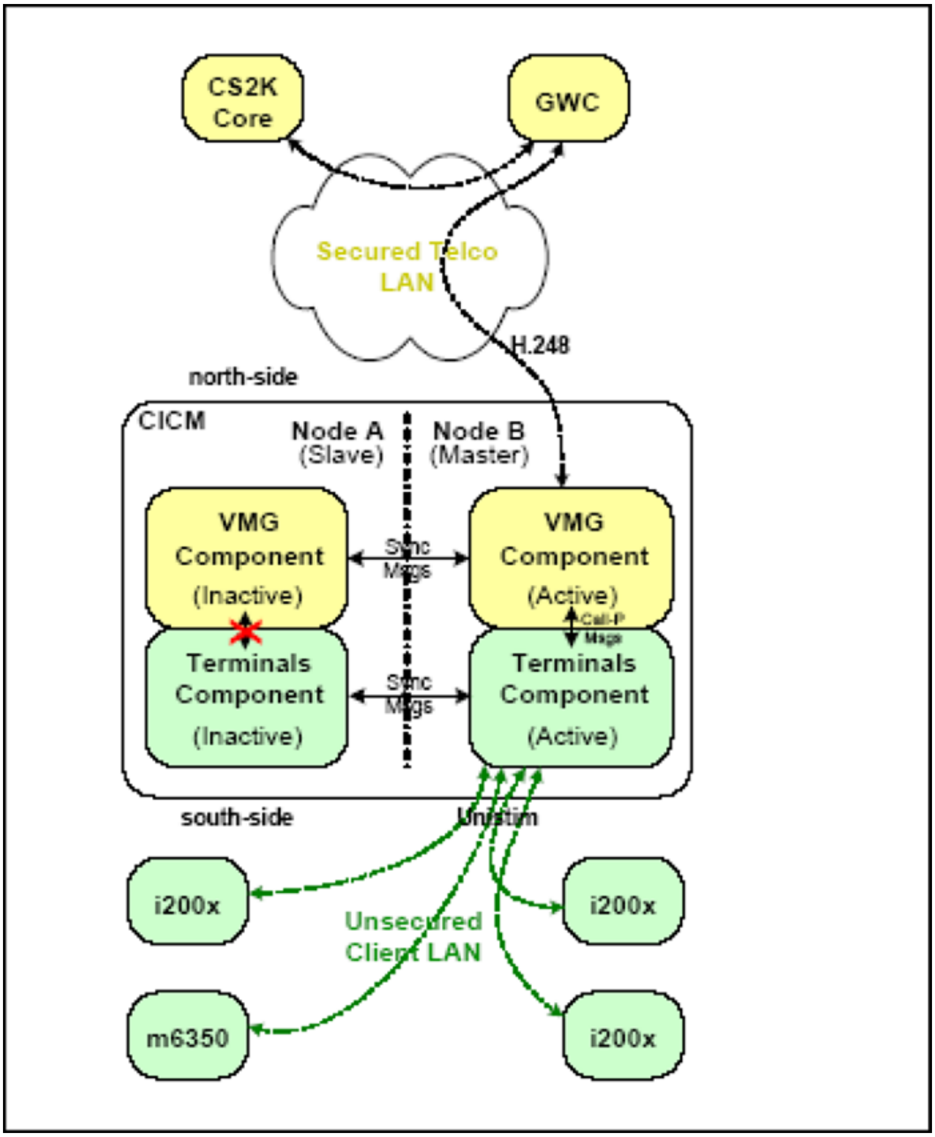
Both the H.248 and UNIStim interfaces each make use of their own floating IP address that is bound dynamically to the master node’s interface. Each component shown in "CICM redundancy model" (page 94) is responsible for managing its floating address and ensuring it is swapped to the mate on a switch of activity (SWACT).

The inactive virtual media gateway (VMG) component keeps in constant near-full synchronization with the active side. The double-headed arrow in the figure indicates the active side. 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 to its mate, slave node. This implies that following a SWACT, communication with the GWC is maintained by the newly promoted master, node B in the next figure. The i200x numbers that appear in the figure, refer to models of IP Phones. The figure is applicable to all Nortel IP phones.

CICM following a switch of activity



A switch of activity is carried out internally one component at a time. The process begins with the VMG and ends with the Terminals component. While 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 after it is completed, both nodes will have entirely exchanged roles. An operator can manually invoke a SWACT but can never select individual components or their order of switching.

As part of the SWACT, the Centrex IP Client Manager (CICM) node ensures that the floating H.248 and UNIStim IP addresses are moved to the newly promoted master. This ensures continued communication with both the GWC and clients (terminals).

A controlled SWACT occurs when initiated manually by an operator. Following a controlled SWACT, the master and slave nodes assume each other's previous role. A manual SWACT is usually executed in order to perform maintenance activities.

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

During 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-dialed call

Hardware of a CICM-EM and CICM node

This section describes the hardware components of a CICM Element Manager (CICM-EM) and a Centrex IP Client Manager (CICM) node.

Navigation

Hardware overview

The Centrex IP Client Manager (CICM) hardware platform provides the functionality that allows CICM clients to access the full range of Centrex services using VoIP.

The CICM configuration 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 Call Sserver 2000 (CS2000).

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

NEBS compliance, product standards, and regulatory requirements

Navigation

- "Product safety standards" (page 98)
- "EMC standards" (page 98)
- "Telecom center installation standards" (page 99)

Additional information on engineering standards, compliance and noncompliance, and compliance testing is in 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 electromagnetic compliance (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, including those for European TTI Standards Institue (ETSI), are:

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

The North America Telecom center installation standards requirements, including those for Network Equipment Building System (NEBS), 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

Hardware frames

Centrex IP Client Manager (CICM) is shipped as a set of components fitted into a standard NEBS3-compliant frame (also called a cabinet). Beginning with release SN08, CICM also uses the Service Application Module Frame (SAMF) and Call Control Frame (CCF).

Navigation

- "SAMF Frame" (page 99)
- "Call Control Frame" (page 100)
- "CICM cabinet" (page 102)

SAMF Frame

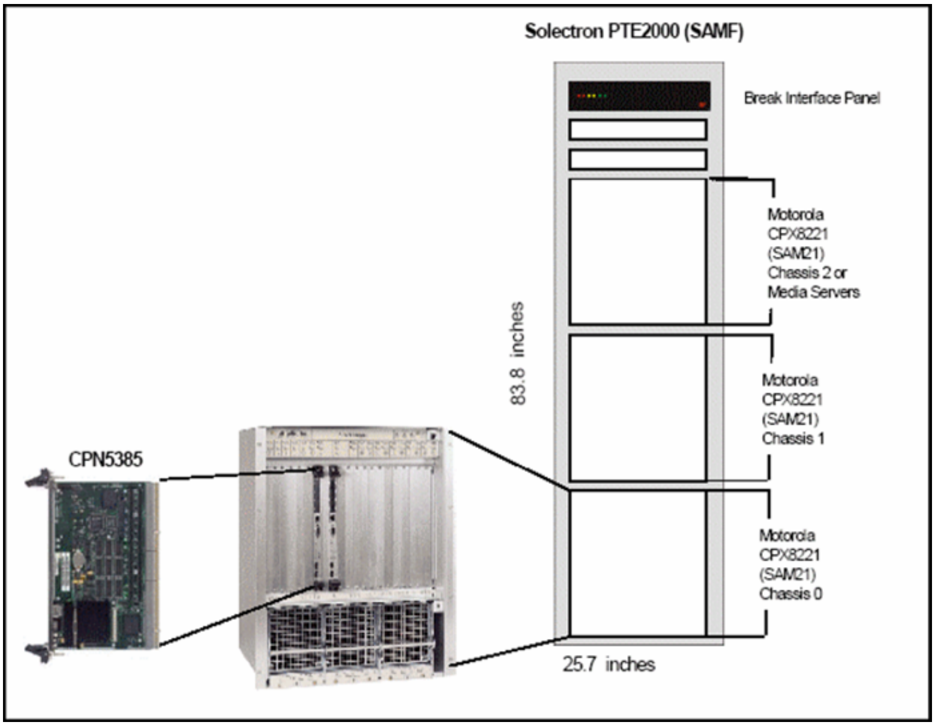
The characteristics of the Service Application Module Frame (SAMF) are:

- NEBS3 compliant
- supported configurations:
  - up to 3 SAM21 chassis
  - up to 2 SAM21 chassis plus up to 6 Media Server Applications (for example, 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 cannot be removed.

This figure shows the components of a SAMF.

SAMF components


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

Call Control Frame

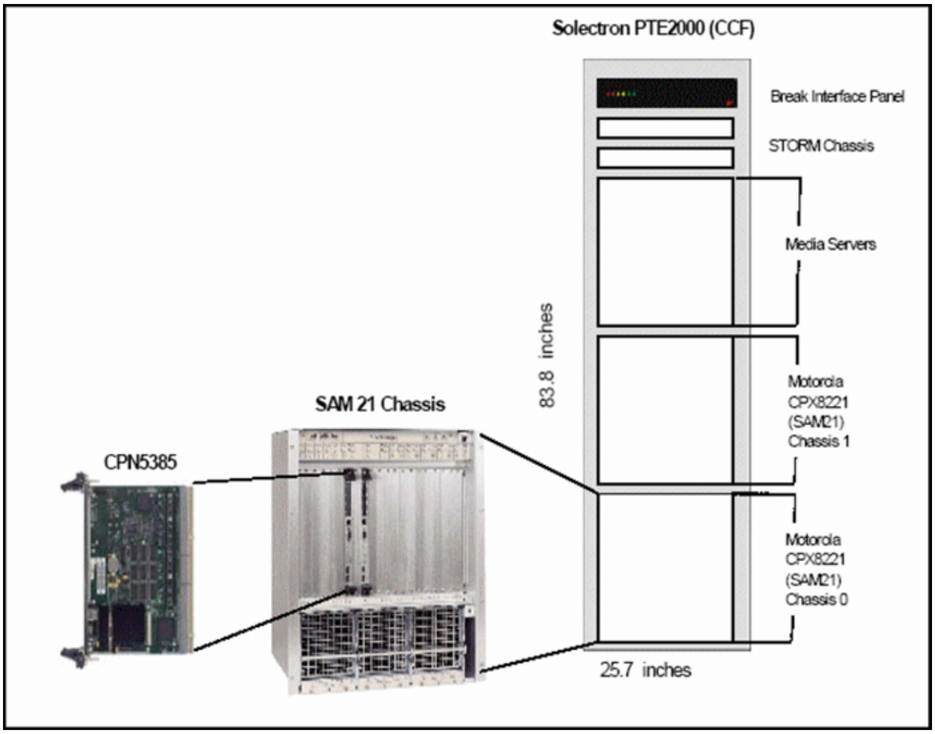
The characteristics of the CCF are:

- NEBS3 compliant

- Configurations supported:
  - maximum of two SAM21 chassis
  - maximum of two SAM21 chassis plus up to 6 Media Server Applications (for example, MS2010 IP Chassis)
  - STORM storage systems
- four system slots already occupied (2 HSC cards and 2 shelf controller cards)
- two 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 Element Manager (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.
  - maximum of eight Centrex IP Client Manager (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.
  - maximum of six gateway controller cards (GWC) (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.

This figure sows the components of a CCF.

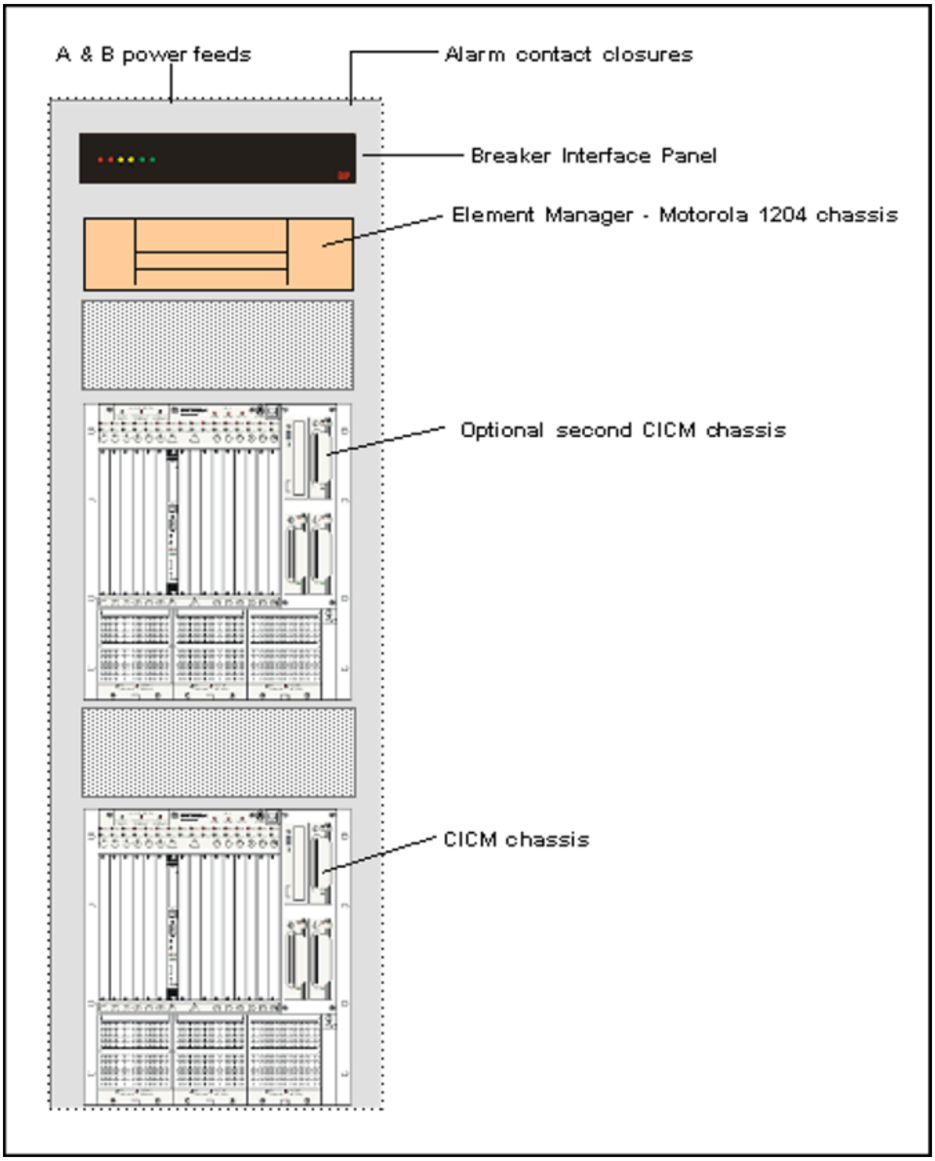
CCF components



CICM cabinet

The Centrex IP Client Manager (CICM) hardware for a SAM16 platform is shipped in a NEBS-compliant 19-inch wide PTE 2000 frame, as shown in "Two SAM16 chassis with hardware in PTE 2000" (page 103). The frame includes a power unit (BIP), element manager in a Motorola 1204 chassis, and one or two SAM16 chassis.

