Carrier VoIP

Carrier Hosted Services Basics

NN10234-100

Document status: Standard
Document version: 06.02
Document date: 20 October 2006

New in this release

The following section details what's new in Carrier Hosted Services Basics (NN10234-100) for (I)SN09U.

- "Features" (page 3)

Features

See the following sections for information about feature changes:

- "VoIP VPN (H.323)" (page 3)
- "Centrex IP services" (page 7)
- "Internet Transparency services" (page 10)
- "SIP lines/services" (page 12)
- "Gateway Controller" (page 25)

VoIP VPN (H.323)

Unless otherwise noted, the functionality applies to all CHS customers and markets.

- Voicemail/Unified Messaging support

  This new feature includes support for a packet-based connection via SIP. This feature supports H.323 access to hosted voice mail (VM) systems, as well as enterprise based VM systems. Supported Communication Server 2000 (CS2000) end points, for example Centrex lines, have access to the enterprise VM systems hosted off a Nortel Succession 1000 or BCM. Likewise, the H.323 end points within the enterprise have access to both local and remote hosted VM systems. Traditional and IP based solutions are supported.

  The following communication protocols are supported:

  — Simplified Message Desk Interface (SMDI) based on GR-283-Core

  — Network Messaging Service (NMS) based on GR-866-Core

  — Message Waiting Service (MWS) using Primary Rate Interface (PRI) based on GR-866-Core

— MWI Service using ISDN based on GR-866-Core

— MWI Service using SIP based on RFC3265 and RFC 3842

Supports interoperability between the VoIP VPN endpoints/user agents:

— CS2000 SIP lines (i2001, i2002, i2004, 3rd party hard clients, PC Client)

— MCS

  – Conferencing Server

  – i2001, i2002, i2004

  – PC Client

  – Web Client

  – SIP PRI gateway

— PVG

— MG9K IP

— I/W SPM

— PacketCable (NCS) entities such as MTAs, E-MTAs, CMTS

— Mediatrix 1104/1124

— Centrex IP (CICM)

— Westell liQ2032

— Cisco IOS gateways (2621/3640)

— BCM

— Model 50 (BCM)

— Audiocodes MP 104/108

— H.323 signaling proxy (Cisco IOS gatekeeper, S1K/1KM GK)

— Cisco Call Manager

— S1K/1KM (SIP/H.323)

Users connected through the following supported CS2000 endpoints can leave voice messages for H.323 endpoints served by the enterprise-based VMS:

— MCS

  – Conferencing Server

  – i2001, i2002, i2004

  – PC Client

  - Web Client
  - SIP PRI gateway

- PVG
- MG9K IP (NA)
- I/W SPM
- Mediatrix 1104/1124
- Centrex IP (CICM)
- Westell liQ2032
- Cisco IOS gateways (2621/3640)
- BCM
- Model 50 (BCM)
- H.323 signaling proxy (Cisco IOS gatekeeper, S1K GK)
- Cisco Call Manager
- S1K

- H.323 Clear Channel Data (UDI) Support

  The bearer capability (BC) is an ISDN layer 3 service indication that defines the characteristics of a given call. The BC of a call is indicated in the Q.931 SETUP message and it is used to distinguish among the different types of voice and data calls. CCD/UDI is an ISDN term to describe the ability (BC) to transfer any bit pattern over a digital channel. Current H.323 standards (H.323, H.225 or H.245, H.323 implementation guide) do not provide specifications for the handling of CCD/UDI within H.245 (for example in TCS, OLC commands). In SN07, Bearer capability (BC) transparency was implemented, and patched back to SN06.2. ISDN CCD/UDI call requests to and from the H.323 GWs need to be supported, once Q.931 Bearer Capability is allowed to pass transparently over the H.323 interface.

- Release Line Trunk (RLT) H.323 support

  This feature adds the Release Line Trunk (RLT) capability to the H.323 protocol. RLT is used to free unused call signaling paths that result from call path changes such as call forwarding. The RLT capability will only be used by CS 1000 components that communicate with the Gateway Controller over H.323 protocol. This capability is not available to all third party H.323 compliant gateways.

  The CS1K is viewed by the GWC as an H.323 gateway. The GWC is the gatekeeper for the H.323 protocol, and as such, is responsible for establishing the H.323 connections and passing the call processing

related messages to the CS2000. The RLT functionality is implemented by adding a Facility message component to existing H.323 messages. The GWC function is to ensure that the RLT facility is passed from the H.323 input to the CS2000, and that the RLT facility is passed from the CS2000 input to the H.323 output.

- GWC H.323 Trace Tool

  This feature adds message trace capability for H.323 messages that traverse the IP network over TCP. The GWC packet trace tool is enhanced to capture both the RAS messages using UDP transport and the call processing messages using TCP transport that traverse the network and view them using Ethereal tool. To facilitate H.323 problem debug in the field, an additional capture is added for the GWC internal Q.931 messages used by the GWC TPT task to communicate with the Core. This allows the user to compare the H.323 Q.931 content against the TPT Q.931 content for missing fields or incorrect content.

  Users can trace:

  — RAS messages

  — Call Processing messages between GWC and H.323 Gateway

  — Call Processing messages between GWC H.323 app. And TPT bound for/to Core

- COLP/COLR Functionality for H.323 Gateways via QSIG Support for the ISDN supplementary services COLP (COnnected Line Presentation) and COLR (COnnected Line Restriction) for H.323 gateways. QSIG signalling is used between the H.323 GWC and the Core. For a given call, party information for the connected party is conveyed in the CoNnected Number IE in the QSIG CONNECT message. This is existing QSIG functionality. This feature implements the necessary H.323/QSIG interworking at the H.323 GWC.
- Provision H.323 gatekeeper for RAS-less operation Registration, Admission and Status (RAS) messages allow endpoints to communicate their capabilities to the H.323 Gatekeeper. H.323 gateway/gatekeeper can be provisioned as RAS-less using the CS2000 Management Tools interface.
- Secure CS2000 messaging:

  IPSec and IKE configuration options have been added to the CS2000 configuration tools, allowing

  — enables IPSec for secure messaging between the IEMS and CS2000

  — configuration of IPSec and IKE parameters for secure messaging between the CS2000 and the GWC

- Int'l H.323 2CLI delivery

  Introduces support for Two Calling Line Identities (2CLI) for International customers. This functionality extends the existing DMS/CS2000 functionality to support 2CLI on H.323 [Q.SIG] VoIP VPNs.

