# Carrier Hosted Services Basics

## What's new in this release?

### Passport Packet Voice Gateway (PVG) naming

The names used for certain gateways in Carrier VoIP have been re-branded in (I)SN07. The table below lists the names used for certain gateways in Carrier VoIP documentation prior to (I)SN07 and provides the new brand names starting in (I)SN07Nortel Networks Multiservice Data Manager

| Pre-(I)SN07 name | Brand name starting in (I)SN07 |
|---|---|
| Passport Packet Voice Gateway (PVG) | Nortel Networks Media Gateway 7400 or 15000 |
| PVG 7400 or PVG 7K | Nortel Networks Media Gateway 7400 |
| PVG 15000 or PVG 15K | Nortel Networks Media Gateway 15000 |
| Passport 7000/15000/20000 | Nortel Networks Multiservice Switch |
| Passport Preside MSS | Nortel Networks Multiservice Data Manager (MDM) |

### H.323 services

Following is what's new for H.323 services in (I)SN07:

- Advice of Charge (AOC) information can now be delivered during a call (AOC-D) and at the end of a call (AOC-E) to ISDN subscribers. AOC-D and AOC-E is deployed for originating agents connected to the Communication Server (CS) 2000 through H.323. AOC-D is a supplementary service that provides users with cumulative charging information during the call. AOC-E is a supplementary service that enables users to receive information on the recorded charges for a call when the call is released. For provisioning information, refer to Provisioning AOC through table TRKOPTS on page 136.
- The CS 2000 can now interwork with H.323 gatekeepers, which can be in the Carrier's private network, another Carrier's network, or an Enterprise's network. For configuration information, refer to *Configuration details for H.323 gatekeeper functionality, Gateway Controller Configuration Management, NN10204-511.*
- Meridian Customer Defined Network (MCDN)-based services can now interwork over an H.323 gateway such as the Business Communications Manager (BCM) or the Succession 1000M. Interworking applies to MCDN-based services supported on p-phone lines hosted off a Centrex IP Client Manager (CICM), and on Integrated Business Network (IBN) lines hosted off a Mediatrix unit. Interworking of these MCDN-based services is supported for nodal calls where the originating and terminating gateways are connected to the same communication server, and calls across multiple communication servers using SIP-T (ETSI ISUP V2+ with QSIG Feature Transparency [QFT]) as the communication protocol. The following interworkings are supported:
  - H.323 GW (e.g. BCM) <-> H.248 GW (e.g. CICM/P-phone)
  - H.323 GW (e.g. BCM) <-> MGCP GW (e.g. Mediatrix/IBN lines)
  - H.323 GW (e.g. Succession 1000M) <-> H.248 GW (e.g. CICM/P-phone)
  - H.323 GW (e.g. Succession 1000M) <-> MGCP GW (e.g. Mediatrix/IBN lines)

- Meridian Customer Defined Network (MCDN)-based services can now interwork between H.323 gateways such as the Business Communications Manager (BCM) or the Succession 1000M, and across multiple communication servers using SIP-T (ETSI ISUP V2+) as the communication protocol. The following interworkings are supported:
  - H.323 GW (e.g. BCM) <-> H.323 GW (e.g.BCM)
  - H.323 GW (e.g. BCM) <-> H.323 GW (e.g. Succession 1000M)
  - H.323 GW (e.g. Succession 1000M) <-> H.323 GW (e.g. Succession 1000M)
- Call Server-controlled switchover to T.38 is now supported in the international market for Call server-routed H.323 calls. This allows standard Group 3 facsimile terminals to interwork over an H.323 gateway such as a Succession 1000 or Cisco 2600/3600. Fax interworking over H.323 is supported for nodal calls where the originating and terminating gateways are connected to the same communication server, and calls across multiple communication servers using SIP-T (ETSI ISUP V2+) as the communication protocol. Fax interworking is supported
  - over SIP-T between CS 2000s when an H.323 gateway is on one CS 2000
  - over an H.248 gateway interworking with an H.323 gateway
  - over an MGCP gateway interworking with an H.323 gateway

  In (I) SN07, T.38 fax is supported on the CSE1000, M1, BCM 3.6 and CISCO IOS 12.2.

  For configuration details on how to configure the GWC node in a CS 2000 to use an existing codec profile with T.38, or to add a new codec file with T.38, refer to procedure *Configure network codec profiles, Gateway Controller Configuration Management, NN10205-511.*
- Various H.323 gateways controlled by the CS 2000 can now interwork with various SIP clients controlled by the Nortel Networks MCS 5200. The CS 2000 and MCS 5200 are interconnected through SIP trunks.

- H.323 gateway and trunk provisioning is now more flexible and allows
  - — changing provisioning information for H.323 gateways and trunk without having to remove and re-add the gateway provisioning in its entirety.
  - — adding H.323 virtual carriers to an H.323 gateway in the range of 4 to 672 as opposed to the fixed carrier block size in previous releases, which was 24 for north america and 32 for international
  - — support for more than one carrier (D-channel) on a single media gateway, therefore more than one trunk group on the XA-core can be mapped to the endpoints (TIDs) provisioned on the Gateway Controller (GWC).

  For provisioning details, refer to *Change gateway attributes, and Add carriers to a GWC, Gateway Controller Configuration Management, NN10205-511.*

### Centrex IP services

Following is what's new for Centrex IP services in (I)SN07:

- The Centrex IP Client Manager (CICM) and CICM manager now reside in the SAM21 shelf. The new SAM21 chassis consolidates the CICM platform so the CICM and CICM manager can co-reside with the Gateway Controller (GWC) and H.323 interface cards.This SAM21 integration reduces the footprint and cost of CICM. The former SAM16 frame is no longer required to support the CICM, so that entire frame is removed from the CICM hardware line-up. This elimination of the SAM16 hardware reduces cost and results in a substantial improvement in the CICM footprint. However, for those users that currently have a SAM16 configuration, SN07 supports SAM16. For SAM21 hardware and integration, refer to *Insertion and removal processes, CICM Basics, NN10044-111.*

  For more detailed information, refer to *CICM Basics, NN10044-111.*
- In the SAM21-based CICM 7.0, the CICM Element manager (CICM-EM) is reduced to a pair of Motorola CPN5385 processors, one active and the other hot stand-by, providing 1+1 redundancy. Only one pair of the CICM-EM processors is required for each CS 2000, and each CS 2000 is capable of supporting up to 100 pairs of the CICM processors. The hot standby CICM-EM resource card is equivalent to what was formerly the Secondary Element Manager (SEM) chassis in the SAM16-based CICM releases.

  For capacity limits refer to the section, *Traffic loading,CICM Performance Management, NN110248-711.*

- A new interface is introduced in the CICM that manages the output used by external OSS to monitor the network element and detect alarm conditions. This new interface is the Integrated Element Management System (Integrated EMS). The Integrated EMS is accessed using a Graphical User Interface (GUI) that gives access to the alarms and logs for a network element.

  The Integrated EMS provides several views of CICM:

  — Alarms, logs, and performance metrics can be monitored and reviewed.

  — Topology information is available:

    – Instances of CICMs and CICM EMs can be viewed.

    – Relationships can be seen showing each CICM blade configured in the SAM21.

    – The GWC that manages each CICM can be monitored.

  — The CICM EM GUI can be launched from the Integrated EMS.

  Refer to the following procedures in the Integrated EMS documentation:

  — *Launching CICM from Integrated EMS, Integrated EMS Basics, NN10329-111.*

  — *Adding CICM Manager to Integrated EMS, Integrated EMS Configuration Management, NN10330-511.*

  — *Adding a CICM NE, in the Integrated EMS Configuration Management, NN10330-511.*

  — *General data collection and report job procedures, Integrated EMS Performance Management, NN10327-711.*

- Flow-through provisioning minimizes line-provisioning time by automatically making available to other levels of the network the provisioning information that is datafilled at one given time.

  The flow through provisioning feature changes the location of the feature key data from being held against a user to being held against a line. These changes are reflected in the CICM EM.

  CICM provisioning allows all provisioning information for the communication server and the CICM gateway to be input from a single user session. Input information flows to each network element as required for service.

  The CICM generated performance and operational measurements integrate with other network elements for reporting to OSSs.

  The CICM generated faults and alarms integrate with the faults and alarms of other network elements for reporting to OSSs. Alarms can

be viewed on the IEMS. The alarms are aggregated with alarms from other components into one machine feed from the IEMS.

Refer to

— *Feature: Flow Through Provisioning, CICM Basics, NN10044-111.*

— *Alarm, CICM Fault Management, NN10233-911*

The introduction of a central authorization database through the Pluggable Authentication Module (PAM) on the SSPFS platform provides the advantage of having a single account management interface for use by all the management tools. The CICM-EM interfaces to PAM through the HTTPS PAM+ proxy on SSPFS. The central authorization database is used for https access to the CICM EM. It is not used for other methods of access to the CICM EM, such as telnet or ftp, which will continue to use the existing methods of login authentication.

For PAM configuration, refer to *Procedure 36 Configure PAM authentication on a CICM-EM, CICM Configuration, NN10240-511*

- The i2001 is introduced to the client internet terminal portfolio. The i2001 is a low-cost, minimal functionality internet terminal. The i2001, together with all other CICM clients, uses the Nortel Networks proprietary Unified Networks Stimulus (UNIStim) protocol to communicate with the CICM.

  UNIStim reflects the input stimulus (key presses) and the display commands sent from the network that are used to drive displays and lamps on the terminals. This approach allows a wide range of Centrex features to be delivered through the CICM. The proprietary protocol, UNISTim, ensures secure signaling between the CICM server and its clients.

  From a functional perspective, the CICM gateway act as a signaling proxy that converts Unified Network IP Stimulus signaling and control messages between the CICM gateway and Centrex IP clients to H.248 messages for interface to the communication server.

  The i2001 Etherset is the first phase II UNIStim terminal. Phase II terminals provide the ability to support the SIP protocol, therefore providing flexibility to use SIP in the future. Phase II terminals of the i2002 and i2004 are also supported in SN07.

  For installation information, refer to the *Centrex IP Client Manager, Series 7.0, Etherset Installation Guide and User Manual, NN10027-113, version 4.2*C

- The IP Key Expansion Module is introduced for the IP Phones i2002 and i2004. It adds the ability to use an additional 22 keys per

expansion module and up to two expansion modules can be attached per phone. The keys operate in a similar manner to the existing feature keys which are available on the i2002 and i2004. This provides the ability to provide Attendant Console functionality by allowing a large number of lines to be monitored from a single phone. The Key Expansion Module is not supported on the IP Phone i2001. For more detailed information, refer to *Feature:i2002/i2004 Key Expansion Module, CM Basics, NN10044-111*

- The i2001 Etherset is the first phase II Unistim terminal. Phase II terminals have a new bootstrap and require some incremental work on the CICM for support. Phase I terminals will be Manufacture Discontinued (MD) when Phase II terminals are fully implemented and easily available. The Phase II terminals can be configured as emulations of Phase I terminals.

  For installation information, refer to *Centrex IP Client Manager, Series 7.0, Etherset Installation Guide and User Manual, NN10027-113, version 4.2*

- A Web-based interface provides functionality for configuring and monitoring a CICM and its clients. A series of Web pages hosted on the Element Manager provide interface access from any platform that supports Microsoft Internet Explorer, version 6.0, or later.

  The Web-based CICM configuration consists of

  — a home page with
    – a link to an overview page that displays the status of the CICM and its components
    – links to detailed status pages for each CICM element
  — read-only status pages that present the current Node status
  — Web-pages for configuring on the CICM
    – a user
    – the network
    – audio and language profiles
    – client terminals

  CICM can support multiple enterprises. Each enterprise has web-based access to the CICM to control changes within their service. This administrative access can include feature key reconfiguration, arrangement of Call Pickup groups and Speed Call groups, and assignment of features to sets within the Centrex tariff to which they have subscribed.

Each CICM provides web access for the management of assigned data within a set of features. Web-based management of this feature-set data can include call forwarding destinations, number of rings before forwarding screening lists for SCA, SCF, and SCR, ring type, and volume controls.

Refer to the *Element Manager Web site Enhancements, CICM Basics, NN10044-111.*

For detailed description of the EM Web page interface and procedures, refer to the *CICM Configuration Management, NN10240-511*, and *CICM Security and Administration, NN10252-611*.

- A set of root (top-level) middleboxes can now be provisioned to support VCAC on CICM gateways. For provisioning details, refer to *Associate a line media gateway (wireline market), Gateway Controller Configuration and Management document, NN10205-511.*

### Internet Transparency services

Following is what's new for Internet Transparency services in (I)SN07:

- Virtual Connections and Admissions Control (VCAC) can now be enabled on the CS 2000. VCAC is a set of actions taken by the communication server during the call set-up or re-negotiation phase to determine if a virtual path or channel can be accepted by the network. A connection can only be established if sufficient network resources are available to establish the connection end-to-end with the required Quality of Service (QoS). If there are insufficient resources for the call or call leg to complete, the call is released, and the user is directed to a treatment (tone). For provisioning information, refer to Enabling VCAC SOC on page 139

  The following provisioning data is new in (I)SN07 to support VCAC:

  — Limited Bandwidth Link (LBL) middlebox (VCAC middlebox), which is a virtual representation of a link identified in the network that has restricted capacity and therefore, warrants bandwidth management. An LBL is a type of middlebox as is a Network Address Translator (NAT). An LBL is configured to support a maximum count value representing the call set-up capacity through the link. Call set-up through an LBL causes an increase in the running total of used bandwidth capacity, and call take-down causes a decrease. If the running total of used bandwidth capacity exceeds the maximum capacity of the LBL, the call attempt is rejected and routed to treatment (tone). For provisioning details, refer to *Configuring NATs and LBLs,*

*Gateway Controller Configuration and Management, NN10205-511.*

— Resource Usage (RU) data for use in the VCAC function of LBLs where each RU entry has a set of values representing the bandwidth used per call. For provisioning details, refer to *Configure resource usage data for limited bandwidth links (LBLs), Gateway Controller Configuration and Management, NN10205-511*

— Sequential linking (chaining) of middleboxes, NATs or LBLs, in a network hierarchy (maximum of 5). For provisioning details, refer to *Configuring NATs and LBLs, Gateway Controller Configuration and Management, NN10205-511*

— Sharing of NATs and LBLs between multiple communication servers. This is accomplished by assigning unique IDs to each CS 2000 in the network. This allows inter-CS 2000 trunks to be configured as intra-domain SIP-T trunks, and NAT VPN information for both ends of the call to be communicated and compared. For provisioning details, refer to procedure *Set the call agent identifier, Gateway Controller Configuration Management, NN10205-511.*

**E911 services**

Following is what's new for E911 services in (I)SN07:

- The Emergency Call Services (ECS) can now handle mobility of Internet Protocol (IP) telephony clients in a Voice over IP (VoIP) Enterprise environment. This functionality is applicable only to the Succession version of the CICM product, and not applicable to TDM CICM. For a more detailed description of this functionality, refer to the *CICM Basics, NN10044-111.*

  The following provisioning data is new in (I)SN07 to support ECS:

  — Location identification information, which is configured at the network level and reported through the network to an ECS application. For provisioning information, refer to procedures *Configure a destination for CICM location information and Enable/disable CICM location change reporting, Gateway Controller Configuration Management, NN10205-511.*

**SIP services**

Following is what's new for SIP services in (I)SN07:

- The Session Server and SIP gateway application are introduced to allow interoperability between the CS 2000 network and third-party SIP-based communication servers and Media Application Servers, and therefore enable the SIP-based servers to access the PSTN

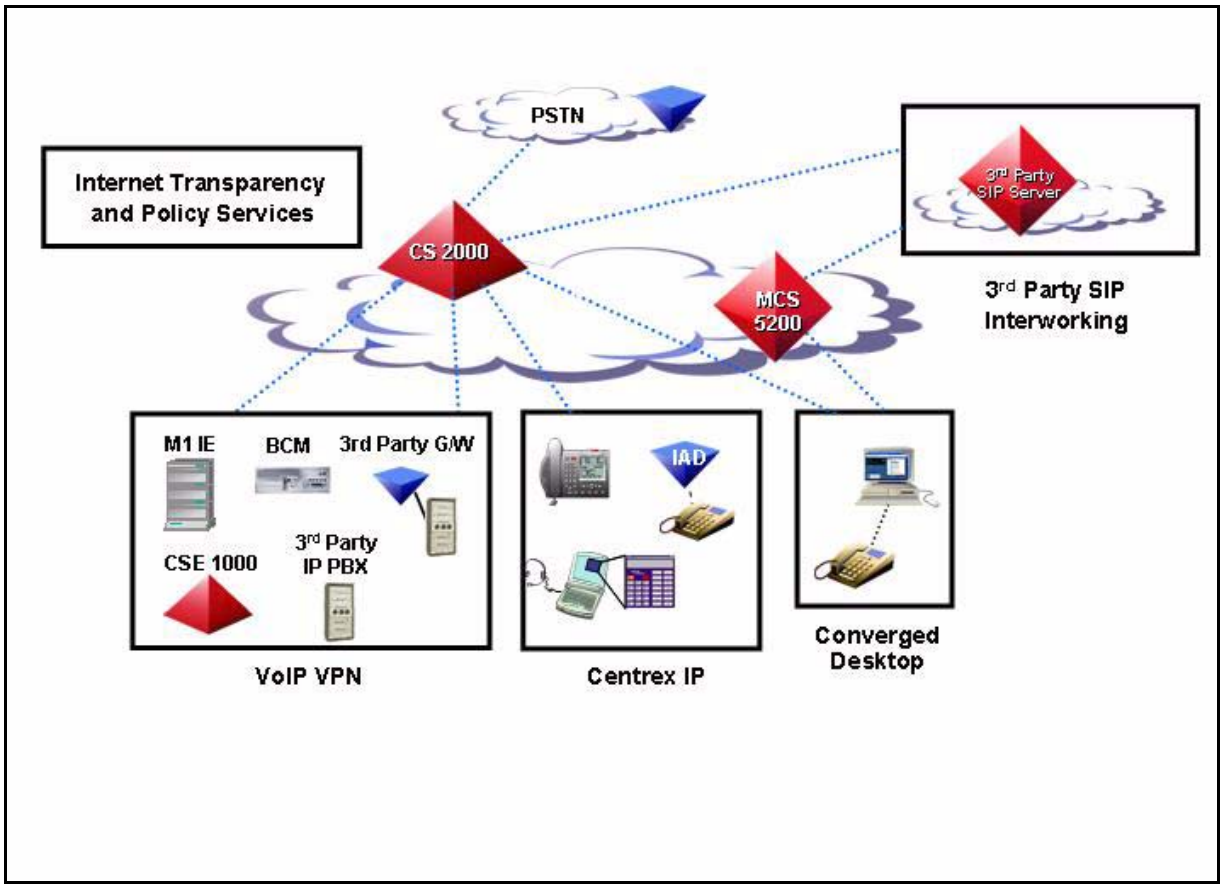
through the CS 2000 network. This eliminate the need for a “slower” VRDN GWC for call routing. The Session Server is a high-capacity, carrier-grade platform that consists of hardware based on SAM-XTS, and software that consists of Nortel Carrier Grade Linux (NCGL) base and shared (SIP-T) layers. The SIP gateway application on the Session Server converts open interoperable SIP messages into messages the communication server, CS 2000 or MCS 5200, can understand. For more detailed information, refer to the Session Server suite of documents listed under Session Server on page 126.

## CHS overview

This section provides a high-level view of the Carrier Hosted Services (CHS). CHS is a portfolio of Nortel Networks products and services that provides IP-based solutions to IP network-based subscribers. This solution delivers legacy Digital Multiplex System (DMS) and Succession-based Centrex capabilities to users connected to an IP network using voice multimedia integration. (Centrex is a portfolio of telecommunications services that emulate the private network capabilities of sophisticated, on-premise switching equipment – such as a key system or Private Branch Exchange [PBX] – using the switch and service resources of the public switch network delivered over voice or data lines, or both.)

The following figure shows a high-level view of the network architecture for CHS.

## CHS architecture




VoIP technology enables voice to be carried over a packet network. Analog voice signals are digitized, compressed, and transmitted as IP packets over an IP network.

A VoIP call can be initiated from:

- a PC equipped with suitable IP telephony client software (such as Nortel Networks m6350 SoftClient)
- a local area network (LAN)-capable telephone (such Nortel Networks i200x Etherset)
- an analog/digital phone off of an IP-enabled PBX

# CHS components

## Overview

The following table lists the components that comprise Carrier Hosted Services, including a brief description of their functions.

**CHS components and their functions**

| Component | Sub-component | Function |
|---|---|---|
| Network intelligence | | |
| Communication Server 2000 (CS 2000)  | | The CS 2000 solution has evolved from the legacy DMS family of TDM CO switches. The CS 2000 reuses much of the existing DMS TDM service software, as well as the carrier grade DMS hardware.<br>CS 2000 provides the following primary functions<br>• call processing (including translations and routing)<br>• Signaling System 7 (SS7) signaling<br>• call feature processing (including features inherited from the DMS switch)<br>• billing |
| CS 2000 | Extended Architecture Core (XA-Core) | The XA-Core is the computing engine of CS 2000. The XA-Core provides maintenance, call processing, and billing functionality. The CS 2000 also sends control messages (for connection set-up) to media gateways (such as the Media Gateway 15000, Multimedia Terminal Adapter, and MG 9000.)<br>The ethernet or high-speed Input/Output Processor (EIOP/HIOP), which resides on the XA-Core, enables the XA-Core to connect to the packet network. |
| CS 2000 | Message Switch (MS) | The MS routes messages from the XA-Core to the Enhanced Network (ENET), Input/Output Module (IOM), Fiberized Link Peripheral Processor (FLPP), and CS 2000 Core Manager. |

## CHS components and their functions

| Component | Sub-component | Function |
|---|---|---|
| CS 2000 | ENET | The ENET is an optional component. The ENET is the enhanced network for the XA-Core. It is a fully duplicated switching fabric that performs call switching. The ENET provides the messaging path from CS 2000 to any legacy peripherals and is required for access to test trunk facilities. |
| CS 2000 | IOM | The IOM provides input/output (I/O) interface to the CS 2000. |
| CS 2000 | Cabinetized Integrated Service Module (CISM)/ Integrated Service Module Enhanced (ISME) and the Office Alarm Unit (OAU) | The CISM/ISME and the OAU provide test and service circuit functions required by the CS 2000 feature set. |
| | Integrated Services Module (ISM) | The ISM is a specialized module designed to accommodate test and service circuit packs used in switch and facility maintenance. In a CS 2000 configuration, the ISM houses IOMs. IOMs provide ports for serial input and output, enabling local and remote devices to communicate with the rest of CS 2000 IOMs through the CS 2000 message switch. The IOMs support datalinks that bring the CS 2000 Core Manager or the CS 2000 into service. Each card supports up to 16 ports for 64 Kb/s synchronous V.35 links or 28.8 Kb/s asynchronous RS232 links. |

## CHS components and their functions

| Component | Sub-component | Function |
|---|---|---|
| | Office alarm unit (OAU) | The OAU connects a CS 2000 with the office alarm system to provide notification of physical or electrical problems. An OAU consists of two main types of functional elements:<br>• Scan points and monitoring devices for collecting environmental input (for example, temperature levels) and detecting state changes in peripheral equipment.<br>• Output devices such as signal distribution points (SDPs) that provide collected information for inclusion in logs and displays, and to activate audible alarms when required.<br>The OAU is directly connected to the Enhanced Network (ENET). The ENET is connected to the MS, which facilitates communication between the ENET and the XA-Core. |
| CS 2000 | Service Application Module 21 (SAM21) | The SAM21 shelf houses the GWC cards.<br>All tools and utilities for the SAM21 are provided by CS 2000 SAM21 Manager. |

## CHS components and their functions

| Component | Sub-component | Function |
|---|---|---|
| CS 2000 | Gateway Controller (GWC)  | The GWCs provide protocol mediation between the XA-Core and media gateways such as the Media Gateway 15000, MG 9000, and the RTP Media Portal. In other words, the GWCs convert proprietary supervision messages from the XA-Core to protocols recognized by the media gateways.<br>The CS 2000 XA-Core and the CS 2000 - Compact also support the GWC.<br>The GWCs support these protocols:<br>• H.248<br>• H.323<br>• Automatic System for Performance Evaluation for the Network (ASPEN)<br>• Session Initiation Protocol for Telephony (SIP-T)<br>• ISDN 1.921-User Adaptation (IUA)<br>• Simple Network Management Protocol (SNMP)<br>• MTP3-User Adaptation Layer (M3UA)<br>• packet cable NCS<br>• packet cable Dynamic Quality of Service (DQoS) and Common Open Policy Services (COPS)<br>• Media Gateway Control Protocol (MGCP)<br>Every GWC uses the same hardware and software. Profiles applied at the GWC Manager define the type of GWC. |