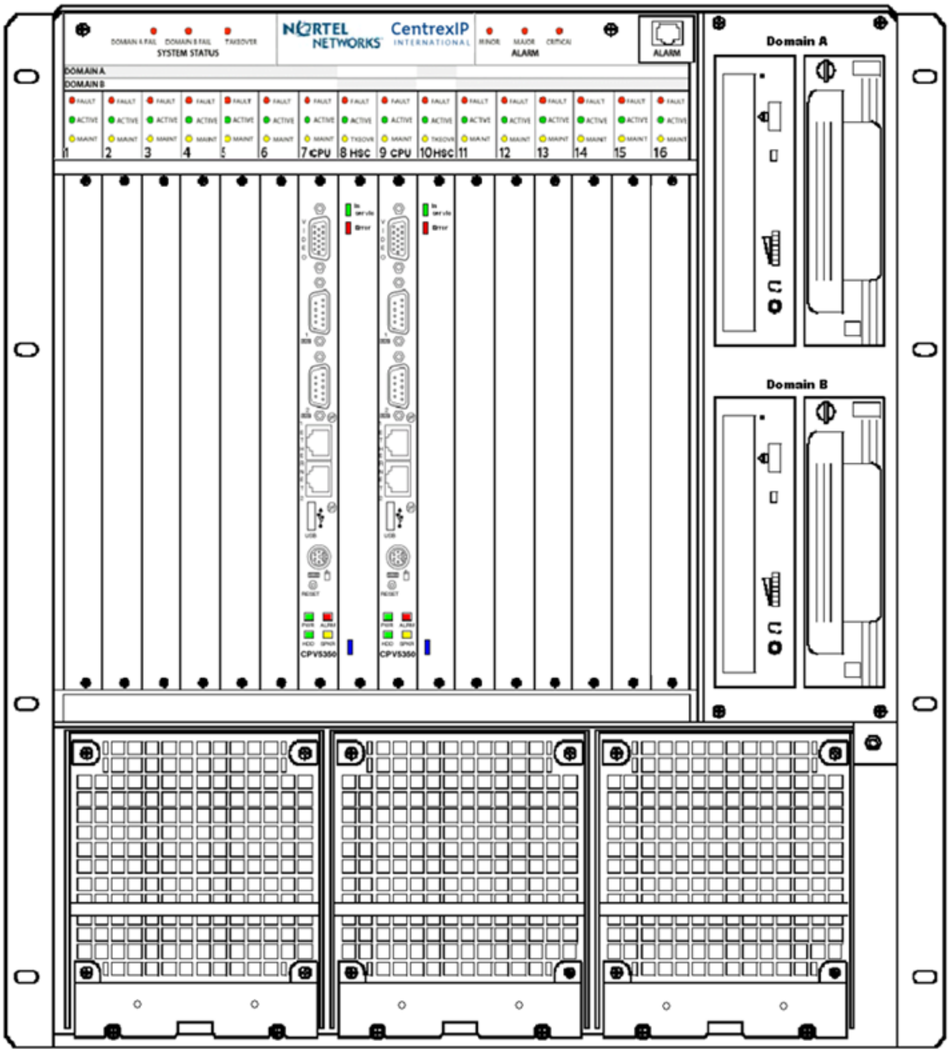
Two SAM16 chassis with hardware in PTE 2000



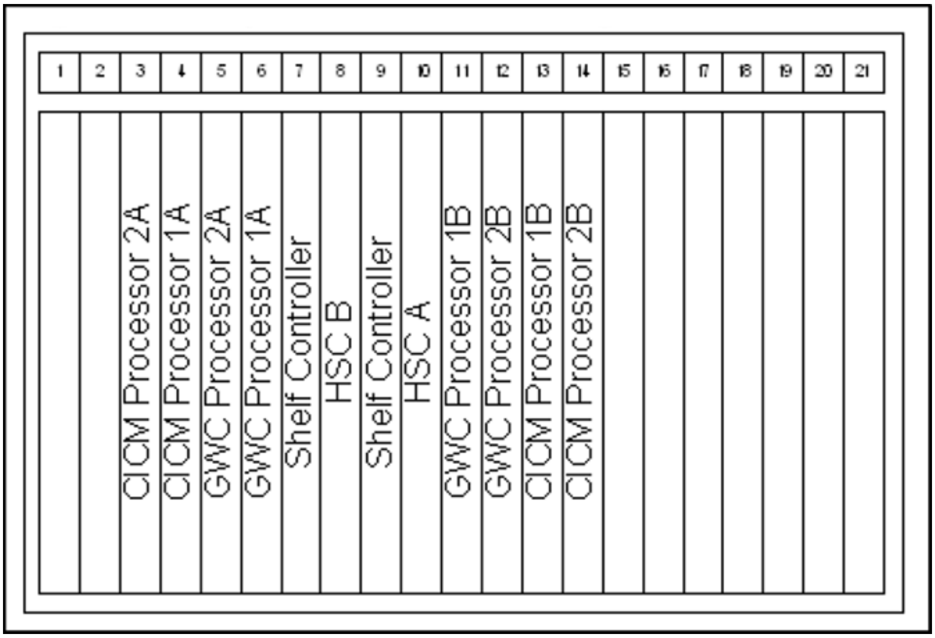
CICM chassis

The Centrex IP Client Manager (CICM) is housed in a Motorola CPX8216T chassis (SAM16) or in a PTE 2000 frame (SAM21). Examples of the chassis are shown in "CICM chassis in a SAM16 frame" (page 104) and "CICM chassis in a SAM21 frame" (page 105). The position, number, and version of each card in the chassis may be different from that shown in the figures.

CICM chassis in a SAM16 frame



CICM chassis in a SAM21 frame



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

In a SAM16, 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.

In a SAM16, 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).

The SAM16 CPV5370 processor card has provision for supporting a single PMC daughter card, which can be used to provide additional processing power.

In a SAM21, each CPU card 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 Centrex IP Client Manager (CICM)
- responding to regular polls from the master CICM Element Manager (CICM-EM)

CICM-EM hardware

The Centrex IP Client Manager Element Manager (CICM-EM) hardware is the principal management platform for each CICM node. The CICM-EM is the device used to configure, monitor, upgrade, 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 active master and the other is a standby slave
- acting as a Web server for the Web-based user interface
- 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 Nortel IP Phonesand the software upgrades for the m6350 SoftClients
- polling the CICM nodes at regular intervals for status information
- providing Simple Network Time Protocol (SNTP) time synchronization for a network of CICM nodes over different timezones.

- supplying the absolute time and each CICM node applies local timezone corrections

The SAM21-based CICM-EM is a pair of Motorola CPN5385 resource cards; one active master and the other hot standby slave. 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.

The CICM-EM in a 1204 chassis with all cards plugged into it (the CPUs, hot swap controllers, disks, and so on).

With SAM16 or SAM21, 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). With SAM16, the slave CICM-EM resource card is equivalent to the Secondary Element Manager (SEM) chassis in the SAM16-based CICM releases (identified with 5370 in the title).

CICM-EM backup and restore tool

The CICM Element Manager (CICM-EM) is supplied with a Backup and Restore Tool (BRT) that allows an operator to take offline disk images of the slave Centrex IP Client Manager (CICM) nodes and slave CICM-EMs. Since this tool requires a shutdown of the EM, its use temporarily prevents access to the Web-based administration interface to the slave EM. Since the software on each node must be identical to its mate, a switch of activity is required before getting the image of the master node or 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.

CICM-EM security

Access to the Web-based Centrex IP Client Manager 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

Processor cards

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 daughter board 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 Centrex IP Client Manager (CICM)
- H.248 Signalling

Administration interfaces to CICM

Access to Centrex IP Client Manager (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:

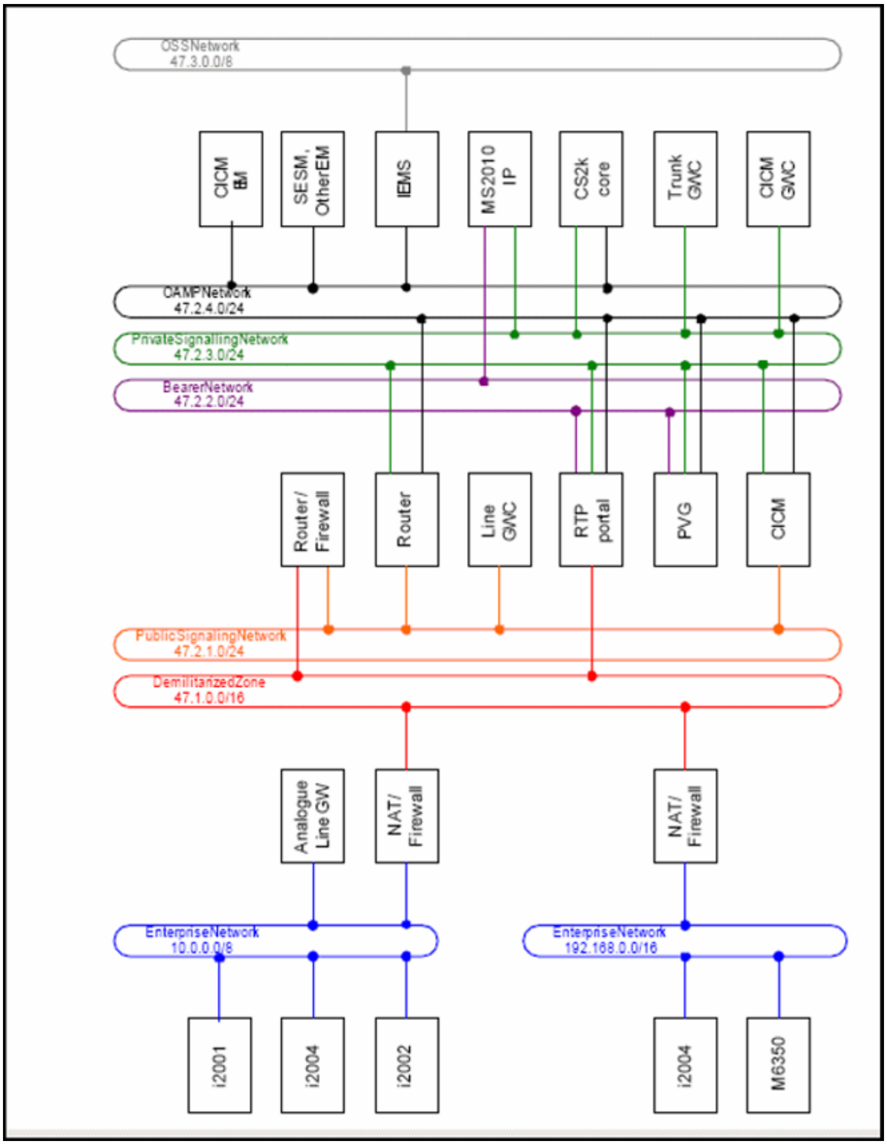
- Any platform running Microsoft Internet Explorer (IE), version 6.0 or later. Note that other Web browsers may use the Web-based management interface, but only Internet Explorer is supported.
- Any Microsoft Windows OS machine with the appropriate access rights on the service provider’s Admin LAN, using a combination of Windows OS remote management functions, and the Nortel CICM management tools accessed through the CICM Element Manager (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.

Network engineering of CICM

Protection against a single point of failure in the Ethernet network is achieved by dividing the connections of each Centrex IP Client Manager (CICM) node and each CICM Element Manager (CICM-EM) to two Ethernet Routing Switch 8600s rather than one. Splitting the connections between switches ensures that the node pairs continue to communicate if one switch or an interfacing card fails. These switches can then be connected to the rest of the telco's network. "CICM in the Call Server 2000 network" (page 109) provides a reference network for CICM in the CS2000 environment.

CICM in the Call Server 2000 network



The subnetworks shown in "CICM in the Call Server 2000 network" (page 109) are described as follows.

- The Operations Support System (OSS) network provides administrator access to Operations, Administration, Maintenance and Provisioning (OAM/P) functions.
- EMs manage their elements (and potentially each other) using the OAM/P 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.
- Each of the two enterprise networks uses a private addressing scheme, and is isolated from the Demilitarized Zone by a NAT device and firewall.

"CICM in the Call Server 2000 network" (page 109) does not distinguish between physical connectivity (a dedicated network adapter) and logical connectivity (VLANs used to multiplex functions onto a single adapter while maintaining isolation at layer 3).

Although the figure 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 node is a large IP lines gateway. Currently the only other large lines gateway is the MG9000. 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 nodes located in the carrier CS-LAN.
- Its Quality of Service (QoS) must be 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 or 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. The configuration of the secure proxy is done by the procedures Configuring PAM on the CICM-EMs, and Configuring the apache proxy on a CICM-EM pair, in *CICM Configuration Management* (NN10240-511).

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

Network interfaces

The network interfaces that are involved with Centrex IP Client Manager (CICM) nodes and CICM Element Managers (CICM-EM) include:

- "CICM node interfaces" (page 111)
- "CICM-EM interfaces" (page 114)

CICM node interfaces

Each Centrex IP Client Manager (CICM) node uses a CPN5385 processor card with three physical network interfaces. The following table lists how the physical characteristics of the CPN5385 are mapped to a set of logical interfaces used by the CICM.

CICM interface summary

Node	Logical interfaces	Physical interface assignment
A	A1	Adapter 1
	A2	Adapter 2 (VLANx)
	A3	Adapter 2 (VLANy)
	A4	Adapter 2 (VLAN4z)
B	B1	Adapter 1
	B2	Adapter 2 (VLANx)
	B3	Adapter 2 (VLANy)
	B4	Adapter 2 (VLANz)

Because the CICM node pair connects to more logical networks than it has physical network adapters, the CICM multiplexes some functions onto one of the adapters using VLAN tagging. "CICM interface summary" (page 111) lists 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 Operations, Administration, Maintenance, and Provisioning (OAM/P) access from the CICM-EM (PA and PB). The other two addresses are used for each of the call signaling interfaces (R for UNIStim and Q for H.248). All four addresses are dynamically bound to one of two adapters based on the current state of the CICM network connectivity. This table lists additional details.