  2CLI involves two calling line identities:

  — The Network Number (NN) identifies the actual network termination point that the call originates.

  In France, NDI refers to the NN and NDS refers to PN.

  — The Presentation Number (PN) is a dialable number displayed by the caller to the called user.

  Both the CS2000 and CS2000–Compact support 2CLI on H.323 VoIP VPNs. The functionality is optional and controlled per trunk group.

Centrex IP services

Unless otherwise noted, the functionality applies to all CHS customers and markets.

- QOS for Centrex IP Client Manager (CICM) lines

  Enhances QoS reporting for newer IP Phone 200x devices. The newer phones support RTPCX protocol, which allows the phones to report a variety of end-of call statistics, such as the following information:

  — jitter

  — latency

  — delay

  — packets sent

  — packets lost

  — packets received

  The following devices support the collection and reporting of end-of-call QOS stats:

  — CICM QOS reporting for client-side media path via H.248 signaling to GWC

  — Media Server 20x0 QoS reporting via signaling to GWC

  — Mediant 2000/3000 QoS reporting via signaling to GWC

  — RTP Portal QoS reporting via signaling to GWC

  Supported QoS parameters include packets sent, packets received, octets sent, octets received, packet lost, jitter, inter-arrival latency.

- Pre-answer CODEC Negotiation For Centrex IP Client Manager (CICM) Lines

  For CICM Originating Lines, the CICM has to accept a change in the codec (G.711 To G.729 Or Vice Versa) prior to the terminating call being answered. This functionality allows CICM to support applications such as MCS 5200 that can re-route calls through Gateways with different CODECs.

  This feature introduces support for pre-answer and mid-call IP address and CODEC renegotiation in the CICM 9.0, and eliminates the requirement for a Media Portal for CICM lines in a flat network.

- Support of i2210, i2211 WiFi CICM clients

  The WiFi phone emulates the i2004. The functionality of the services are offered via the Function key at the bottom of the set. i2210 should support UNIStim Security or method to disable security for these specific phones until vendor supports UNIStim Security. The differences between i2210 and i2211 is physical robustness not logical functionality.

  introduces two new 802.11b compliant VoIP handsets: the i2210 and the i2211. The key features of the new devices are:

  — The 2210 is a cost-effective low end model and the 2211 is a high end unit with advanced features.

  — Both handsets support the UNIStim signaling protocol so they can access most of the Meridian and Succession 1000 feature set, within the limits of the handsets.

  — Both handsets can be connected to an external application server which can deliver third party applications to the sets.

  — The 2211 handset has a Push to Talk feature.

- CICM Robustness patching and Selective Binary Component Patching

  In release (I)SN09FF, the Maintenance Release (MR) process is complimented with new functionality to allow the application of patches containing application, operating system, or third party corrective content to the CICM or CICM-EM. Patches will be built and released by Nortel CICM GNPS, and will be applied onto the CICM or CICM-EM via the maintenance pages on the CICM-EM.

  This feature provides the following enhancements:

  — —automated delivery of maintenance releases through Network Patch Manager (NPM)

  — manual and automated back-out procedure if a maintenance release fails to apply or creates problems with CICM

— focus content of maintenance release on software fixes, and restrict introduction of feature content within a maintenance release

— faster deployment of critical software fixes

— closer integration between CICM and NPM

Patches

— are delivered on an “as needed” basis

— contain a single fix for a specific issue.

— may contain application, operating system, or third party corrective content, but typically not a combination of the three.

— only replace application binaries needed to deliver the corrective content.

— installation does not always require a system restart.

- Media Portal Removal for Inactive CICM Clients

  This feature removes the dependency of the requirement that Media Portals be deployed in all CICM networks even if the NAT traversal capabilities usually associated with MPs are not required. Current behavior can continue without the requirement for an MP.

- CICM Enhancement to IP Phone 2001

  The IP Phone 2001 was designed as a low cost alternative to the 2002 and 2004 terminals and with this cost reduction, the IP Phone 2001 was designed without any feature keys. This feature provides a more manageable approach to feature interactions in the 2001 and emulations, such as the 2033.

  The soft keys on the IP Phone 2001 are used as feature keys, acting in the same manner as the feature keys provided on the 2002/2004 phones. Feature Activation is available to the user from the Call Services menu, available from the main menu.

  Features provisioned on user lines are available when users are logged into an IP Phone 2001 terminal. Feature keys assignments are made by two methods:

  — The first time a user logs into the IP Phone 2001, the soft keys are automatically provisioned for them, based on the assignments made on the IP phone. The method for this provisioning is based on the numerical order of the feature keys on the core.

  — The new Call Services menu presents the entire list of features that a user has assigned. From here, a user can activate a feature by selecting it from the menu, or reassign it to one of the soft keys, thus providing an interface suitable to them.

Internet Transparency services

Unless otherwise noted, the functionality applies to all CHS customers and markets.

- H.248 and SCTP NAT Traversal for CPE Gateways

  —

  CPE gateways such as the MG3200 (Mediant 2000) support packet network access for legacy PBXs. Such gateways use H.248 for device-media control and IUA/SCTP for signalling backhaul. If the gateway is behind a NAT, the Communication Server 2000 (CS2000) GWC needs to discover the IP address to use for the gateway, because the source IP address in packets received from the gateway is a public IP address on the NAT, not that of the gateway. The IP address discovery process used to achieve this is initiated by the gateway when it is brought into service (or when its IP address changes), and the connection is maintained via heartbeat messaging.