## CHS components and their functions

| Component | Sub-component | Function |
|---|---|---|
| | Fiberized Link Peripheral Processor (FLPP)/Link Peripheral Processor (LPP)  | The FLPP/LPP functions as the default SS7 signaling server for evergreen hybrid applications when an existing DMS switch (supporting legacy peripherals) is converted to a CS 2000. FLPP uses SR 128 sub-rate fiber links to connect the CS 2000 to the SS7 network. |
| CS 2000 | Universal Audio Server (UAS)  | The UAS provides media services, such as the delivery of voice announcements, the collection of dual-tone multi-frequency (DTMF) digits, speech recognition, text-to-speech synthesis, speaker verification, audio conferences, and facsimile. The UAS provides voice announcements and facilitates the lawful electronic surveillance of voice and voice-band data traffic in the network (LI). The UAS resides on the SAM16 hardware platform. The UAS has 100 BaseT Ethernet connections to the CS LAN for UAS bearer traffic, as well as for H.248 call control messaging between the UAS and the CS 2000 and for OAM&P messaging between the UAS and the UAS manager. |
| CS 2000 | Audio Provisioning Server (APS) | The APS is a subcomponent of UAS. The APS is required whenever the UAS is used as the announcement server. The APS assures that all UASs in the network use the same announcements. The APS is a non-call processing component. It uses a user-friendly web interface to provision audio services and to set up distribution of announcements to UASs in the network. |

## CHS components and their functions

| Component | Sub-component | Function |
|---|---|---|
| CS 2000 | Universal Signaling Point (USP) and USP Compact  | The USP is the default SS7 signaling server for new installations (greenfield). The USP supports a redundant 10/100BaseT IP interface. This release provides the following capabilities:<br>• high-speed link interface support to signaling transfer point (STP): DS-1 asynchronous transfer mode (ATM) Signaling ATM Adaptation Layer (SAAL) SS7 links (8 DS-0 equivalent)<br>• high-speed link interface support to simple control transmission protocol (SCTP): IETF SIGTRAN SCTP/M2PA IP high-speed link (8-20 DS-0 equivalent)<br>• DS0A, V.35, and channelized T1/E1 low-speed link support<br>• direct messaging to the GWC using M3UA/UDP for TDM ISDN User Part (ISUP) trunking<br>• load sharing between SS7 links<br>• supports co-resident STP capability<br>• support for American National Standards Institute (ANSI) and ETSI ISUP trunks<br>• high service availability of 99.999% and in-service software upgrades during which no calls are lost<br>• in-service LIU7 application upgrade from FLPP to USP<br>• access to HMI through the Ethernet<br>• support for up to 16 multi-point codes<br>• support for up to 440 low-speed SS7 links |

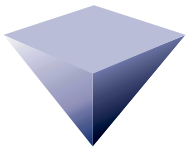
## CHS components and their functions

| Component | Sub-component | Function |
|---|---|---|
| CS 2000 | Universal Signaling Point (USP) and USP Compact | The USP - Compact provides the same basic functionality as the USP, but is used for networks with smaller call capacities.<br>The USP - Compact resides on two identical blades in a CS 2000 - Compact or SAM21 shelf and supports up to 16 channelized T1/E1 links and up to 8 multi-point codes. |
| CS 2000 | Communication Server local area network (CS LAN) | The CS LAN provides secure, carrier-grade, fully-redundant routing of call processing, signaling, and management messages between the CS 2000 and the other components in the solution (for example, the Media Gateway 15000, MG 9000, GWCs). (Optionally, the CS LAN can provide a bearer path between components). The CS LAN is fully integrated with the CS 2000, and consists of a dual Passport 8600 router configuration with 10/100 BaseT Ethernet links to components. |
| CS 2000 - Compact  | | The CS 2000 - Compact is a full-featured, small-footprint alternative to the CS 2000, which is designed for new installations. The CS 2000 - Compact performs call processing, messaging, routing, translations, centralized systems delivery, and storage of office images and system data. |
| CS 2000 - Compact | Call Agent | The Call Agent is the computing engine of CS 2000 - Compact. The Call Agent provides maintenance, call processing, and billing functionality. The Call Agent also sends control messages (for connection setup) to media gateways (such as the Media Gateway 15000 and MG 9000) |

## CHS components and their functions

| Component | Sub-component | Function |
|---|---|---|
| CS 2000 - Compact | STOrage Management (STORM) | The STORM card provides network file system (NFS) services to applications running in the CS 2000 - Compact. An NFS is a distributed file system that allows applications to access files and directories on remote computers. STORM acts as an NFS server for the clients running on the Call Agent, and the USP - Compact. Each STORM card is attached to a persistent data storage (PDS) device. |

## CHS components and their functions

| Component | Sub-component | Function |
|---|---|---|
| Gateways | | |
| Media Gateway 15000  | | Media Gateway 15000 serves as a media gateway in the Succession Network. The Media Gateway 15000 supports the H.248 protocol for communication between the GWCs and Media Gateway 15000.<br>The Media Gateway 15000 supports the following functions:<br>• tone generation on the TDM side of the gateway, such as basic service tones, basic call progress tones, and expanded call progress tones<br>• in-band DTMF digit collection for ISUP and primary rate interface (PRI) trunk agencies<br>• clear channel data functionality for test trunk capability<br>• modem and fax services over G.711 CODEC standard<br>• software maintenance and release upgrade<br>• carrier-grade attributes, such as Network Equipment Building System (NEBS) Level 3 compliancy, hot swap capability of CP cards, and cold swap capability of voice services processor (VSP) cards<br>• T108 test trunk termination<br>• interworking with TDM trunks through Interworking Spectrum Peripheral Module Internet Protocol (IW-SPM-IP)<br>• two-port Gigabit Ethernet on the VSP3 card |

## CHS components and their functions

| Component | Sub-component | Function |
|---|---|---|
| Core Network | | |
| Network management | | |
| Nortel Networks Multiservice Switch(MSS)  | | The Nortel Networks Multiservice Switch (MSS) is a suite of element management software that runs on approved hardware platforms. MSS provides the overall OAM&P functionality for Succession solutions. MSS supports the full range of functions defined in the Open Systems Interconnection (OSI) model:<br>• Fault management<br>• Configuration management<br>• Accounting management<br>• Performance management<br>• Security management<br>MSS consists of the following software packages and managers:<br>• CS 2000 Core Manager<br>• CS 2000 Management Tools<br>• CS 2000-Compact Manager<br>• USP Manager<br>• Nortel Networks 8600 Device Manager<br>• RTP Media Portal Manager<br>• Nortel Networks Multiservice Data Manager (MDM) |

## CHS components and their functions

| Component | Sub-component | Function |
|---|---|---|
| Nortel Networks Multiservice Switch (MSS) | CS 2000 Core Manager  | The CS 2000 Core Manager provides OAM&P functionality for the XA-Core and the subtending TDM components of the CS 2000. It resides on the SuperNode Data Manager (SDM) platform and includes much of the SDM's existing OAM&P functionality. CS 2000 Core Manager also provides access to logs for the MG 9000, GWC, UAS, Media Gateway 15000, SAM21 and XA-Core. In addition, the CS 2000 Core Manager provides performance metrics for the XA-Core, MDM, and Media Gateway 15000.<br><br>The CS 2000 Core Manager provides access to logs, alarms, and performance monitoring data relating to call processing on the CS 2000 - Compact. |

## CHS components and their functions

| Component | Sub-component | Function |
|---|---|---|
| Nortel Networks Multiservice Switch (MSS) | CS 2000 Management Tools  | CS 2000 Management Tools is a suite of network management tools used in Succession solutions. The CS 2000 Management Tools suite consists of the following network management tools:<br>• GWC Manager<br>• UAS Manager<br>• APS<br>• APS Manager<br>• SAM21 Manager<br>• Network Patch Manager (NPM)<br>• Nodes Configuration<br>• Trunks Configuration<br>• Carrier Endpoint Provisioning<br>• Lines Configuration<br>• Trunk Maintenance Manager (TMM)<br>• Line Test Manager (LTM)<br>• Lines Maintenance Manager (LMM)<br>• V5.2 Configuration<br>• V5.2 Maintenance<br>• PM Poller<br>• QoS Collector Application<br>• Batch Provisioning Tool (BPT)<br>• Batch Configuration Monitor<br>• OSSGate<br>• USP Bootp Server |

## CHS components and their functions

| Component | Sub-component | Function |
|---|---|---|
| Nortel Networks Multiservice Switch (MSS) | CS 2000 Management Tools | The following CS 2000 Management Tools are embedded in specific EMs:<br>• Nodes Configuration<br>• Trunks Configuration<br>• Carrier Endpoint Provisioning<br>• Lines Configuration<br>• Line Test Manager (LTM) |
| Nortel Networks Multiservice Switch (MSS) | CS 2000 GWC Manager  | The primary function of the CS 2000 GWC Manager is to coordinate the configuration of the CS 2000 GWCs.<br>Also, the CS 2000 GWC Manager is used for fault management of a CS 2000 GWC node. |
| Nortel Networks Multiservice Switch (MSS) | Universal Audio Server Manager (UAS Manager)  | The UAS Manager configures the UAS, and monitors fault and performance data for the UAS. The UAS Manager is used with the APS Manager to completely manage the UAS. |
| Nortel Networks Multiservice Switch (MSS) | APS Manager  | The APS Manager provides a Web-based GUI that manages announcements from any workstation. The APS Manager client runs on a PC. |

## CHS components and their functions

| Component | Sub-component | Function |
|---|---|---|
| Nortel Networks Multiservice Switch (MSS) | CS 2000 SAM21 Manager  | The CS 2000 SAM21 Manager is a graphical user interface (GUI) that provides access to OAM&P functions such as platform the software load, platform diagnostics, platform upgrade, and NFS mount provisioning.<br><br>In addition, the CS 2000 SAM21 Manager provisions the hardware of a CS 2000 GWC, for fault management of a CS 2000 GWC card, and to upgrade the firmware of a CS 2000 GWC.<br><br>CS 2000 SAM21 Manager has two components: the EM server and the EM client.<br><br>The CS 2000 SAM21 EM server resides on the same server that hosts the Succession Server Platform Foundation Software (SSPFS) non-CM load (NCL) software package (part of the CS 2000 Management Tools software). Currently, the SSPFS package runs on a Netra t1400.<br><br>***Note:*** The CS 2000 SAM21 EM server does not have a GUI.<br><br>The CS 2000 SAM21 EM client runs on either a PC or Sun Solaris machine and provides a GUI of the physical layout of the SAM 21 shelf for fault management and configuration management of the SAM21 shelf. |

## CHS components and their functions

| Component | Sub-component | Function |
|---|---|---|
| Nortel Networks Multiservice Switch (MSS) | Network Patch Manager (NPM)  | The NPM is used to support individual patching of software loads for the following components:<br>• CS 2000 GWC<br>• MG 9000<br>• MG 9000 Manager<br>• Network Patch Manager (NPM)<br>• Patching Server Element (PSE)<br>• SAM21 EM<br>• CS 2000 Management Server |
| Nortel Networks Multiservice Switch (MSS) | Trunk Maintenance Manager (TMM)  | The TMM provides an XML interface that allows client applications (GUIs) to perform basic maintenance operations on GWC-managed trunks, such as posting, busying, and returning to service. |
| Nortel Networks Multiservice Switch (MSS) | Lines Maintenance Manager (LMM)  | The LMM application is used to post lines and perform maintenance activities on them. |
| Nortel Networks Multiservice Switch (MSS) | V5.2 Configuration and Maintenance  | The V5.2 Configuration and Maintenance applications are used to manage V5.2 interfaces within a Succession Network.<br><br>***Note:*** These applications are available only in the international version of the software. |

## CHS components and their functions

| Component | Sub-component | Function |
|---|---|---|
| Nortel Networks Multiservice Switch (MSS) | Performance Monitoring (PM) Poller  | The PM Poller is delivered as a subpackage in the Succession Server Platform Foundation Software (SSPFS). The PM Poller provides a SNMP-based system to gather performance information from the GWC, UAS, and the SSPFS on the CS 2000 Management Tools server. |
| Nortel Networks Multiservice Switch (MSS) | QoS Collector Application (QCA)  | The QCA stores QoS reports for processing and analysis by a customer OSS. QoS records contain a set of QoS parameters collected on an individual call basis. The QoS parameters that are collected:<br>• packets sent and received<br>• packet loss<br>• octets sent and received<br>• inter-arrival latency<br>• jitter |
| Nortel Networks Multiservice Switch (MSS) | Patch Provisioning Tool (BPT)  | The BPT provides users with the following capabilities:<br>• perform bulk configuration of Succession lines<br>• perform bulk flow through configuration of ADSL for MG 9000<br>• view the log and output files associated with each batch provisioning process<br>• delete the log and output files associated with each batch provisioning process |

## CHS components and their functions

| Component | Sub-component | Function |
|---|---|---|
| Nortel Networks Multiservice Switch (MSS) | Batch Configuration Monitor  | The Batch Configuration Monitor is a web-browser interface to view provisioning output files in a readable format. |
| Nortel Networks Multiservice Switch (MSS) | OSSGate  | The OSSGate is a GUI application that provides a machine interface for provisioning components in Succession. The main functionality of the OSSGate is to act as a gateway to the node, carrier, trunk, line, and ADSL provisioning applications, and the trunk maintenance application. |
| Nortel Networks Multiservice Switch (MSS) | Trunk Maintenance Manager (TMM)  | The TMM provides an XML interface that allows client applications (GUIs) to perform basic maintenance operations on GWC-managed trunks, such as posting, busying, and returning to service. |
| Nortel Networks Multiservice Switch (MSS) | Call Agent Manager  | The CS 2000 - Compact Call Agent Manager is a menu-driven console application that provides access to SAM21 platform alarms, platform performance monitoring, platform logs, platform connectivity, and platform patching. In addition, the Call Agent Manager is the primary interface for platform functions such as a cold SWACT, routine exercise text, jamming, and synchronization of the call processing application. |

## CHS components and their functions

| Component | Sub-component | Function |
|---|---|---|
| Nortel Networks Multiservice Switch (MSS) | STORM Manager  | The STORM Manager is used with CS 2000 - Compact. The STORM Manager is a Web-server application that runs on the STORM card. The STORM Manager allows you to<br>• Provision and control application-level STORM functions.<br>• Modify STORM file systems.<br>• View STORM logs. |
| Nortel Networks Multiservice Switch (MSS) | Universal Signaling Point (USP) Manager  | The USP Manager is a Windows 2000 workstation that provides a GUI for provisioning and monitoring SS7 interfaces. The bootp server for the USP is part of the CS 2000 Management Tools server. |
| Nortel Networks Multiservice Switch (MSS) | Nortel Networks Multiservice Switch 8600 Device Manager  | The Device Manager (for Nortel Networks Multiservice Switch 8600) is a suite of GUI applications that manages and configures a Nortel Networks Multiservice Switch 8600 Device Manager chassis. It can be launched independently or as part of Optivity. |
| Nortel Networks Multiservice Switch (MSS) | RTP Media Portal Manager  | For the RTP Media Portal, the System Management Console is used to perform fault and configuration management. The RTP Media Portal management data is stored on the Management Module and the Database Module. The Management Module stores alarm, log, and OM data. The Database Module stores configuration data. |

**CHS components and their functions**

| Component | Sub-component | Function |
|---|---|---|
| Nortel Networks Multiservice Switch (MSS) | Nortel Networks Multiservice Data Manager (MDM)  | The Nortel Networks Multiservice Data Manager (MDM) manages the Media Gateway 15000. The MDM performs fault management, configuration management, data collection, performance management, and security management. In addition, the MDM forwards Media Gateway 15000 performance management, and fault management information to the CS 2000 Core Manager. The MDM resides on a Sun-based workstation. |
| Centrex IP | | |
| Centrex IP Client Manager | | The CICM delivers Centrex capabilities to users connected to an IP network using VoIP technology on a PC SoftClient or an IP P-phone. |

## MCS 5200 required functional components

The MCS 5200 includes several functional components, some of which are required and others that are optional. Both the MCS 5200 and the CS 2000 utilize MCS RTP Media Portals for NAT/firewall transversal. There are two possible management system configurations for MCS RTP Portals associated with a CS 2000: shared and dedicated.

In the shared configuration, the MCS RTP Media Portals associated with the CS 2000 are managed using the management system modules that are provided with an MCS 5200 system.

In the dedicated configuration, the MCS RTP Portals associated with the CS 2000 are managed by separate MCS Management and Database Modules, and System Management Console. The dedicated configuration can be used when an MCS 5200 is not present or when an MCS 5200 is present but with its own set of dedicated MCS Management and Database Modules, and System Management Console.

The following table shows the required functional components that comprise the MCS 5200 platform.

**MCS 5200 functional components (required)**

| MCS 5200 components | Description |
|---|---|
|  | The SIP Application Module is the MCS 5200 service execution engine that provides the following software functionality:<br>• SIP Proxy Server<br>• Back-to-Back User Agent (BBUA)<br>• SIP Registrar<br>• CPL Interpreter<br>• address resolution and routing capabilities<br>The SIP Application Module is dual-homed. As an optional software feature of the SIP Application Module, the SIP Presence Module processes information for presence subscription and notification.<br>For more information, refer to *MCS 5200 SIP Application Module Basics, NN10029-111,* and *MCS 5200 Presence Basics, NN10236-111.* |

## MCS 5200 functional components (required)

| MCS 5200 components | Description |
|---|---|
|  | The Management Module enables communication between the System Management Console and other network components. It provides the software functionality that:<br>• manages the following functions for the MCS 5200 components, media server, and the gateways:<br>— faults<br>— configuration<br>— performance<br>• collects operations, administration, and maintenance (OAM) information for display on the System Management Console<br>The Management Module is located in the private MCS 5200 network. The System Management Console is the administrators interface to the Management Module.<br>For information on the Management Module, refer to *MCS 5200 Management Module Basics, NN100030-111.* For information on the System Management Console, refer to *MCS 5200 System Management Console Basics, NN10247-111.*,<br>For information on the Management Module in the dedicated configuration to support MCS RTP Media Portals associated with the CS 2000, refer to the *CVoIP Management Module Basics, NN10369-111.* For information on the System Management Console in the dedicated configuration to support MCS RTP Media Portals associated with the CS 2000, refer to the *CVoIP System Management Console User Guide, NN10370-111*. |

## MCS 5200 functional components (required)

| MCS 5200 components | Description |
|---|---|
|  | The Database functionality is comprised of several software components: Oracle database software, Database Module component, and the Oracle Monitor component. The Oracle database is accessed by some network components in order to provide storage and retrieval for:<br>• subscriber location information<br>• registration status based on information received with SIP client registration<br>• routing and translation entries<br>• system configuration data<br>The Database functionality is located on the private MCS 5200 network. For more information, refer to *MCS 5200 Database Module Basics, NN10031-111.*<br>For information on the Database Module in the dedicated configuration to support MCS RTP Portals associated with the CS 2000, refer to the *CVoIP Database Module Basics, NN10368-111.* |
|  | The Accounting Module provides a mechanism for receiving, storing, formatting, and transmitting accounting information for billing purposes.<br>The Accounting module is located on the private MCS 5200 network. For more information, refer to *MCS 5200 Accounting Module Basics, NN10037-111.* |

## MCS 5200 functional components (required)

| MCS 5200 components | Description |
|---|---|
|  | The Provisioning Module provides the interface for the access clients (Multimedia PC Client, Multimedia Client Set, Provisioning Client, and Personal Agent) to securely access the data stored in the Oracle Database. It supports the following tasks:<br>• service provider provisioning through the Provisioning Client<br>• customer domain provisioning through the Provisioning Client<br>• setting up network services functions, such as the network address book<br>• enabling the administrator to do bulk provisioning either through an API or through a command line interface (CLI)<br>Within the Provisioning Module, a Sun ONE Web Server* processes HTTP requests from the Multimedia Web Client, Personal Agent, and Provisioning Client to support self provisioning and network-based services.<br>The Provisioning Module is dual-homed. For more information about the Provisioning Module, refer to *MCS 5200 Provisioning Module Basics, NN10242-111,* and *Provisioning Client User Guide, NN10043-113*. For more information on provisioning tasks that the Provisioning Module processes, refer to the following documents:<br>• *Multimedia PC Client User Guide, NN10041-113*<br>• *Multimedia Web Client User Guide, NN10040-113*<br>• *i2002 Internet Telephone User Guide, NN10319-113*<br>• *i2004 Internet Telephone User Guide, NN10042-113* |

## MCS 5200 functional components (required)

| MCS 5200 components | Description |
|---|---|
| System Management Console<br>  <br> | The System Management Console is the element manager GUI for MCS 5200. With this GUI you can:<br>• administer system, database, and service components<br>• configure MCS 5200 system sites, servers, modules/components, and services<br>• monitor the MCS 5200 system using alarms, logs, and performance measurements<br>• manage collection of operations, administration, accounting, and maintenance information<br>The System Management Console runs on a personal computer (PC) and communicates with the Management Module on the private MCS 5200 network. For more information about the System Management Console, refer to *MCS 5200 System Management Console Basics, NN10247-111*.<br>For information on the System Management Console in the dedicated configuration to support MCS RTP Media Portals associated with the CS 2000, refer to the *CVoIP System Management Console User Guide, NN10370-111.* |

## MCS 5200 optional functional components

The following table lists the optional functional components that comprise the MCS 5200.

**MCS 5200 functional components (optional when using Sun Netra servers)**

| MCS 5200 component | Description |
|---|---|
|  | The IP Client Manager manages the i2002 and i2004 Internet Telephones. It provides them access to MCS 5200 SIP services. The IP Client Manager provides access to the following features:<br>• Instant Messaging<br>• information delivery services<br>• session-handling services<br>• call management services<br>The IP Client Manager is dual-homed. It performs the SIP to UNIStim conversion that enables the interworking of i2002 and i2004 Internet Telephones with the SIP Application Module.<br>For more information on the IP Client Manager, refer to the following documentation:<br>• *MCS 5200 IP Client Manager Basics, NN10032-111*<br>• *i2002 Internet Telephone User Guide, NN10319-113*<br>• *i2004 Internet Telephone User Guide, NN10042-113* |
|  | The Web Client Manager manages the Multimedia Web Client and enables subscribers to access the MCS 5200 SIP services from a Web browser.<br>The Web Client Manager also provides the Multimedia Web Client feature set and enables the interworking of the Multimedia Web Client and the SIP Application Module.<br>The Web Client Manager is deployed from the System Management Console.<br>For more information on the Web Client Manager, refer to *MCS 5200 Web Client Manager Basics, NN10277-111.* |

## MCS 5200 Media Servers

The following table lists brief descriptions of the MCS 5200 media servers.