CICM IP addresses

Network	IP addresses	Logical interfac e	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

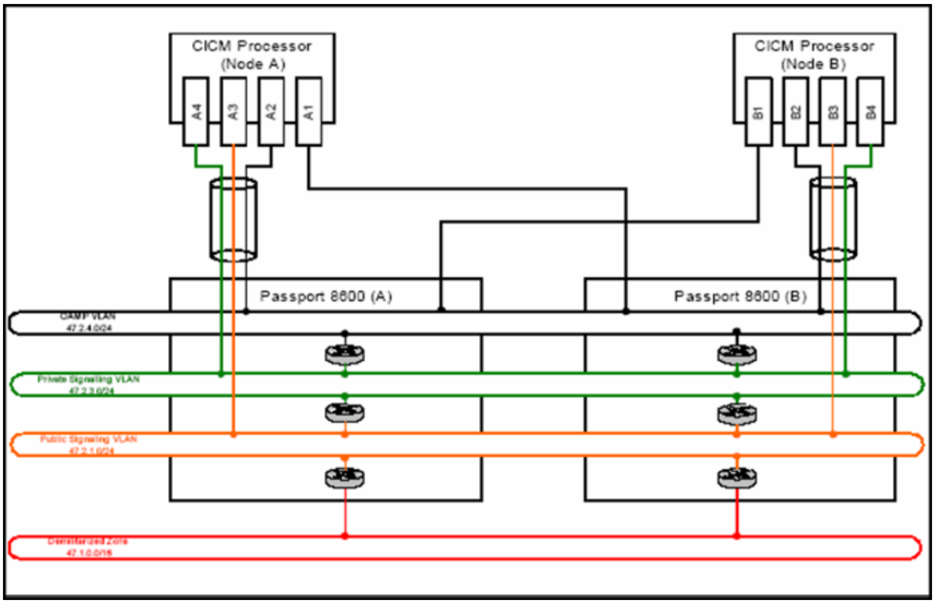
The CICM requires eight system IP addresses: one for each of the logical adapters on each of the CICM nodes (SA1-SA4 and SB1-SB4 on nodes A and B, respectively).

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 node. 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 node connected to a single Ethernet switch should have a unique IP address range reserved for its system addresses.

The CICM node pair must be cross-connected to a pair of redundant Ethernet switches. By default, this will be Ethernet Routing Switch 8600, as shown in the next figure. 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.

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 Centrex IP Client Manager Element Manager (CICM-EM) interfaces connect to different network segments, they behave in a similar manner to those on the Centrex IP Client Manager (CICM) node. 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 Integrated Element Management System (IEMS). Like a CICM node, a 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 CICM-EM signaling and communications between the CICM-EM and the CICM node (note that it is always the CICM-EM that initiates communications with the CICM node). 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 this table.

CICM-EM interfaces

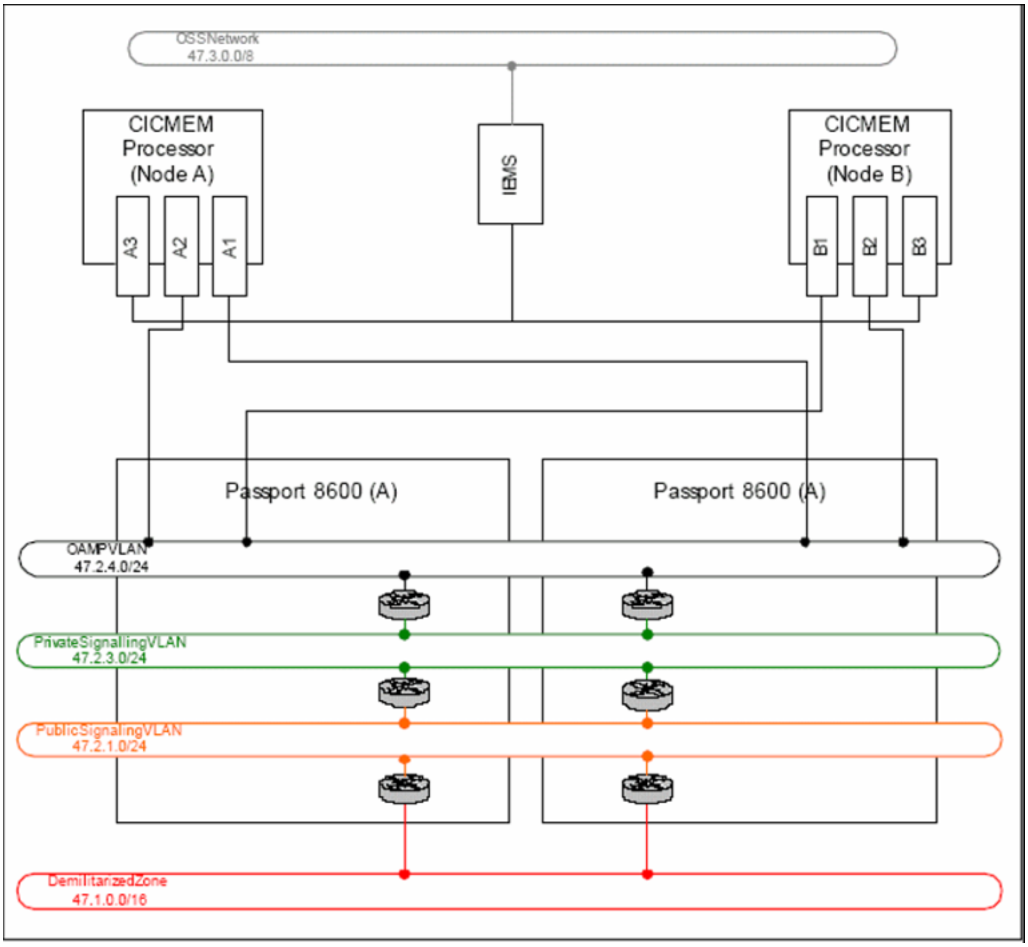
Network	IP addresses	Logical interface	Purpose
O (OSS)	O	Adapter 3 on Node A or Node B	OSS machine and GUI interfaces This access is through secure proxy through the IEMS.
P (CICM Administration)	PA	Adapter 1 or 2 on Node A	Node A OAMP and inter-node signalling
	PB	Adapter 1 or 2 on Node B	Node B OAMP 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 pair to communicate with the CICM node pair, 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 illustrated in this figure.

CICM-EM network connectivity



Each adapter on the CICM-EM sends 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 for 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 VVoIP variant of the Centrex IP Client Manager (CICM) requires an H.248 IP address to enable communication between it and the GWC. This floating address is dynamically managed by the CICM node pair, and is always bound to the master node's H.248 interface.

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

The CICM also supports using the Client VLAN for H.248 communication with the GWC. For better security, the default and strongly recommended option is to use the separate H.248 VLAN option.

UNIStim interface

The Carrier VoIP variant of the Centrex IP Client Manager (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 node’s UNIStim interface.

The CICM node 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 Centrex IP Client Manager (CICM) for release SN08 or later must be collocated with the CS2000 to use the 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 Ethernet connectivity to the CICM node and the CICM Element Manager (CICM-EM) resource cards, support various CICM node and CICM-EM VLANs, and also function as the default gateway routers for WAN communications.

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 with SN08 also use these switches to provide network connectivity.

ATTENTION

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

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

- 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 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 a WAN interface)
- Multiservice Switch 8672 ATME 2-slot MDA Baseboard, supporting up to eight OC-3 or two OC-12 ports for an ATM WAN interface

The key features of the 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)

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.

Connectivity of CICM to the network

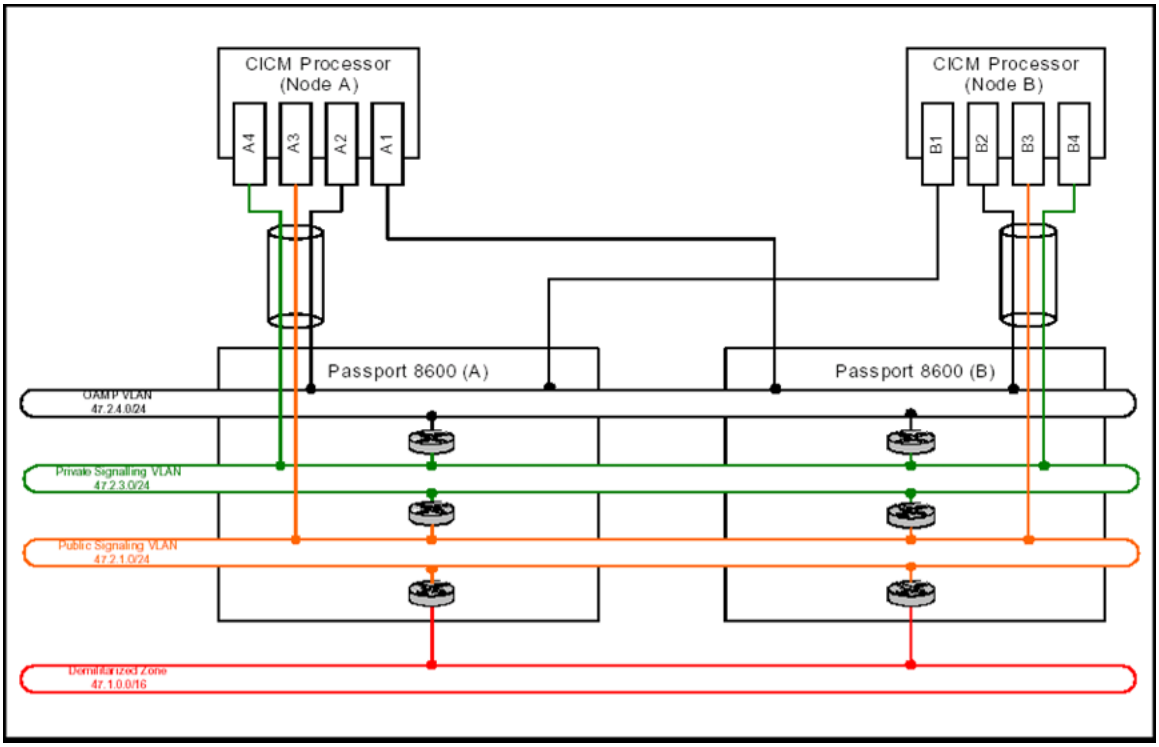
The Operations, Administration, Maintenance, Provisioning (OAM/P) network, private signaling network and public signaling network are commonly referred to collectively as the Call Server LAN (CS-LAN). A pair of Ethernet Routing Switch 8600 routers provides the connectivity and routing capabilities of the CS-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 Ethernet Routing Switch 8600 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 Centrex IP Client Manager (CICM) will require additional Ethernet connectivity.

The next figure shows a typical deployment scenario for the Carrier Voice over IP (VoIP) CICM in a central office. The figure is associated with "CICM in the Call Server 2000 network" (page 109). 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.

Network connectivity for LAN redundancy



IP addressing

Assuming the network configuration shown in "Network connectivity for LAN redundancy" (page 120), "IP addressing example" (page 120) provides a list of the IP addresses required by a pair of Centrex IP Client Manager (CICM) processing nodes.

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

This table summarizes the redundancy model used for each network interface on the Centrex IP Client Manager (CICM).

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

CICM software

This section defines the software loads, delivery, upgrades and maintenance releases applicable to Centrex IP Client Manager (CICM) products.

Navigation

Software loads

The base load for Centrex IP Client Manager (CICM) is release (I)SN07, SN08, or SN09.

A CICM Element Manager (CICM-EM) running release SN09FF can support releases SN08 or SN09 in CICM nodes, provided both nodes of the configured redundant pair have the same software version.

Software upgrades

The types of software upgrades are either a product release upgrade 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).

Software patches

Beginning with release SN09, a maintenance release (MR) can be updated by applying a software patch. Patches are applied between MRs and each subsequent MR includes the previous patches. A patch is not considered an upgrade. The description of patches and the procedures to apply a patch are in *Upgrading CICM* (NN10230-461).

CICM clients with the IP Phones or m6350 SoftClient

This section provides an overview of the Centrex IP Client Manager (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 Nortel IP Phones and the m6350 SoftClient in "CICM document suite and related documents" (page 27).

An administrator can prevent clients from logging on to the CICM node if they do not have the required level of software (in the m6350 SoftClient) or firmware (in the Nortel IP Phones). The CICM administrator may also configure the CICM nodes to upgrade the terminals automatically in a controlled manner. For the procedure to upgrade a terminal, refer to the chapter Upgrading firmware on IP phone sets, in *Upgrading CICM* (NN10230-461).

Navigation

Datafilling to use IP Phones and m6350 SoftClient

Centrex IP Client Manager (CICM) lines are datafilled on the Call Server 2000 as standard Meridian Business Set (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

Centrex IP Client Manager (CICM) clients use the Nortel proprietary Unified Networks IP Stimulus (UNIStim) protocol to deliver the full range of Call Server 2000 Centrex service set which would not be possible to deliver with standardized protocols and terminals.

Stimulus protocols reflect the stimulus input by user 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 Nortel IP Phones

A compression/decompression algorithm (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 Centrex IP clients.

A client is assigned a CODEC in an Audio Profile through the Element Manager Web Interface. The profile (and the CODEC) can be overridden from the client’s interface.

Centrex IP Client Manager (CICM) supports three standardized CODEC types for VoIP:

- G.711 Speech coding standard

  This is the standard of the PSTN at a full rate of 64 Kbit/s. 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 at 8 Kbit/s for G.729A (compressed) or 8 Kbit/s with VAD/silence suppression (compressed) for G.729AB, but it 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 IP Phones (terminals).

- G.729A and G.729A annex B

For information on CODEC negotioation rules, see *CODEC negotiation rules* in *CICM Configuration Management* (NN10240-511).

QoS reporting for Nortel IP phones

Quality of service (QoS) statistics can be enabled and reported per Centrex IP Client Manager (CICM) node. Refer to the description of the capability in "Quality of Service reporting for CICM node calls" (page 69).