  IP address discovery for small gateways controlled via MGCP was implemented by a previous feature. This feature implements it for H.248 and SCTP. GWC datafill for a CPE gateway behind a NAT specifies the gateway name, the NAT that it is located behind, and an IP address of 0.0.0.0 to indicate that IP address discovery is required. Separate address discovery processes are used for H.248 and SCTP, which are functionally equivalent but differ in some details.

  Currently, neither the H.248, nor the SCTP protocols can work over a NAT without special datafill in place. This feature enables these protocols to work automatically when the gateway is located behind a NAT. The CS2000 and the GWCs must remain within the core network.

- Internet Transparency Media Proxy

  The Media Proxy selection feature allows customers to provision Media Proxy preferred groups. These groups are used at Call Setup time to select the most appropriate Media Proxy for the VoIP data stream. Customers are able to better allocate MPs, taking into account speed/cost/locale and reliability of the chosen Media Proxy.

  Customers facilitate the creation, deletion, and alteration of Media Proxy Groups (MPG) by means of a graphical user interface (GUI) incorporated into the CS2000 management tools GUI. A MPG consists of up to 5 MPs selected from a list of available MPs and are allocated to Itrans middleboxes.

- RTP Media Portal now detects lost connections and notifies the CS2000 GWC. RTP Media Portal has two timers: an inactivity timer and a log call duration timer. If either timer expires, the RTP Media Portal notifies the CS2000 GWC.

— If the call is active, the CS2000 GWC resets the times. The call continues.

— If the call is inactive, the CS2000 GWC notifies the RTP Media Portal to clear the connection.

- TDM trunk call recording

  Calls can be recorded by a call recording device which taps into the TDM trunk involved in the call. The CTI server (an ICM host) receives the information from the CS2000 through the existing ICM messages that include the PM Type, PM Number, Carrier Number and Channel Number of the trunk.

  The TDM trunk information is sent to the call recording device by a CTI server.

- Provisioning of CS2000 trunks on a GW and Carrier basis

  Trunk TID's on CS2000 core based on GW and carrier, using CM tables GATWYINV and a new table, GWEPCARR.

  Previously, provisioning GWs and carriers for CS2000 trunking was done on the CS2000 EM (SESM). Provisioning of trunk groups and individual trunk members was done in the CS2000 CM. A trunk member in the CM was mapped to a channel on a carrier in SESM using a node and terminal number (TID). No GW or carrier information was available on the CM for trunks configured on gateways.

  The trunk data can now be provisioned in a one-step process, for North America and International software loads:

  — new table GWEPCARR

  — CktLoc command in MAPCI, TTP level modified to display Gateway and Carrier information

- Size of the ICM temporary queue increased to support 1024 messages at a time

  This ensures that during high traffic conditions, message loss is minimized. The temporary queue size is increased for both X.25 and TCP/IP links.

- NI2 PRI/ISUP user-to-user information (UUI) over Switch Computer Application Interface (SCAI) support

  The CS2000 provides a SCAI messaging link to a host computer, allowing applications running on the CS2000 to communicate with the host applications. To provide this support, the ICM message size is increased from 256 to 512 bytes.

- CS2000 DPNSS Message Waiting Indicator for Unified Messaging Server (UMS)

  The UMS can connect to the CS2000 by SIP line or SMDI, and send MWI activation or deactivation requests to the CS2000.

- Compact Call Agent: Geo Support for Gigabit Ethernet (GigE)

  This feature enables synchronization of data between two Compact Call Agent (CCA) blades over a Gigabit Ethernet link. The current design uses Fiber Channel (FC) for keeping data synchronized. This feature provide an additional option of synchronization over GigE.

  GigE is an Ethernet technology that provides an alternative for high-speed data transmission (1 gigabit per second) to achieve memory synchronization between active and inactive CCA. It provides an Ethernet transport option between two MCPN905-based CCA cards.

SIP lines/services

The main new Session Server capability in release (I)SN09FF is support for SIP Dynamic Packet Lines (DPLs). These are hosted on Session Servers under GWC control. The Session Servers are variously referred to as Session Server - Lines (SSL) units, Multimedia Session Manager (MSM) units or simply as Session Managers. They provide signalling gateway functionality, not media gateway functionality. For example, SIP signalling terminates on the MSM, but media streams terminate on remote SIP clients, which may be dedicated terminals or PC-based soft clients.

Each Session Server supports a maximum of 35,805 DPL endpoints and there can be up to five Session Servers in a CS2000 configuration, which means that the maximum number of DPLs that can be supported by a CS2000 is 179,025. DPLs are assigned to Virtual Media Gateways (VMGs), each of which can support up to 6,138 DPLs belonging to six line groups with 1,023 endpoints each.

Signalling between the GWCs and the Session Servers they control is based on the Generic Call Processing (GCP) architecture. GCP messaging is used both for call control and device/media control. The VMGs on a given Session Server may be controlled by different GWCs; the VMGs all use the same logical IP address, that of the Session Server, but each VMG has a unique VMG name for GWC use.

Release (I)SN09FF support for SIP DPLs is provided by a number of related activities, which address the development work required on one of the different components involved (Core, GWC and Session Server).