**MCS 5200 media servers**

| Media servers | Description |
|---|---|
|  | The SIP Audio Server provides network-wide, Ad hoc audio conferencing for the MCS 5200 access clients. These capabilities include:<br>• support for up to 32 port audio conferences<br>• independent Coder/Decoder (CODEC) negotiation for each conference call port<br>• mid-session broadcast of SIP info signals to all conference parties (for example, a Web page URL)<br>• hold/retrieve<br>• round-robin resource allocation (for selecting media resources for conference calls)<br>• long call service<br>• call transfer<br>• chaining conferences together (During a conference call on the SIP Audio Server, any client may add additional clients onto the conference call.)<br>• authenticating SIP Application Module sending a request<br>The SIP Audio Server is located on the private MCS 5200 network. For more information on the SIP Audio Server, refer to *MCS 5200 SIP Audio Server Basics, NN10034-111.* |

## MCS 5200 media servers

| Media servers | Description |
|---|---|
|  | The RTP Media Portal is a network-distributed component that provides the following functions:<br>• performs media-stream network address translation and network address port translation (NAT/NAPT)<br>• provides a media firewall<br>• provides third-party media controls<br>• enables a client firewall/NAPT traversal mechanism<br>The RTP Media Portal handles media streams using the Real-time Transport Protocol (RTP) and Real-time Transport Control Protocol (RTCP).<br><br>For more information on the RTP Media Portal, refer to *MCS 5200 RTP Media Portal Basics, NN10035-111.* |
|  | The Media Application Server (MAS) is a generic media processing platform that combines the latest voice over IP (VoIP) protocols and standards with the most successful internet development specifications and paradigms. It uses commercial hardware platforms and common operating systems without the presence of hardware-based digital signal processor (DSP) resources.<br><br>The MAS platform is a stand-alone component that interfaces to both the control-planes and bearer-planes of the network. The control-plane uses Session Initiation Protocol (SIP) for signaling, while the bearer-plane uses both the RTP and RTCP for media.<br><br>The MAS supports the following services:<br>• Ad hoc audio conferencing<br>• Meet me audio conferencing<br>These services run on separate MASs. For more information on the MAS, refer to *MCS 5200 Media Application Server Basics, NN10010258-111.* |

### RTP Media Portal

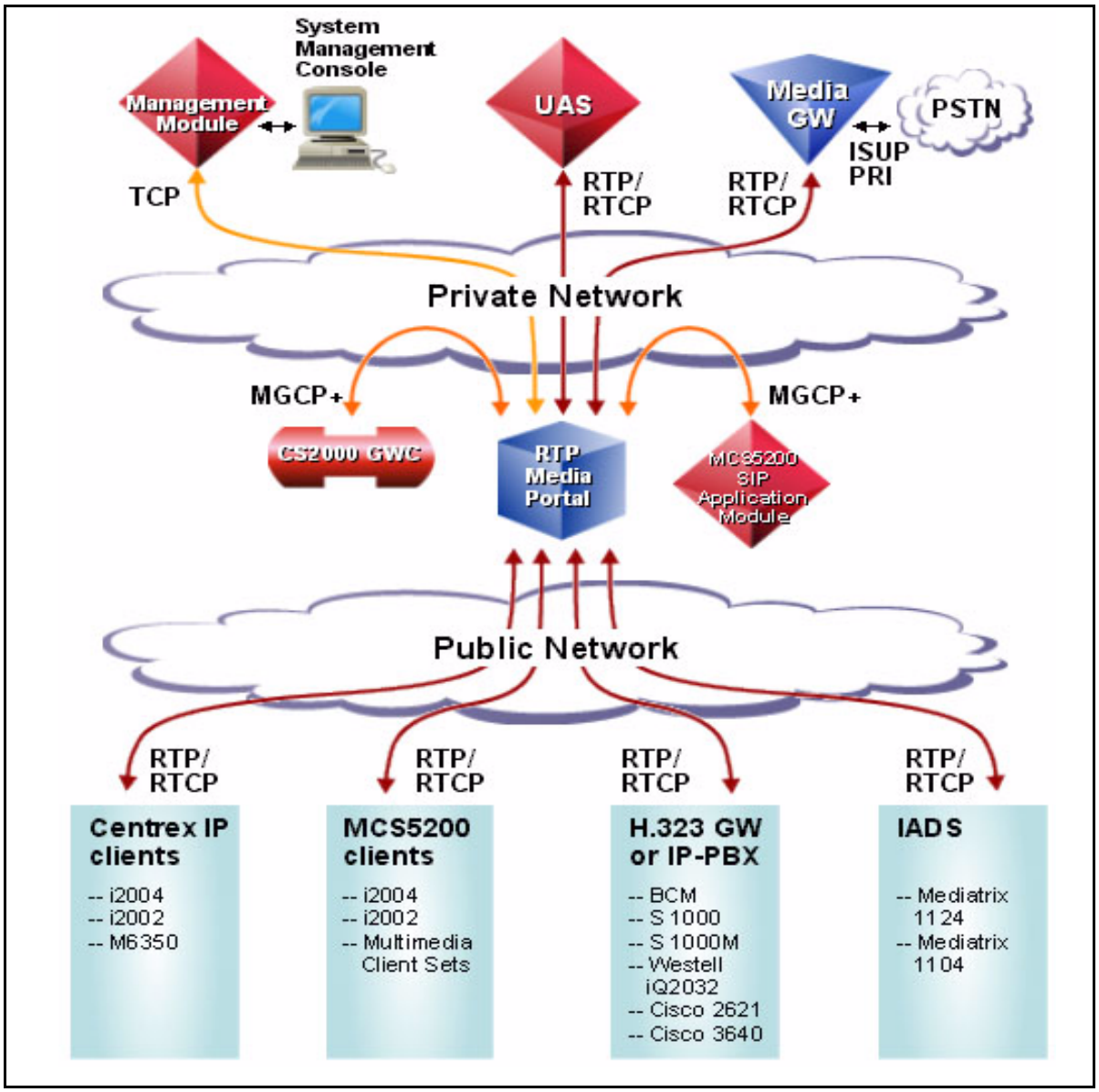
The RTP Media Portal service addresses media-specific issues with advanced service delivery, Internet addressing efficiencies, and system security. It functions as a media Network Address Port Translation (NAPT) point that shields private network components from external

exposure through leaks in the media streams. The RTP Media Portal also enables elements in the private network to communicate safely with elements in the private network.

The RTP Media Portal provides IP address/port pair mapping between internal and external network components, and media anchoring and media pivot abilities for terminals. For NAPT functionality, the media portal relays packets between two end points located in different networks using the same or different IP address spaces. The RTP Media Portal can perform NAPT on both the source and destination IP addresses for every media packet authorized to traverse.

The following figure shows RTP Media Portal interworking among other components.

**RTP Media Portal network interoperability**




In this figure, the clouds represent two distinct networks. The private network cloud interacts with the public network cloud through the different edge components. The RTP Media Portal provides media-layer functionality for RTP, Real Time Transport Control Protocol (RTCP), and User Datagram Protocol (UDP) transmissions.

A call control signaling channel is established between the H.323 gateway and the CS 2000. If the GW and the CS 2000 reside in separate IP-VPNs (different IP address domains that cannot route directly to one another), dynamic discovery and keepalive are

supported on the gateways and GWCs to provide another mechanism for GW->CS2K communication. Discovery provides another mechanism for GW->CS2K communication.

The RTP Media Portal is only required if endpoints are on different network domains and IP address spaces. These endpoints can be different IP VPNs or between a Carrier and Enterprise IP VPN domains.

## MCS 5200 gateway

The following table lists brief descriptions of the MCS 5200 gateway.

**MCS 5200 Gateway**

| Gateway | Description |
|---|---|
|  | The SIP PRI Gateway converts packet-based voice streams to circuit-based voice streams to allow SIP endpoints the ability to connect to PSTN devices. Some of its functions include:<br>• PRI call handling<br>• CODEC negotiation<br>• calling party name and number delivery to SIP<br>• parameter mapping between SIP and PRI protocols<br>The SIP PRI Gateway is located on the MCS 5200 private network. For more information on the SIP PRI Gateway, refer to *MCS 5200 SIP PRI Gateway Basics, NN10250-111.* |

## MCS 5200 access clients

The MCS 5200 access clients include SIP user agents that provide subscribers access to the MCS 5200 network, administrator and subscriber provisioning interfaces, and an interface for administrative system management. User agents can be hardware components, such as an IP phone, software applications running on a PC, or software applications executed from a web browser.

The following table lists brief descriptions of the MCS 5200 access clients.

**MCS 5200 access clients (Sheet 1 of 5)**

| Access client | Description |
|---|---|
| ***Note:*** Subscriber access to the SIP services network requires one of the following clients: Multimedia PC Client, i2002 Internet Telephone, i2004 Internet Telephone, Multimedia Web Client, or Multimedia Client Set. | |
|  | The Multimedia PC Client is a stand-alone SIP-enabled user agent installed on a Personal Computer (PC) that provides access to SIP features and services such as:<br>• traditional telephone services<br>• multimedia communications<br>— video calls<br>— Instant Messaging<br>— file sharing/file transferring<br>— whiteboard session<br>— Web page push<br>• communication management<br>— directory<br>— call logs<br>— Friends Online<br>— address book<br>The Multimedia PC Client is located on the managed public network. It accesses the SIP services network through the SIP Application Module. For more information on this multimedia client, refer to the *Multimedia PC Client User Guide, NN10041-112,* and *MCS 5200 Feature Description Guide, NN10251-115.* |

## MCS 5200 access clients (Sheet 2 of 5)

| Access client | Description |
|---|---|
|  | The i2002 and i2004 Internet Telephones provide voice services, while the PC provides all other services. When the Multimedia PC Client is configured to control the i2002 and i2004 Internet Telephones, the configuration is known as the Multimedia Client Set. The Multimedia Client Set provides access to SIP features and services such as:<br>• traditional telephone services<br>• multimedia communications<br>— video calls<br>— Instant Messaging<br>— file sharing/file transferring<br>— whiteboard session<br>— Web page push<br>• communication management<br>— global address book<br>— call logs<br>— Friends Online<br>— personal address book<br>For more information on the Multimedia Client Set, refer to the *Multimedia PC Client User Guide, NN10041-112; i2002 Internet Telephone User Guide, NN10319-113; i2004 Internet Telephone User Guide, NN10042-113*; and *MCS 5200 Feature Description Guide, NN10251-115*. |

## MCS 5200 access clients (Sheet 3 of 5)

| Access client | Description |
|---|---|
|  | The i2002 Internet Telephone is a MCS 5200 hard client device that provides a traditional looking telephone set enhanced with multimedia features for accessing IP-based MCS 5200 SIP services. It provides a two line display to enable multimedia services. Some of the i2002 Internet Telephone advanced features include:<br>• Instant Messaging<br>• stock query<br>• call forward<br>• do not disturb<br>• multiple user login (4 simultaneous users)<br>• bulletins<br>• Quality of Service (QoS) information<br>The IP-based i2002 Internet Telephone is located on the managed public network and is managed by the IP Client Manager (IPCM). For a complete list of features, refer to of this chapter. For more information on the i2002 Internet Telephone, refer to the *i2002 Internet Telephone User Guide, NN10041-112,* and *MCS 5200 Feature Description Guide, NN10251-115.* |

## MCS 5200 access clients (Sheet 4 of 5)

| Access client | Description |
|---|---|
|  | The i2004 Internet Telephone is a Nortel Networks MCS 5200 hard client device that provides a traditional looking telephone set enhanced with multimedia features for accessing IP-based MCS 5200 SIP services. It provides a large, multiple line display to enable multimedia services. Some of the i2004 Internet Telephone advanced features include:<br>• Instant Messaging<br>• stock query<br>• call forward<br>• do not disturb<br>• multiple user login (6 simultaneous users)<br>• bulletins<br>• QoS information<br>The IP-based i2004 Internet Telephone is located on the managed public network and is managed by the IP Client Manager (IPCM). For more information on the i2004 Internet Telephone, refer to the *i2004 Internet Telephone User Guide, NN10042-113,* and *MCS 5200 Feature Description Guide, NN10251-115.* |
|  | The Provisioning Client is a browser-based tool that allows service providers to provision:<br>• administrators<br>• domains<br>• gateways<br>• IP Client Managers<br>• voice mail servers<br>• service packages<br>• telephony routing translations<br>The Provisioning Client is accessed from the public network. It is accessed by administrators for communicating provisioning data to the MCS 5200 network. For more information on the Provisioning Client, refer to the *Provisioning Client User Guide, NN10043-113.* |

## MCS 5200 access clients (Sheet 5 of 5)

| Access client | Description |
|---|---|
|  | The Personal Agent is a browser-based client that allows users to perform network-based management with their own MCS 5200 services and communication preferences. Features include:<br>• Routes: to define call screening and routing behavior<br>• Preference: to modify personal information and services<br>• Directory: to manage key contact information; access personal and global address books<br>• Click-to-call: to establish a call between two parties<br>• Multimedia Web Client: to launch multimedia web client<br>For more information on the Personal Agent, refer to the *Personal Agent User Guide, NN10039-112,* and *MCS 5200 Feature Description Guide, 10251-115.* |
|  | The Multimedia Web Client is a Web-based access client that provides various multimedia and telephony features such as:<br>• traditional telephone services<br>• multimedia services<br>— video calls<br>— Instant Messaging<br>— Web page push<br>• communication management<br>— global address book<br>— call logs<br>— Friends Online<br>— personal address book<br>The Multimedia Web Client is located on the managed public network. Because this multimedia client is browser-based, it is easy to add and deploy new services as they become available. When the Web Client Manager is updated, subscribers automatically have access to any updated Multimedia Web Client functionalities.<br>For more information on the Multimedia Web Client, refer to the *Multimedia Web Client User Guide, NN10040-112,* and *MCS 5200 Feature Description Guide, NN10251-115.* |

# Call processing in Carrier Hosted Services

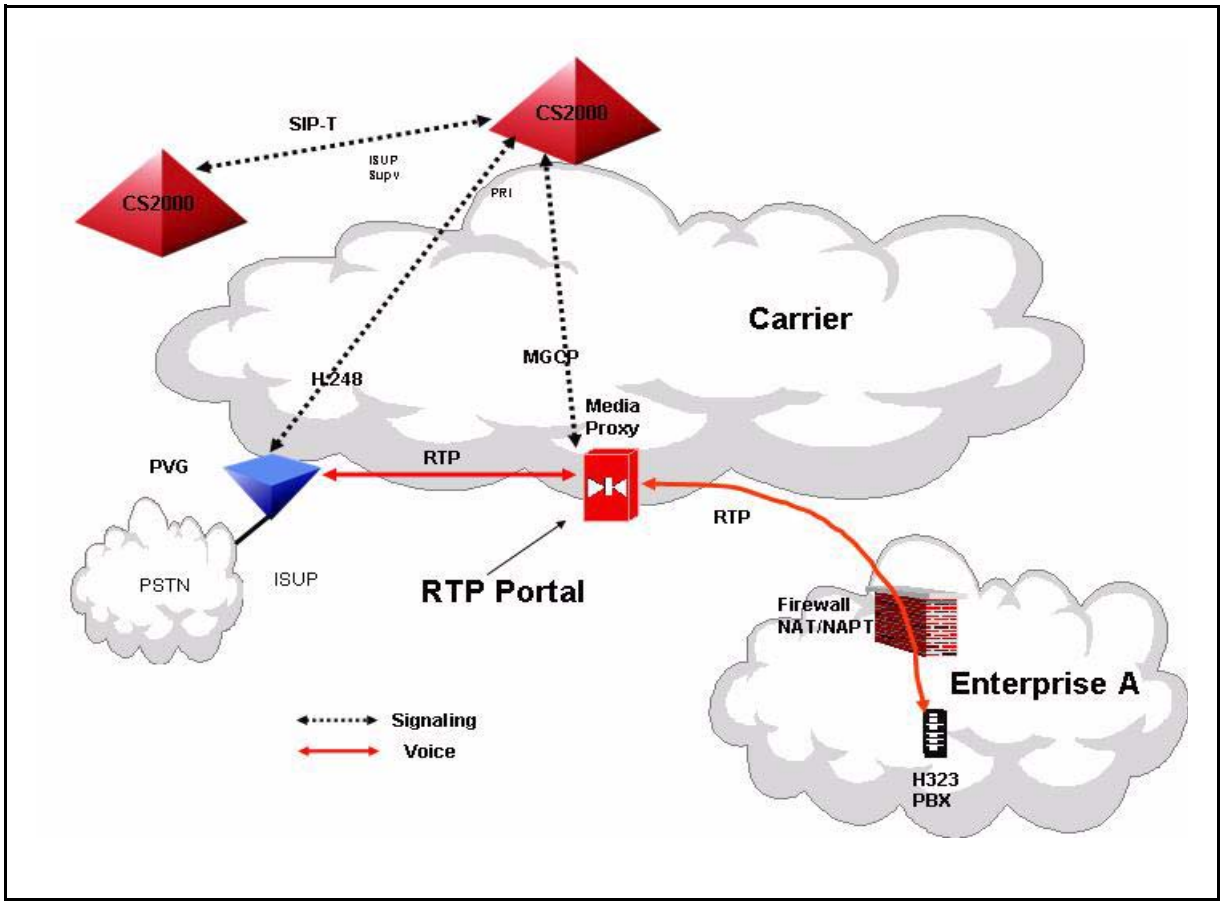
## Overview

This section briefly describes the call processing flows for the products and applications associated with the Carrier Hosted Services.

### VoIP VPN

The following figure shows a high-level view of the call control and media paths in a network with VoIP VPN.

### VoIP VPN call flow




### CICM

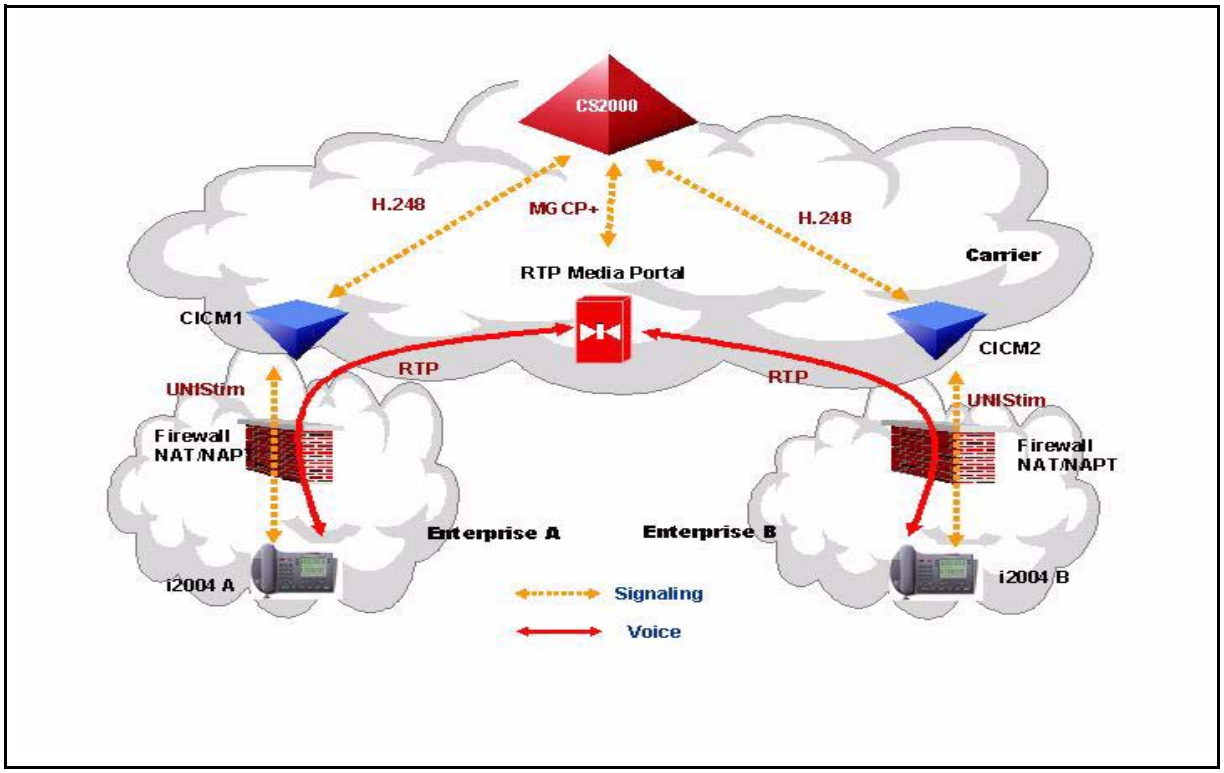
Succession CICM converts UNIStim messages between the Succession CICM and the Centrex IP clients to H.248 messages to the Communication Server.

Unlike TDM CICM, the Succession CICM does not transport the media streams. The RTP Media Portal proxies the voice packets between the

two end points if they are in different IP-VPNs or network address domains. If they are not in different IP-VPNs or network address domains, then the RTP voice packets are routed directly between the two endpoints. (For example, a call between two gateways in the same IP-VPN does not go through the RTP Media Portal. The RTP Media Portal is required only if there is a need to traverse an IP-VPN boundary.)

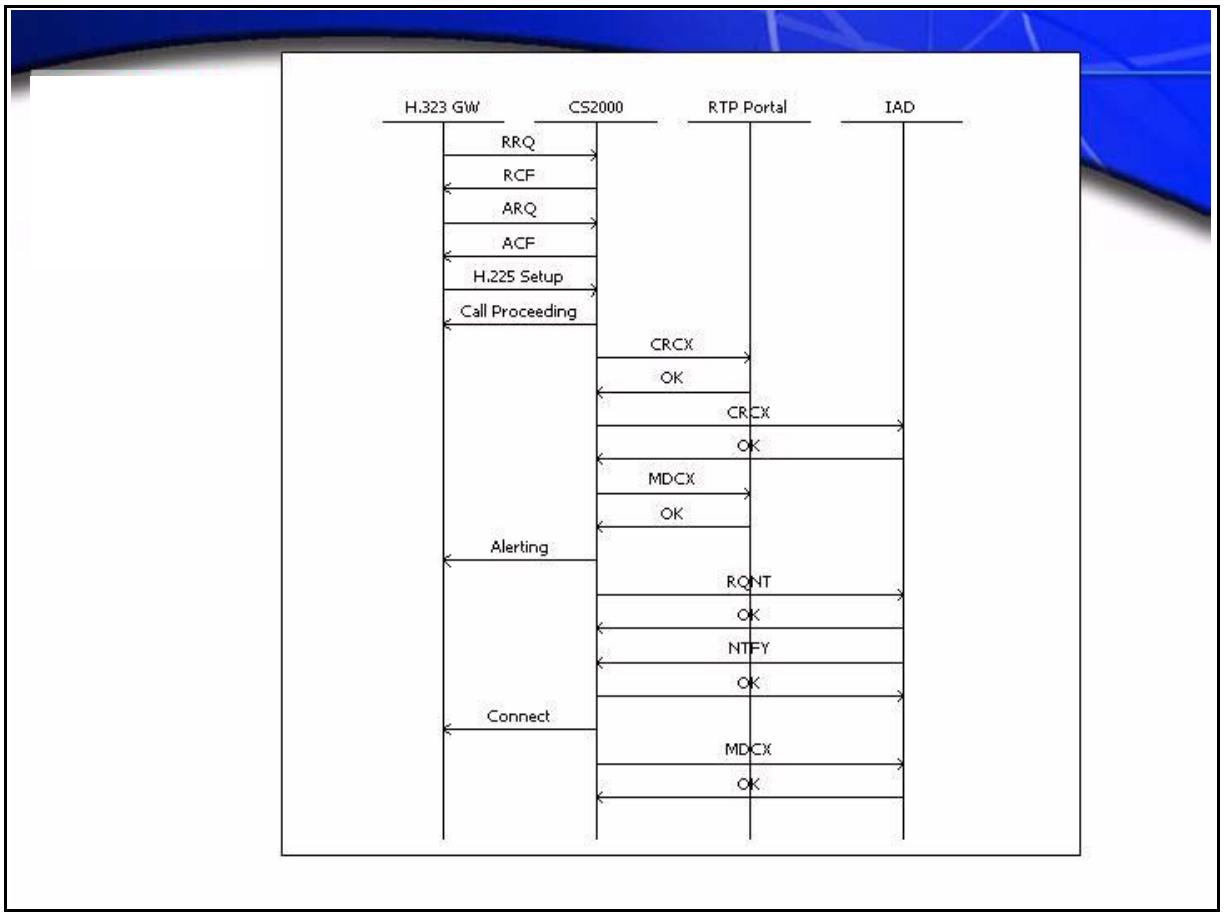
The following figure shows a call flow using Succession Centrex IP and the Succession CICM.

### Succession Centrex IP call flow




The following figure shows an example of a call setup for an H.323-to-MGCP IAD call.

## VoIP VPN-to-MGCP IAD call setup




In the VoIP VPN-to-MGCP IAD call setup figure, the H.323 gateway registers with the communication server, which functions as a gatekeeper. The H.323 gateway sends an Admission Request (ARQ) to the communication server for the call. The communication server responds with an Admission Confirmation (ACF) to indicate that the gatekeeper-routed signaling applies for this call. The H.323 gateway then sends the H.225 setup message to the communication server. (Translations and routing determine that the terminating node is an MGCP IAD.)

After translations and routing has completed, the communications server determines that an RTP Media Portal must be inserted. A Create Connection (CRCX) message is sent to the portal, which responds with an embedded RTP message port to the terminating IAD.

The communication server sends an MGCP Modify Connection (MDCX) message to the RTP Media Portal to set up the second leg of the connection. The RTP Media Portal responds with the RTP port that is to be used by the originating H.323 gateway.