IP Phone models

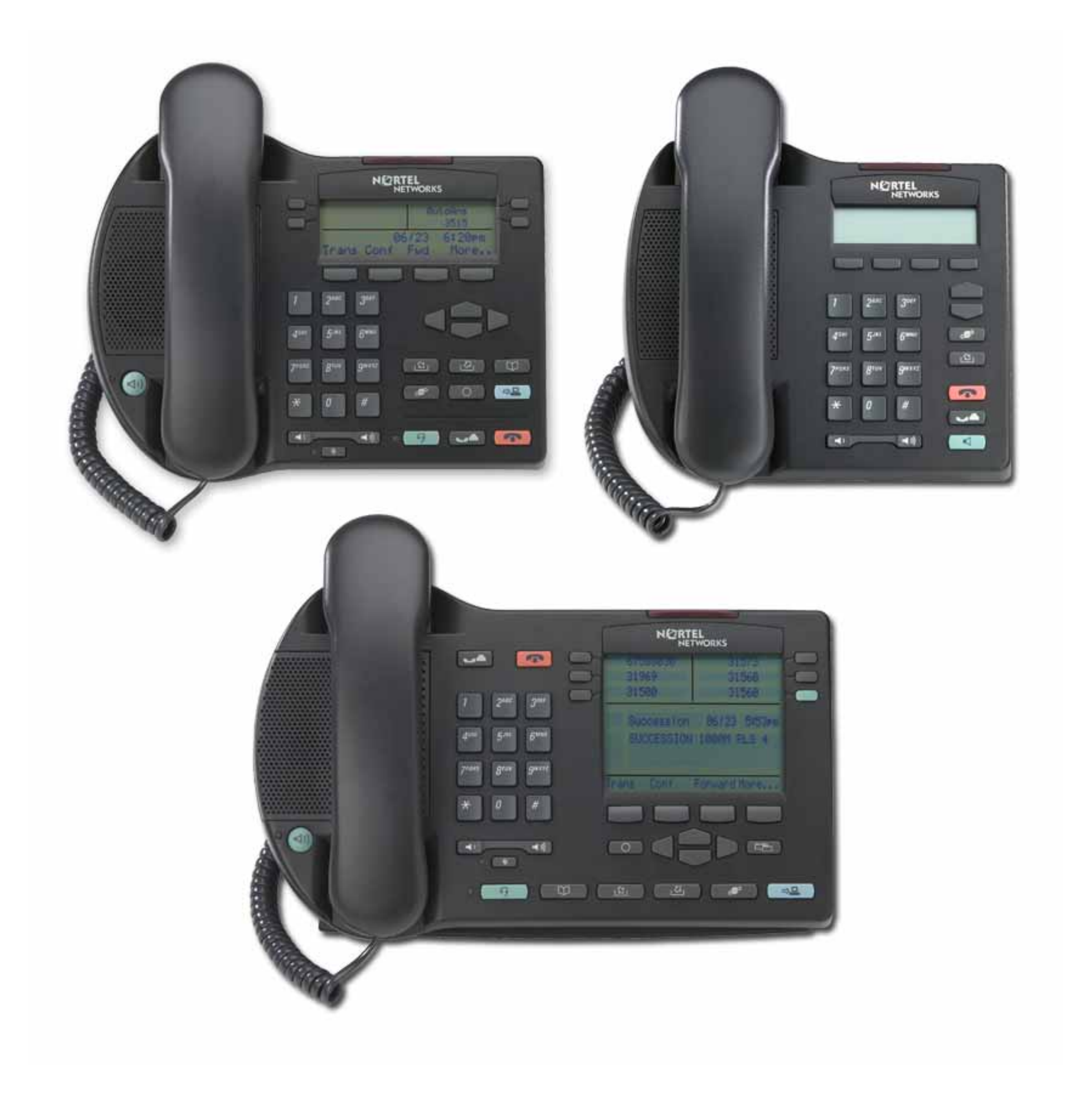
The Centrex IP Client Manager (CICM) hardware clients include these Nortel IP Phones:

- IP Phone 2001
- IP Phone 2002
- IP Phone 2004
- IP Phone 2007
- IP Phone 1120E
- IP Phone 1140E
- IP Phone Key Expansion Modules
- IP Audio Conference Phone 2033
- Wireless IP Phone 2210
- Wireless IP Phone 2211
- Wireless IP Phone 2212

The capabilities and distinctions of each IP Phone model are described in the user guides listed in "CICM document suite and related documents" (page 27). The physical appearances of the phones are shown in the figures:

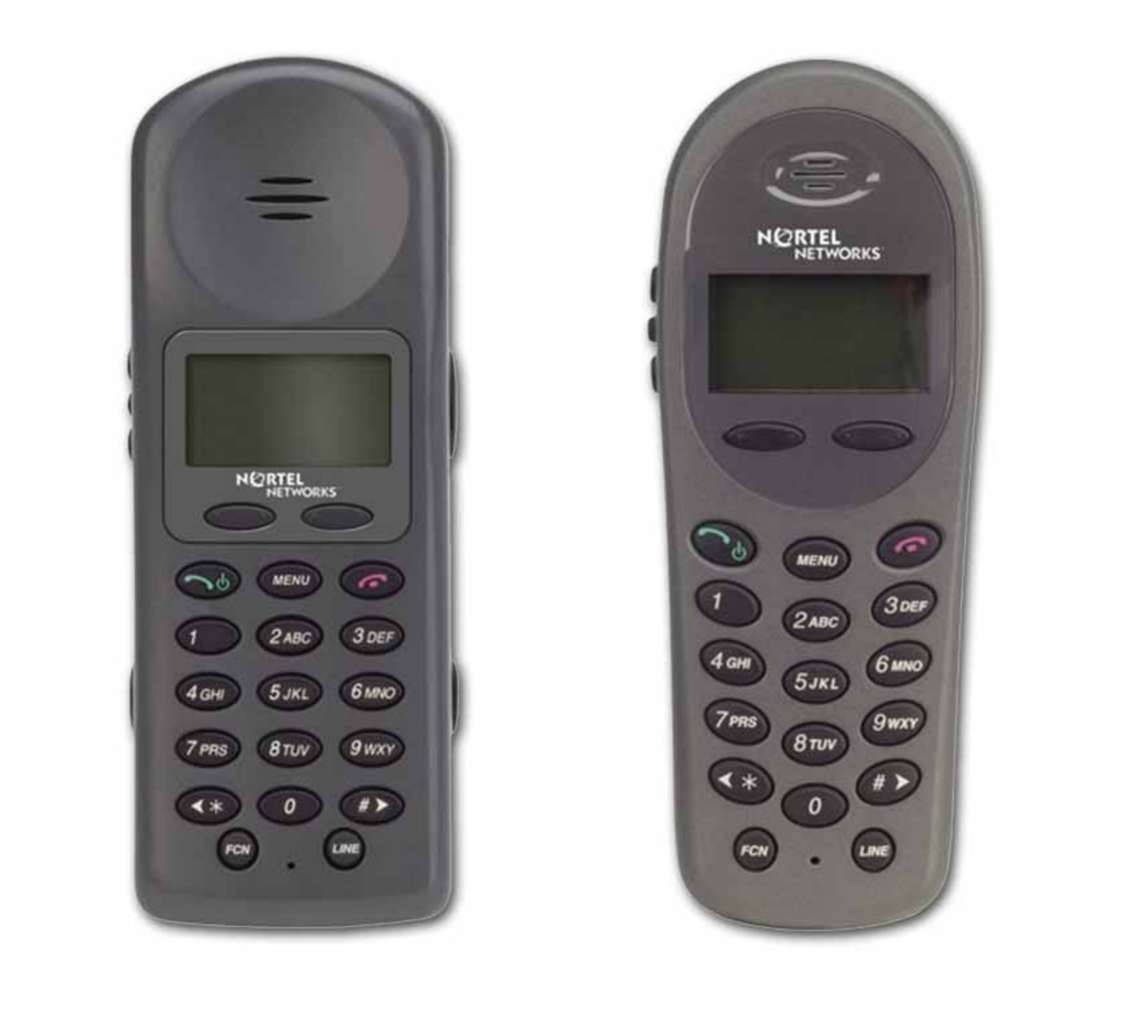
- "IP Phones 2002 (left), 2001 (right), and 2004 (center)" (page 129)
- "IP Audio Conference Phone 2033" (page 130)
- "IP Phones 2211 (left) and 2210 (right)" (page 131)
- "IP Phone 2212" (page 132)
- "IP Phones 1120E and 1140E" (page 133)
- "IP Phone 2007" (page 134)
- "IP Phone Key Expansion Module" (page 135)

IP Phones 2002 (left), 2001 (right), and 2004 (center)

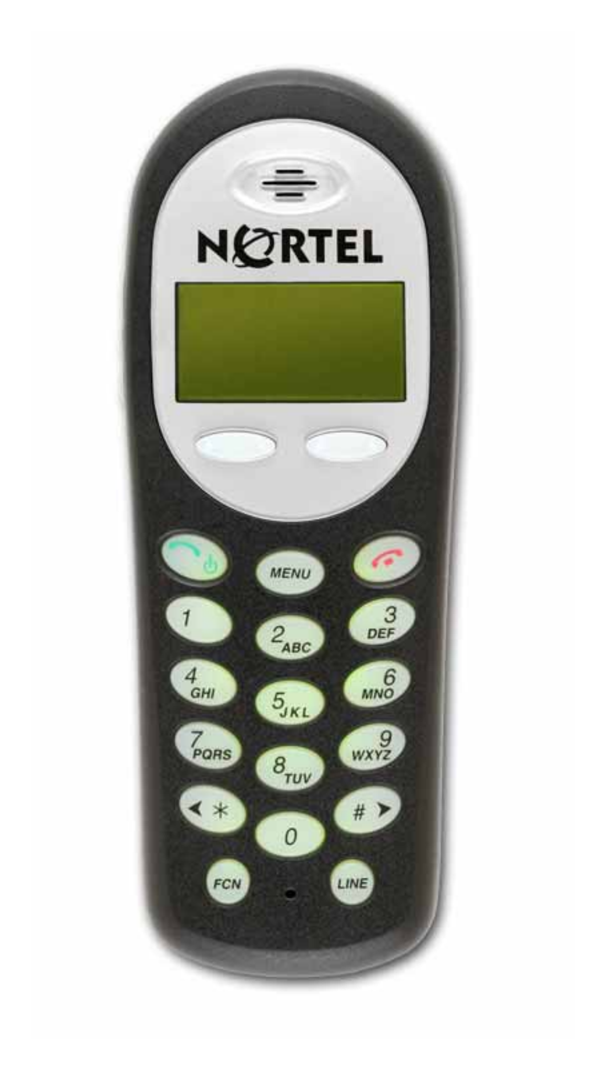


IP Audio Conference Phone 2033

IP Phones 2211 (left) and 2210 (right)

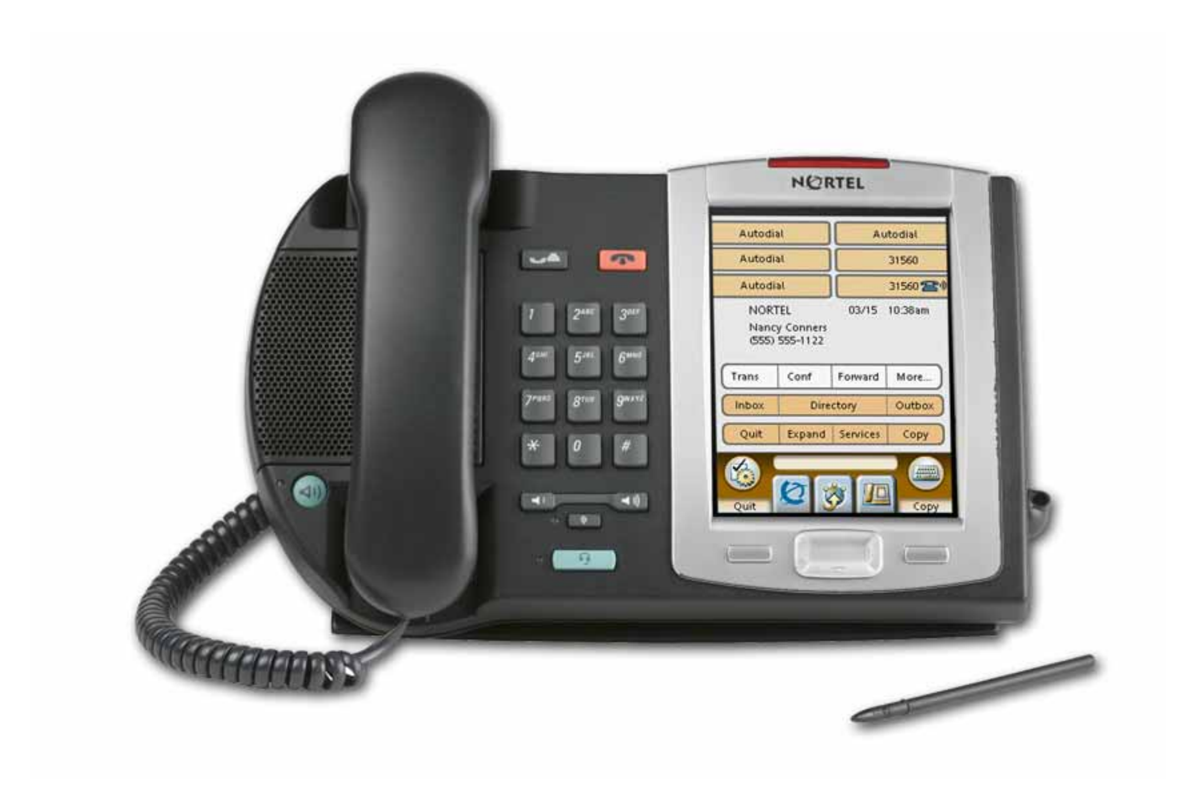


IP Phone 2212



IP Phones 1120E and 1140E

IP Phone 2007



IP Phone Key Expansion Module

Key Expansion Module for Nortel IP Phones

Nortel IP Phone Key Expansion Module (KEM) is an optional component available for use with Nortel IP Phones 2002, 2004, and 2007. Connecting one or two KEMs to an IP Phone increases the number of feature keys available, and expands the amount of data displayed on the LCD screen.

The KEM is provisioned through both the DMS and the Centrex IP Client Manager Element Manager (CICM-EM). Before any features can be assigned to the keys on the KEM, the M522 line option must be assigned to the associated terminal on the DMS. The M522 line option includes the specification of one or two KEMs.

Within the CICM-EM, the page *Terminal Configuration*, configure a KEM by providing the following Feature Key Attributes:

- the number of supported extension modules
- the number of features available on each extension module

Both the M522 line option and the CICM-EM information must have synchronize provisioning. The M522 line option on the DMS enables the provisioning of features on the additional keys, while the CICM-EM data controls the use of any KEMs connected to a terminal (IP Phone).

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

For information on the installation and operation of a KEM, refer to *Nortel IP Phone Key Expansion Module User Guide* (NN10300-011).

Functional components of IP Phones

The following tables list the functional components of Nortel IP Phone s:

- "Nortel IP Phones 20xx functional components" (page 136)
- "Nortel IP Phones 221x functional components" (page 137)
- "Nortel IP Phones 11xx functional components" (page 138)

Nortel IP Phones 20xx functional components

Component	2033	2007	2004	2002	2001
Handset	N	Y	Y	Y	Y
Speaker	Y	Y	Y	Y	Y
Microphone	Y	Y	Y	Y	N
Headset connector for handsfree operation	N	Y	Y	Y	N
Standard keypad	Y	Y	Y	Y	Y
Release key	Y	Y	Y	Y	Y
Hold key	Y	Y	Y	Y	Y
Volume control	Y	Y	Y	Y	Y

Component	2033	2007	2004	2002	2001
Mute key	Y	Y	Y	Y	Available when Mute assigned to soft key; Displayed in Call Services menu
Number of navigation keys	2 (Up or Down)	4 (Up or Down, Left or Right)	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	Y
Number of keys	4 soft keys	4 soft keys	4	4	4 soft keys
Number of features available to assign to keys	14	11	14	11	14
Number of line or DN keys	3 plus 1 main key (based on how soft keys are assigned)	6 (on-touch screen)	6	4	3 plus 1 main key (based on how soft keys are assigned)
Transducer control	0	2 (HF or HS)	2 (HF or HS)	2 (HF or HS)	0
Other keys	0	2 (Stop or Copy)	2 (Stop or Copy)	2 (Stop or Copy)	0
Audio capabilities	High end audio. Full duplex speaker phone only	High-end audio. Full duplex speaker phone with wideband transducers (only available in handsfree model)	High-end audio. Full duplex speaker phone with wideband transducers (only available in handsfree model)	Standard audio. Full duplex speaker phone with narrowband transducers	Basic audio. Onhook dial or listen with narrowband handset and no handsfree capability

Nortel IP Phones 221x functional components

Component	2210	2211	2212
Handset	Y	Y	Y
Speaker	N	N	N

Component	2210	2211	2212
Microphone	N	N	N
Headset connector for handsfree operation	Y	Y	Y
Standard keypad	Y	Y	Y
Release key	Y	Y	Y
Hold key	N (function key FCN to access)	N (function key FCN to access)	N (function key FCN to access)
Volume control	Y	Y	Y
Mute button	Y	Y	Y
Number of navigation keys	2 (Up or Down)	2 (Up or Down)	2 (Up or Down)
Function/display LCD	Y	Y	Y
Number of keys	4 soft keys	4 soft keys	4 soft keys
Number of features available to assign to keys	6 (function key FCN to access)	6 (function key FCN to access)	6 (function key FCN to access)
Number of line or DN keys	6 (function key FCN to access; primary DN key to access default DN)	6 (function key FCN to access; primary DN key to access default DN)	6 (function key FCN to access; primary DN key to access default DN)
Transducer control	0	0	0
Other keys	0	0	0

Nortel IP Phones 11xx functional components

Component	1120E	1140E
Handset	Y	Y
Speaker	Y	Y
Microphone	Y	Y
Headset connector for handsfree operation	Y	Y
Standard keypad	Y	Y
Release key	Y	Y
Hold key	Y	Y
Volume control	Y	Y
Mute key	Y	Y

Component	1120E	1140E
Number of navigation keys	5 (Up or Down, Left or Right, Send)	5 (Up or Down, Left or Right, Send)
Function/display LCD	Y	Y
Number of keys	4 soft keys	4 soft keys
Number of features available to assign to keys	11	11
Number of line or DN keys	4	6
Transducer control	2 (HF or HS)	2 (HF or HS)
Number of LED indicator lamps	6	6
Other keys	2 (Stop or Copy)	2 (Stop or Copy)
Audio capabilities	Standard audio. Full duplex speaker phone with narrowband transducers	High-end audio. Full duplex speaker phone with wideband transducers (only available in handsfree model)

The Nortel 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.