What's new for SIP lines/services in CHS Solutions (I)SN09FF:

- Subscriber Edge Service Manager (SESM) enhancements:
  - additional provisioning for SIP lines using SERVORD and query commands

— additional auditing data from SIP lines, such as directory number (DN), and virtual media gateway (VMG) information

— maintenance enhancements for the command line user interface (CLI), eventually to replace the lines test position (LTP) of the MAPCI

- Non-Call Associated Signaling (NCAS) Link for Services The NCAS link provides a non-call associated link between the CS2000, the Session Server Trunks, and the CS2000 core. The NCAS link is used by the SIP network support using RFC 3842. The SCPLite functionality will provide the NCAS link from the Session Server into the core. This link allows TCAP on IP support between the Session Server and the core. The SCPLite additionally provides various APIs to provide NMS functionality between core and Session Server. Additionally, the SCPLite logic allows AIN and INAP messages to be sent between the Session Server and the core.

  The Message Waiting (MWT) service is a CS2000 Core-based service. The complete service includes voice mail, communication link between CS2000 core and VM, the MWT service control in the core, end user devices to provide MWT Indication (MWI) and core based Redirection Services, such as Call Forward Do Not Answer. The feature extends the MWT service to include the SIP network. It develops and expands necessary software in Session Server and Core in order to support SIP VM and SIP networked MWI in a converged network.

- GWC Support for SIP Lines

  One of several activities in (I)SN09FF that together provide support for SIP Dynamic Packet Lines (DPLs) on CS2000. This feature focuses on the GWC component of the development work. GWC support for SIP DPLs has been designed to achieve the following specific objectives:

  — Support of DPLs on GWCs with the LARGE_LINEINTL GWC profile

  — Support for six line groups per Virtual Media Gateway (VMG).

  — Support for a total of 6,138 (6 x 1,023) DPL endpoints per VMG.

  — Support for an endpoint naming convention that allows DPL endpoints to be mapped on to CS2000 Core LENs.

  — Support of GCP architecture and messaging for Session Server control

  — Support for new DPL gateway profile, new DPL trmtype and new DPLEX exec lineup.

  — Allowing the VMGs on a given Session Server to be controlled by different GWCs; the VMGs all use the same logical IP address, that of the Session Server, but each VMG has a unique name for GWC use.

— Allowing a given GWC to control both SIP DPL line groups and CentrexIP line groups

- SIP Lines Client Services Interworking on core

  MWT Support for SIP Lines, for example (de)activation of the Message Waiting Indicator (MWI) on the line. For SIP lines, MWI is provided either by the SIP client or by an edge device, such as Optical Network Terminator (ONT). MWI (de)activation is triggered by receipt of a SIP NOTIFY message with Message Waiting header from the network and/or voice mail system. For SIP lines, only Message Waiting Lamp (MWL) is valid in CS2000 voice mail datafill, not Stutter Dial Tone (STD). The type of notification actually provided depends on the end user device.

- Provisioning for Media Proxy insertion for SIP lines

  In release (I)SN09FF, SIP lines is supported on the CS2000 through the Session Server. It is necessary to allow SIP lines to reside in private VPNs, as is already provided for fixed VoIP line gateways and CICM terminals. This is achieved by appropriate Media Proxy insertion by the CS2000. This feature provides the provisioning necessary to support Media Proxy insertion for SIP lines.

  During a call, the VPN ID of a SIP line is determined by the Session Server, while the VPN ID of a fixed VoIP/CICM line is determined by the GWC, through SESM provisioned IP-VPN (NAT) Network Zones and distributed VPNs. In order to allow correct comparison if the VPN IDs at the two ends of a call and Media Proxy insertion if required, the VPN IDs GWC and Session Server must be consistent. This feature ensures that both the GWC and the Session Server have the same VPN ID information to allow the correct insertion of Media Proxies, by flow-through provisioning of IP-VPN (NAT) network zones and Distributed VPNs from SESM to the Session Server.

- Packet Media Anchor for SIP Lines

  This feature extends the existing PMA functionality available to Dynamic Packet Trunks (DPTs) to Dynamic Packet Lines (DPLs) such as SIP lines. This feature allows the Packet Media Anchor (PktMA) to be inserted into the bearer path of a line BWC when the DPL needs to collect additional digits or play tones that cannot be played by the DPL gateway. SIP lines use the PMA to access CS2000 based features that require the collection of additional digits. The PMA is needed for the following:

  — collection of digits required after the initial SIP invite was sent

  — collection of additional digits for CS2000-based North American and International features such as Call Screening Override and Speed Dial Programming

— playback of certain application tones not played by the session server or end user

DPLs also require a mechanism to remove the PMA from the call when its use is no longer required. The removal of the PMA is not currently supported and represents an area of new functionality for the PMA.

- Session Server Support for Enhancement to Interoperability with MCS Software support for option vnd.nortelnetworks.digits

  Enables a Session Server - Trunks to support OOB (Out Of Band) DTMF tones when communicating with a far-end SIP server that does not support RFC2833, and specifically when communicating with MCS 5200. Take the scenario where an incoming call via a PVG trunk gateway is to be connected to a SIP DPT. When the caller presses a digit key, the PVG uses H.248 to inform its GWC about the digit, and the GWC sends an INFORM message to the SIP GWC with the digit payload.The SIP GWC then sends a GCP message to the SST with the corresponding tone information. If the remote server (e.g. MCS 5200) does not support RFC2833, the SST will send it a SIP INFO message with the tone information.

- SIP Lines: Core Network Services Support

  Network base services that are expected to work transparently with SIP clients or to work acceptably with documented limitations. The initial release of SIP on CS2000 has some limitations:

  — flash is not supported by SIP clients and can not be used to activate CS2000 network services such as 3 Way Calling. Flash can not be used to receive a second dial tone for the entry of feature activation codes.

  — all digits required for a phone call must be sent in the initial SIP INVITE message. Collection of digits after the message is not supported—the call will end if CS2000 translations request digit collection.

  — special ringing, automatic call back, ring splash, teen service, long distance alerting, and distinctive ringing is supported in release (I)SN09FF

  — Meet Me Conferencing—The conference can not be locked using flash. The STD conference type is not supported by CS2000 and therefore will not be supported by SIP. The conference type of FLASHONLY should be used even though flash is not supported. No interaction with the Attendant Console is supported.