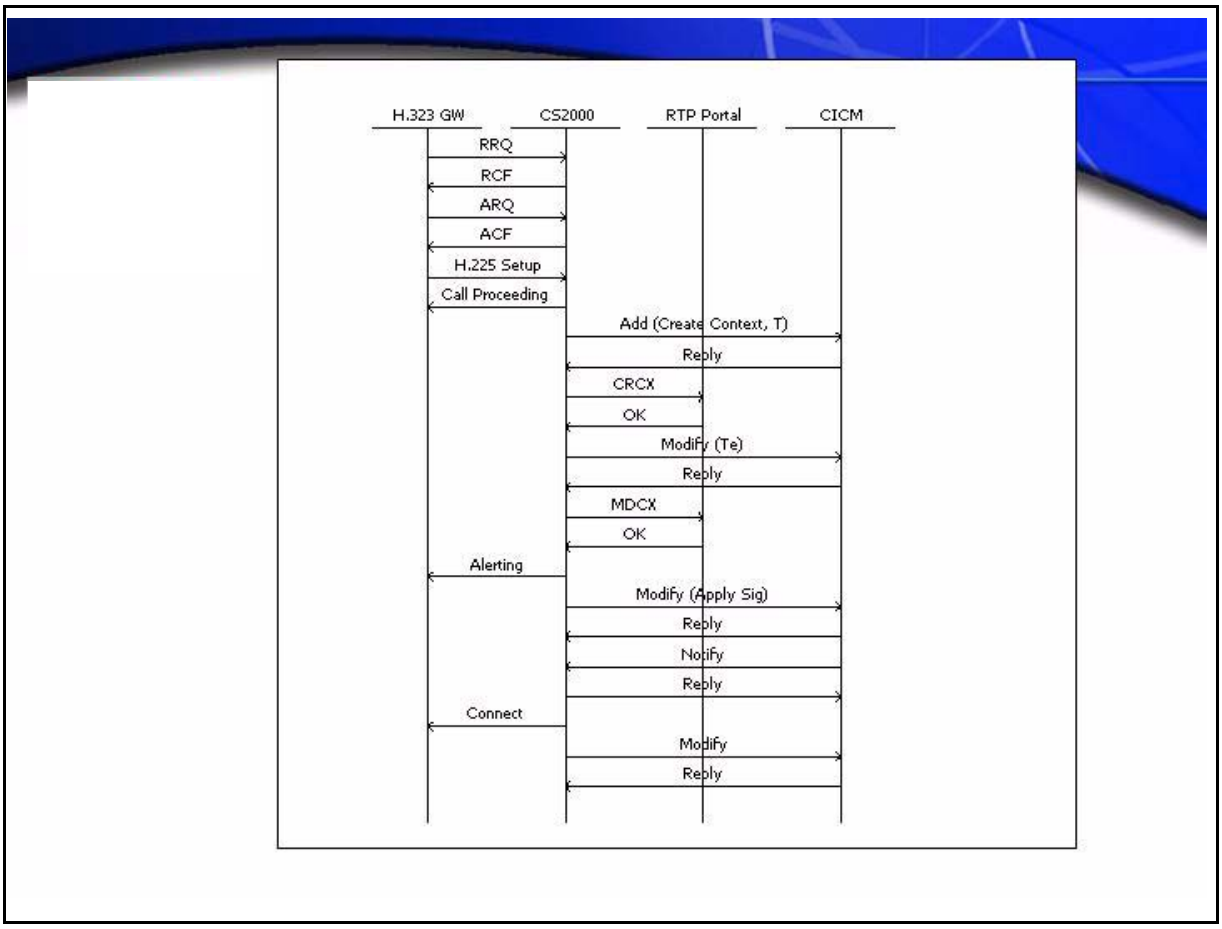
The communication server sends the Alerting message to the originating H.323 gateway, including the RTP port that should be used on the RTP Media Portal. The communication server then sends a Request Notification (RQNT) to the terminating IAD, directing it to apply ringing and provide notification when it has detected an off-hook.

The IAD sends a Notify (NTFY) when it has detected an off-hook. The communication server sends a Connect message to the originating H.323 gateway, and an MDCX message to the terminating IAD for the following purposes:

- to remove ringing
- to set the connection mode to SENDRECV
- to request notification when it detects flash or on-hook has occurred

The following figure shows an example of a call setup for an H.323-to-H.248 CICM call.

## VoIP VPN-to-H.248 CICM call setup




In the VoIP VPN-to-H.248 CICM call setup figure, the H.323 gateway registers with the communication server, which functions as a gatekeeper. The H.323 gateway sends an ARQ to the communication server for the call. The communication server responds with an ACF to indicate that the gatekeeper-routed signaling applies for this call. The H.323 gateway then sends the H.225 setup message to the communication server. (Translations and routing determine that the terminating node is a CICM.)

The communications server sends an H.248 Add message to the CICM to create a new context identifier with a termination. (The context identifier is returned in the H.248 response.)

The communications server determines that an RTP Media Portal must be inserted. A CRCX message is sent to the portal, which responds with an embedded RTP message port in an H.248 Modify message. The H.248 Modify message updates the ephemeral termination in the CICM context.

The communication server sends an MDCX message to the RTP Media Portal to set up the second leg of the connection. The RTP Media Portal responds with the RTP port that is to be used by the originating H.323 gateway.

The communication server sends the Alerting message to the originating H.323 gateway, including the RTP port that should be used on the RTP Media Portal. The communication server then sends an H.248 Modify message to the CICM, directing it to apply ringing and provide notification when it has detected an off-hook.

The CICM sends an H.248 NTFY message when it has detected an off-hook. The communication server sends a Connect message to the originating H.323 gateway, and an H.248 Modify message to the CICM for the following purposes:

- to remove ringing
- to set the connection mode to SENDRECV
- to request notification when it detects flash or on-hook has occurred

For more information on the RTP Media Portal, refer to *MCS 5200 RTP Media Portal Basics, NN10035-111.*

For more information on the RTP Media Portal when in association with a CS 2000 refer to *CVoIP RTP Media Portal Basics, NN10367-111.*

## CHS Services

CHS includes the following services:



## VoIP VPN

Carrier Hosted Services VoIP VPN is a hosted service that enables carriers to cost effectively manage multiple enterprise voice networks over their managed IP infrastructure.

The following products interwork to the CS 2000 through PRI and H.323:

- CS1000 and CS1000M (Release 3.0)
- Business Communications Manager (BCM) (Releases 3.5 and 3.6)

The following functionality is new to (I)SN07:

- Enabling H.245 tunneling on the CS 1000 R3 to interwork with the CS 2000.

  ***Note:*** Refer to patch number (MPLR19387) to enable H.245 tunneling.

- AOC support over H.323
- H.323 Gatekeeper to CS 2000 Gatekeeper interoperability
- H.323 support for Meridian Customer Defined Network (MCDN) services. The following interworkings are supported:
  - H.323 GW (BCM) to MGCP GW (Mediatrix, IBN lines)
  - H.323 GW (S1000 and S1000M) to H.248 GW (CICM, P-phone)
  - H.323 GW (S1000 and S1000M) to MGCP GW (Mediatrix, IBN lines)
- Call Server controlled switchover to T.38 (or G.711) for Call Server routed H.323 fax calls.

- North American and International Interworking of H.323 to SIP MCS 5200
- Tunneling of MCSN-based services information between MCDN-capable gateways and inter-communication server configurations using SIP-T
- Flexibility in H.323 provisioning, including:
  - capability to change provisioning information for H.323 gateways without having to remove and re-add the gateway provisioning
  - capability to add H.323 virtual carriers in the range of 4 to 672 to an H.323 gateway
  - increased mapping of D-channels on an H.323 gateway
- Introduction of the Session Server and SIP gateway application allowing interoperability between the CS 2000 network and third-party SIP-based call servers and Media Application servers
- International tunneling of DPNSS Feature Transparency (DFT) between PBX and the CS 2000 over an H.323 IP connection. Refer to international H.323 DPNSS tunneling on CS 2000 on page 58

The Carrier Hosted Services VoIP VPN service offers the following benefits:

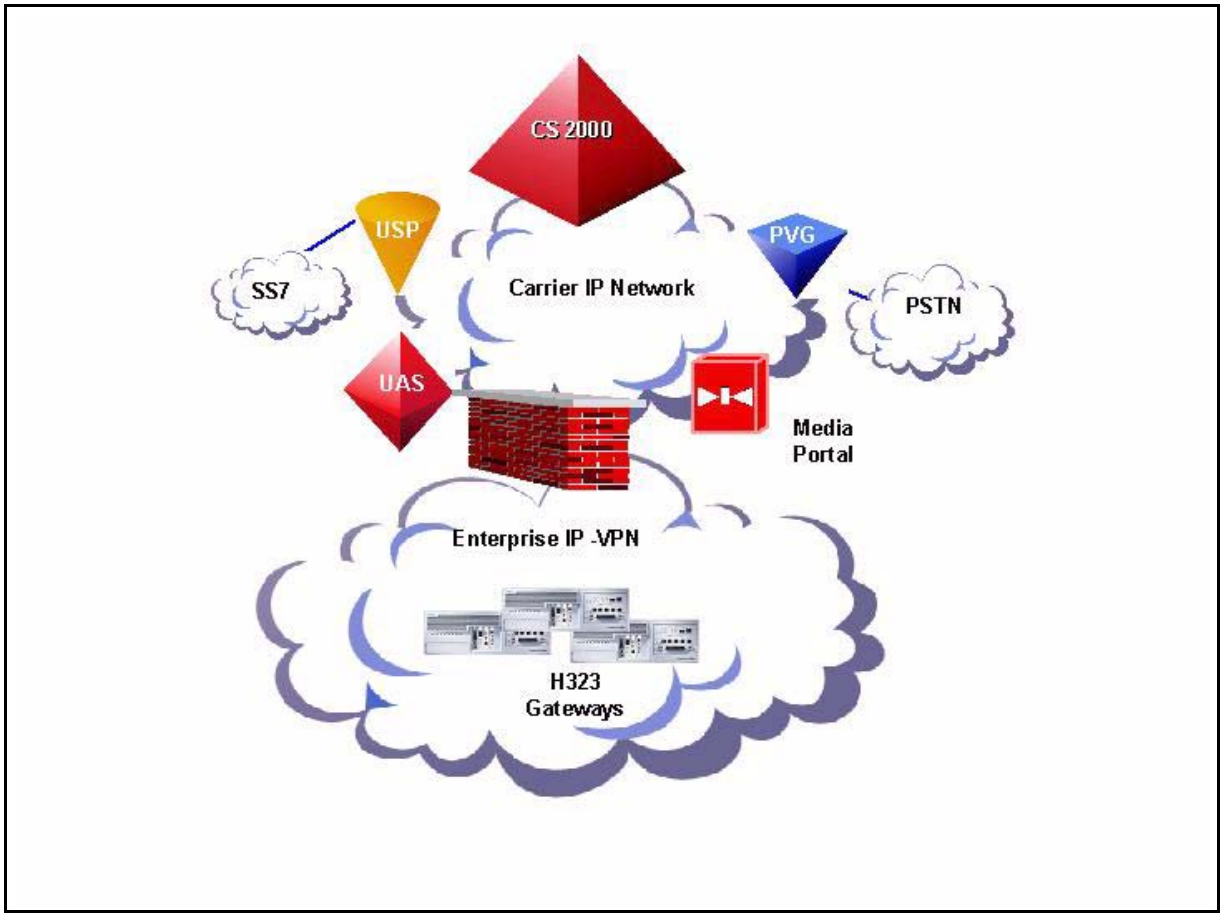
- reduced network connections
- simplified call routing
- seamless connections to remote locations
- streamlined network management
- increased network services and CPE revenue for carrier customers
- cost savings to enterprise customers through converged access and long-distance bypass

This service is available on the CS 2000 and the Communication Server 2000 - Compact (CS 2000 - Compact).

The Carrier Hosted Services VoIP VPN service combines the extensive voice VPN translations capabilities of the communication servers with H.323 multi-vendor IP PBX networking. With VoIP VPN, rather than having a mesh of links, only one integrated access link is required to each site, thereby collapsing multiple voice networks onto a single, managed packet infrastructure. All services – local, long distance, intranet, and Internet – are delivered over this one link. Additional leased lines and data changes are no longer required at the other sites.

The following figure shows a high-level view of the network architecture for the Carrier Hosted Services VoIP VPN program.

**Carrier Hosted Services VoIP VPN architecture**




## VoIP VPN deployment

The Carrier Hosted Services VoIP VPN program is deployed in two primary applications:

- Single site access for small-to-medium enterprises, which supports integrated access and support of existing CPE.
- Large enterprise multi-site hybrid VPN, which eliminates leased lines and provides a centrally managed dial plan.

## H.323 access to VoIP VPN

H.323 access enables the direct H.323 connectivity of customer sites to the VoIP VPN service.

A range of IP-enabled PBXs, IP PBXs, and gateways are supported including

- BCM Releases 3.5 and 3.6
- CS1000/CS1000M Release 3.0
- third-party gateways

H.323 is the most widely deployed VoIP protocol used in enterprise networks today. This feature enables carriers to cost-effectively extend the reach of the VoIP VPN service offering to H.323-based CPE. IP access also enables carriers to bundle multiple voice and data services over a single converged access path.

**international H.323 DPNSS tunneling on CS 2000**
The DPNSS signaling from the Westell H.323 DPNSS interface is tunnelled transparently by the CS2000 to either of the following:

- another DPNSS PBX connected to the CS2K via a Westell H.323 gateway
- IBN7 trunks supporting the existing Nortel proprietary DPNSS feature transparency capability (DFT).

Limitations and restrictions

- This feature provides VPN transit functionalities for the hosted CS 2000. Therefore, any originating or end-node functionalities that relate to DPNSS features are not supported by the host CS 2000. Any support for originating/terminating DFT as end-node functionalities on CS 2000 IAD gateway lines, require DFT (IBN7 TDM/SIP-T) looparounds.
- Direct BTUP interworking for PSTN breakout calls from the CS 2000 are not supported. DFT looparounds will be required for such calls.
- ROP functionality as required by the transit exchange is supported. However, the ROP billing as a DPNSS feature is not supported over the QSIG trunk.
- Billing records in general will be based on the incoming QSIG trunk rather than the DPNSS.
- Data calls are not supported by Westell gateway
- Name Display service is not supported (as currently is not supported in DMS100 for DPNSS).
- Tables TMTMAP and FAILMSG are not supported by QSIG. This results in not being able to provide flexible treatments and cause mapping in IBN7/ QSIG interworking call scenarios. This implies that we can not use table TMTCNTL in conjunction with table

TMTMAP to be able to flexibly apply announcements locally by the CS2K, while letting the tones to be applied remotely by the PABX based on specific causes. This restriction together with H.323 gateway limitation in applying tones such as user_busy, means that we should always set the AUDTRMT option in table LTDATA to 'N'.

- Westell gateway (together with other current H.323 gateways) can not be made to apply RingBack tone after the Connect. This means for certain services which rely on CS2K to apply the RingBack tone after connection, the CS2K will not be able to apply the tone.

For a list of supported DPNSS/Centrex features, refer to Features and services on page 87:

For a complete listing of all documentation associated with Carrier Hosted Services VoIP VPN refer to Where to get customer documentation on page 123

In particular, refer to the following sections:

- BCM on page 124
- CS1000 and CS 1000M on page 124
- Meridian 1 on page 125
- MCS 5100 on page 125

## MCDN

CHS introduces enhanced Meridian customer defined networking (MCDN) support:

- transparent tunneling of MCDN information between multiple CS 2000s with Succession 1000M/Business Communication Managers (BCM) connected at either end
- interworking support that allows the CS 2000 to terminate MCDN functionality and interwork with Centrex lines, providing enhanced support for Enterprises with users split between IP-PBXs, integrated business network (IBN) Centrex lines, and Centrex IP lines of the CICM

### North American H.323 for Networked MCDN services

H.323 can be configured to allow interworking of Meridian Customer Defined Network (MCDN) based PBXs with certain hosted NA CS2K centrex lines for use within the Enterprise network. The specific set of MCDN services are based on the following network configurations:

- Interworking on a per nodal basis. These specific set of MCDN services are supported and interworked over a PRIH.323 Trunk

facility between either an S1000 or BCM, and a hosted centrex line on a NA CS2K switch.

- Interworking on a per inter-Call Server basis. These specific set of MCDN services are supported and interworked over a SIP-T Trunk facility between either a S1000 or BCM, and a hosted centrex line on a NA CS2K switch.

The following H.323 interworkings are supported for MCDN services:

- H.323 GW (BCM) <--> H.248 GW (CICM, P-phone)
- H.323 GW (BCM) <--> MGCP GW (Mediatrix, IBN lines)
- H.323 GW (S1000 and S1000M) <--> H.248 GW (CICM, P-phone)
- H.323 GW (S1000 and S1000M) <--> MGCP GW (Mediatrix, IBN lines)

The following supported MCDN services are listed in the Features and services on page 87:

- BCM interworking to CICM and Mediatrix for nodal calls and through SIP-T
- S1000 and S1000M interworking to CICM and Mediatrix for nodal calls and through SIP-T

For provisioning information, refer to *Provisioning the trunk group and trunks for an H.323 gateway, CS 2000 Configuration Management, NN10324-511.*

**Pre-requisites**

An H.323 Nortel North American (NTNA) PRI Trunk, referred to as a PRIH.323, is utilized to connect a GWC with an H.323 profile to the CS 2000 on a NA CM load.

SIP-T is defined as an ANSI ISUP Trunk facility which contains Tunneled MCDN data.

## Limitations and Restrictions

The limitations and restrictions for NA H.323 support for Networked MCDN services are as follows:

- A subset of MCDN services are supported by this feature.

  For supported MCDN services, refer to Features and services on page 87.

- Line side development (P-phone, IBN lines) is not part of this feature.

- Development on the H.323 agents (BCM, S1000) is not part of this feature.
- MCDN Services which are not supported either by an H.323 agent or the CS 2000 CICM or Mediatrix line agent, will not be supported by this feature.
- Tunneling of MCDN data between Enterprises is outside of the scope of this feature.
- For Calling Name and Number delivery, the appropriate feature must be provisioned against the subscriber (i.e., CND - Calling Number Delivery, CNAMD - Calling Name Delivery, etc.).
- In the CICM (CS2K) to S1000M direction, only private Numbering Plan Indication (NPI) calls will contain this privately built MCDN tunneled data - public calls will not contain MCDN tunneled data.

  In the CICM (CS2K) to S1000M direction, private NPI with Local Type of Number (TON) is coded as an UIPE ESN CDP TON.
- CS2K Core Calling Name Delivery remains unchanged by this activity to either line agents or trunk agents; therefore, existing functionalities, restrictions or limitations of Calling Name Delivery remain applicable.

**International H.323 support for MCDN services**

International H.323 support of Meridian Customer Defined Network (MCDN) Services includes:

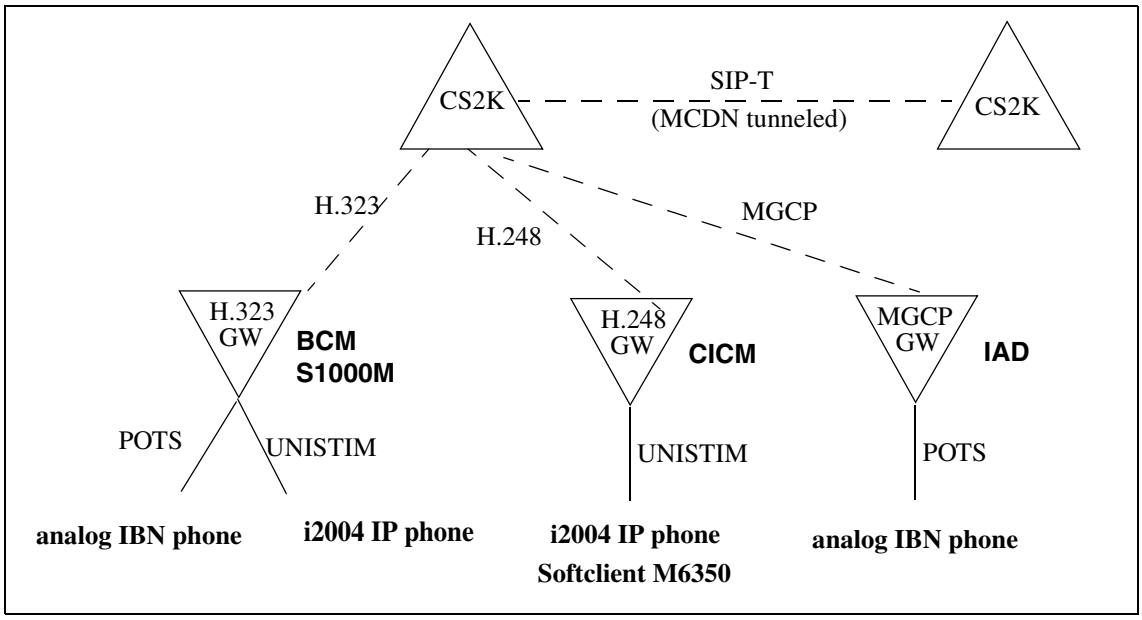
- MCDN interworking on nodal calls and via SIP-T (ETSI ISUP V2+ QFT) for inter-Call Server calls.
- MCDN based service interworking between the S1000M or BCM (H.323 GWs) on one call leg and CICM (H.248 GW) or Mediatrix IAD (MGCP GW) on the other call leg.
- MCDN services which are supported on P-phone agents or IBN lines agents.
- MCDN based services for the CS2000 international load.

MCDN interworking includes:

- H.323 GW (BCM) <--> H.248 GW (CICM, P-phone)
- H.323 GW (BCM) <--> MGCP GW (IBN lines)
- H.323 GW (S1000M) <--> H.248 GW (CICM, P-phone)
- H.323 GW (S1000M) <--> MGCP GW (IBN lines)

### Associated network drawing

The following figure displays the VoIP network configuration for H.323 support for MCDN services.




### Limitations and Restrictions

The limitations and restrictions for H.323 support for Networked MCDN services are as follows:

- A subset of MCDN services are supported by this feature.

  For supported MCDN services, refer to Features and services on page 87.

- Interworking between call servers is solely achieved via SIP-T (ETSI ISUP v2+) with QFT (QSIG Feature Transparency) activated. No other interworking types between call servers are supported for this feature.

- Tunneling of MCDN data between enterprises (different customer groups) is out of scope of this feature.

- Limitation on Connected Number Delivery: In the software load of the S1000M Gateway and BCM gateways, which this feature will be based upon, no functionality exists to transport the Connected Number Information Element of H.323 call control messages in the non-private portion of the messages. Therefore, this functionality is

not supported for the interworkings between Mediatrix and S1000M gateways, and between Mediatrix and BCM gateways.

- Limitation on Called Number Delivery: In the software load of the BCM gateway, which this feature will be based upon, no functionality exists to transport the Original Called Number Information Element of H.323 call control messages in the non-private portion of the messages. Therefore, this functionality is not supported for the interworkings between Mediatrix and BCM gateways.

For a complete list of MCDN services, refer to Features and services on page 87.

## Centrex IP

The Centrex IP Client Manager (CICM) uses VoIP technology to deliver Centrex capabilities to users connected to an IP network.

The CICM provides

- the interface between the Centrex feature set and an IP network
- transcoded voice between IP data from the client network and PCM data from the XPM
- connectivity with the CS 2000 via H.248
- CICM support on the SAM21
- multiple IP-VPN and Network Address Translation (NAT)/firewall traversal
- multiple NAT domain support using virtual gateways
- codec negotiation based on audio profile
- Dual Node Redundancy

The CICM is an integral component of the Carrier Hosted Services. Functionally, the CICM refers to all the CICM processors on a SAM21 chassis associated with a single CS 2000. The CICM processors used in the SAM21 are faster and provide three times the density of the older 5365 cards used in the SAM16.

CICM and the CICM EM reside on blades in the SAM21 chassis.

- CICM resides on a pair of high-density Motorola 5385 processors.
- CICM EM resides on a single processor.

Moving CICM to the SAM21 chassis consolidates the platform so the CICM and CICM-EM can co-reside on the SAM 21along with the Gateway Controller (GWC) and H.323 interface cards.The former

SAM16 frame is no longer required to support the CICM, and that entire frame is removed from the following list of (i)SN07 CICM hardware. This elimination of the SAM 16 hardware reduces cost and results in a substantial improvement in the CICM footprint.

The CICM functions as a terminal server or signaling gateway in a Carrier VoIP network and performs the following functions:

- interprets the client terminal Unified Network IP Stimulus (UNIStim) messaging
- associates the information with a userid
- forwards the message to the communication server

CICM does not transport media in the Carrier VoIP market.

- If the end points are in the same IP VPN or network address domain, the CS 2000 GWC routes the media directly between the two endpoints.
- If the end points are in different IP VPNs or network address domains, a media proxy routes the media.

The CICM element manager (EM) software performs the following functions:

- CICM configuration and connection monitoring through a web-based interface
- support of remote terminal telnet access
- user profiling (user ID, password, audio profile, language)
- maintenance of central database of configuration data
- CICM gateway backup
- CICM software upgrades

### Centrex services through CICM

The CICM product allows for transparent access to 200-plus, Centrex-featured voice services.

The CICM offers enhanced capabilities over the standard Centrex.

- Mobility. A user can log on and access Centrex services from any location that has IP connectivity with the CICM.
- Choice of client. Users can choose between the m6350 SoftClient or three versions of the physical etherset: the i2001, i2002 or i2004. An etherset is recommended for a user based at one location, and the SoftClient is recommended for mobile users to access from a variety of locations.