IP Phone user interface

To use a Nortel IP Phone, log on to the Centrex IP Client Manager (CICM) node, supplying a user name and password. After you are logged on, 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.

These tables summarize the user interface of each IP Phone:

- "Nortel IP Phones 20xx user interfaces" (page 139)
- "Nortel IP Phones 11xx user interfaces" (page 140)

Nortel IP Phones 20xx user interfaces

Option	2033	2007	2004	2002	2001
Display contrast	Y	Y	Y	Y	Y
Feature key configuration	Y	Y	Y	Y	Y
Language selection	Y	Y	Y	Y	Y

Option	2033	2007	2004	2002	2001
Time and date format selection	Y	Y	Y	Y	Y
Audio configuration	Y	Y	Y	Y	Y
Firmware upgrades at the phone	Y	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 (Cannot assign contacts to soft keys. Dialing is available from within the directory menu.)	Y	Y	Y	N (Cannot assign contacts to soft keys. Dialing is available from within the directo ry menu.)
Call history feature, providing access to CICM-hosted inboxes (incoming calls) and outboxes (outgoing calls).	Y	Y	Y	Y	Y

Nortel IP Phones 11xx user interfaces

Option	1120E	1140E
Display contrast	Y	Y
Feature key configuration	Y	Y
Language selection	Y	Y
Time and date format selection	Y	Y
Audio configuration	Y	Y
Firmware upgrades at the phone	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.	Y	Y
Call history feature, providing access to CICM-hosted inboxes (incoming calls) and outboxes (outgoing calls).	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 following tables list the hardware features of Nortel IP Phones:

- "Nortel IP Phones 20xx hardware features" (page 141)
- "Nortel IP Phones 221x hardware features" (page 142)
- "Nortel IP Phones 11xx hardware features" (page 142)

Nortel IP Phones 20xx hardware features

2033	2007	2004	2002	2001
Lies flat on desk	Adjustable-angle stand	Adjustable-angle stand	Fixed-angle stand	Fixed-angle stand
For desk only	Wall mount	Wall mount	Wall mount	Wall mount
1 RJ-45 jack(no Ethernet switch)	2 RJ-45 jacks with built-in 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 (on-touch screen)	6 line keys	4 line keys	0 or 1 line key
2-line display area	4-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	Extended low-frequency speaker	Standard Stetron LS19 speaker (no tuned cavity)	Basic audio
No AEM or ACM	ACM accessory port	AEM accessory port for KEMs and ACM accessory port	AEM accessory port for KEMs	No AEM or ACM

2033	2007	2004	2002	2001
Handsfree microphone for wide-band audio	Handsfree microphone for wideband audio	Handsfree microphone for wideband audio	Standard Primo EM-80 handsfree microphone	No active speakerphone; on-hook listen only
not power over Ethernet capable	Power over Ethernet capable	Power over Ethernet capable	Power over Ethernet capable	Power over Ethernet capable

Nortel IP Phones 221x hardware features

2210	2211	2212
Portable	Portable	Portable
Charged by desk charger	Charged by desk charger	Charged by desk charger
Wireless LAN connectivity to 2245 WLAN Telephony Manager	Wireless LAN connectivity to 2245 WLAN Telephony Manager	Wireless LAN connectivity to 2245 WLAN Telephony Manager
1 line key	1 line key	1 line key
4-line display area	4-line display area	4-line display area

Nortel IP Phones 11xx hardware features

1120E	1140E
Fixed-angle stand	Adjustable-angle stand
Wall mount	Wall mount
2 RJ-45 jacks with built-in Ethernet switch	Plug-in Ethernet switch (on older models), plus built-in Ethernet switch (2 RJ-45 jacks) in newer models
4 line keys	6 line keys
2-line display area	4-line display area
Standard Stetron LS19 speaker (no tuned cavity)	Extended low-frequency speaker
AEM accessory port for KEMs	AEM accessory port for KEMs and ACM accessory port
Standard Primo EM-80 handsfree microphone	Handsfree microphone for wideband audio
Power over Ethernet capable	Power over Ethernet capable

The m6350 SoftClient

The m6350 software client (SoftClient) application is an IP telephony software client installed on a PC running a Microsoft Windows operating system and connected to a LAN. It uses with a headset and adapter which plugs into a USB port on the PC. The m6350 software emulates the operation and function of a Nortel IP Phone.

The m6350 software is accessed through a Microsoft Windows interface and uses Microsoft Internet Explorer. The supported versions or Windows and Explorer are identified in *m6350 SoftClient Installation Guide* (NN10182-113).

The m6350 SoftClient communicates with the Centrex IP Client Manager (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.

It is not possible to guarantee the voice quality provided by the m6350 SoftClient, 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.

For an m6350 SoftClient client:

- The speech path represents the headset mode of MBS operation. Handsfree mode is not directly supported by the m6350, since handsfree 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 *m6350 SoftClient Installation Guide* (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.

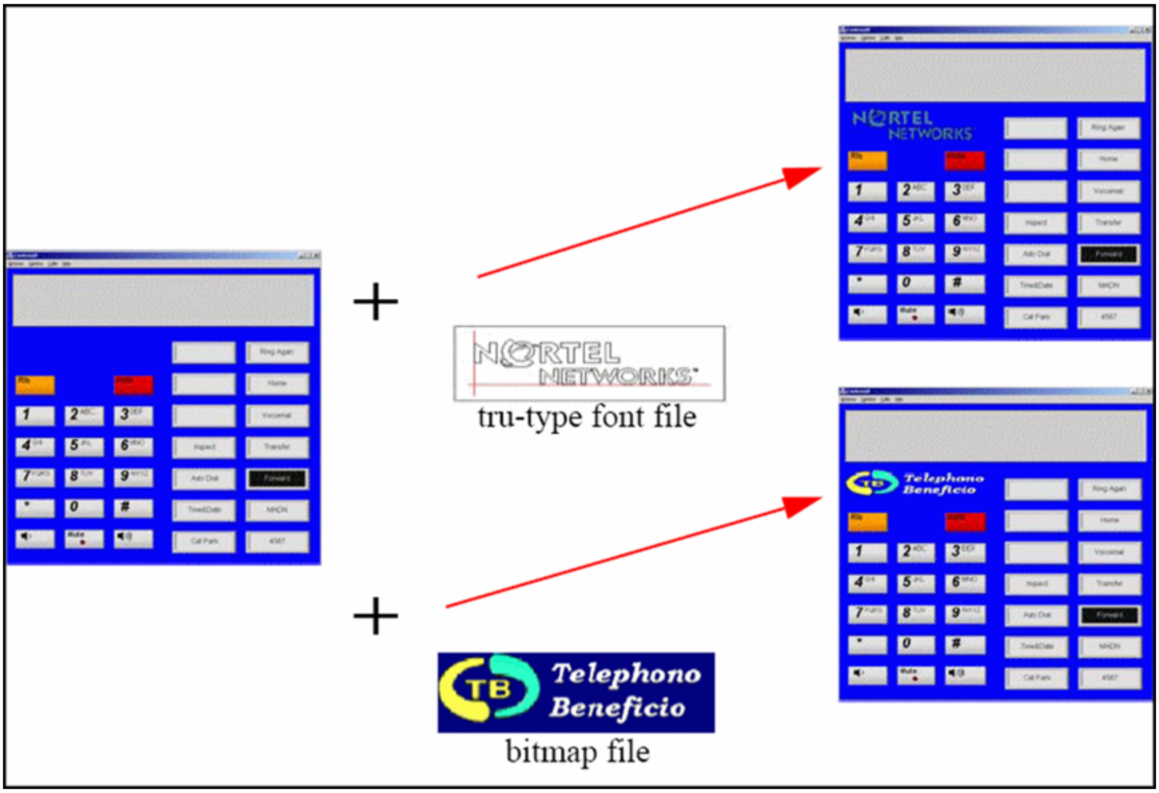
m6350 user interface

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

After logging on to m6350, the you then log on to the Centrex IP Client Manager (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 next figure. 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.

m6350 SoftClient user interface with 2 additional banks of feature keys



Features of the m6350 SoftClient 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 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.

The TAPI service provider can be installed after the m6350 has been installed and provides access to the m6350 from Windows applications such as Outlook.

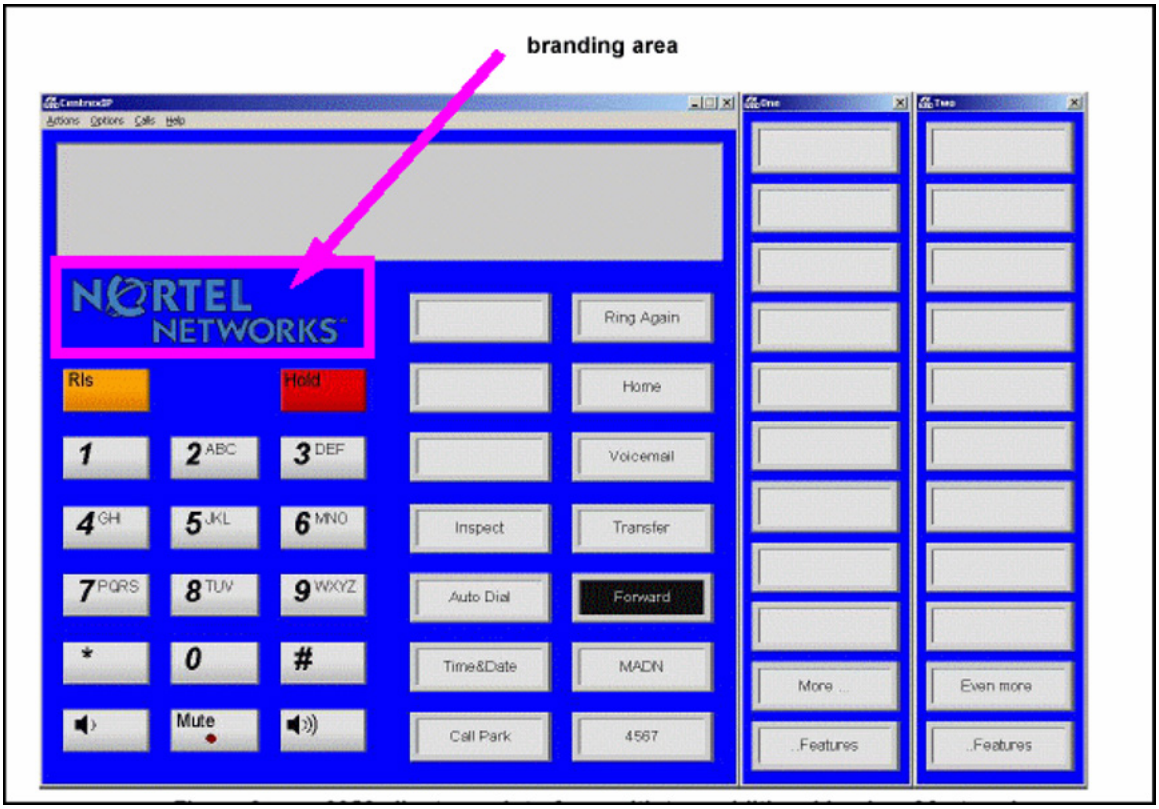
For more information on installation and configuration, refer to the chapter on TAPI in *m6350 SoftClient Installation Guide*.

Client branding

An OEM customizer is available to allow a service provider to create a custom version of the m6350 SoftClient. A service provider can brand the appearance of the m6350 with their own logo. The m6350 graphical user interface (GUI) includes an area that contains a configurable brand logo, as shown in the next figure. 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

m6350 SoftClient Branding



The branding facility allows the service provider to brand the m6350 GUI and produce an installation kit where the company/product information and default software placement details are tailored to represent the service provider, and not Nortel.

Refer to the chapter on branding in *m6350 SoftClient Installation Guide* (NN10182-113).

Configuring CICM resident options

The m6350 users can view, and in some cases modify, option data on the Centrex IP Client Manager (CICM) node 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 to display HTML pages served by the CICM node. If the user's PC does not have the appropriate version of installed, the m6350 will continue to function normally, but will not provide access to this new functionality.

For detailed information on the m6350 SoftClient system requirements and installation procedures, refer to the *m6350 SoftClient Installation Guide* (NN10182-113).

Call History and Contacts Directory features

Nortel IP Phones and m6350 SoftClients 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 Centrex IP Client Manager (CICM).

The Inbox allows the user to display information about the 10 most recent incoming calls. Incoming call information is captured, regardless whether the user is logged on at the time.

The Outbox allows the user to display information about the 10 most recent outgoing 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 Nortel IP Phone through an assigned feature key, or on the m6350 from a drop-down list on the main menu.

Cooperative sessions between m6350s and IP Phones

Beginning with release (I)SN09FF, cooperative sessions between an m6350 SoftClient application and an IP Phone are supported for TDM SN2.5.

A user can be logged on from both an m6350 SoftClient application and an IP Phone at the same time in a cooperative session. The user can dial or answer from either the m6350 or the phone during a cooperative session. lamps will light on both clients (for example, a call is waiting) and both displays show parallel information.

The audio for such a cooperative session will always be handled by the physical IP Phone client, because the voice quality is usually superior to that of a PC with the m6350 SoftClient.