  — Preset Conference—Conference classes of A (alternate conferee class) and C (secondary conference on another switch) are not

supported by CS2000 and therefore not supported by SIP. Pressing # (pound key) to start the conference before all conferees answer is not supported by CS2000 and is not supported by SIP. The field IMMEDIATE in table PRECONF must be set to Y.

The ADDON field in table PRECONF is not supported by CS2000, nor by SIP. The ATD field in table PRECONF is not supported by CS2000 or SIP

— Equal Access—ICS (Overlap Carrier Selection) is not supported because this feature starts translations and outpulsing while the subscriber is still dialing digits. With SIP, all digits reach the CS2000 in one SIP INVITE message.

— Virtual Facility Groups—The VFG Look Ahead feature is not supported. The field ORIGHOLD in tables VIRTGRPS and VFGDATA is not supported. Operator hold for E911 is not supported.

Network Hold for E911 calls is supported in release (I)SN09FF.

— Station Message Detail Recording (SMDR)—Auth Codes and Account Codes can not be entered using flash. If CS2000 translations prompts the user for digits, the call ends.

— Multi Switch Business Groups (MBG)—Reverse name display and redirection reason display are not supported.

— E911—Operator hold is not supported. Physical location of caller can not be determined.

— Advanced Intelligent Network (AIN)—All dialed digits arrive in one SIP INVITE message so TDP-2 is not encountered. (More to come on this)

— Customer Originated Trace (COT)—Second level activation with the CS2000 prompting the user for digits is not supported in the initial release.

— Call Forward—Ring splash on the base station for forwarded calls is supported in release (I)SN09FF. If the SIP client can send the Call Forwarding programming code and the remote DN in one INVITE message, the CS2000 will program the base station. The format must match the following example: *72#6212150#.

— Call Forward programming is also supported by Call Forward Remote Activation (CFRA) using loop around trunks to perform the digit collection.

In release (I)SN09FF, Call Forwarding Indicator and Call Forwarding Reminder are supported for SIP agents that connect the CS2000, using the GWC and CS2000 Session Servers.

— Simultaneous Ringing (SIMRING)—Supported from the SIP client using feature codes. SIMRING can also be programmed by using loop around trunks and a DISA DN to perform the digit collection.

— Call Forward Remote Activation (CFRA)—CFRA programming is supported directly from the user's SIP clients using feature codes. CFRA programming is also supported using loop around trunks and a DISNA DN to perform digit collection. Station Programmable Pin (SPP) is not supported because the digits must be entered interactively from the user's SIP client using feature codes and this is not supported in this release.

— Direct Inward System Access (DISA)—Supported in release (I)SN09FF.

— Do Not Disturb (DND)—Programming the SLE list for enhanced DND is supported in this release.

— Make Set Busy, Make Set Busy Intragroup (MSB, MSBI)—Ring splash is supported.

— Station Origination Restrictions (SOR)—A SIP client can not be a SOR controller (SORC). A SOR controller must be able to enter digits interactively in response to prompts from the CS2000.

— Station Programmable Ringing (SPRING)—SPRING can be programmed directly from the SIP client using feature codes.

— SIP lines can be used in the same hunt groups as non-SIP line. Hunt and hunt sub-options are supported as follows:

  – DNH: Directory Number Hunt
  – MLH: Multi-Line Hunt
  – DLH: Distributed Line Hunt
  – BNN: Bridged Night Number
  – PRH: Preferential Hunt
  – CFGD-CFGDA: Call Forward Group Don't Answer sub-option
  – LOD: Line Overflow to DN sub-option
  – LOR: Line Overflow to Route sub-option
  – CIR: Circular Hunt sub-option
  – SHU: Stop Hunt sub-option
  – RMB: Remote Make Busy sub-option

— SIP lines can be added to the same Series Completion (SCMP) groups as non-SIP lines

— the following Call Waiting variants are supported on SIP lines:

  - CWI: Call Waiting Intragroup
  - CWO: Call Waiting Originating
  - CWD: Dial Call Waiting
  - CWX: Call Waiting Exempt
  - CWTACT: Call Waiting Activate
  - SCWID: Spontaneous Call Waiting Identification

- LI Support of SIP Lines

  This feature provides the Call Data and Call Content interception functionality required to support Lawful Interception (LI) of calls originated by/terminated on SIP clients.

  In the CS2000 core, SIP lines are represented as basic IBN agents with Dynamic Packet Line (DPL) appearance. These lines interface with a Gateway Controller which in turn interfaces with a Session Server platform which provides the direct communication with SIP clients.

- SIP Lines Core OAMP

  This feature provides the Core OAMP functionality required to support SIP clients as a line appearance on the CS2000. This feature involves the following 9 components:

  — SOC Implementation

  — GWC Provisioning

  — Phoenix-GWC Association

  — DPL Lines Provisioning

  — Journal File

  — NCAS Link Provisioning

  — Core Maintenance

  — Tools

  — NCAS Link Logs

  The provisioning of DPLs (Dynamic Packet Lines), i.e. SIP lines, affects the CS2000 Core, the GWC and the SSL (Session Server - Lines), each of which is provisioned via its own SESM application. The list below provides an overview of the process:

  — Install the Session Server - Lines and activate the DPL application.

  — Configure commissioning data on the SSL using the SSL EM.

  — Use OSSGATE to add a GWC with the following characteristics:

    - GWC profile = DPL

- Term type = DPL_TERM
- Exec Data = DPLEX

  The new GWC was added to table SERVRINV with exec lineup DPLEX and term_type DPL_TERM. This causes a static data download of DPLEX execs to the GWC, and the GWC is configured as a type DPL GWC with parameter DPLSupported set toTRUE.