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

**CICM capacity**

The CICM has the following capacity limits.

- For each CICM Motorola CPN 5385 resource card pair:
  - 1,023 subscriber line -provisioning capacity
  - 7,200 busy hour half-call attempts (BHHCA)
  - 512 active calls
- The CICM is scalable by adding more CICM processors
- One pair of CICM-EM cards is needed for each CS 2000
  - Able to support up to 100 CICM resource card pairs
- Per GWC resource card pair:
  - 8,200 subscriber line-provisioning capacity
  - 38,000 BHHCA

For more information, refer to the CICM documentation suite in the CHS collection in Helmsman Express. The CICM documents are listed in CICM documentation on page 125

## Internet Transparency

Internet Transparency and security-related products include the following capabilities:

- Multiple IP-VPN and NAT/firewall traversal
  - Lawful Intercept (LI)
- Emergency 911 (E911) enhanced support on the Enterprise network
- Virtual Call Admission Control (VCAC)

In CHS SN06, Media Proxies were datafilled on every Gateway Controller (GWC).

In CHS (I)SN07, Media Proxies are datafilled on line GWCs with NAT'd lines and SIP-T GWCs.

To provision the VCAC SOC option, refer to the following procedures in the section:Enabling VCAC SOC on page 139:

- Enabling the VCAC SOC option on the CM on page 140
- Datafilling the CM for VCAC-SOC and treatment on page 139
- Disabling the VCAC SOC option on the CM on page 140

### VCAC

Virtual Call Admissions Control (VCAC) is a Quality of Service (QoS) mechanism that allows the Communication Server 2000 (CS 2000) to cancel post-dial, pre-ringing calls that would overload a segment of the packet network.

VCAC depends on a logical model of the packet network. This logical model starts with the Service Provider's core packet network and points of bandwidth concentration. These points could, for example, be customer enterprises that are made up of a collection of sites or a regional broadband aggregation point. These sites are connected by a mix of Limited Bandwidth Links (LBLs) and NATs. The VoIP GWs and, hence, the lines are located within the sites in each enterprise.

### Internet Transparency and security-related products

The Internet Transparency and security products deliver the following capabilities:

- In (I)SN07 CHS introduces enhanced support for emergency services, such as E911, on an Enterprise network. Enhanced support includes the following functionality:
  - location identification involving the use of softclients and mobile terminals
  - Public Safety Answering Point (PSAP) selection, which requires the client's location to determine the closest PSAP
- Internet Transparency, in which the solution can traverse any firewall and NAT devices without the need to add additional firewalls or NAT devices on the customer's network. Internet Transparency involves the use of a media proxy on the public side of a NAT in the service provider premise to detect the public side IP address and transport port information for RTP and RTCP flows on an individual call basis.
- Lawful Intercept (LI) consists of electronic surveillances that meet mandatory market requirements across all markets. The Communications Assistance for Law Enforcements Act (CALEA) requires that telecommunications equipment manufacturers provide operating companies with the capability to support lawfully authorized electronic surveillances (LAES) activity. Electronic surveillance refers to the mechanism used to access intercepted call content and call data from a switch-based subject, and deliver this information to one or more law enforcement agencies (LEA).

For more information, refer to the *North American Lawful Intercept Product and Technology Fundamentals, NN10190-113*

## MCS 5200 to CS 2000 Interworking

Multimedia Communication Server 5200 (MCS) to CS 2000 Interworking includes the following capabilities:

- MCS 5200 3.0 interworking via SIP.
- North American market support for Converged Desktop between the MCS 5200 and CS 2000 via IN-to-SIP signaling gateway:
  - Personal agent
  - Multimedia collaboration
  - Click to call to chosen device
  - Origination from telephone

MCS 5200 to CS 2000 interworking supports the CS 2000 and various H.323 gateways controlled by a CS 2000, and the various SIP clients controlled by the MCS 5200 system. The MCS 5200 is part of a carrier hosted voice virtual private network (VPN). The CS 2000 and MCS 5200 are interconnected through a SIP trunk.

Interoperability between MCS hosted users and CS 2000-hosted H.323 gateways is supported in the same or different Enterprise/IP address spaces.

In order to create a VPN spanning the CS 2000 and the MCS 5200, each customer group on the CS 2000 is mapped onto one domain on the MCS 5200. For each VoIP VPN/domain, there is exactly one SIP trunk between the CS 2000 and the MCS. Several VoIP VPNs may exist in a configuration consisting of a CS 2000 and an MCS.

The VPN support comprises a set of supplementary services and a common dial plan. The dial plan typically consists of a concatenation of a location code and an extension. The SIP trunk is assigned a specific location code.

This feature supports G.711 and G.729 codecs at packetization rates of 10 and 20 ms.

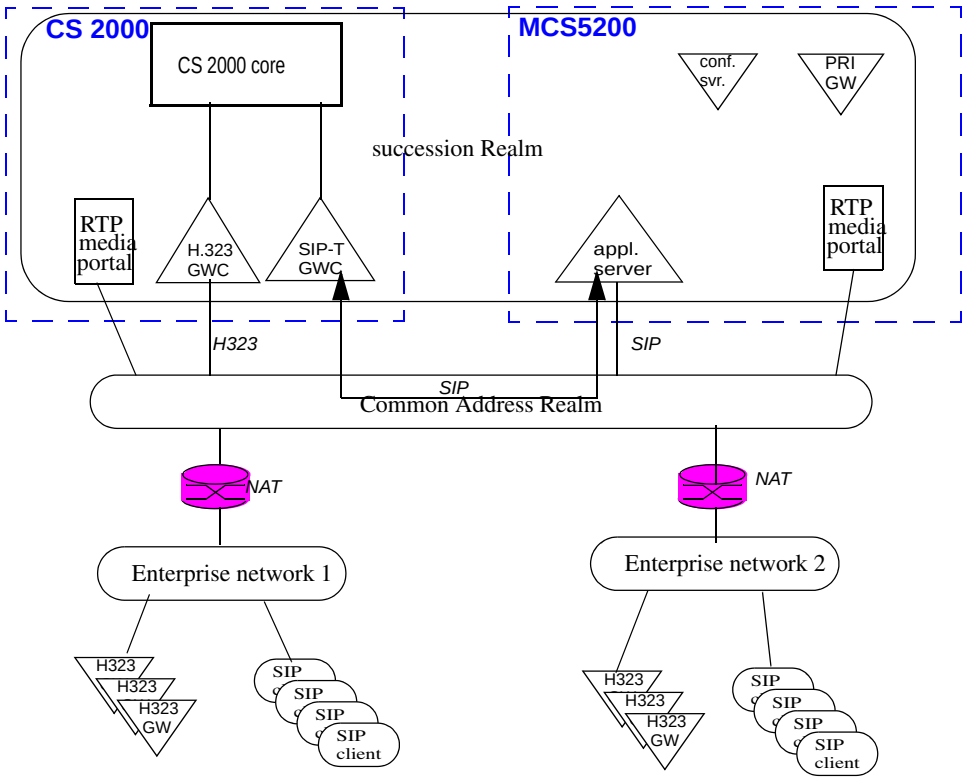
The following MCS 5200 clients are supported:

- PC client
- Web client
- i2004 and i2002 internet telephones

The interworking configuration follows:

***Note:*** For the MCS 5200 configuration, the PRI gateway is supported in the international market only.

### H.323 to MCS 5200 interworking configuration




This activity supports VPN networks with the following topology:

- VPNs hosted by one CS 2000
- VPNs hosted by several CS 2000 interconnected by a SIP-T trunk

On the CS 2000, the following H323 gateways are supported:

- S1000
- S1000M
- BCM

- Westell (international market only)
  - — liQ2031 supporting 1 E1 with DPNSS
  - — ilQ2032 supporting 2 E1 with DPNSS
- Cisco internetworking operating system (IOS) gateways (GW)

***Note 1:*** The Cisco call manager is not supported.

***Note 2:*** The Cisco router 2600 is not supported (international only).

**Media portal insertion**

The media portal must be inserted on both the MCS 5200 and the CS 2000 independent of whether the MCS 5200 clients and the H323 gateway reside in the same enterprise network.

For calls that originate and terminate in the enterprise network - regardless of whether it is the same or a different enterprise network - the media portals will always perform a public/public NAT; that is, the Media streams between the MCS and the CS 2000 media portal are always routed through the common address realm, and not through the succession realm.

**Supplementary services**

Support for the following supplementary services is available from the H.323 gateways and SIP clients.

- Call Forward

  You can forward your calls to other locations.
- Conference

  The Ad Hoc audio conferencing service is provided through the MAS which resides in the MCS configuration. (Meet Me audio conferencing is not supported.)

  ***Note:*** Ad Hoc audio conferencing is provided through a UAS-based conference server (international only).
- Call Transfer

  You can transfer an active call without talking to the person you are transferring the call to (blind transfer), or you can consult with the person who will receive your transferred call (consult transfer).
- Redirect

  You can enter an address where the call will be redirected.
- Decline

The Decline Call feature releases the call.

- Caller ID

  This feature provides the caller identification number or caller name.

- Hotline

  You can configure an i2002 or i2004 Internet Telephone such that a specific hotline number is called when the subscribed user that is registered on the i2002 or i2004 Internet Telephone goes off hook.

Refer to the MCS 5200 documentation for more information, in particular

- *Provisioning Client User Guide, NN10043-113*
- *i2004 Internet Telephone User Guide, NN10042-113*
- *Multimedia PC Client User Guide, NN10041-113*

**Support to DTMF**

Exchange of out-of-band dual-tone multifrequency (DTMF) is not possible with the current implementation.

H.323 does not send inband DTMF tones.

**Software requirements or dependencies**

The feature depends on the following software version of the different gateways:

- S1000: release 3.5 (SSE-2.11.03)
- S1000M: release 3.5 (SSE-2.11.03)
- BCM: release 3.6
- Westell liQ 2031, IPH-DP 1-6-11, supporting 1 E1 with DPNSS (international market only)
- Westell liQ 2032, IPH-DP 1-6-11, supporting 2 E1 with DPNSS (international market only)
- Cisco routers 3600/3725 (Cisco IOS GW): releases 12.2 and 12.3
- Cisco router 2600 (Cisco IOS GW): release 12.2
- MCS 5200: release 3.0

**Limitations and restrictions**

Calls originated by an MCS client that terminates on an H323 client that is not connected to the same CS 2000 as the MCS cannot be treated as private calls; that is, the private information will be lost. This limitation

is caused by the private information not being tunnelled through the SIP trunk between the different call servers.

Support for MCS SIP clients as subscribers in a CS 2000 hosted VPN assumes the MCS clients will be treated as a single network class of service (NCOS). Specifically, the MCS clients will be treated as the NCOS assigned to the integrated business network (IBN) SIP trunk.

Support for the MCS hosted users in the same Enterprise/IP address space as the H.323 gateways is based on the current MCS implementation that both the MCS and the CS 2000 would insert RTP media portals on both the MCS 5200 and the CS 2000.

This feature is restricted by the availability of supplementary services specified in the section Supplementary services on page 70

The virtual private network (VPN) is realized by a universal dialing plan consisting of a location code and extension, for example: 740 1234.

The Decline/Reject reason text transmitted by the MCS client is not transported across the CS 2000 to the H.323 client.

The conference server and PRI gateway in the international market are UAS based.

The conference server in the north american market is the Media Application Server (MAS).

The PRI gateway is not supported in the north american market.

For the Caller ID supplementary service, the calling name is not provided for calls originated by MCS.

## SIP interworking

SIP interworking includes the following capabilities:

- integration ready for third-party SIP application servers
- integration ready for third-part SIP call servers
- SIP support for RFC3261 compliance

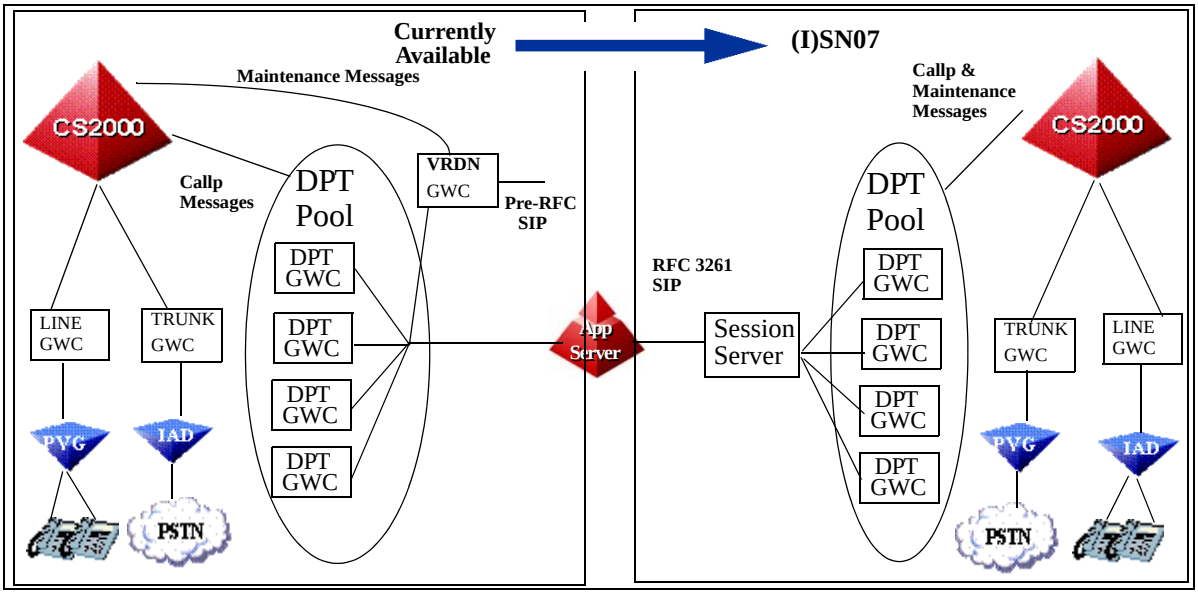
(I)SN07 includes the Session Server which uses SIP-T, an extension of the Session Initiation Protocol (SIP) that allows SIP to be used to facilitate the interconnection of the Public Switched Telephone Network (PSTN) with packet networks. SIP-T encapsulates the ISDN User Part (ISUP) messages in the SIP messages and translates ISUP information into the SIP header for routing purposes.

For more information about SIP-T in (I)SN07, refer to the documents on the component, Session Server on page 126

## Session Server platform

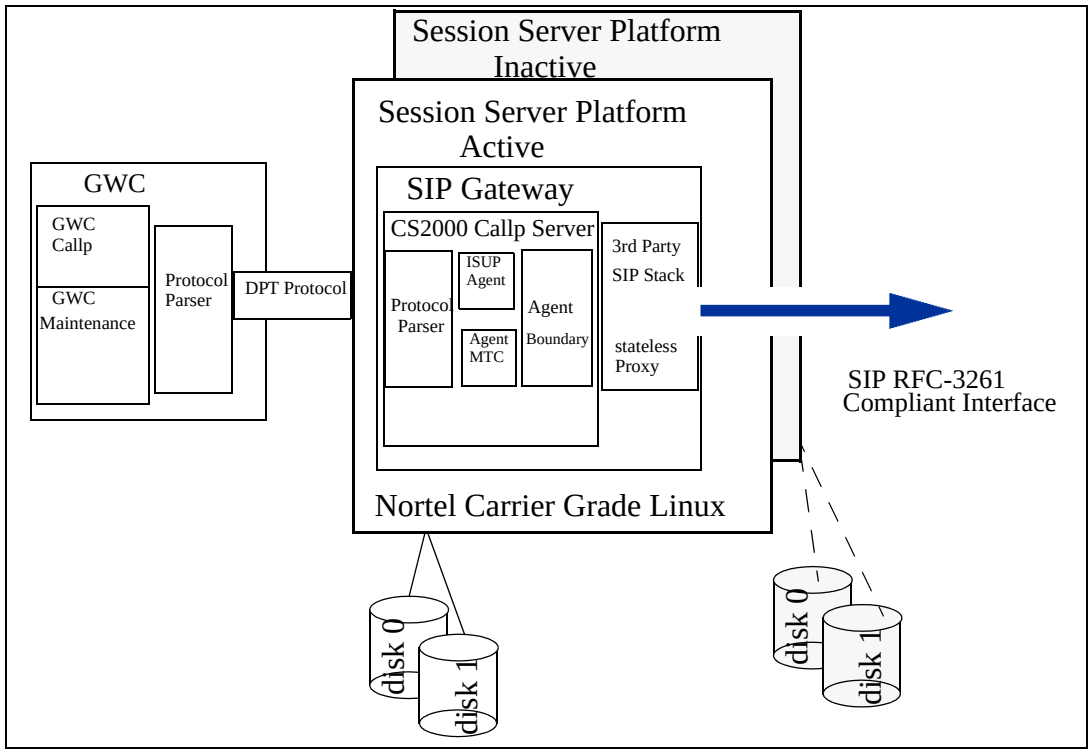
The purpose of this design is to create a highly available base platform for delivery of multiple applications. The Session Server consists of a Network Equipment-Building System (NEBS) Level 3 compliant hardware platform plus a software framework and architecture for developing highly available applications and services.

### Design intent of Session Server platform



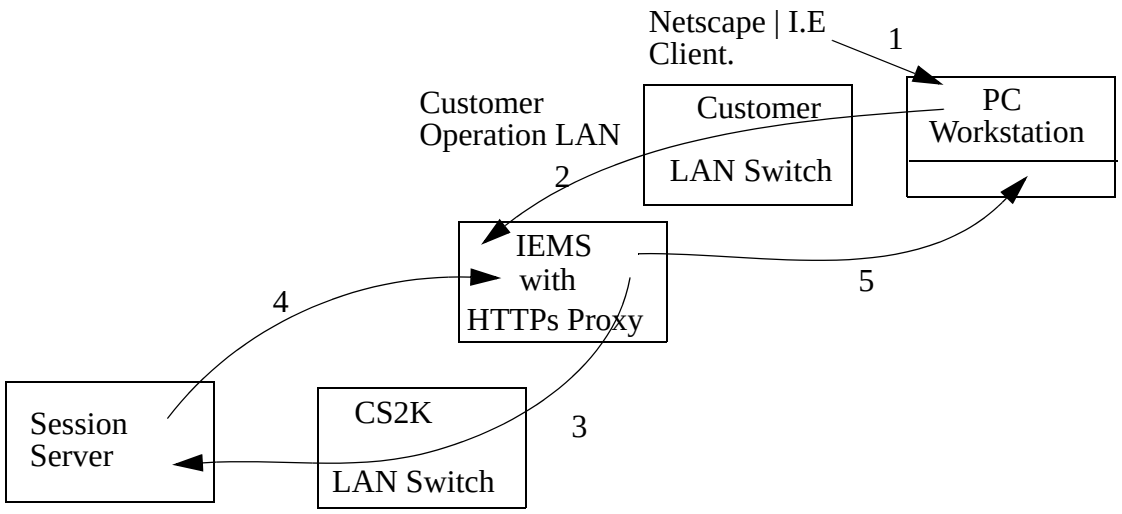

In the (I)SN07 release, the architecture for the Session Server will consist of a mated pair of Services Application Module- eXtreme Thin Servers (SAM-XTS) with a configuration similar to that of a gateway controller. Each unit is interconnected through a gigabit ethernet link as shown in the Mated pair Session Server on page 74. Each server provides processor capacity, local disk storage, and high-bandwidth network connectivity.

## Mated pair Session Server




The Session Server can be configured to use the Integrated Element Manager System (IEMS) between the customer operation LAN and the Call Server 2000(CS2K) LAN or it can be configured without the IEMS. The following figure shows a proposed configuration with IEMS, where an Hypertext Transfer Protocol (HTTP) proxy is configured on the IEMS to redirect the Netscape/Internet Explorer browser to the Session Server.

## Configure Session Server with IEMS




An overview of the configuration steps include:

- User points the browser to web link on the IEMS.
- IEMS invokes the HTTPs proxy.
- The HTTPs proxy on the IEMS redirects the link to the Session Server.
- Session Server replies back to IEMS.
- IEMS responds to user request.

The SIP Gateway application is the initial application for the Session Server platform with the intent to provide a reusable infrastructure that can support additional applications.

For more information about the Session Server, refer to the following documents located in the CHS Solution collection in Helmsman Express. For a listing of documents, refer to Session Server on page 126

## Limitations and Restrictions

The following limitations are included in the section CS 2000 H.323 limitations and restrictions on page 77 and are new to both SN06.2 and (I)SN07:

- In order to prevent Glare on the H.323 trunk, trunk selection must be set as either ASEQ or DSEQ. All other trunk types may lead the glare on the H.323 trunks.
- When a call originates from either Cisco GW, BCM, or M1/S1000, where the originator has blocked his calling party number and name, then those fields are NOT delivered to the CS2K marked as 'private'. Instead, those fields are sent to the CS2K marked as 'unavailable'. This action causes a terminator to reject all incoming private calls, and the feature, that is ACRJ, will not to work.
- When a BCM is configured to route calls to lines (MG9K, Mediatrix, or native) using the Private route type on the BCM, the calling number will be delivered as an 'unknown' number. To allow the calling number to be presented to lines when calling from a BCM, a route type other than Private should be used.

## CS 2000 H.323 limitations and restrictions

The following limitations apply to the CS 2000 H.323 network.

- The CS2K H323 system does not support silence suppression codecs: G.729b or G.729ab, G.723.
- Comfort noise on the CS2K-H.323 system is not supported.
- Currently T.38 fax support is limited to the S1000M1 and S1000 only. The Nortel Networks Media Gateway 15000 (PVG), BCM, and Westell, currently do not support T.38 fax.
- You can increase capacity without taking the GW OSS out of service. You can also change an IP/port of an H.323 without taking the GW OSS; however, the GW must be behind a NAT.

  If the GW is behind the NAT, then the trunks must be Bsy/INB in order to change the capacity or IP address.
- The NAT dynamic mapping time-out in the router should be set high enough to keep those long duration calls active - where the user tries to invoke a feature after talking for a long period of time. (See Configuration notes on page 83.)

- DISA Services:
  - For CS2K H.323, DISA DN hosted off of BCM is NOT supported.
  - When a Carrier Based Line (CICM, MediaTrix, etc.) dials a DISA DN hosted on the CS2K, the DISA DN grants access to a Hosted IPPBX Enterprise (that is an S1000) without a work-around requirement of going over the ISUP loop-around first.
  - DISA is NOT supported when a Carrier Based Line (CICM, MediaTrix, etc.) dials a DISA DN hosted on the S1000/S1000M/BCM.
  - When an H.323 IPPBX Line (BCM, S1000, S1000M, etc.) dials a DISA DN hosted on the S1000/S1000M, DISA calls work without any work around.
  - When an H.323 IPPBX Line (BCM, S1000, S1000M, etc.) dials a DISA DN hosted on the CS2K, the call should route to ISUP looparounds (on a Media Gateway 15000) before terminating to DISA.
- To preserve DPNSS VPN network capabilities, calls between the Westell LIQ 2032/2016 GW DPNSS trunks and other agents (line or Media Gateway 15000) must be routed through SIP-T IBN7(DFT) loop-around trunks to preserve DPNSS VPN network capabilities. Also trunks and lines should be in the same network (i.e. the customer groups of the line and trunk have the same NETNAME value) and the CLID option for the line's customer group are set to ONNET to get a CLI display for all VPN calls (or OFFNET if you want CLI display for all calls).
- Currently, the CS2K H.323 system uses H.450 for DPNSS tunneling only and does not support any H.450 based supplementary features.
- The TCP keepalive is disabled by default to prevent the active calls after the warm swact from dropping (except when the call involves Cisco 2600 and 3620 GW, in which case the call drops after the warm swact).
- Inter-working between H.323 and the IW SPM is not supported. A loop-around trunk should be used instead.
- Slow start calls are supported with G.711 only.
- The CNDB (Calling Number Delivery Blocking) and CNNB (Calling Name and Number Delivery Blocking) features work with the following datafill.

  In Table LTDATA in the H.323 PRI Trunk enter:

  ```
  "Serv Serv Y N Screened Always PRI_IP_PROT H.323"
  ```

- In order to prevent Glare on the H.323 trunk, trunk selection must be set as either ASEQ or DSEQ. All other trunk types may lead the glare on the H.323 trunks.
- When a call originates from either Cisco GW, BCM, or M1/S1000, where the originator has blocked his calling party number and name, then those fields are NOT delivered to the CS2K marked as 'private'. Instead, those fields are sent to the CS2K marked as 'unavailable', which causes feature ACRJ not to work where a terminator chose to reject all incoming private calls. In order to prevent interworking with E911, lines on the H.323 GWs must not be provisioned with private DN on the H.323 GW.
- When a BCM is configured to route calls to lines (MG9K, Mediatrix, or native) using the Private route type on the BCM, the calling number will be delivered as an 'unknown' number. To allow the calling number to be presented to lines when calling from a BCM, a route type other than Private should be used.