If a user is logged on and attempts to log on from another client, the system presents three options.

- Join the current session.

- Log out—the system logs out the previous session and presents the user with a new login screen.
- Cancel this login.

The following restrictions apply to cooperative sessions.

- Only the IP Phone will receive audio.
- A cooperative session can only be established between clients connected to the same master CICM node. If two clients are connected to different nodes, and a user attempts to log on the second client with the same user name as the first, then the user can only force out the first client or cancel the login attempt. A cooperative session cannot be established.
- If a logged-on client is making a call and an attempt is made to force it out, the call is cleared.

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 SoftClients, standard Microsoft Windows DHCP capabilities can be used, although additional manual configuration is required to enter the Centrex IP Client Manager (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.

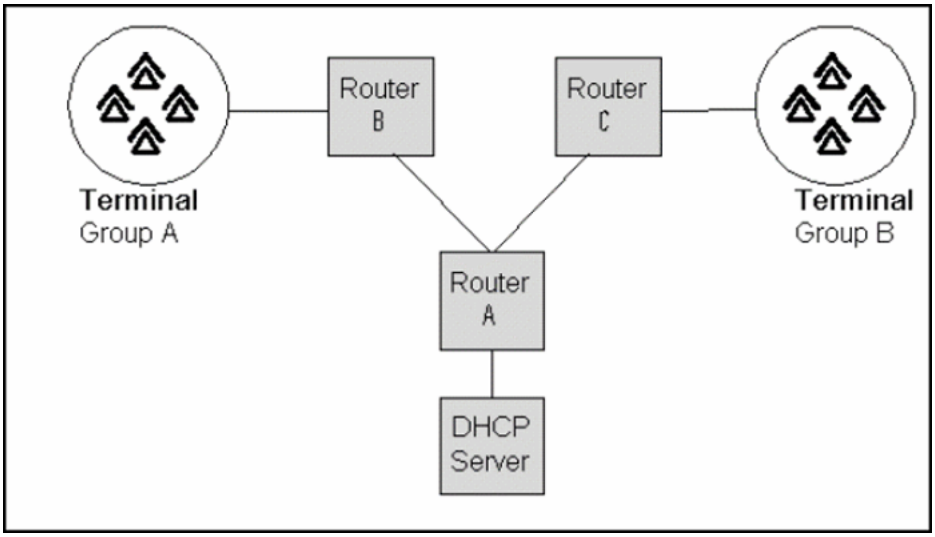
The CICM node ignores the IP address of a client provided it remains constant while the client is logged onto the CICM.

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) Centrex IP Client Manager (CICM) node. This CICM may not be the CICM node that the terminal was previously connected to. These two solutions 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 next figure, 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.

DHCP scoping diagram



Other client-related features

The features related to the IP Phone clients and SoftClient client are:

- "Auto-upgrade firmware" (page 151)
- "Emergency Call Services Location Identification Support" (page 151)

Auto-upgrade firmware

When the firmware auto-upgrade feature is enabled, the client is offered an upgrade. When the client is not logged on, the upgrade occurs automatically. When the client is logged on, an on-screen prompt indicates that an upgrade is available, and gives the user an option to accept it or post-pone it. Ignoring the prompt causes the upgrade to occur automatically. For the behaviour of the client during the upgrade, refer to the procedure Upgrading firmware on the IP Phone sets, in *Upgrading CICM* (NN10230-461).

Emergency Call Services Location Identification Support

The Centrex IP Client Manager (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. When configured, the CICM requests the location information from the telephony client when the user logs on, 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 Centrex IP Client Manager (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 node.
- The Call Server can support multiple feature assignments to each feature key, but the CICM shows only one label per key.

Diagnostics for Nortel IP Phones

A diagnostic utility is available to:

- test the end-to-end connectivity of a Nortel IP Phone
- verify operational statistics and settings
- retrieve phone set information

The IP Phone diagnostic utilities are in *IP Phones Description, Installation, and Operation*, 553-3001-368.

User interfaces for CICM

The normal mode of access to the Centrex IP Client Manager Element Manager (CICM-EM) is through a PC connected to the Administration LAN. The procedures in the CICM document suite, identified in "CICM document suite and related documents" (page 27), all use this method. The administrator user ID and password is required to log on to the CICM-EM.

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

Navigation

CICM-EM Web interface

The Centrex IP Client Manager Element Manager (CICM-EM) interface uses a Web browser on the Internet to access the Element Manager Web pages. The CICM-EM Web site provides most of the functionality necessary for configuring and monitoring a Centrex IP Client Manager (CICM) node and its clients (IP Phones or m6350 SoftClients).

This Web-based CICM-EM interface can be run from any platform that supports Microsoft Internet Explorer, version 6.0 or later.

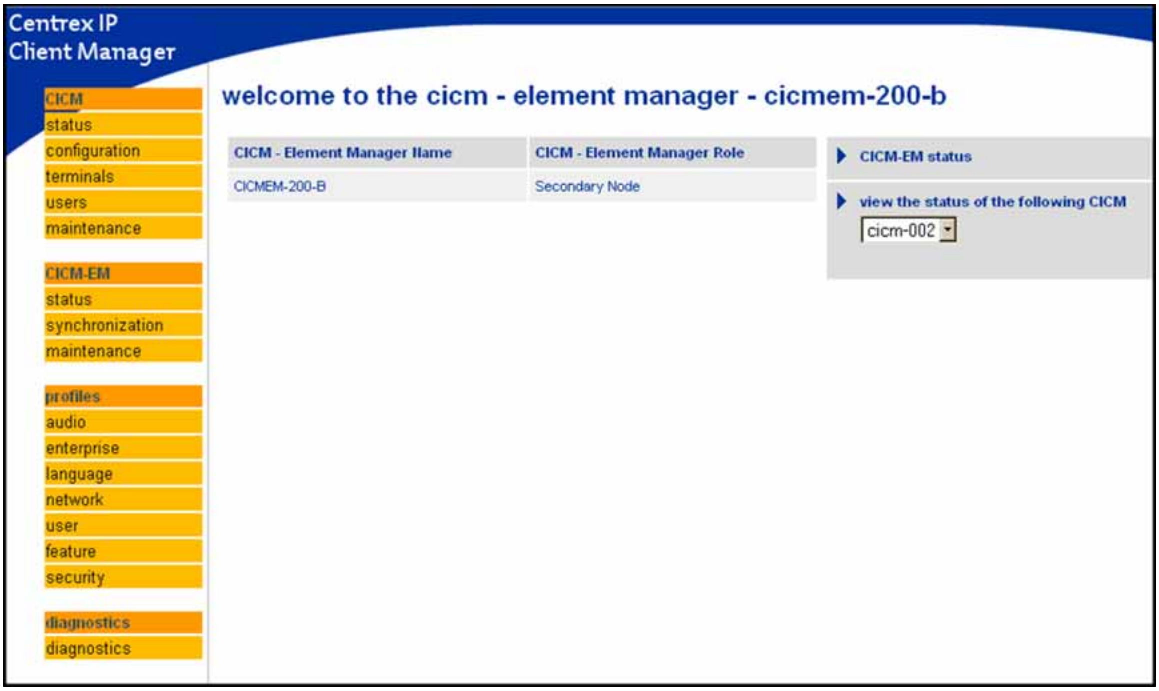
A Web page for the CICM-EM interface refers to a display of the main menu of commands and a particular set of static and dynamic fields of information for a CICM node or a CICM-EM. The CICM-EM Web-based interface consists of:

- the welcome page, as shown in "CICM welcome page" (page 154)
- an EM home page, shown in "CICM home page" (page 155), and the main menu that can be accessed from every page on the site, 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

CICM welcome page

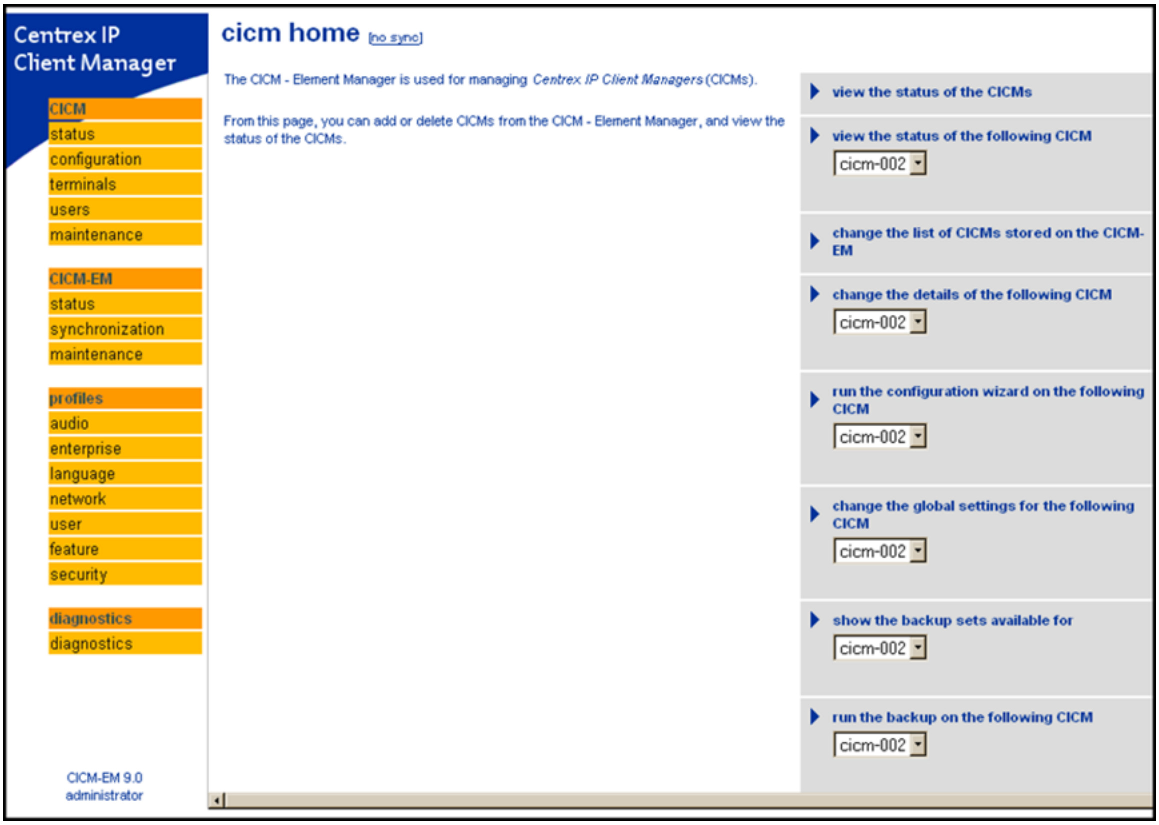


welcome to the cicm - element manager - cicmem-200-b

CICM - Element Manager Name	CICM - Element Manager Role
CICMEM-200-B	Secondary Node

view the status of the following CICM: cicm-002

CICM home page


Centrex IP
Client Manager
CICM
status
configuration
terminals
users
maintenance
CICM-EM
status
synchronization
maintenance
profiles
audio
enterprise
language
network
user
feature
security
diagnostics
diagnostics
CICM-EM 9.0
administrator
cicm home
[no sync]
view the status of the CICMs
view the status of the following CICM
cicm-002
change the list of CICMs stored on the CICM-EM
change the details of the following CICM
cicm-002
run the configuration wizard on the following CICM
cicm-002
change the global settings for the following CICM
cicm-002
show the backup sets available for
cicm-002
run the backup on the following CICM
cicm-002

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.

IEMS interface

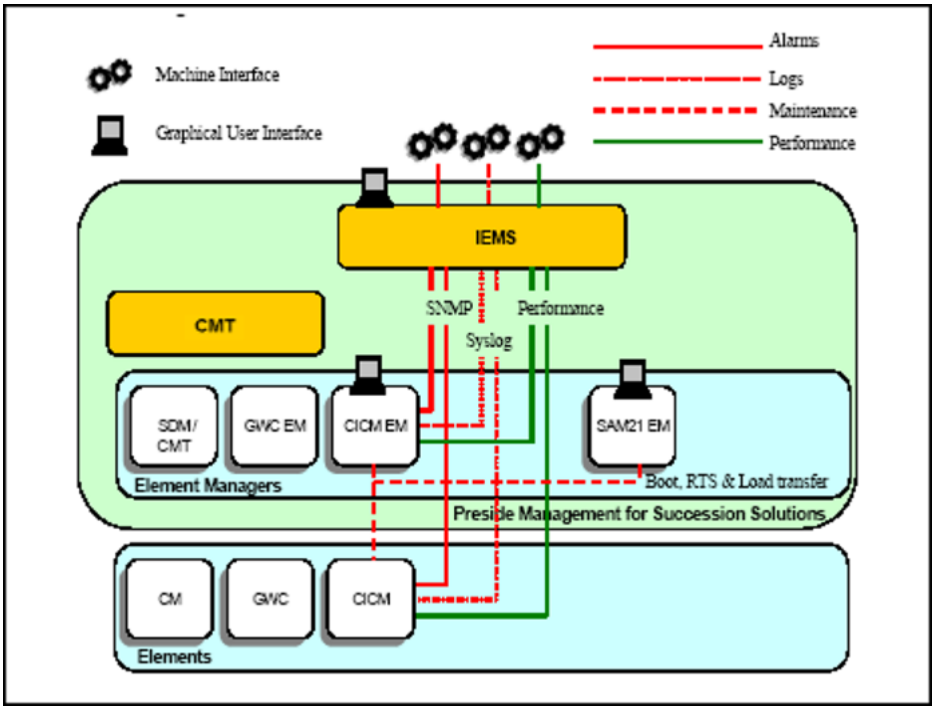
The Integrated Element Management System (IEMS) product provides Operations, Administration, Maintenance, and Provisioning (OAM/P) capabilities in a Carrier Voice over IP (VoIP) network. IEMS especially interfaces with the service provider's OSS equipment. The Centrex IP Client Manager Element Manager (CICM-EM) and Centrex IP Client Manager (CICM) nodes are supported by IEMS.