— Use OSSGATE to associate the SSL signalling gateway with its controlling GWC, as follows:

- Enter the gateway (SSL) name and IP address and the name of the GWC that is to control it.
- Select CS2KSS as the gateway profile name.
- Enter the number of reserved terminations. This must be a multiple of the CS2000 line group size 1023, the maximum value being 6138.
- Select the gateway site name as previously provisioned in table SITE.
- The signalling protocol type will default to GCP for the SSL.
- Enter protocol port and version.

  The data entered is used to update tables LGRPINV and table LNINV.A line group entry is created in table LGRP for each increment of 1023 reserved terminations. 1023 entries are then added to table LNINV for each line group.

  Static data is downloaded to the GWC for each line. The term type for each SIP line TID is DPL. The SSL is registered in the GWC as a type D gateway with CS2KSS as the lines profile name and GCP as the protocol. The gateway name can have up to 32 characters, e.g. sipgw1.region.company.com.

  The endpoint identifiers created in the GWC for SIP lines have the format:

  <sitename>/0-511>/</0-9/,0000-1022>

  An example is MOP1/000/2/0478. Line provisioning is performed using SERVORD+. SIP lines can be identified either by LEN format or by gateway name and endpoint ID.

The Core perceives SIP lines as IBN lines with the DPL option, which is compatible with the IBN Line Class Code (LCC). Table IBNLINES records the DN and LEN of each IBN line and lists the features assigned to it. Table IBNFEAT provides supplementary feature-related information when this is required for a feature

assigned to an IBN line (e.g. a forward-to number for Call Forward). For SIP lines, table IBNFEATprovides the following information:

— The DF (Data Feature) field is set to DPL.

— The FEATURE field is set to DPL.

— The DATA field has three subfields:

– SIP

A Boolean that is set to Y for SIP lines.

– MAX_NUM_CALLS

The maximum permitted number of simultaneous calls.

– ALLOW_BSY_TERM

A Boolean that determines whether a busy SIP line can take an additional call termination. In practice, a SIP line cannot be busy unless it is already participating in the maximum number of sessions, but it can be necessary for it to appear busy to ensure that services such as Call Waiting operate correctly.

- NCAS and QSIP Development on CS2000

  The Non-call Associated Signaling Link on CS2000 Session Server platform with query SIP line data (QSIP) application feature provides a lightweight switching control point like functionality. This NCAS link supports a QSIP (Query SIP Line) command provided by the Core CI interface for retrieving a snapshot of static and dynamic line data for a SIP line from the SSL. This feature implements the software that gathers this line data and provides it to the Core in response to the QSIP CI command.

- Core Call Processing for SIP Lines

  This feature provides the CS2000 call processing functionality required to support SIP clients as a line appearance in the CS2000. In the CS2000 core, a basic IBN agent serves as a Dynamic Packet Line appearance through the addition of a new line option called DPL. These lines interface with a GWC, which in turn interfaces with a Phoenix system that provides the direct communication with SIP clients. Support includes:

  — support for multiple call appearances for DPL lines

  — signaling interface between core and the TPT in the GWC

  — basic call processing functionality for a DPL line in the CS2000 core

- Automatic Call Back (ACB) and Automatic Recall (AR) are now supported for Dynamic Packet Lines (DPL) using SIP.

  - ACB places a call to the last outgoing number dialed by the subscriber
  - AR places a call to the last incoming call to the subscriber

- Long Distance Alerting (LDA) feature is integrated with SIP Lines. Distinctive ringing patterns are provided for long distance calls.
- The CS2000 end office Busy Line Verification (BLV) and Barge In (BI) capability now supports SIP Dynamic Packet Lines (DPL).
  - BLV allows a Public Switch Telephone Network (PSTN) Operator verify if a line is in an idle or busy state
  - the PSTN operator can perform an emergency barge-in of a busy line if required
- The CS2000 end office Directed Call Pickup Barge-in (DCBI) and Directed Call Pickup Barge-in Exempt (DCBX) capability supports Dynamic Packet Lines (DPL) using SIP:
  - DCBI permits an IBN station to pick up a ringing line within the same customer group
  - if the called station answers the call before the IBN station completes the call pickup, the IBN station can barge in to the answered call, resulting in a conference state
  - an optional warning tone can be applied to both parties of the call before the activating station is barged-in, using a customer group option in table CUSTSTN
- Teen Service is supported for SIP lines:
  - Teen Service allows multiple DNs to be associated with one line.
  - Each DN has an associated ringing pattern.
- Account/ Auth Codes Flash Entry for SIP Lines is supported. The Account code allows a subscriber to enter a billing number into a Station Message Detail Recording (SMDR) record for charge-back purposes.

  An authorization code is a specified set of digits assigned to and used by station end users. Authorization codes control access to specified networks.
- Three Way Call (3WC) and Usage Sensitive Three Way Call (U3WC) services are extended to IBN (3WC applicable only) and RES type SIP Lines, providing activation/deactivation of the Three Way Calling on the line:

— the conferencing service is provided by an edge device such as an Optical Network Terminator (ONT) or by the CS2000 Session Server, instead of the core

— the calls appear as separate calls in the core

— the U3WC feature is invoked in the same way as 3WC, if the office parameter U3WC_FLASH_ONLY is set to Y. Otherwise, the U3WC feature is invoked by dialing the proper access code.

- Expansion of the SIP lines multiple appearance directory number (MADN) support single call (SCA) features. The following MADN options are supported:

  — SCA: special call arrangement

  — SCA bridging (MTM ports must be available)

  MADN Bridging requires that the MTM is idle. If MTM ports are not available, the COMPACT2 log is generated.