## H.323 Gateway limitations and restrictions

The following limitations and restrictions apply to the (I)SN07 Base application.

- For the calls terminating on the S1000M1 and S1000, the NET_RINGBACK_ON option must be provisioned in the TABLE LTDATA for all S1000M1 and S1000 trunk CLLIs in order to get the audiable ringback tone during the Call Setup (at the time of ALERTing).
- The BCM GW does not support SlowStart signaling on origination.
- The CS2K H323 System currently interoperates with Cisco's H323 IOS- version 12.2(24) 2600 and 3620 GWs; however, there are a number of restrictions to be addressed in a future load release from Cisco:
  - Cisco calls are terminated by the GW 1 minute after a GWC warm SWACT.
  - Cisco 2600 and 3620 GWs must be configured in a 1:1 static bind NAT configuration
  - For call scenarios where the 2600 or 3620 Cisco GW is to connect to the UAS (in SN06.2) and the UAS/AMS [in (I)SN07], and the Media Portal is present in the call topology due to NAT/FW traversal, the Cisco GW must be configured to transmit/receive immediately from the Cisco configuration level: `voice rtp send-recv`to
- For Core Cold and Reload restarts and for GWC Cold SWACT, H.323 calls may not get dropped in the H.323 GWs and will be

dropped in the Core. The audit system in the CS2K will clear such calls.

- After a warm SWACT on the GWC, any attempted tcp messaging caused by a feature activation or dtmf key press (if it is conveyed by out of bandmsgs) will cause a warm swacted call to drop.
- The following are a few features that are not currently supported on the CS2K H.323 IPPBX.
  - Executive Busy Override (EBO)
  - Automatic Call Back (ACB); however, Network Ring Again is supported for calls within the same customer group.
  - Release Link Trunk (RLT)
  - Malicious Call Hold (MCH); however, MCH is supported on the Carrier Based Lines (CICM, MediaTrix, etc).
  - Network ACD
- Codec Provisioning: If an H.323 GW can support both G.711 and G.729, then G.711 should be provisioned as a defualt codec and G.729 should be provisioned as a preferred codec. No GW should be configured as having only a G.729 codec. Configure BCM3.5 to have no preferred codec and to have G711 as the default codec. For the BCM3.5 Unified Manager, there is a need to set G711 as the default codec for the Nortel IP terminal. Configure BCM 3.6 gateways to have G.711 as default and G.729 preferred.
- H.323 calls with only a Symmetric codec and ptime are supported (the H.323 GW must receive what is sent; that is, if a GW sends G711, then the H.323 GW must receive G711; if a GW sends 20ms, then the GW must receive 20ms).
- M1 Conference Keys only work after the conference party answers the call.
- H.323 GWs do not send any packets till the CONNECT. So we need to change to the loss timer on the Media Gateway 15000 to 0 - see the third bullet of the Configuration notes on page 83.

- There are three different ways to carry DTMF digits:
  - Carry DTMF digits as an inband DTMF tone. But low bit-rate voice codecs such as G.729 cannot be guaranteed to reproduce these tone signals accurately enough for automatic recognition.
  - Use out-of-band DTMF digits in signaling.
  - Use the RTP payload to carry DTMF digits, Telephony Tones, and Telephony Signals as specified in RFC 2833.
- An inband DTMF tone is not sufficient for certain codecs such as G.729. RFC 2833 solves the problem by carrying DTMF digits in the RTP Payload with special encoded RTP packets, but currently, certain H.323 GWs such as BCM, S1000M/S1000 do not support RFC 2833.

  Following is a list of ways to carry DTMF digits between different GWs:

| **Termination**<br>**Origination** | **To H.323 GWs which Support RFC 2833** | **H.323 GWs which do Not support RFC 2833** |
|---|---|---|
| From H.323 GWs which Supports RFC 2833 | RFC 2833 | Out of Band DTMF Signaling |
| From H.323 GWs which do Not Support RFC 2833 | Out of Band DTMF Signaling | Out of Band DTMF Signaling |

| Termination Origination | To H.323 GWs which Support RFC 2833 | H.323 GWs which do Not support RFC 2833 |
|---|---|---|
| From the Nortel Networks Media Gateway 15000 Supports (PVG RFC 2833) | RFC 2833 | DTMF digits pressed on the phone off H.323 GW are delivered to the Media Gateway 15000 in out-of-band dtmf signaling; the Media Gateway 15000 will play out the tone.<br>DTMF digits pressed on the phone off Media Gateway 15000:<br>- G.711 Codec<br>H.323 does not request to collect DTMF digits; so, DTMF from the Media Gateway 15000 will be delivered as an in-band tone.<br>- G.729 Codec<br>H.323 GWs do request the Media Gateway 15000 to collect DTMF digits; so, the DTMF from the Media Gateway 15000 will be delivered as out-of-band signaling. |
| Mediatrix Supports (Mediatrix supports RFC 2833) | RFC 2833 | DTMF digits pressed on the phone off the H.323 GW are delivered to the Mediatrix GWC in out-of-band dtmf signaling, but the Mediatrix side will NOT play out the tone.<br>H.323 does not request Mediatrix to collect DTMF digits; so, DTMF pressed on Mediatrix will be delivered as an in-band tone. |

## H.323 Protocol limitations

H.323 protocol does not support providing audible ringback tones to the H.323 subscriber after a call has been answered. Due to this limitation, the H.323 subscriber will hear silence in certain feature interaction scenarios instead of audible ringback.

In these scenarios, the service interaction will function as normal, except for the fact the H.323 subscriber will hear silence as opposed to audible ringback. Since all of these scenarios involve answered calls, the H.323 subscriber will most likely know that they are on hold and waiting for some action to complete.

These scenarios include:

- A line gateway (such as Mediatrix) invokes Call Park on a call that is received from an H.323 subscriber. In this scenario, the H.323 subscriber will hear silence until the call is retrieved.
- A line gateway (such as Mediatrix) is involved in a call with an H.323 subscriber, followed by the line gateway initiating a conference to another party. If the third party is conferenced into the call while still alerting, the H.323 subscriber will not receive audible ringback.

  ***Note:*** If the third party is connected through a TDM ISUP trunk, then audible ringback will be provided by the terminating office and audible ringback will be heard.)

- A line gateway (such as Mediatrix) performs a call transfer of an answered call from an H.323 subscriber to an alerting party.
- Certain ACD/UCD scenarios cause the call to be queued after answer.

## Configuration notes

The following notes apply to the H.323 Gateway configuration:

- Add the NET_RINGBACK_ON in the table ltdata to the get the network ringback for the S1000M terminating call.

  Examples include:

  — ISDN 13 SERV

  — SERV Y Y ALWAYS ALWAYS (NET_RINGBACK_ON) (PRI_IP_PROT H323) $

  — ISDN 14 SERV

  — SERV Y Y ALWAYS ALWAYS (NET_RINGBACK_ON) (PRI_IP_PROT H323) $

- The Media proxy (RTP Portal) must be associated in CS 2000 Mgmt. Server -> GWC# ->Provisioning -> Media Proxies -> for those GWCs that have at least one GW behind the NAT.
- Most of the H.323 GWs do not send any packets till the CONNECT. So we need to change the loss timer on the Media Gateway 15000 (PVG) to 0.

  **Changing the loss timer on the Media Gateway 15000 to zero**

  ***at the command line te***

**1** Telnet to your Nortel Networks Media Gateway 15000, and check the card slot you are using on the Media Gateway 15000.

**2 St prov**

**3 set nsta/13 vgs brag/1 loss 0**

**4 set nsta/13 vgs brag/2 loss 0**

**5 set nsta/13 vgs brag/16 loss 0**

**6 act prov**

**7 confirm prov**

- Make sure that the RFC 2833 is clicked in the CS 2000 Mgmt. Server 'Configure Network' GUI, if the RFC 2833 support is required for the in-band DTMF tones.
- Codecs are added to the CS 2000 Mgmt. Server in a preferred order to align with the Gateway codec settings.
- The two configuration rules must be setup for each H.323 GW that is in the Enterprise IP-VPN on the NAT router. The first rule maps the RAS port of the GW (UDP transport) to NATed IP(of the NAT router) + port (X open on the NAT router). The second rule maps the Call signalling port of the GW (TCP transport) to the NATed IP(of the NAT router) + port (X+1open on the NAT router).

  Examples include:

  — 10.19.199.195(NAT Router IPAddress):7000(port on the NAT router)<-> 10.88.88.55(H.323 GW IP address):1719(RAS port on the GW)

  — 10.19.199.195(NAT Router IPAddress):7001(port on the NAT router)<-> 10.88.88.55(H.323 GW IP address):1720(Call Sig. port on the GW)

- For gateways such as Cisco GWs that do not provide a static RAS port, N:1 addressing is not an option as mapping the port must be done dynamically. This is a NAT 1:1 configuration and is supported by giving port 0 in the CS 2000 Mgmt. Server for the Cisco GW.
- If a H323 gateway in the International market does not support overlap signaling for termination, then the translation in the core should be set to do en-bloc signaling by using the TABLE PXCODE and minmax mm option to control for the en-bloc sending.
- The "INTER DOMAIN" bool is in the TABLE TRKOPTS for the SIP-T Trunks should be set as follows

  — "INTER DOMAIN" bool should be set to Y (that is, inter-domain) for all SIP-T trunks except loop-around trunks.

  — "INTER DOMAIN" bool should be set to N (that is, intra-domain) for SIP-T loop-around trunks.

- Do not enable e.164 registration in the H.323 GW as this kind of registration is not supported by GWC.
- For NATs with per-protocol time-outs, the recommended timer values are
  - For TCP (for Call Signaling), a bind time-out of 35 minutes.
  - For UDP (for RAS), a bind time-out of 3 minutes.

  For NATs that have a single global time-out value, a bind time-out value of 35 minutes is recommended.

# Features and services

This section lists the services that CHS supports.

## CICM services, NA and international

The following table lists the North American and international services that are currently supported by the CICM clients.

***Note:*** Not all services are supported by both North American and international markets. Notice the applicable footnotes at the end of this table.

| Option | Service | i2004 | i2002 | m6350 SoftClient |
|---|---|---|---|---|
| 3WC | Three Way Calling | x | x | x |
| AAB | Automatic Answer Back | x | x | x |
| ACB | Automatic Call Back | x | x | x |
| ACD | Automatic Call Distribution | x | x | x |
| ACD - AAK | ACD - Answer Agent Key | x | x | x |
| ACD - ACDNR | ACD - Automatic Call Distribution Not Ready | x | x | x |
| ACD - ASL | ACD - Agent Status Lamp | x | x | x |
| ACD - CAG | ACD - Call Agent | x | x | x |
| ACD - CIF | ACD - Controlled Interflow | x | x | x |
| ACD - CLSUP | ACD - Call Supervisor | x | x | x |
| ACD - DASK | ACD - Display Agent Status | x | x | x |
| ACD - DQS | ACD - Display Queue Status | x | x | x |
| ACD - DQT | ACD - Display Queue Threshold | x | x | x |
| ACD - ECM / ICM | ACD - Extended Call Management | x | x | x |
| ACD - EMK | ACD - Emergency Key | x | x | x |

| Option | Service | i2004 | i2002 | m6350 SoftClient |
|---|---|---|---|---|
| ACD - FAA | ACD - Forced Agent Availability | x | x | x |
| ACD - LOB | ACD - Line of Business | x | x | x |
| ACD - NGTSRVCE | ACD - Night Service | x | x | x |
| ACD - OBS | ACD - Observe Agent | x | x | x |
| ACD - SUPR | ACD - Supervisor | x | x | x |
| ACRJ | Anonymous Caller Rejection | x | x | x |
| AIN | Advanced Intelligent Network | x | x | x |
| AINDN | AIN Directory Number | x | x | x |
| AINMWT | AIN Message Waiting | x | x | x |
| AMATEST | Automatic Message Accounting Test Call Capability | x | x | x |
| AMSGDENY | Access to Messaging Deny | x | x | x |
| AR | Automatic Recall | x | x | x |
| ARDDN | Automatic Recall Dialable DN | x | x | x |
| ATC | Automatic Time and Charges | x | x | x |
| AUD | Automatic Dial | x | x | x |
| AUL | Automatic Line | x | x | x |
| AUTODISP | Automatic Display | x | x | x |
| AVT | AUTOVON Termination | x | x | x |
| BLF | Busy Lamp Field for Meridian Business Sets | x | x | x |
| BNN | Bridged Night Number | x | x | x |
| CBE | Call Forwarding Busy Internal Calls Only | x | x | x |

| Option | Service | i2004 | i2002 | m6350 SoftClient |
|---|---|---|---|---|
| CBI | Call Busy Intragroup (or Channel Bus Interface) | x | x | x |
| CBU | Call Forwarding Busy Unrestricted | x | x | x |
| CCW | Cancel Call Waiting | x | x | x |
| CDC | Customer Data Change | x | x | x |
| CDE | Exclude External Calls from Call Forwarding | x | x | x |
| CDI | Exclude Intragroup Calls from Call Forwarding | x | x | x |
| CDU | Call Forwarding Do Not Answer Unrestricted | x | x | x |
| CFB | Call Forwarding Busy | x | x | x |
| CFCW | Call Forward Call Waiting | x | x | x |
| CFD | Call Forwarding Do Not Answer (Business sets) | x | x | x |
| CFDVT | Call Forwarding Do Not Answer Variable Timer | x | x | x |
| CFF | Call Forwarding Fixed | x | x | x |
| CFGD | Call Forwarding Do Not Answer for Hunt Group | x | x | x |
| CFI | Call Forwarding Intragroup | x | x | x |
| CFK | Call Forwarding on a per Key Basis | x | x | x |
| CFMDN | Call Forwarding MADN Secondary Member | x | x | x |
| CFRA | Call Forwarding Remote Access | x | x | x |
| CFS | Call Forwarding Simultaneous Screening | x | x | x |
| CFTB | Call Forward Timed for CFB | x | x | x |

| Option | Service | i2004 | i2002 | m6350 SoftClient |
|---|---|---|---|---|
| CFTD | Call Forward Timed for CFD | x | x | x |
| CFU | Call Forwarding Universal | x | x | x |
| CFWVAL | Call Forwarding Validation | x | x | x |
| CID (NTS_CID) | Calling Party Identification | x | x | x |
| CIR | Circular Hunt | x | x | x |
| CLI | Calling Line Identification | x | x | x |
| CMCF | Control Multiple Call Forwarding | x | x | x |
| CNDBO | Calling Number Delivery Blocking Override | x | x | x |
| CNF | Station Controlled Conference | x | x | x |
| COT | Customer Originated Trace | x | x | x |
| COTAMA | Customer Originated Trace with AMA | x | x | x |
| CPU | Call Pickup | x | x | x |
| CTD | Carrier Toll Denied | x | x | x |
| CTW | Call Transfer Warning | x | x | x |
| CWD | Dial Call Waiting | x | x | x |
| CWI | Call Waiting Intragroup | x | x | x |
| CWO | Call Waiting Originating | x | x | x |
| CWR | Call Waiting Ringback | x | x | x |
| CWT | Call Waiting | x | x | x |
| CWX | Call Waiting Exempt | x | x | x |
| CXR | Call Transfer | x | x | x |
| DCBI | Directed Call Pickup Barge-In | x | x | x |

| Option | Service | i2004 | i2002 | m6350 SoftClient |
|---|---|---|---|---|
| DCBX | Directed Call Pickup Barge-In Exempt | x | x | x |
| DCF | Denied Call Forwarding | x | x | x |
| DCPK | Directed Call Park | x | x | x |
| DCPU | Directed Call Pickup | x | x | x |
| DCPX | Directed Call Pickup Exempt | x | x | x |
| DENYCTFP | Deny Call Transfer Fraud Prevention | x | x | x |
| DENYISA | Deny In-Session Activation | x | x | x |
| DID | Direct Inward Dialing | x | x | x |
| DIN | Denied Incoming | x | x | x |
| DISA | Direct System Inward Access | x | x | x |
| DISP | Display | x | x | x |
| DLH | Distributed Line Hunt | x | x | x |
| DND | Do Not Disturb | x | x | x |
| DNH | Directory Number Hunt | x | x | x |
| DMCT | Deny Malicious Call Termination | x | x | x |
| DNID (NTS_DNID) | Dialed Number Identification Delivery | x | x | x |
| DOD | Direct Outward Dialing | x | x | x |
| DOR | Denied Origination | x | x | x |
| DRCW | Distinctive Ringing/Call Waiting | | | |
| DRING | Distinctive Ringing | x | x | x |
| DTM | Denied Termination | x | x | x |
| E911 | Emergency Services (interaction support) | x | x | x |

| Option | Service | i2004 | i2002 | m6350 SoftClient |
|---|---|---|---|---|
| EBO | Executive Busy Override | x | x | x |
| EBX | Executive Busy Override Exempt | x | x | x |
| ELN | Essential Line | x | x | x |
| Int'l Emergency Call | International Emergency Call Routing | x | x | x |
| EMW | Executive Message Waiting | x | x | x |
| EXT | Extensiopossible Issued-On | x | x | x |
| FCTDINT | Full Carrier Toll Deny for International Carriers | x | x | x |
| FCTDNTER | InterLATA Full Carrier Toll Denied | x | x | x |
| FCTDNTRA | IntraLATA Full Carrier Toll Denied | x | x | x |
| FGA | Feature Group A | x | x | x |
| FNT | Free Number Terminating | x | x | x |
| FTRGRP | Feature Group | x | x | x |
| FTRKEYS | Feature Keys | x | x | x |
| FXR | Fast Transfer | x | x | x |
| ICSDEACT | In Call Service Deactivation | x | x | x |
| IECFB | Internal/External Call Forwarding Busy | x | x | x |
| IECFD | Internal/External Call Forwarding Do Not Answer | x | x | x |
| ILB | Inhibit Line Busy | x | x | x |
| IN (CS-X) | Intelligent Networks (CS-X) | x | x | x |
| INSPECT | Inspect Key | x | x | x |
| INTPIC | International Primary Carrier | x | x | x |
| IRR | Inhibit Ring Reminder | x | x | x |

| Option | Service | i2004 | i2002 | m6350 SoftClient |
|---|---|---|---|---|
| JOIN | Conference Join | x | x | x |
| KSH | Key Short Hunt | x | x | x |
| KSMOH | Key Set Music on Hold | x | x | x |
| LCDR | Local Call Detail Recording | x | x | x |
| LI | Lawful Intercept | x | x | x |
| LMOH | Line Music on Hold | x | x | x |
| LNP | Local Number Portability (LRN based) | x | x | x |
| LNR | Last Number Redial | x | x | x |
| LNRA | Last Number Redial Associated with Set | x | x | x |
| LOD | Line Overflow to DN | x | x | x |
| LOR | Line Overflow to Route | x | x | x |
| LPIC | IntraLATA PIC | x | x | x |
| LVM | Leave Message | x | x | x |
| MBK | Make Busy Key | x | x | x |
| MBSCAMP | Meridian Business Set Station Camp-On | x | x | x |
| MCH | Malicious Call Hold | x | x | x |
| MDN MCA | Multiple Appearance Directory Number (MADN) Multiple Call Arrangement | x | x | x |
| MDN SCA | MADN Single Call Arrangement | x | x | x |
| MDNNAME | MADN Member Name | x | x | x |
| MEETME | Meet Me Conference | x | x | x |
| MEMDISP | MADN Member Display | x | x | x |

| Option | Service | i2004 | i2002 | m6350 SoftClient |
|---|---|---|---|---|
| MLAMP | MADN Lamp | x | x | x |
| MLH | Multi-line Hunt | x | x | x |
| MREL | MADN Release | x | x | x |
| MRF | MADN Ring Forwarding | x | x | x |
| MRFM | MADN Ring Forwarding Manual | x | x | x |
| MSB | Make Set Busy | x | x | x |
| MSBI | Make Set Busy Intragroup | x | x | x |
| MWIDC | Message Waiting Indication | x | x | x |
| MWINK | MADN Message Waiting Indicator | x | x | x |
| MWQRY | Message Waiting Query | x | x | x |
| MWT | Message Waiting | x | x | x |
| NAME | Name Display | x | x | x |
| NOH | No Receiver Off-Hook Tone | x | x | x |
| OLS | Originating Line Select | x | x | x |
| ONI | Operator Number Identification | x | x | x |
| OP | Operator Services Access | x | x | x |
| PBL | Private Business Line | x | x | x |
| PCWT | Precedence Call Waiting Termination | x | x | x |
| PDO | Prevent Delete Option | x | x | x |
| PF | Power Features | x | x | x |
| PIC | Primary InterLATA Carrier | x | x | x |
| PILOT | Pilot DN Billing | x | x | x |
| PLP | Plug-up (Trouble Intercept) | x | x | x |

| Option | Service | i2004 | i2002 | m6350 SoftClient |
|---|---|---|---|---|
| PORT | 10-digit unconditional LNP trigger | x | x | x |
| PPL | PVN Priority Line | x | x | x |
| PREMTBL | Call Pre-emption | x | x | x |
| PRESET CONF | Preset Conference | x | x | x |
| PRH | Preferential Hunting | x | x | x |
| PPK | Call Park | x | x | x |
| PRL | Privacy Release | x | x | x |
| PRV | Privacy for MADN | x | x | x |
| QBS | Query Busy Station | x | x | x |
| QCK | Quick Conference Key | x | x | x |
| QTD | Query Time and Date | x | x | x |
| RAG | Ring Again | x | x | x |
| RCF/RCFEA | Remote Call Forwarding (Access to) | x | x | x |
| RCVD | Received Digits Billing | x | x | x |
| REASDSP | Reason Display | x | x | x |
| RPA | Repeated Alert | x | x | x |
| RSP | Restricted Sent Paid | x | x | x |
| RSUS | Requested Suspension | x | x | x |
| SACB | Subscriber Activated Call Blocking | x | x | x |
| SBLF | Set Based Lamp Field | x | x | x |
| SCA | Selective Call Acceptance | x | x | x |
| SCF | Selective Call Forwarding | x | x | x |
| SCL | Speed Calling Long | x | x | x |

| Option | Service | i2004 | i2002 | m6350 SoftClient |
|---|---|---|---|---|
| SCMP | Series Completion | x | x | x |
| SCRJ | Selective Call Rejection | x | x | x |
| SCS | Speed Calling Short | x | x | x |
| SCU | Speed Calling User | x | x | x |
| SDSDENY | Special Delivery Service Deny | x | x | x |
| SDY | Line Study | x | x | x |
| SEC | Security | x | x | x |
| SETMODEL | Set Model | x | x | x |
| SIMRING | Simultaneous Ringing | x | x | x |
| SL | Secondary Language | x | x | x |
| SLQ | Single Line Queuing | x | x | x |
| SLU | Subscriber LIne Usage | x | x | x |
| SMDI | Simplified Message Desk Interface | x | x | x |
| SMDR | Station Message Detail Recording | x | x | x |
| SOR | Station Origination Restriction | x | x | x |
| SORC | Station Origination Restrictions Controller | x | x | x |
| SPB | Special Billing | x | x | x |
| SPR | Selective Suppression of MDCR/SMDR | x | x | x |
| SSAC | Station Specific Authorization Codes | x | x | x |
| SUPPRESS | Suppress Line Identification Information | x | x | x |
| SUS | Suspended Service | x | x | x |

| Option | Service | i2004 | i2002 | m6350 SoftClient |
|---|---|---|---|---|
| SVCGRP | Service Group | x | x | x |
| TBO | Terminating Billing Option | x | x | x |
| TERM | Terminating DN Billing | x | x | x |
| TES | Toll Essential | x | x | x |
| TFO | Terminating Fault Option | x | x | x |
| TLS | Terminating Line Select | x | x | x |
| TollFree | Toll Free Services | x | x | x |
| UCD | Uniform Call Distribution | x | x | x |
| UCDLG | Uniform Call Distribution Login | x | x | x |
| WML | Warm Line | x | x | x |
| WUCR | Wake Up Call Ring Timeout | x | x | x |

### Tandem for VoIP VPN, NA services

The following table lists the North American services that are currently supported by H.323 Tandem for VoIP VPN.