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 node or EM

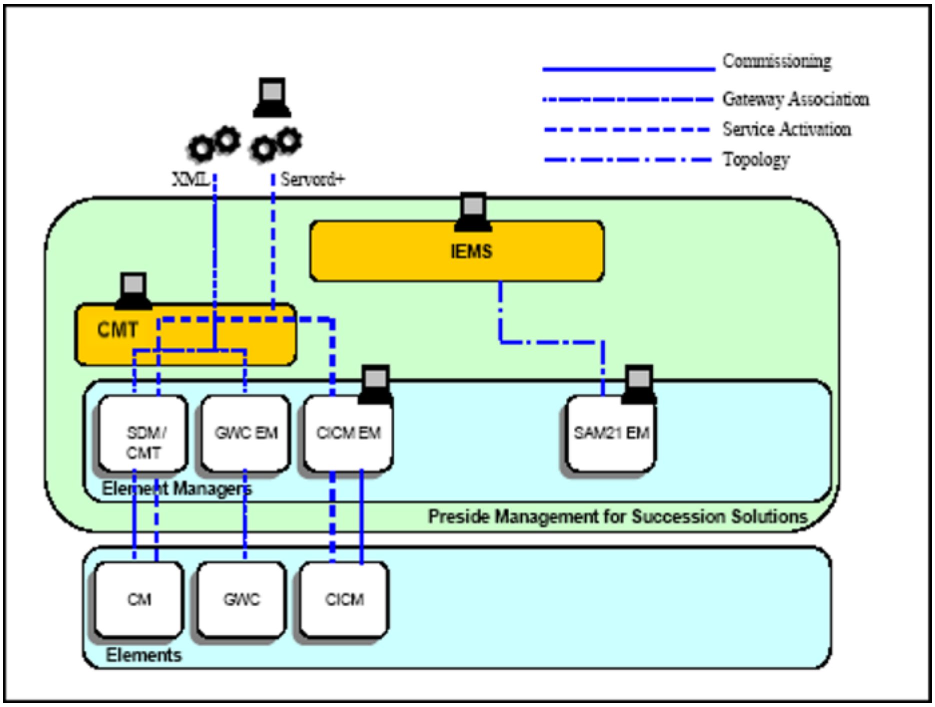
The next figure illustrates how the IEMS and CICM-EM, and CICM nodes work monitor fault and performance. The IEMS takes the alarms, logs, and performance monitoring data produced by the CICM nodes and CICM-EMs and passes it to the OSS systems in a choice of industry standard formats.

Carrier VoIP CICM fault and performance overview



A flow-through provisioning system is implemented, as shown in the next figure. Beginning with release SN08, it is possible to use the Call Server 2000 Management Server OSSGate or Web interface to associate a CICM with a gateway. 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. See also "Flow-through provisioning" (page 57).

Carrier VoIP CICM configuration overview



Telnet interface

Telnet is a terminal emulation program for TCP/IP networks such as the Internet. A Telnet session may be used to perform certain (but not all) administrative functions for a Centrex IP Client Manager Element Manager (CICM-EM) or Centrex IP Client Manager (CICM) node.

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 Administration network. To access CICM nodes, use the `cicmconnect` commands

Telnet can be used to perform the following operations of the CICM-EM or CICM node:

- 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 *CICM Administration and Security* (NN10252-611).

SNMP interface

Centrex IP Client Manager (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

Centrex IP Client Manager (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 this table.

Protocols relevant to VoIP

Network Area	Protocols	Purpose
Call/session and device or CICM control	UNIStim	Ensures 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	Ensures that voice traffic gets priority over less time-sensitive services like file transfer and fax
Device or media control	H.248	Supports device control and media control capabilities

Navigation

UNIStim

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

Centrex IP Client Manager (CICM) clients use the UNIStim protocol to communicate with the CICM node. 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 Centrex IP Client Manager (CICM) nodes, 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 that 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.

Software configuration for CICM

Navigation

Commissioning

Commissioning is the process whereby a Centrex IP Client Manager (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.

The software that is used by Nortel to initially configure the CICM setup is referred to as the preboot software in this document. (The same preboot software is used by telco administrators to roll back a software upgrade.)

Commissioning is a two-stage process. The preboot software 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 Element Manager (CICM-EM).

After it is 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 Centrex IP Client Manager Element Manager (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 initially configured to automatically back up the configuration data of all Centrex IP Client Manager (CICM) nodes once per 24-hour period (for example, the default is 2:00 am when enabled).

Backup and restore

Data can be backed up in two ways:

- as part of a regularly scheduled task
- on demand from the Centrex IP Client Manager Element Manager (CICM-EM)

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 a preboot software sequence. It is possible to select a particular image to restore, and to select either a full or partial restoration.

The procedures back up a pair of CICM-EMs or a pair of Centrex IP Client Manager (CICM) nodes and to apply a back-up file (restore the registry) is in *CICM Configuration Management* (NN10240-511).

Gateway association

For gateway 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.

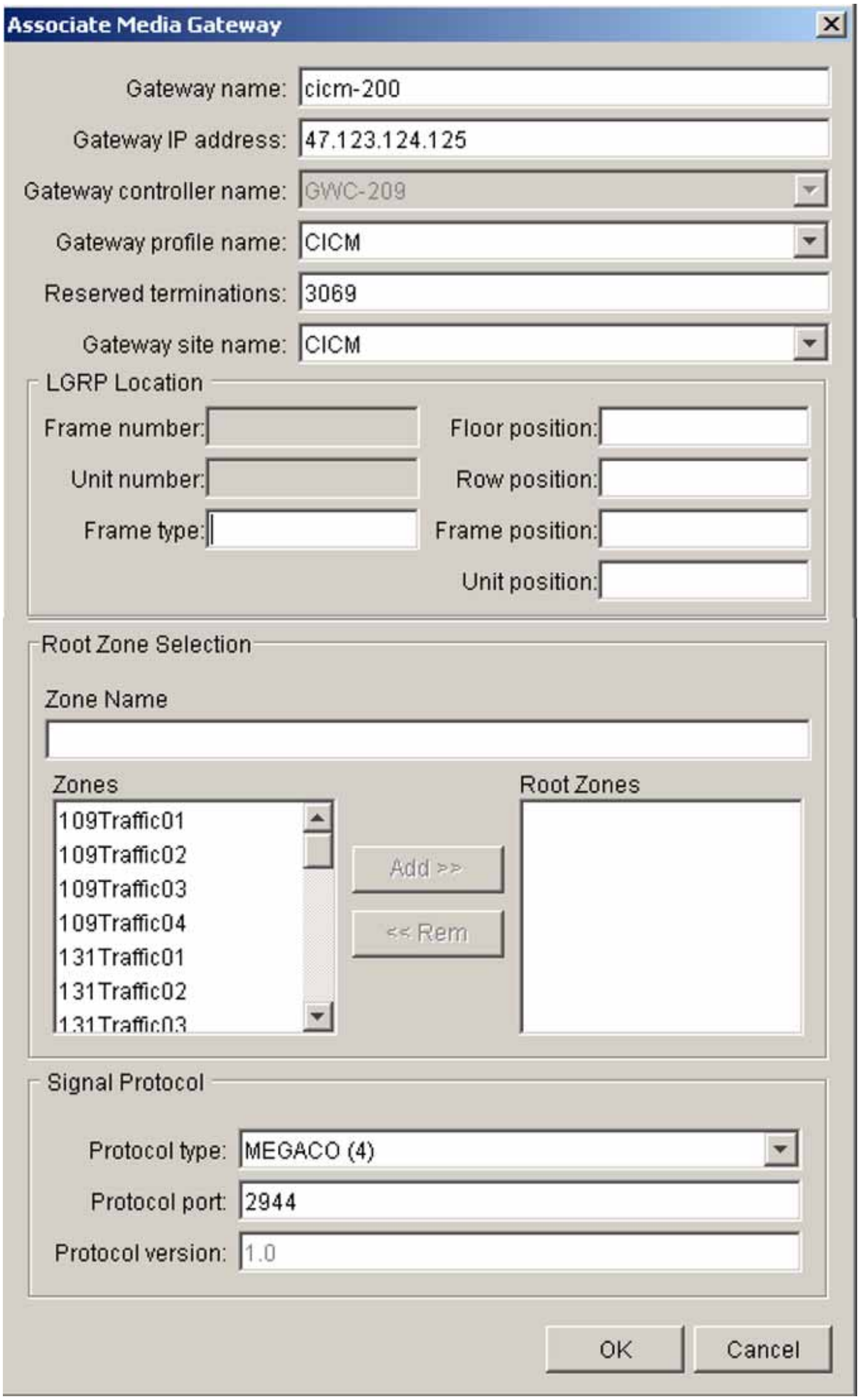
Before subscribers can be added to a Centrex IP Client Manager (CICM) node, it is necessary to assign the CICM to a GWC. This process is called gateway (GWC) association.

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 Gateway 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

This figure shows an example of the associating a CICM using the GUI.

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.

Refer to the procedure Provisioning CICM client lines, in *CICM Configuration Management* (NN10240-511).

Subscriber provisioning

Centrex IP Client Manager (CICM) subscribers and their features are added, changed, and deleted through OSSGate and the CS2000 Management tool.

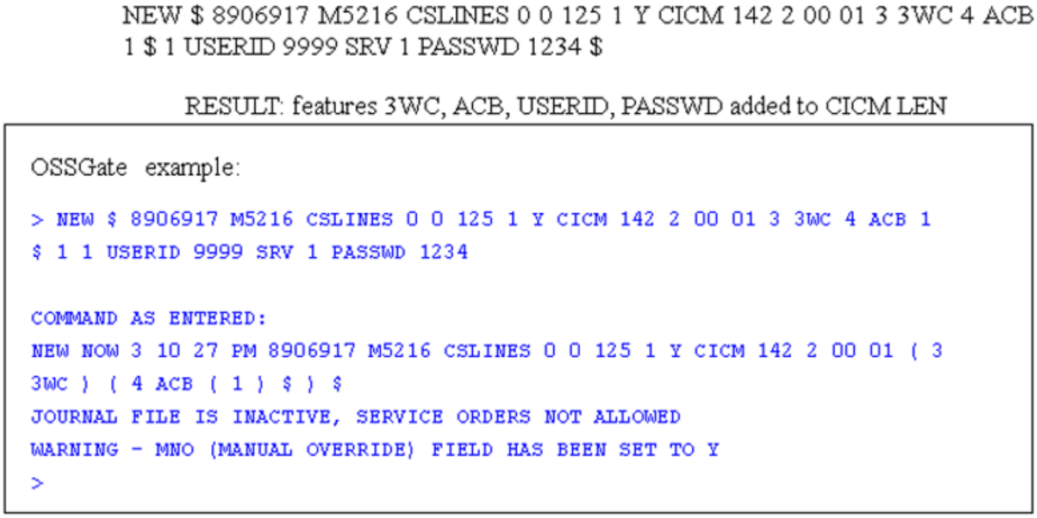
To configure subscribers, an authorized user must connect to OSSGate in CI mode. Any commands which contain a line equipment number (LEN) of the format - CICM nnn n nn nn - are intercepted on the CS2000 Management Tool. The command is passed onto the Line Provisioning application so that the line can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

In addition, the following data, if present, is passed onto the Centrex IP Client Manager Element Manager (CICM-EM):

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

The figure below provides an example of a line being added with the Servord+ NEW command:

Example of OSSGate NEW Command



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

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

OSSGate example:

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

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

CICM supports all 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 provisioning of CICM clients

The procedure used to provision a Centrex IP Client Manager (CICM) client on the CS2000 is similar to the method used to provision a line on other lines gateways. Refer to the procedure Provisioning CICM client lines, in *CICM Configuration Management* (NN10240-511).

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

Terminal gain profiles

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

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

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

Restrictions

- Terminal gain profiles are not supported on third-party terminals or the m6350 soft client. For a complete list of supported terminals, see the CICM-EM help text for terminal gain settings.
- Handsfree gain parameters cannot be adjusted.
- Headset settings apply only to terminals with native headset capabilities, for example IP Phone 2004 and IP Phone 2002.

For additional information refer to Terminal gain profiles in *CICM Configuration Management* (NN10240-511).

Administration and security in CICM

For the full description and procedures involving Centrex IP Client Manager (CICM), refer to *CICM Administration and Security* (NN10252-611).

Navigation

Element Manager security

Centrex IP Client Manager Element Manager (CICM-EM) operator authentication and authorization is tied into the Carrier Voice over IP (VoIP) Server Platform Foundation Software (SSPFS) authorization database.

Log on from and log on to the CICM-EM is performed over Hypertext transfer Protocol Secure (HTTPS). Centrex IP Client Manager (CICM) does not administer users locally; it delegates the authentication to the SSPFS Authentication Database through the HTTPS PAM Proxy on the SSPFS platform. The procedures Configuring PAM on the CICM-EMs, and Configuring the apache proxy on a CICM-EM pair, are in *CICM Configuration Management* (NN10240-511).

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. Telnet connections are secured by SSH. To access CICM nodees, use `cicmconnect` commands on the Centrex IP Client Manager Element Manager (CICM-EM).

UFTP security

The UFTP connection between a Centrex IP Client Manager (CICM) node and its clients with IP Phone firmware has a secure download. The protection is provided by the Unified Network IP Stimulus (UNIStim) security feature. UFTP is supported on the UNIStim signaling port (UDP port 5000) of phase 1 Nortel 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 Nortel IP Phones.

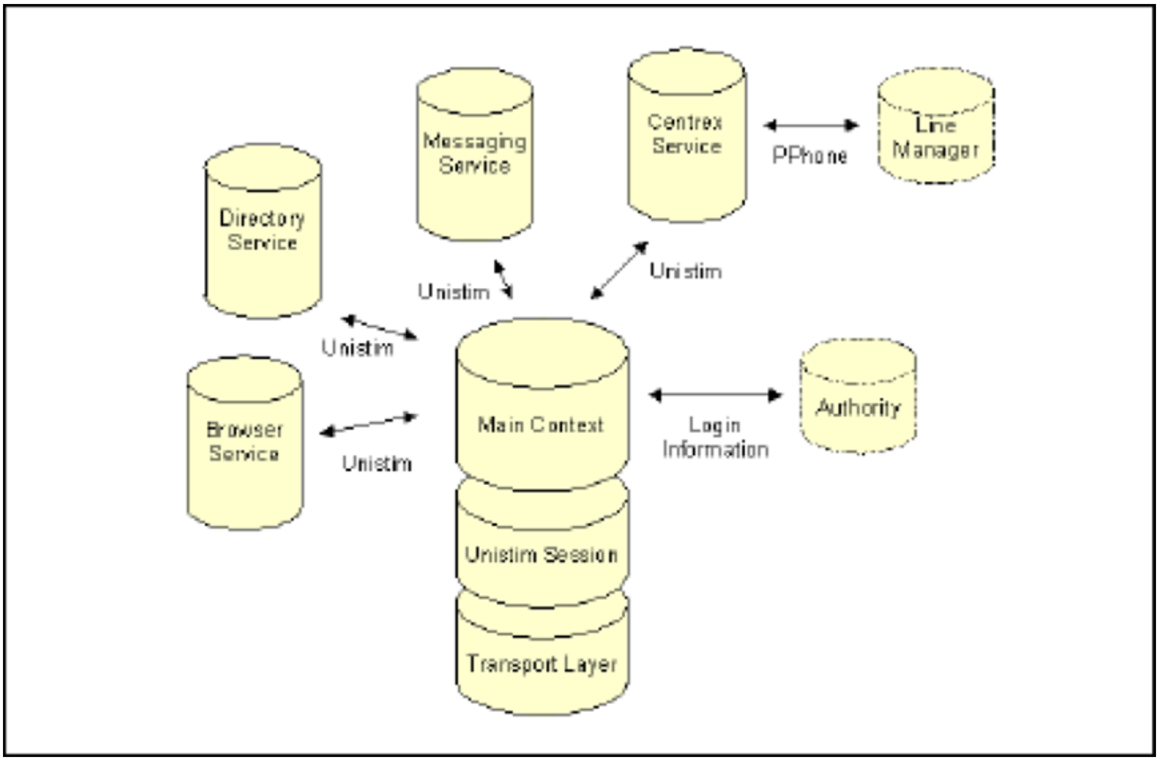
UNIStim security

A Centrex IP Client Manager Element Manager (CICM-EM) hosts sessions between end-user terminals (clients) and the Centrex IP Client Manager (CICM) node (gateway, in this context). Terminals can be physical devices, such as the Nortel IP Phones, or software applications running on a remote computer, such as the m6350 SoftClient on a personal computer (PC). The terminals connect to the CICM node pair and communicate using unified networks IP stimulus (UNIStim). By interacting with the terminal, an end-user can use the services that are hosted by the CICM nodes (gateways).