  — PRL: MADN Privacy Release, PRLA and PRLC activation code

  — SCA MREL: MADN release of bridging

  MADN is supported for a restricted set of SIP devices:

  — comply with MADN engineering rules for SIP lines with DPL option:

    – MADN group can have 32 members in the SCA arrangement

    – maximum of 16 members of one MADN group can appear on a single GWC

    – all members of a MADN group must belong to the same customer group

  — multiple SIP sessions are not supported except for a second session using a Vertical Service Code (VSC) feature during an active (stable) call

  — BLV/BI is not supported for a busy call that involves a MADN SIP DPL. The Operator is provided busy line treatment if either the BLV line or the connected party is a MADN SIP DPL.

  The following MADN options are not supported on SIP clients:

  — MCA - Multiple Call Arrangement

  — CACH - Call Appearance Call Handling

  — EXB - Extension Bridging

  — MRFM - MADN Ring Forward Manual

  — MRF - MADN Ring Forward

MRF is not supported; however RF will be supported through client based RF.

— CFMDN - Call Forward MDN Secondary Members - MCA

— MLAMP - MADN Lamp

— PRV - MADN Privacy

— MHOLD - MADN HOLD

MHOLD is not supported; however Hold is supported through client-based hold.

- IP security using Public Key Infrastructure (PKI) is supported for SIP lines, used to protect traffic flow between endpoints on a network. The endpoints are verified (verify endpoint identity) and the transmitted data is encrypted. PKI is a standard that allows entities to establish trust relationships between endpoints which establish IPsec sessions.

  PKI features are used to authenticate IPsec sessions to the Element Manger (EM) and to the Gateway Controller (GWC).

- Call Transfer Screening supported for SIP Lines. The screening service is provided for both the Blind and the Consultation Call Transfers, specific to the DPL Lines agents or ONT. The Call Transfer and the screening function for TDM Line agents is unchanged.

  The Transfer is invoked from the SIP Lines agent and sent to the CS2000 core as a feature message. The screening is performed on the call transfer as provisioned on the CS2000 for the SIP Line.

- E911 features E911 Network Hold, and Ringback are supported on SIP Lines

  The Network Hold feature provides the ability to hold the Network of the 911 call in the event that the Network goes on-hook prior to disconnect from PSAP operator.

  Ringback provides the E911 PSAP operator with the ability to ring back the 911 caller who has gone on-hook, and who is being held by the Network Hold Feature.

- Data Protection for SIP Lines

  Data protection is provided by assigning the No Double Connect (NDC) option to a SIP line. A line assigned NDC cannot use the call transfer, or any of the conference features, nor participate when a conference attempt is made by another subscriber.

- Malicious Call Hold support for SIP Lines

  When the terminating agent of the SIP lines initiates the MCH feature, a message with an authorization code is sent to the CS2000 which terminates the call.

- Malicious Call Trace for SIP lines

  The Calling Line Identification with Flash (CLF) feature is used to identify and log malicious callers.

- Support for Call Completion to Busy Subscriber (CCBS) for SIP lines

  CCBS allows a user, encountering a busy destination, to have the call completed without having to make a new call attempt. The user activates CCBS after getting busy tone from the destination, and goes on-hook.

  When the destination is idle, the user is notified by recall ringing. Single digit activation of CCBS and CEPT CCBS is supported for SIP lines.

- Wake Up Call Reminder (WUCR) and CEPT WUC is supported for SIP lines.

- Payment Ceiling Advice (PCA) for SIP lines

  Network Advice Of Charge (NAOC) is the tariffing of calls over the network boundaries. Two network configurations are supported:

  — single/multiple carrier environment, where the originating exchange is able to determine the tariff; supporting all versions of ETSI ISUP interconnection trunks

  — multiple carrier environment where the originating exchange (Charged Generation Point, CGP) must retrieve the AOC information over the network

- AMA SIP Line Identification

  Support for AMA type 260 module, which captures component and protocol information for the originating and terminating agents involved in a packet network call, as follows:

  — Component role:

    – Originating or terminating

    – CPE, network edge, gateway, and so on

  — IP protocol:

    – SIP, SIP-T, SIP-I, H.323, H.248, MGCP, etc

      This feature provides a framework that can capture information for all protocol variants, but it implements only the capturing of information for SIP lines. Information capture is activated by setting option RECORD_MC260 in table AMAOPTS to ON. This option does not cause a billing record to be created. Instead, it appends information about originating and terminating packet network clients for calls that are already being billed.

- GCP Handling of SIP Refer/3XX/4XX Signalling

Used in supporting MWT for SIP lines. See feature SIP Lines Client Services Interworking on Core for details.

- LI support for INTL SIP lines

  This feature provides the Call Data and Call Content interception functionality required to support Lawful Interception (LI) of calls originated by / terminated on SIP (Session Initiation Protocol) clients for the International Market using DNBD (Deutch Network Broadcast Delivery).

- IP Lines Telemetry feature extends the CS2000 Core functions of Utility Telemetry Service (UTS) and Suppressed Ringing Access (SRA) to SIP Lines. UTS and SRA calls are established from automated systems owned by utility companies to Telemetry Interface Unit (TIU) devices that are attached to the subscriber phone line. Both UTS and SRA suppress ringing of the subscriber phone and allow the TIU to pick up the call.

Gateway Controller

Unless otherwise noted, the functionality applies to all CHS customers and markets.

- Media Proxy Group Selection

  Release (I)SN09FF enables a finer granularity for selection of Media Proxies (MPs) used during call setup. Release (I)SN09FF introduces the capability to enable provisioning of a preferred MP group against an element in the network topology. The MP group specifies the preferred list of MPs from which to select an MP from. Also calls from different geographical locations within the same network should be able to select from different MPs depending on the geographical location of the parties involved in the call. The existing functionality of provisioning MPs against a GWC will remain.

  The GWC receives and stores the MP information on the GWC. The MP groups will then be used at Call setup time to select the most appropriate MP for the VoIP media stream. This feature

  — Creates a new GWC static data table: the Media Proxy Group table.

  — Extends two existing GWC static data tables: the MiddleBox table and the Media Proxy table.

  — Enables the provisioning of these tables via SNMP MIBs from SESM.