| Service | H.323 Access | Media Gateway 15000 PRI Access | Media Gateway 1500 ISUP Access | DPT Access |
|---|---|---|---|---|
| Access Options | x | x | x | x |
| AIN Services | x | x | x | x |
| AIN 15d support of IDDD | x | x | x | x |
| AIN 0, 1 /NFA I/W | x | x | x | x |
| AIN ATC Trunk Support | x | x | x | x |
| AIN Feature Code Trigger | x | x | x | x |
| AIN DCR Interworking | x | x | x | x |

| Service | H.323 Access | Media Gateway 15000 PRI Access | Media Gateway 1500 ISUP Access | DPT Access |
|---|---|---|---|---|
| AIN Default Routing | x | x | x | x |
| AIN SE R7 OCM METT | x | x | x | x |
| AIN SE R8 Carrier Usage | x | x | x | x |
| AIN Display Services | x | x | x | x |
| AIN SSP Services Enhancements | x | x | x | x |
| AIN Office Trigger Flex | x | x | x | x |
| AIN SE R4 - Collect Info | x | x | x | x |
| AIN SE R4 - OHD for PX Trun | x | x | x | x |
| AIN SE R4 - OTS | x | x | x | x |
| AIN SE R4 - Collect Info | x | x | x | x |
| AIN SE R4 - OHD Esc ICM | x | x | x | x |
| AIN SE R5 - OnePlus PFX | x | x | x | x |
| AIN SE R5 - Spfd Cxr PFS | x | x | x | x |
| AIN SE R5 - International PFX | x | x | x | x |
| AIN SE R5 - OperSvcs PFX | x | x | x | x |
| AIternate Routing | x | x | x | x |
| Automatic Route Selection (ARS) | x | x | x | x |
| AMA Base | x | x | x | x |
| AMA Mod (CAMA modules) | x | x | x | x |
| BAS ANI | x | x | x | x |
| BAS Two-Digit ANI-CAMA | x | x | x | x |
| BAS Generic - OAM | x | x | x | x |

| Service | H.323 Access | Media Gateway 15000 PRI Access | Media Gateway 1500 ISUP Access | DPT Access |
|---|---|---|---|---|
| BAS Offnet Access Services | x | x | x | x |
| BAS Flex Bellcore AMA | x | x | x | x |
| BAS SDM Table Access | x | x | x | x |
| Call Back Queuing | x | x | x | |
| Call Center Services (CPE-based) | x | x | x | x |
| Calling Card Services | x | x | x | x |
| Centralized Attendant Service | x | x | x | x |
| Centralized Audioconferencing Services | x | x | x | x |
| Centralized Custom Announcements | x | x | x | x |
| Centralized IVR | x | x | x | x |
| Centralized Voice Mail | x | x | x | x |
| DCR Dynamic Call Routing | x | x | x | x |
| DCR Base Class 5 Office | x | x | x | x |
| DCR Base Toll Office | x | x | x | x |
| DCR Base | x | x | x | x |
| DCR DNM Mess Robust | x | x | x | x |
| DCR Dual X25 Link | x | x | x | x |
| DCR Hand Rem Dual Home | x | x | x | x |
| DCR Mult. Net Access | x | x | x | x |
| DCR Non-DCR Calls | x | x | x | x |
| DCR Universal Translation | x | x | x | x |

| Service | H.323 Access | Media Gateway 15000 PRI Access | Media Gateway 1500 ISUP Access | DPT Access |
|---|---|---|---|---|
| Second Leg O/F Routing | x | x | x | x |
| DISA | x | x | x | x |
| Direct Termination Overflow | x | x | x | x |
| EQA Toll | x | x | x | x |
| EQA C7ISUPlerLta Conn AT | x | x | x | x |
| EQA ISUP Intermed. Tandem | x | x | x | x |
| EQA Intermediate Tandem | x | x | x | x |
| EQA Tandem AMA Control | x | x | x | x |
| Expensive Route Warning | x | x | x | x |
| Forced On-net | x | x | x | x |
| Government Emergency Telephony System (GETS) | x | x | x | x |
| Head-end Break-in | x | x | x | x |
| IDDD via ARS | x | x | x | x |
| ISP7 Base ISUP | x | x | x | x |
| ISP7 Aut Cngst Controls | x | x | x | x |
| ISP7 Flexible CAUSEMAP | x | x | x | x |
| ISP7 Hop Counter | x | x | x | x |
| ISP7 ISUP ChgNumb/OLIP | x | x | x | x |
| ISP7 TFP/TFC Rtng Options | x | x | x | x |
| ISUP Cellular | x | x | x | x |
| LEA LEAS Toll | x | x | x | x |
| LEA SS7 I/W with LEAS | x | x | x | x |

| Service | H.323 Access | Media Gateway 15000 PRI Access | Media Gateway 1500 ISUP Access | DPT Access |
|---|---|---|---|---|
| LNR LNP | x | x | x | x |
| LNP to Treatment on FOD | x | x | x | x |
| LNP 800+ interworking | x | x | x | x |
| Network Dial Plan Display | x | x | x | x |
| Network Information Signals | x | x | x | x |
| Network Overflow | x | x | x | x |
| Network-Wide Automatic Route Selection | x | x | x | x |
| NI0 Circular Hunt - NA | x | x | | |
| NI0 Circular Hunt - NI | x | x | | |
| NI0 ISDN Base | x | x | | |
| NI0 ISDN PRI Base | x | x | | |
| NI0 ISDN PRI CNAM | x | x | | |
| NI0 PRI Hotel/Motel | x | x | | |
| NI0 PRI NI-1 Base | x | x | | |
| NI0 PRI NI-2 Base | x | x | | |
| NI0 E911 Scrn NI-2 | x | x | | |
| NI0 PRI Message Services | x | x | | |
| NI0 Message Services SMDI Replacement | x | x | | |
| NI0 CFW I/F Busy | x | x | | |
| NI0 CFW I/F Busy NI-2 | x | x | | |
| OAM EADAS DC and HW Inv. | x | x | x | x |

| Service | H.323 Access | Media Gateway 15000 PRI Access | Media Gateway 1500 ISUP Access | DPT Access |
|---|---|---|---|---|
| OAM Enhanced E/DC Buffer | x | x | x | x |
| OAM EADAS MTC Busy Usage | x | x | x | x |
| OAM EADAS NM I/f | x | x | x | x |
| OAM NetMinder I/F | x | x | x | x |
| Off-Hook Queuing (OHQ) | x | x | x | |
| OHQ Enhanced | x | x | x | |
| Off-net-to-On-net Routing | x | x | x | x |
| On-net-to-Off-net Routing | x | x | x | x |
| PBX-PBX Feature Transparency (MCDN) | x | | | x |
| PBX-PBX Feature Transparency (DPNSS) | x | x | x | x |
| Private Network Calling (On-net-to-On-net) | x | x | x | x |
| Private Numbering Plan | x | x | x | x |
| Private Virtual Networking (ESN, PVT, MBG) | x | x | x | x |
| Tail-end Hop-off | x | x | x | x |
| Time-of-Day Routing | x | x | x | x |
| Time-of-Day NCOS | x | x | x | x |
| Toll-Free Services | x | x | x | x |
| NTS ANI II 25 Screening | x | x | x | x |
| NTS Extended Capability | x | x | x | x |
| NTS PRI I/W to 800 | x | x | x | x |

| Service | H.323 Access | Media Gateway 15000 PRI Access | Media Gateway 1500 ISUP Access | DPT Access |
|---|---|---|---|---|
| NTS 800+CID DID Display/ CMS | x | x | x | x |
| NTS 800+CID DNID Display/ MDC | x | x | x | x |
| NTS Dial Nu Display/BCLID | x | x | x | x |
| NTS Per DN Subscription Controls | x | x | x | x |
| NTS 800 Expansion - 888 Cod | x | x | x | x |
| NTS 888 Expansion for EO | x | x | x | x |
| NTS 800 Billing Enhancement | x | x | x | x |
| NTS 800 CID Number Delivery | x | x | x | x |
| NTS RLT w/No Third-Party Itctn | x | x | x | x |
| NTS SSP-800 CarID in AMA | x | x | x | x |
| NTS FANI for Toll Free | x | x | x | x |
| Trunk Queuing | x | x | x | |
| UDD Services | x | x | x | x |
| UDD FANI Tandem Screen | x | x | x | x |
| Uniform Numbering Plan Capability | x | x | x | x |
| Virtual On-Net | x | x | x | x |
| VPN Tariffs | x | x | x | x |
| a. Does not apply to North American markets. | | | | |

### BCM interworking to CICM, NA services

The following table lists the north american (NA) services that are currently supported by H.323 for BCM interworking to CICM and IAD gateway for nodal calls and calls through SIP-T.

| Service | BCM interworking to | | | |
|---|---|---|---|---|
| | CICM (nodal) | CICM (SIP-T) | IAD gateway (nodal) | IAD gateway (SIP-T) |
| Basic Call | x | x | x | x |
| Calling Line Identification (CLID) | | | | |
| Calling Number Delivery | x | x | x | x |
| Connected Number Delivery | Note 2 | Note 2 | Note 2 | Note 2 |
| Called Number Delivery | x | x | x | x |
| Network Call Party Name Display | | | | |
| Calling Party Name Delivery | x | x | x<br>Note 3 | x<br>Note 4 |
| Connected Party Name Delivery | - | - | - | - |
| Original Called Party Name Delivery | - | - | - | - |
| Called Party Name Delivery | - | - | - | - |
| Redirecting Party Name Delivery | - | - | - | - |
| Redirection Party Name Delivery | - | - | - | - |
| Network Call Redirection | | | | |
| Network Call Forward All Calls | x | x | x | x |
| Network Call Forward No Answer | x | x | x | x |
| Network Call Forward Busy | x | x | x | x |
| Network Hunting | - | - | - | - |
| Call Transfer | x | x | x | x |

| Service | BCM interworking to | | | |
|---|---|---|---|---|
| | CICM (nodal) | CICM (SIP-T) | IAD gateway (nodal) | IAD gateway (SIP-T) |
| Call Pickup | - | - | - | - |
| Network message services | | | | |
| Message Waiting Indication | Note 1 | Note 1 | Note 1 | Note 1 |
| Network Camp-on | - | - | - | - |
| Network Break-In | - | - | - | - |
| Trunk Anti-Tromboning (TAT) | - | - | - | - |
| Multi-location business group (MBG) | Note 1 | | | |
| Virtual Access to Private Networks (VAPN) | - | - | - | - |
| Direct Inward System Access (DISA) | - | - | - | - |
| yes: supported MCDN service | | | | |
| Note 1: Priority 1 service, not supported. | | | | |
| Note 2: Priority 1 service, not supported by this activity; although, this service is supported as an MCDN service interworking between two H.323 gateways. | | | | |
| Note 3: For this activity's CS 2000 to S1000M direction, only private calls contain the MCDN private data (for displaying Calling Name). For CS 2000 to S1000M direction, public calls do NOT contain private MCDN data. Therefore, the public CS 2000 to S1000M direction calls, Calling Display is not applicable/displayed. | | | | |
| Note 4: Calling Name Delivery within the Core remains unchanged by this activity to either line agents or trunk agents; therefore, existing functionalities, restrictions, or limitations of Calling Name Delivery remain applicable. | | | | |

### BCM interworking to CICM, international services

The following table lists the International services that are currently supported by H.323 for BCM interworking to CICM for IAD gateway nodal calls and calls through SIP-T.

| Service | BCM interworking to | | | |
|---|---|---|---|---|
| | CICM (nodal) | CICM (SIP-T) | IAD gateway (nodal) | IAD gateway (SIP-T) |
| Basic Call | x | x | x | x |
| Calling Line Identification (CLID) | | | | |
| Calling Number Delivery | x | x | x | x |
| Connected Number Delivery | x | x | | |
| Called Number Delivery | x | x | | |
| Network Call Party Name Display | | | | |
| Calling Party Name Delivery | x | x | x | x |
| Network Call Redirection | | | | |
| Network Call Forward All Calls | x | x | x | x |
| Network Call Forward No Answer | x | x | x | x |
| Network Call Forward Busy | x | x | x | x |
| Call Transfer | x | x | x | x |
| Call Pickup | x | x | x | x |

### S1000M interworking to CICM, NA services

The following table lists the north american (NA) services that are currently supported by H.323 for S1000M interworking to CICM and IAD gateway for nodal calls, and calls through SIP-T.

| Service | S1000M interworking to | | | |
|---|---|---|---|---|
| | CICM (nodal) | CICM (SIP-T) | IAD gateway (nodal) | IAD gateway (SIP-T) |
| Basic Call | x | x | x | x |
| Calling Line Identification (CLID) | | | | |
| Calling Number Delivery | x | x | x | x |
| Connected Number Delivery | Note 2 | Note 2 | Note 2 | Note 2 |
| Called Number Delivery | x | x | | |
| Network Call Party Name Display | | | | |
| Calling Party Name Delivery | x | x | x<br>Note 3 | x<br>Note 4 |
| Connected Party Name Delivery | - | - | - | - |
| Original Called Party Name Delivery | - | - | - | - |
| Called Party Name Delivery | - | - | - | - |
| Redirecting Party Name Delivery | - | - | - | - |
| Redirection Party Name Delivery | - | - | - | - |
| CLID in Call Detail Record (CDR) | Note 1 | | | |
| ISDN Signaling Link (ISL) | - | - | - | - |
| Network Ring Again | Note 1 | | | |
| Network Call Redirection | | | | |
| Network Call Forward All Calls | x | x | x | x |
| Network Call Forward No Answer | x | x | x | x |

| Service | S1000M interworking to | | | |
|---|---|---|---|---|
| | CICM (nodal) | CICM (SIP-T) | IAD gateway (nodal) | IAD gateway (SIP-T) |
| Network Call Forward Busy | x | x | x | x |
| Network Hunting | - | - | - | - |
| Call Transfer | x | x | x | x |
| Call Pickup | x | x | x | x |
| Network Automatic Call Distribution (NACD) | | | | |
| Make Set Busy Key | - | - | - | - |
| Not Ready Key | - | - | - | - |
| Individual DN Key | - | - | - | - |
| Dialed Number Identification Service and Name Display | - | - | - | - |
| ACD-C and ACD-D reports | - | - | - | - |
| Network message services | - | - | - | - |
| Message Waiting Indication | Note 1 | | | |
| Network Authorization Code | - | - | - | - |
| Network Speed Call | - | - | - | - |
| Network Class of Service (NCOS) | x | x | x | x |
| Remote Virtual Queuing | - | - | - | - |
| Attendant and Network Wide Remote Call Forward | - | - | - | - |
| Flexible Numbering Plan | - | - | - | - |
| Network Wide Calling Party Privacy | - | - | - | - |
| Display of Calling Party Denied | - | - | - | - |

| Service | S1000M interworking to | | | |
|---|---|---|---|---|
| | CICM (nodal) | CICM (SIP-T) | IAD gateway (nodal) | IAD gateway (SIP-T) |
| Trunk Anti-Tromboning (TAT) | - | - | - | - |
| Calling Party Privacy Enhancements | - | - | - | - |
| Integrated Services Access (ISA) | - | - | - | - |
| Network Alternate Route Selection | | | | |
| NARS Access Codes | - | - | - | - |
| Uniform Dialing Plan | - | - | - | - |
| Coordinated Dialing Plan | - | - | - | - |
| Time of Day Routing | - | - | - | - |
| Network Routing Control | - | - | - | - |
| Satellite link control | - | - | - | - |
| Digit screening | - | - | - | - |
| Digit manipulation | - | - | - | - |
| Auto on-net to off-net overflow | - | - | - | - |
| Automatic least cost routing | - | - | - | - |
| Automatic OCC access | - | - | - | - |
| Expensive Route Warning Tone | - | - | - | - |
| Data packet network Access | - | - | - | - |
| Customer Network Manipulation | - | - | - | - |
| Direct Private Network Access | - | - | - | - |
| Electronic Tandem Network | - | - | - | - |
| Meridian Switched Network Variable Types of Outpulsing on Same Call | - | - | - | - |

| Service | S1000M interworking to | | | |
|---|---|---|---|---|
| | CICM (nodal) | CICM (SIP-T) | IAD gateway (nodal) | IAD gateway (SIP-T) |
| Network CLID and NCOS Display Interaction with 3WC | - | - | - | - |
| Network Dial Plan Display | - | - | - | - |
| Network Reason Display | - | - | - | - |
| Network Information Signals | - | - | - | - |
| Network Queuing, Main Network Signaling (NSIG) | - | - | - | - |
| Network Traffic Measurement | - | - | - | - |
| Time-of-Day Network Class of Service (NCOS) | - | - | - | - |
| Multi-location business groups (MBG) | Note 1 | | | |
| Virtual Access to Private Networks (VAPN) | - | - | - | - |
| Direct Inward System Access (DISA) | - | - | - | - |
| Note 1: Priority 1 service, not supported. | | | | |
| Note 2: Priority 1 service, not supported except as an MCDN service interworking between two H.323 gateways if tunneled through a CS 2000. | | | | |
| Note 3: Succession 1000M requires Calling Name to be tunneled within an H.323 Setup message. In addition, for the CS 2000 to S1000M direction, only private calls contain the MCDN private data for displaying Calling Name; public calls do NOT contain private MCDN data. Therefore, for public CS 2000 to S1000M direction, Calling Display is not displayed. | | | | |
| Note 4: Calling Name Delivery within the Core remains unchanged to either line agents or trunk agents; therefore, existing functionalities, restrictions, or limitations of Calling Name Delivery remain applicable. | | | | |

### S1000M interworking to CICM, international services

The following table lists the International services that are currently supported by H.323 for S1000M interworking to CICM and IAD gateway for nodal calls, and calls through SIP-T.

| Service | BCM interworking to | | | |
|---|---|---|---|---|
| | CICM (nodal) | CICM (SIP-T) | IAD gateway (nodal) | IAD gateway (SIP-T) |
| Basic Call | x | x | x | x |
| Calling Line Identification (CLID) | | | | |
| Calling Number Delivery | x | x | x | x |
| Connected Number Delivery | x | x | | |
| Called Number Delivery | x | x | | |
| Network Call Party Name Display | | | | |
| Calling Party Name Delivery | x | x | x | x |
| Network Call Redirection | | | | |
| Network Call Forward All Calls | x | x | x | x |
| Network Call Forward No Answer | x | x | x | x |
| Network Call Forward Busy | x | x | x | x |
| Call Transfer | x | x | x | x |
| Call Pickup | x | x | x | x |
| Network Class of Service (NCOS) | x | x | x | x |

### International DPNSS services on CS 2000

The following table represents the set of DPNSS services as part of (I)SN07.

| DPNSS Service | Nodal Transit (Note 1) | Net-work Transit (Note 2) | End Node Calling/ Called | Comment |
|---|---|---|---|---|
| CLI Display | X | X | X | |
| Busy Information | X | X | X | |
| CBWF | X | X | X | |
| Executive intrusion | X | X | X | This feature is blocked and not supported for lines where the intruded party is on the CS 2000. |
| Divert on No Reply | X | X | X | Both with/without drop-back diversion |
| Divert on Busy | X | X | X | Both with/without drop-back diversion |
| Divert-Immediate | X | X | X | Both with/without drop-back diversion |
| HOLD | X | X | X | |
| Call Offer | X | X | X | |
| Call Waiting | X | X | X | |
| ROP | X | X | X | |
| Three-Party Call | X | X | X | |
| Non-Specified Information | X | X | X | |
| Service-Independent strings | X | X | X | |
| Redirection | X | X | | |
| Series Call | X | X | | |

| DPNSS Service | Nodal Transit (Note 1) | Net-work Transit (Note 2) | End Node Calling/ Called | Comment |
|---|---|---|---|---|
| Night Service | X | X | | |
| Centralized Operator | X | X | | |
| Extension Status | X | X | | |
| Controlled Diversion | X | X | | |
| Three-Party takeover | X | X | | |
| Remote Alarm Reporting | X | X | | |
| Add-on Conference | X | X | | |
| Time Synchronization | X | X | | |
| Call Back When Next Used | X | X | | |
| Do not Disturb | X | X | | |
| Remote Registration of Diversion | X | X | | |
| Remote Registration of Do not Disturb | X | X | | |
| Priority Breakdown | X | X | | |
| Call Back Messaging | X | X | | |
| Forced Release | X | X | | |
| Text Message | X | X | | |
| Charge Reporting | X | X | | |

| DPNSS Service | Nodal Transit (Note 1) | Net-work Transit (Note 2) | End Node Calling/ Called | Comment |
|---|---|---|---|---|
| Network Address Extension | X | X | | |
| Call Park | X | X | | |
| Call Distribution | X | X | | |
| Route Capacity Control | X | X | | |
| Wait on Busy | X | X | | |
| Call Pick-up | X | X | | |
| Traveling Class of Service | X | X | | |
| Number Presentation Restriction | X | X | | |
| Note 1: Nodal Transit refers to a a transit configuration where CS 2000 acts as a "pure transit" with Westell gateways serving as both Ingress and Egress gateways. | | | | |
| Note 2: Network transit refers to a supporting DPNSS signaling transparency (DFT) across the network through IBN7 DFT (or SIP-T) proprietary signaling. | | | | |

### International DPNSS / Centrex services

The following table represents the set of DPNSS / Centrex services as part of (I)SN07.

| DPNSS Service | Nodal Transit | Net-work Transit | End Node Calling/ Called | Comment |
|---|---|---|---|---|
| Meet Me Conference (Flash only) | X | X | X | |
| Station Controlled Conference | X | X | X | |

| DPNSS Service | Nodal Transit | Net-work Transit | End Node Calling/ Called | Comment |
|---|---|---|---|---|
| Permanent hold | X | X | X | |
| Three-Way Call | X | X | X | |
| Call Waiting (Direct Answer) | X | X | X | |
| Make set Busy | X | X | X | |
| Malicious call hold | X | X | X | |
| Blind Call Transfer | X | X | X | |
| Call Transfer | X | X | X | |
| Call Park | X | X | X | |
| Call Park Retrieve | X | X | X | |
| Call Pick-up | X | X | X | |
| Call Forward Don’t Answer | X | X | X | The forwarding is over UKISUP. |
| Call Forward Immediate | X | X | X | The forwarding is over UKISUP. |
| Call Forward Busy | X | X | X | The forwarding is over UKISUP. |

# Customer support

## Solution and customer support

Nortel Networks provides solution support using standard Customer Service Center (CSC) and Global Product Support (GPS) policies and procedures. For issues that cannot be resolved, contact Nortel Networks regional CSC and a representative to open a Change Request (CR). If the regional representative cannot resolve the problem, the CSC representative refers the matter to the next level of support to provide either an answer to the problem or corrective action.

Corrective action can include the following:

- amendment in a future software release
- incremental software update (patch)
- customer information change
- request for feature development to address new or changed functionality

Once the problem is resolved, the customer is notified and the CR is closed.

## Customer information

### Software release and support policy

A Succession software release consists of the Call Server PCL (solution computing load) and the Nortel Networks brand network element software loads that are required for the solution. The third-party software support policy remains in effect for third-party network element software sold by Nortel Networks in conjunction with a Succession software release.

### Ordering and support overview

A Succession Software Release can be ordered either before or within 12 months after reaching First Volume Ship (FVS) status. It is priced at the applicable contract terms for right-to-use and generic load insertion fees.

Nortel Networks does not recommend using retired (unsupported) software releases in existing offices and does not deploy a retired release to an initial (new) Succession installation or an extension. Therefore, each individual Succession Software Release application of a given software release must be scheduled to occur before the retirement of that release. This requirement must be considered when

placing an order toward the end of the active stage of a particular release.

Full software support—including both emergency-outage and non-emergency support—is available until 12 months after FVS of the release. Support is available for retired releases only under a separate service contract, and is limited to support that does not require patching or other design effort.

### Software upgrade path overview

Generally, Succession software releases reach FVS status about every 6 months. Thus, at the end of the 6 months after FVS of a Succession software release, another new release becomes available for ordering and loading. The network provider can choose either to deploy this next Succession software release in sequence or to skip to one release. If skipping more than one release is required, one or more of the skipped releases must be temporarily inserted (at extra cost) to enable loading of the desired release.

***Note:*** Any updates or exceptions to the Succession Software Release and Support Policy must be made through Solution/Service Update and/or Solution/Service Information publications. Contact your Nortel Networks representative for more information about Nortel Networks software development cycles and software administrative policy.

### Optional support package overview

The following table lists the components that require optional support packages for software support. Some of these optional support packages require the network element be upgraded to the latest software release when the standard software support expires.