All signaling messages between a CICM node and its clients (Nortel IP Phones or m6350 SoftClient) are encrypted when the UNIStim security feature is used. Userid, password, and other call control information are not identifiable on the system. 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. The following figure illustrates the relationships with services associated with CICM.

UNIStim security and services



Performance management for CICM

For the full description and procedures involving Centrex IP Client Manager (CICM), refer to *CICM Performance Management* (NN10248-711).

Navigation

Capacity and performance limitations

Centrex IP Client Manager (CICM) supports up to eight 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 this table.

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**

  is the maximum number of lines. A CICM line corresponds to a LEN on the CS2000. Each line is for a user that a CICM node can accommodate.

- **Simultaneous Terminal Sessions**

  is the maximum number of terminals that may be connected and presented with a login prompt by the CICM node at any given time. A user that logs on to a joint session uses two session resources on the CICM node. On a CPN5385-based CICM (SAM21), 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 two of their terminals connected to the CICM node, which prevents n users from connecting to a terminal.

- **Historical Terminal Entries**

  is information about a new terminal that is automatically added to the CICM MIB, for instance, firmware load. 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, because 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 Element Manager (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**

  is the number of half-calls in progress. Even if the second half of a call is also hosted by the same CICM node, 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. After 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**

is the number of Busy Hour Half Call Attempts (BHHCA), which represents the maximum rate at which half call attempts can be made per hour. After the BHHCA reaches 80% capacity, a minor alarm is raised. At 100% capacity, a major alarm is raised, and at 150% a critical alarm is raised and no additional calls are permitted. The critical alarm clears automatically after the BHHCA drops to below 100% for more than 5 minutes. The major alarm is cleared after the BHHCA drops to below 80% for 5 minutes. The minor alarm clears after BHHCA drops below 80% for 15 minutes.

- **RUDP Messages/Sec**

  is the number of Reliable User Datagram Protocols (RUDPs), which 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**

  is the incoming rate of the H.248 messaging protocol that is used between the CICM node and the GWC. The incoming message rate from the GWC is throttled to prevent the CICM node from becoming overloaded.

CICM-EM card pairs

One pair of Centrex IP Client Manager Element Manager (CICM-EM) cards is needed per CS2000. The CS2000 is able to support up to 100 Centrex IP Client Manager (CICM) resource card pairs.

GWC resource card pairs

Each GWC resource card pair supports:

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

Interface with IEMS

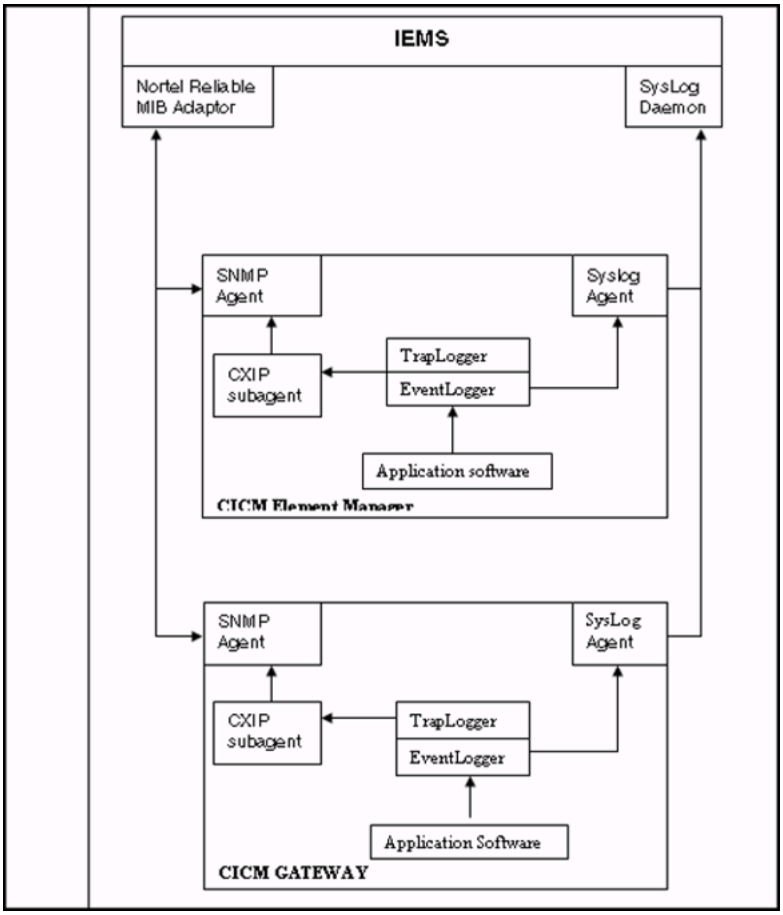
The interface of Centrex IP Client Manager (CICM) products with the Integrated Element Manager System (IEMS) manages the output used by external OSS to monitor the network element and detect alarm conditions. The IEMS is accessed using a Graphical User Interface (GUI), which gives access to the alarms and logs for a network element and interacts with the CICM Element Manager (CICM-EM) GUI.

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

Both a CICM node and a CICM-EM can raise alarms and faults to the IEMS. The EM raises alarms associated with the platform, and from communication with the CICM nodes that it manages. The CICM sends alarms as SNMP traps directly to the IEMS.

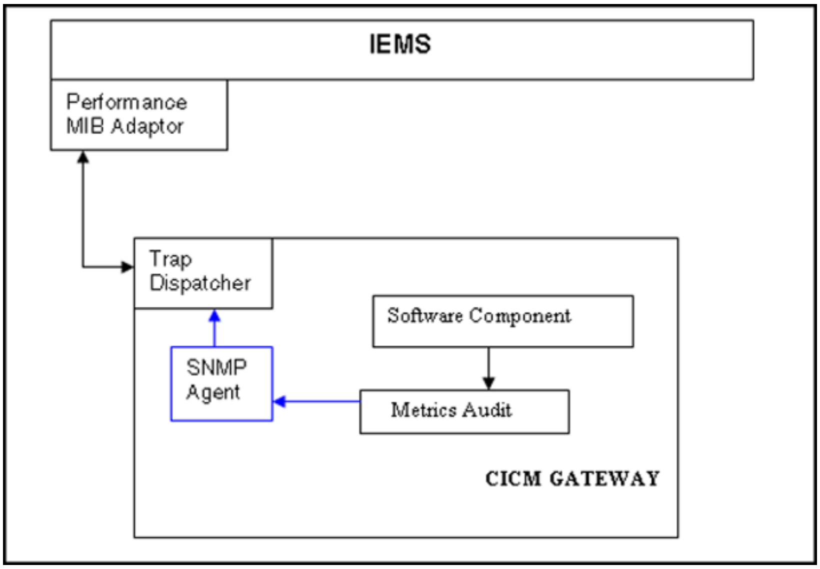
This tables shows an overview of the CICM fault architecture.

CICM fault architecture



This table shows an overview of the CICM performance architecture.

CICM performance architecture



Alarms available through IEMS

All alarms are sent to the Integrated Element Management System (IEMS) as an SNMP trap, and as a log to SYSlog. Each trap sent from a Centrex IP Client Manager (CICM) node includes:

- the sequence number
- the severity indicator
- the component ID
- the category of alarm as one of the following:
  - — communications
  - — quality of service
  - — processing error
  - — equipment
  - — environment
- a notification ID
- a description of the activity or event
- a time stamp
- a probable cause
- a specific problem
- a correlation ID list

Alarm severity classification is listed in this table.

Alarm severity

	Critical	Major	Minor	Warning
Service Affecting	Yes	Yes	No (or few affected)	No
Action Required	Yes	Yes	Yes	No
Recommended Timeliness of Action	Immediately - drop everything	Rapidly - in next work shift	Soon - could be delayed until next day	Later - investigat e if reoccurrence
Target Reporting Time	Within 2 Sec	Within 30 Sec	Within 2 Min	Within 5 Min

Fields which are valid for raising alarms are:

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

Fields which are valid for clearing alarms are:

- nortelNMIcurrentTxNotificationSequenceNum
- nortelNMIalarmComponentId
- nortelNMIalarmDescription
- nortelNMIalarmTimeStamp
- nortelNMIalarmCorrelationIdList

Component IDs

The Centrex IP Client Manager (CICM) products are divided into these objects for reporting alarms:

- the CICM Element Manager (CICM-EM)

- a CICM node
- the platform which the CICM-EMs and the CICM nodes use

These objects contain sub-objects, which are combined with the alarm type, to form the component identifier (ID) as listed in this table.

Component IDs

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

Logs for performance indicators

The Centrex IP Client Manager (CICM) nodes and the CICM Element Manager (CICM-EM) send their logs to the Integrated Element Management System (IEMS). Logs are not exchanged between a CICM node and its CICM-EM. Logs are sent to the IEMS using CUSTLOG or security log formats through a syslog agent. Three log streams are used to send logs to up to three different syslog daemons (that is, IEMS). This is a change from previous CICM releases where all logs were stored on the CICM nodes. Beginning with release SN07, logs are still stored on the CICM nodes, but the nodes also send logs to CUSTLOG, Audit Log, and Security Log streams. Each log is formatted specifically for each of the three streams.

The CICM uses the syslog protocol to send logs to the IEMS. The CICM nodes and CICM-EMs act as log senders. They are only able to send syslog messages. They are not able to receive or relay syslog messages. UDP port 514 is the syslog port that is used to send the syslog messages to the IEMS. The log packet sizes are no greater than 1024 bytes.

Custlogs

The Centrex IP Client Manager (CICM) logs the following events in the custlog format to send into the custlog stream:

- service-affecting state changes
- specific customer/blm requested events
- data corruptions/data mismatches
- shutdown and restart of processes

Security logs

Security logs are generated from a Centrex IP Client Manager (CICM) node as follows:

- upon successful or unsuccessful login from a Nortel IP Phone or m6350 SoftClient
- logout from a Nortel IP Phone or m6350 SoftClient

Security Logs are generated from a CICM Element Manager (CICM-EM) upon launching CICM-EM from Integrated Element Management System (IEMS).

Audit logs

Audit logs are generated from a Centrex IP Client Manager (CICM) node on executing flow-through commands at OSSGATE (for example, commands **`ado`** or **`deo`**).

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

- all configuration changes made by the CICM Element manager (CICM-EM) administrator (for example, adding CICM nodes)
- All maintenance actions done by the device (for example, a restart)

Debug logs

Debug logs are used by Nortel support personnel only, not the service provider. Beginning with release SN07, debug logs can be viewed using the Centrex IP Client Manager Element Manager (CICM-EM) Web page interface. Debug logs remain viewable only at the Web interface and are not sent through syslog to the Integrated Element Management System (IEMS).

Metrics of CICM performance

Performance metrics are generated by both the Centrex IP Client Manager (CICM) node pair and the CICM Element Manager (CICM-EM) pair. They are passed northbound into the Integrated Element Management System (IEMS), where they are available for display and are aggregated with other IEMS southbound feeds into a single OSS feed.

- Transmitted Bytes per Second
- Received Bytes per Second
- Logged In Users
- Half Call Attempts
- Active Connections
- Percentage CPU Used
- Percentage Memory Used
- Number of Logs
- Active Sessions

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 five 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 CICM

For the full description and procedures, see *CICM Fault Management* (NN10233-911).

Navigation

SNMP alarms

Alarms are raised by each Centrex IP Client Manager (CICM) and CICM Element Manager (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 node 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 Integrated Element Management System (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:

```
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 Centrex IP Client Manager (CICM) or CICM Element Manager (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 light-emitting diodes (LED) relate only to a Centrex IP Client Manager (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 light-emitting diodes (LED) are used to signify faults on the Centrex IP Client Manager (CICM) cards and components. Minor, Major and Critical alarms are consistent with CS2000 alarms, and are defined as:

- **Minor**

  A minor chassis alarm is an occurrence when one, but not both, domains are reporting a minor alarm.

- **Major**

  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**

  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**

  No alarms are raised on the Centrex IP Client Manager (CICM).

- **Component Out of Service**

  One or more minor or major chassis alarms have been reported.

- **System Out of Service**

  One or more critical alarms have been reported.

CICM logs

The Centrex IP Client Manager (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.

These are the 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 successfully logs on.

- **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 on 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)

See also "Logs for performance indicators" (page 181).

Northbound logs

Centrex IP Client Manager (CICM) and the CICM Element Manager (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:

Custlog fields description

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:

```
V2_~I=CICM~H=cicm100~A=CICM/GW ~S=0001~~CICM 675 MINOR
TBL CICM/GW34400 CWin32ServiceConstructor called with
0 instances
```

Upgrades for CICM

The full description of supported software upgrades and methods of upgrading a Centrex IP Client Manager Element Manager (CICM-EM) or a Centrex IP Client Manager (CICM) node are identified in *Upgrading CICM* (NN10230-461). The document also includes the task flows of procedures for doing upgrades and rollbacks from upgrades.

Accounting in CICM

Centrex IP Client Manager (CICM) does not affect the way that billing is implemented on the CS2000. All calls, regardless of destination, generate automatic message accounting (AMA) records on the CS2000.

All existing CS2000-hosted billing functions appropriate to the Meridian Business Set (MBS) terminal (phone) are also available for CICM clients (terminals).

Specific call rates for CICM calls are not implemented at this time. For service providers to charge a special rate for CICM calls, it needs to be implemented in the downstream billing system.

There are no unique accounting management tools or utilities for the CICM component.

Billing policies

Centrex IP Client Manager (CICM) uses these policies for billing:

- When a client terminal is disconnected from the CICM, the call is billed. This is necessary to prevent the practice of disconnecting deliberately 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.

Accounting management procedures

The accounting management procedures related to the Centrex IP Client Manager (CICM) level are the existing CS2000 procedures. Refer to the CS2000 suite of Nortel publications.

Customer resources

Navigation

Nortel customer support

For customer support information, contact your Nortel account prime.

Customer documentation

Nortel provides customer information on a CD ROM. Documentation for Centrex IP Client Manager (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 http://www.nortel.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 (1-800-466-7835).

Nortel Web link

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

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.

For technical support in North America call: 1-800-4NORTEL (1-800-466-7835)

Carrier VoIP

CICM Basics

Publication: NN10044-111
Document status: Standard
Document version: 07.02
Document date: 20 October 2006

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

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