#### Standard software support policy

| Components | Standard software support policy |
|---|---|
| Contivity 600 | Software support is available for the last published software release and one release back (including their associated patches, fixes, and workarounds). |
| Passport 8600/Device Manager | Software support is available for the last published software release and one release back (including their associated patches, fixes and workarounds). |

### Standard software support policy

| Components | Standard software support policy |
|---|---|
| Nortel Networks Multiservice Data Manager 15000 | Software releases are supported for 2 years (24 months) after declaration of General Availability (GA). This policy applies to PCR 3.0 and later software releases. |
| Nortel Networks Multiservice Data Manager (MDM) | Software releases are supported for 2 years (24 months) after declaration of GA. This policy applies to MDM 13.3 and later software releases. |

***Note:*** In addition to the optional support packages, Nortel Networks offers extended warranty support at an additional charge based on agreements with your account representative. For more information on the software support policies available for these components, contact your regional Nortel Networks representative.

### Service bundling

Customers can purchase the following additional services:

- software upgrades
- technical support services
- emergency recovery services such as disaster recovery options
- hardware repair services outside of warranty coverage
- applications and migration support
- audits and evaluations
- operations training
- call response coverage
- electronic software delivery
- mentoring services

### Web site information

Nortel Networks Web site, www.nortelnetworks.com, is a valuable site for customer information, support, and services. From this site, the customer can acquire information on customer service, training, and documentation, professional services, and other areas of business.

## Customer responsibilities

The information in this section is intended for use by Nortel Networks Sales, Business and Development, and Marketing personnel who are

responsible for ensuring that customers are aware of and agree with their responsibilities when discussing the solution. Additionally, these responsibilities must be written into any subsequent contracts which result from such discussions or negotiations.

This section includes the following:

- Hardware baseline
- Electronic software delivery requirements

### Hardware baseline

Unless stated otherwise, all equipment used for this Succession solution has the same hardware release lineup as that of the concurrent release.

### Electronic software delivery requirements

Information on electronic software delivery (ESD) patches is included in the document *Upgrading the Succession Network, NN10261-450.* Succession solution electronic software delivery requirements include:

- Nortel Networks Media Gateway 15000 and Nortel Networks Multiservice Data Manager (formerly Passport) software delivery

  Software for Nortel Networks Media Gateway 15000 and Nortel Networks Multiservice Data Manager software loads is delivered using BaaN 145 ordering system, and the Software Tracking and Navigating (STAN) system. STAN is a tool offered as part of the Performance On Line (POL) suite of services. This system allows customers to download software or request shipment of software CD ROMs and documentation. STAN is accessed, as part of the POL system, from the Nortel Networks web-based center located at:

  http://www12.nortelnetworks.com/cgi-bin/cnss/cs/main.jsp

- DMS and SPM software delivery

  To perform electronic software delivery, the software order codes that comprise the Succession solution load is retrieved from a software vault. The appropriate formatting (pre-mastering) is applied and the load is stored on a Nortel Networks electronic software delivery server.

  There are two main ways to employ electronic software delivery.

  — Customers using the “pull” method are notified and provided with the details and the directory structure of the load on the Nortel Networks electronic software delivery server. The customer can

connect over to the Nortel Networks electronic software delivery server to pull the load.

— For customers requiring the “push” method, Nortel Networks sends the loads to the CS 2000 Core Manager repository server or drop box. The drop box can either be customer provided in the customer’s network, or Nortel provided in Nortel’s network. The Nortel account team and Software Delivery works with customers to choose the best option based on their needs and security requirements. If a repository is set up in the customer’s network, it must be externally accessible to Nortel Networks. A customer E-mail address is required for subsequent notification of software load delivery.

The loads are transmitted in a compressed form. After they are received at the destination, decompression of the load occurs.

As an example of the load transmission time, if the available connectivity from the customer network to Nortel Networks is 1.544 Mbit/s (a T1 connection), then the transmission time for a 2-Gbyte load is approximately 3 hours. The available data connection bandwidth proportionately affects the transmission time.

After the customer retrieves the load from the Nortel Networks electronic software delivery server, the load enters their LAN/WAN infrastructure and can be stored on their local server. Thereafter, an application on the CS 2000 Core Manager is used to pull the load. The customer is expected to have the Distributed Computing Environment (DCE) application for security and authentication on the WAN to which the CS 2000 Core Manager is connected.

For satisfactory performance, Nortel Networks recommends that the customer LAN/WAN have a throughput of 300 Kbyte/s (or greater) to transmit the load files to the destination CS 2000 Core Manager. With a throughput of 375 Kbyte/s and a load size of 2 Gbytes, it takes approximately 1.5 hours to move a complete Succession load from the customer server to the CS 2000 Core Manager.

The following table lists the approximate comparative download times for throughput over selected dedicated connection links. The customer must consider what transmission time is acceptable to

their operations in order to determine the throughput requirements for their network.

**Comparative transmission times for 100 Mbytes**

| Type of data link | Data rate | Time |
|---|---|---|
| 28 Kbit/s modem | 28.8 Kbit/s | 10+ h |
| 56 Kbit/s modem, ISDN, EIU, X25, DataPac, ISDN | 56-64 Kbit/s | 5+ h |
| T1 | 1.5 Mbits/s | 10+ min |
| 10 BaseT Ethernet | 10 Mbit/s | 80 s |
| OC-3 | 84 x T1 (155 Mbit/s) | 6 s |

The peak demand for network resource for electronic software delivery occurs when a milestone software upgrade is scheduled. A lesser demand occurs when an NCL or a maintenance NCL (MNCL) is transmitted by electronic software delivery. The frequency of the former is approximately twice a year, and the later can have a frequency of approximately once a month.

In summary, requirements for electronic software delivery are:

- Customers must have their network engineer work with the Nortel Networks electronic software delivery engineer to discuss technical details.
- The link from the Nortel Networks electronic software delivery server to the customer LAN/WAN server must have a minimum throughput of 1.544 Mbit/s.
- Customers should have storage of 36 Gbyte on their server.
- The CS 2000 Core Manager and the LAN/WAN server must be integrated into the DCE cell of the customers, if DCE is used for security.
- The customer LAN/WAN must have a minimum throughput of 300 Kbyte/s to transmit Succession Network loads in a reasonable time period.

**Security requirements for DMS and SPM based-equipment software loads**

Access from the Nortel Networks electronic software delivery server to a customer's server is over a switched circuit, and user identification and password provide security. To log in from the Nortel Networks electronic software delivery server to the customer LAN/WAN, the

security algorithm is used. For Nortel Networks Multiservice Data Manager software loads, the Nortel Networks electronic software delivery system uses a secure-access system. The customer login ID and passwords are managed as part of the POL suite.

## Training and documentation

This section provides information about who to contact and where to get customer documentation and training.

### Contacting Nortel Networks for help on customer information

Contact the Nortel Networks account prime for help on customer information.

### Customer information

Nortel Networks provides customer information on a CD. The customer CD provides component-level and solution-level customer information, which includes information in the following areas:

- Basics
- Network upgrades
- Fault management
- Operational configuration
- Accounting
- Performance
- Security and administration

### Legacy information

For legacy information, refer to the DMS-100 Family suite of documents that are available through Helmsweb.

### Where to get customer documentation

Documentation for each Succession Network solution is delivered on a CD ROM.

For valuable customer information, refer to the Nortel Networks Web site for customer information, support, and services:

www.nortelnetworks.com

From this site, you can get information on customer service, training and documentation, professional services, and other areas of business.

Refer to the corresponding documentation on the following components associated with the CHS solution:

- CS 2000
- CS 2000 - Compact
- CS 2000 Management Tools
- Gateway Controller
- Nortel Networks Multiservice Switch 15000 and 20000
- Nortel Networks Multiservice Data Manager
- MDM
- UAS
- USP
- USP - Compact
- XA-Core

### BCM

BCM information is located in the Business Communications Manager 3.6 collection in Helmsman. In particular, refer to:

***Note:*** These documents are also distributed on each BCM hard drive, and can be accessed through the BCM's Unified Manager interface.

| BCM documents | Title |
|---|---|
| PO609326 | Programming Operations Guide |
| PO609327 | IP Telephony Configuration Guide |
| PO609619 | BCM 3.6 Software Upgrade Guide |

### CS1000 and CS 1000M

Refer also to the following CS1000 and CS1000M documents located in the Succession 3.0 collection in Helmsman Express.

| CS 1000 / CS 1000M | Title |
|---|---|
| 555-3001-000 | Library Navigator (contains a description of all NTPs in the collection) |
| 555-3001-213 | IP Peer Networking |

| CS 1000 / CS 1000M | Title |
|---|---|
| 555-3001-363 | IP Trunk: Description, Installation and Operation |
| 553-3001-365 | IP Line: Description, Installation and Operation |
| 553-3031-258 | Succession 1000 System: Upgrade Procedures |

**Meridian 1**

Meridian 1 information is located in the **Meridian 1** collection in Helmsman Express.

**MCS 5100**

For SIP Converged Desktop Services information on the MCS 5100 3.0 documentation suite, refer to the **Multimedia Communication Portfolio** collection in Helmsman Express.

**CICM documentation**

Refer to the following Centrex IP Call Manager (CICM) documentation located in the **Succession Network Solutions** documentation under **Global - Carrier Hosted Services Solutions** in Helmsman Express.

| CICM | Title |
|---|---|
| NN10027-111 | CICM Series 2.5 Product and Technology Fundamentals |
| NN10027-113 | CICM Series 2.5 Etherset Installation Guide and User Manual |
| NN10182-113 | CICM Series 2.5 m6350 SoftClient Installation Guide |
| NN10183-114 | CICM Series 2.4 m6350 SoftClient Branding Kit |
| 972-5551-901 | m6350 TAPI Service Provider Installation and Troubleshooting Guide |
| NN10234-100 | CICM Basics |
| NN10230-461 | CICM Upgrades |
| NN10233-911 | CICM Fault Management |
| NN10240-511 | CICM Configuration Management |
| NN10244-811 | CICM Accounting Management |

| CICM | Title |
|---|---|
| NN10248-711 | CICM Performance Management |
| NN10252-611 | CICM Security and Administration |

### Session Server

In (I)SN07, the CHS architecture has expanded to include the Session Server.

Refer to the following Session Server documentation located in the **Succession Network Solutions** documentation under **Global - Carrier Hosted Services Solutions** in Helmsman Express.

| Session Server | Title |
|---|---|
| NN10332-911 | Session Server Fault Management |
| NN10333-111 | Session Server Basics |
| NN10338-511 | Session Server Configuration |
| NN10342-711 | Session Server Performance Management |
| NN10346-611 | Session Server Security and Administration |
| NN10349-461 | Session Server Upgrades |
| NN10332-911 | Session Server Fault Management |

### RTP Portal

For more information about the dedicated configuration to support MCS RTP Media Portals associated with the CS 2000, refer to the following table of documents located in the **Multimedia Communication Portfolio** collection in Helmsman Express.

| RTP Media Portal dedicated configuration | Title |
|---|---|
| NN10369-111 | CVoIP Management Module Basics |
| NN10368-111 | CVoIP Database Module Basics |
| NN10370-111 | CVoIP System Management Console Basics |

For more information on the MCS RTP Media Portal when in association with a CS 2000 refer to the following document located in the **Multimedia Communication Portfolio** collection in Helmsman Express.

| RTP Media Portal interop with CS 2000 | Title |
|---|---|
| NN10367-111 | CVoIP RTP Media Portal Basics |

For more information on the RTP Media Portal, refer to the following document located in the **Multimedia Communication Portfolio** collection in Helmsman Express.

| RTP Media Portal | Title |
|---|---|
| NN10035-111 | MCS 5200 RTP Media Portal Basics |

### MCS 5200 interworking

For MCS 5200 interworking information, refer to the following document.

| MCS interworking | Title |
|---|---|
| NN10033111 | MCS 5200 Interworking |

For more information on the MCS 5200 documentation suite, refer to the **Multimedia Communication Portfolio** collection in Helmsman Express.

### Where to get training information

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

***Note:*** For the most recent curriculum information, contact Nortel Networks Training and Documentation representative. For enrollment assistance, contact Training registration at 1-800-4-NORTEL (1-800-466-7835), express routing code #280.

## Professional services

An extensive set of professional services accompany the IP solutions. These services are offered in addition to the engineering, installation, and commissioning services that are part of the base solution.

Services are defined and selected according to the needs of the customer and range from turnkey solutions to products that assist the customer in specific tasks and in acquiring needed skills.

The initial set of services offered as part of the IP solutions are as follows:

- business and market planning services
- network planning and design to cover the packet network, TDM network, operations networks, and access networks
- operations planning realization
- business contingency and disaster recovery planning
- program and project management
- translations for CS 2000 and for the Nortel Networks Media Gateway (formerly Passport) 15000
- packet configuration
- LAN design and setup and manager setup
- MSS and security planning, implementation, and integration
- network test and verification
- feature migration services
- facility cut-over services
- surveillance, maintenance, provisioning, and customer care services
- enhanced Technical Assistance Service (TAS) support services
- removal of old equipment

Additional services are available on a custom basis, if required. For more details, refer to the Service bundling section.

### Operations support services

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

Requests and operational problems are classified according to severity and overall effect on the system.

### Routine TAS, S1 and S2

The service provides the following help for customers:

- coverage during Nortel Networks business hours or as scheduled with a TAS supervisor
- response from Nortel Networks as soon as practical, according to the severity of the problem. Assistance is provided through telephone and/or remote access.
- diagnosis of cause and recommended actions to restore operational stability
- TAS-initiated on-site assistance made necessary by non-emergency conditions and covered by the Service and Support Plan (S&SP)
- Customer-initiated, on-site assistance available through mutual agreement and dispatched within 4 hours of mutual agreement. Additional charges are billed for travel and per diem expense, plus the current hourly rate.

Technical Assistance Support can be reached between the hours of 8:00 a.m. and 5:00 p.m. (CST), Monday through Friday.

### ETAS, E1 and E2

This service provides the following help for customers:

- Coverage 24 hours a day, 7 days a week
- Immediate assistance through telephone and/or remote access
- Diagnosis of cause and recommended actions to restore operational stability
- ETAS-initiated on-site assistance made necessary by emergency conditions and covered by the S&SP
- Customer-initiated on-side assistance, available through mutual agreement and dispatched within 4 hours of mutual agreement Additional charges are billed for travel and per diem expense, plus the current hourly rate.

Emergency Technical Assistance Support can be reached 24 hours a day, 7 days a week.

### Escalation procedure

If customer needs are not met at the TAS representative level, the matter can be escalated by contacting the following persons, in sequential order:

- Manager, Technical Assistance Service
- Senior Manager, Technical Assistance Service
- Director, Technical Assistance Services
- Director, Service Operations

# Carrier Hosted Services Configuration Management

## What's new in (I)SN07?

Initial Carrier Hosted Services (CHS) configuration is performed by Nortel Networks installation personnel.

Refer to the following procedures reflected in (CHS) Configuration Management:

- Enabling Advice of Charge on page 133
- Enabling VCAC SOC on page 139

## Integrated Element Management System

Many fault, configuration, accounting, performance, and security activities in (I)SN07 may now be performed using the Integrated Element Management System (Integrated EMS). For more information, refer to the *Integrated EMS Basics NTP, NN10329-111.*

To launch the CS 2000 GWC Manager or the CS 2000 SAM21 Manager, refer to the following procedures in the *Integrated EMS Basics NTP, NN10329-111:*

- "Launching GWC Manager"
- "Launching SAM21 Manager"

# Enabling Advice of Charge

## Overview

Advice of Charge (AOC) gives the CS2000 Call Server the ability to send network incurred charges to the ISDN subscriber within call control or facility messages.

For Advice of Charge (AOC) datafill considerations, refer to “Enabling Advice of Charge” on page 133

For APDU timing message considerations, refer to “Conditions for APDU timing messages” on page 134

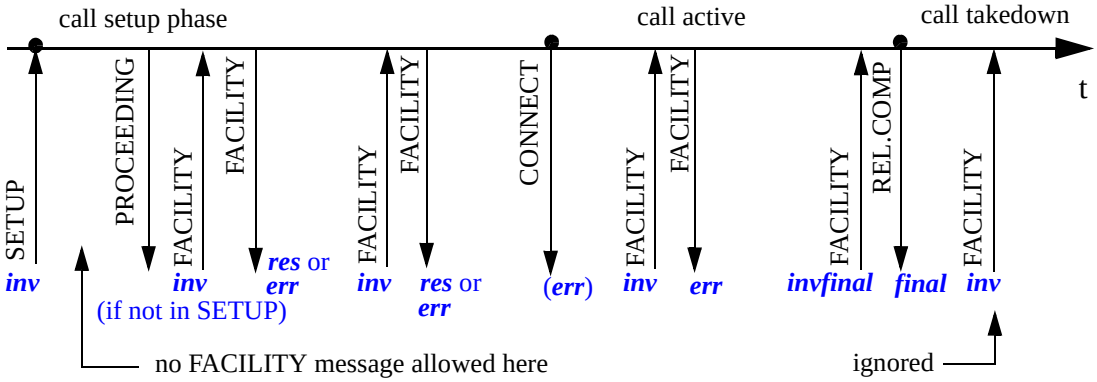
The following figure shows the per-call sequence of AOC requests and responses on a relative time scale, as supported by this activity.

The following AOC APDU types are used.

**AOC APDU types**

| Request | Definition |
|---|---|
| inv | invoke APDU requesting AOC-D |
| res | returnResult APDU reporting positive acknowledgement for an AOC-D request |
| err | returnError APDU reporting negative acknowledgement for an AOC-D request (with error values ‘notAvailable’ or ‘supplementaryServiceInteraction NotAllowed’) |
| invfinal | invoke APDU requesting AOC-E |
| final | invoke APDU reporting AOC-E final charge |
| | Bullets on the time axis delineate call phases. Only messages relevant for AOC request handling are shown. |

### Timings of AOC requests and responses




### Conditions for APDU timing messages

APDU timing messages include the following conditions:

- An inv APDU may be sent in either SETUP or FACILITY message, but not in both.
- An inv APDU in a FACILITY message may be sent after PROCEEDING and before CONNECT. Instead of PROCEEDING there may be a SETUP ACK message.
- An err APDU in the CONNECT message will only be sent if an inv APDU was previously received, and the AOC service is not provisioned in table TRKOPTS.
- An inv APDU received after CONNECT and before RELEASE will be replied with an err APDU in FACILITY (supplementary Service Interaction Not Allowed).
- An inv APDU received after RELEASE COMPLETE will be discarded by the CS2000 without reply.
- An invfinal APDU may be sent in a FACILITY message up to the beginning of the call takedown phase.

  Please note that H323 does support a special forward clearing procedure for AOC calls: the originating gateway may send getFinalCharge.inv in a FACILITY message which triggers a call release initiated by the CS2000.

## Application

Use this procedure to provision the Advice of Charge (AOC) option. The AOC option can be provisioned as follows:

- for trunk groups, the AOC option is provisioned through table TRKOPTS

  Refer to “Provisioning AOC through table TRKOPTS” on page 136.

- for GWCs, the AOC option is provisioned through table SERVRINV

  Refer to procedure *Provisioning Advice of Charge, Gateway Controller Configuration Management document, NN10205-511.*

- for the communication server, the AOC option is provisioned through the following Software Optionality Control (SOC) codes:

  — NETK0024 (Network AOC tariff)

  — NSUP0020 (NAOC/PCA Supp Svcs)

  — NSUP0023 (PCA SW Metering Support for Billing)

  — PBXT0011 (ETSI PRI Info)

  — PBXT0018 (QSIG AOC)

  Refer to “Provisioning AOC through SOC” on page 137.

### Restrictions and limitations

The following restrictions and limitations apply to AOC:

- Sending of AOC charge information as currency units is not supported for H.323 trunks.
- AOC calculation based on the charging interval is not supported.
- A delta may exist between the number of charge units saved in the AMA record by the CM (controlled by SOC NSUP0023) and the number of charge units provided by the AOC metering counter in the GWC. This is due to charge interval-based calculations done in the CM.
- The GWC calculation of the AOC does not influence or change AMA records extension. There are no direct interactions between the AMA billing system and the AOC functionality in the GWC.
- AOC on H.323 is only supported for bearer cals. AOC on H.323 for non-bearer calls is not supported. Facility IEs with AOC operations for these calls are transparently passed through the CS 2000.

## Prerequisites

None

# Action

### Provisioning AOC through table TRKOPTS

***At the MAP terminal***

**1** Start the table editor, and access table TRKOPTS by typing

```
> TABLE TRKOPTS
```

and pressing the Enter key.

*Example response:*

```
TABLE: TRKOPTS
```

**2** Set the following fields:

- AOCD - to enable or disable AOC-D. If set to Y, facility messages are sent to provide the ISDN subscriber with the charge unit count on a regular basis during a call
- AOCE - to enable or disable AOC-E. If set to Y, the final charge unit count is sent at the end of the call in a standard call control message during the disconnect phase
- DSCNT - to specify the discount class number to which the subscriber belongs
- AOCREL - to enable or disable releasing a call if AOC is not available, that is, if the datafill on both the CS 2000 and GWC is not complete. Emergency calls and Priority calls are not released although this flag is set.

  For H.323, you must set AOCREL to N, otherwise a GW misconfiguration may cause calls to be released.

  If AOCREL is TRUE, the Q.931 RELEASE COMPLETE message contains no AOC information.
- AOCCHGOV - to enable or disable tariff and discount changeover during time of day changeover. This flag also controls if changes in the tariff tables apply directly to active calls.
- PROTOCOL - to choose the AOC protocol.

  If set to KEYPAD, the AOC information will be sent in the national defined KEYPAD protocol to the user. If set to FUNCTIONAL, the FUNCTIONAL protocol will be used instead.

  For H.323, you must set PROTOCOL to FUNCTIONAL.
- UNITS - to choose which units shall be used to send the charging information.

If set to CURRENCY, the charging information will be given in currency units of the specified market.

If set to CHARGING, charging units will be used.

For H.323, you must set UNITS to CHARGING.

- REQUEST - to choose if AOC is only invoked if it is explicitly requested by the user if the SETUP message (REQUEST = Y) or if it is invoked for every call (REQUEST = N).

  For H.323, REQUEST must be set to Y.

**3** Exit the table editor.

**4** You have completed this procedure.

### Provisioning AOC through SOC

#### *At the MAP terminal*

**1** Set the right-to-use (RTU) flag for the required SOCs by typing

> **ASSIGN RTU <keycode> TO <SOC>**

and pressing the Enter key.

*where*

**keycode**
is the keycode Nortel Networks provided you

**SOC**
is the SOC code (NETK0024, NSUP0020, NSUP0023, PBXT0011, PBXT0018)

**2** Activate the SOC code by typing

> **ASSIGN STATE ON TO <SOC>**

and pressing the Enter key.

*where*

**SOC**
is the SOC code (NETK0024, NSUP0020, NSUP0023, PBXT0011, PBXT0018)

**3** You have completed this procedure.

# Enabling VCAC SOC

## Overview

The following procedures address the Computing Module (CM) datafill changes and treatment on the XA-Core required for the VCAC-SOC option (CS2Q0002).

**ATTENTION**

For H.323 gateways using VCAC, datafill is **REQUIRED** in table TMTMAP.

Treatment NBLN **must** be datafilled for the signaling protocol being used on the H.323 trunk, and this treatment must release the call back to the originating node. The treatment **must not** be played locally.

### Datafilling table TMTMAP for NBLN

***at the command line***

**1** Refer to the following example to datafill Q767 signaling for NBLN in Table TMTMAP.

***Note:*** Use the 'Normal unspecified' release cause to send the call back to the originator:

**Example datafill for TABLE: TMTMAP**

```
Q767 NBLN     ALLBC  ISUP  NOLOCAL   NORMUNSP RPRIVNET N
```

### Datafilling the CM for VCAC-SOC and treatment

**ATTENTION**

For line gateways using VCAC, datafill is **REQUIRED** in table TMTCNTL.

Treatment NBLN **must** be datafilled and **must** be set to a tone before you enable the VCAC SOC option.

***at the command line***

**1** Datafill the NBLN treatment in table TMTCNTL:OFFTREAT

**2** Refer the CLLI to a tone, not an announcement.

**Example: NBLN Y S  CONGESTION**

### Enabling the VCAC SOC option on the CM

**ATTENTION**
You **must** datafill line treatment NBLN, and you **must** set treatment NBLN to a tone **before** you enable the VCAC SOC option.

***at the command line***

**1** Type the following to set the Right to Use (RTU) flag to Y and enable the VCAC-SOC option:

**ASSIGN RTU <keycode> TO CS2Q0002**

***Note:*** The RTU flag is set to Y.

**2** Type the following to change the option state from IDLE to ON:

**ASSIGN STATE ON TO CS2Q0002**

### Disabling the VCAC SOC option on the CM

***at the command line***

**1** Type the following to set the Right to Use (RTU) flag to Y and disable the VCAC-SOC option:

**REMOVE RTU <keycode> FROM CS2Q0002**

**2** Type the following to change the option state from IDLE to ON:

**ASSIGN STATE IDLE TO CS2Q0002**