  — Provides interfaces for call processing to access data from these tables.

- GNPS Trace Tool Enhancements

  GNPS Trace Tool Enhancements

This feature introduces several improvements to the generic TAPI trace level, as well as interconnecting it to specific trace tools and incorporating existing debug information from several protocols, such as SIP, H.323, GCP. The existing TAPITRACE tool will be enhanced to include the SIP and H.323 protocols and allow for better filtering and redirection of output. In addition, it will be better integrated with the SIP-Trunking tracing feature to better restrict per call captures.

— GWC TAPITRACE base improvements to support the requirements for SIP, H.323, and GCP tracing. These improvements include
  – enabling realtime output to pmdebug
  – enhanced filtering capabilities for capturing and/or displaying logs
  – ensure that the minimal set of timestamp data to sync logs between CS2000 devices is output

— Instrumentation of SIP/GCP/H.323/H.248 protocols to capture comprehensive debug and protocol information within TAPI trace, associating with a tid where possible.

— Functional integration with the current SIP trace framework for activation/deactivation, as well as extending the current Calltrak tracing capabilities to capture individual calls, as well as prep work to allow pmdebug captures.

CHS overview

Carrier Hosted Services (CHS) is a comprehensive suite of business and residential hosted services that delivers revenue-generating opportunities for service providers. These services protect and extend a service provider's network and enable a seamless, cost effective migration to packet-based networks.

Unless otherwise noted, the functionality applies to all CHS customers and markets.

Navigation

Introduction

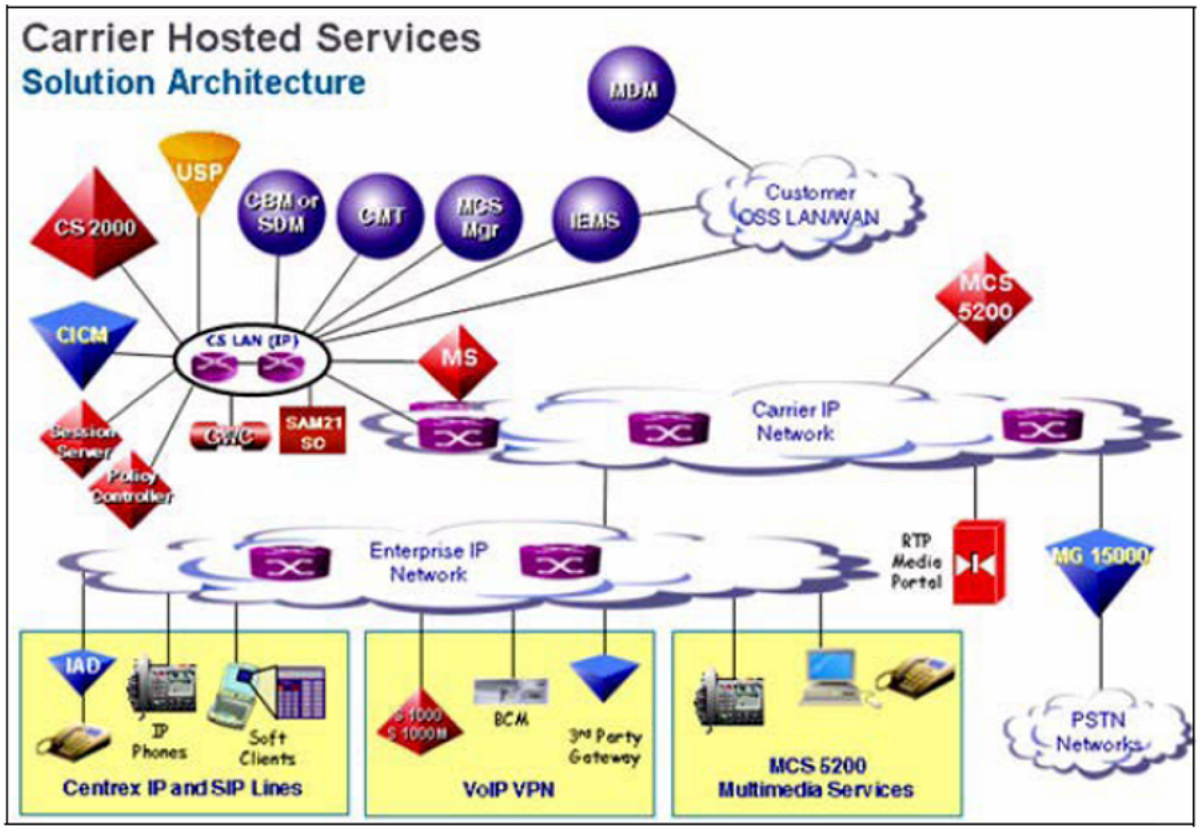
CHS Solutions includes the following Nortel suites:

- Voice over IP Virtual Private Network (VoIP VPN)
- Centrex Internet Protocol (Centrex IP) and SIP lines
- Multimedia Communications Server 5200 (MCS 5200) Carrier Hosted multimedia services

CHS is a suite of business and residential hosted services that delivers a portfolio of Nortel 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 Solutions.

CHS Solutions 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

Availability

CHS is available to North America and International customers as a Greenfield or an Evergreen network.

- A Greenfield network is a new network. Nortel installs a new switch for the customer.

- An Evergreen network is a hybrid network. Nortel extends the functionality of existing DMS equipment with new Carrier VoIP equipment.

VoIP VPN

This section provides an overview of the VoIP VPN program.

Overview

VoIP VPNs enable hosted voice networking and cost-effective converged access for enterprises. The VoIP VPN suite combines the extensive voice VPN translations capabilities of the CS2000 with H.323 multi-vendor IP private branch exchange (PBX) networking. This combination allows multiple voice networks to be collapsed onto a single, managed packet infrastructure.

The VoIP VPN program offers the following capabilities:

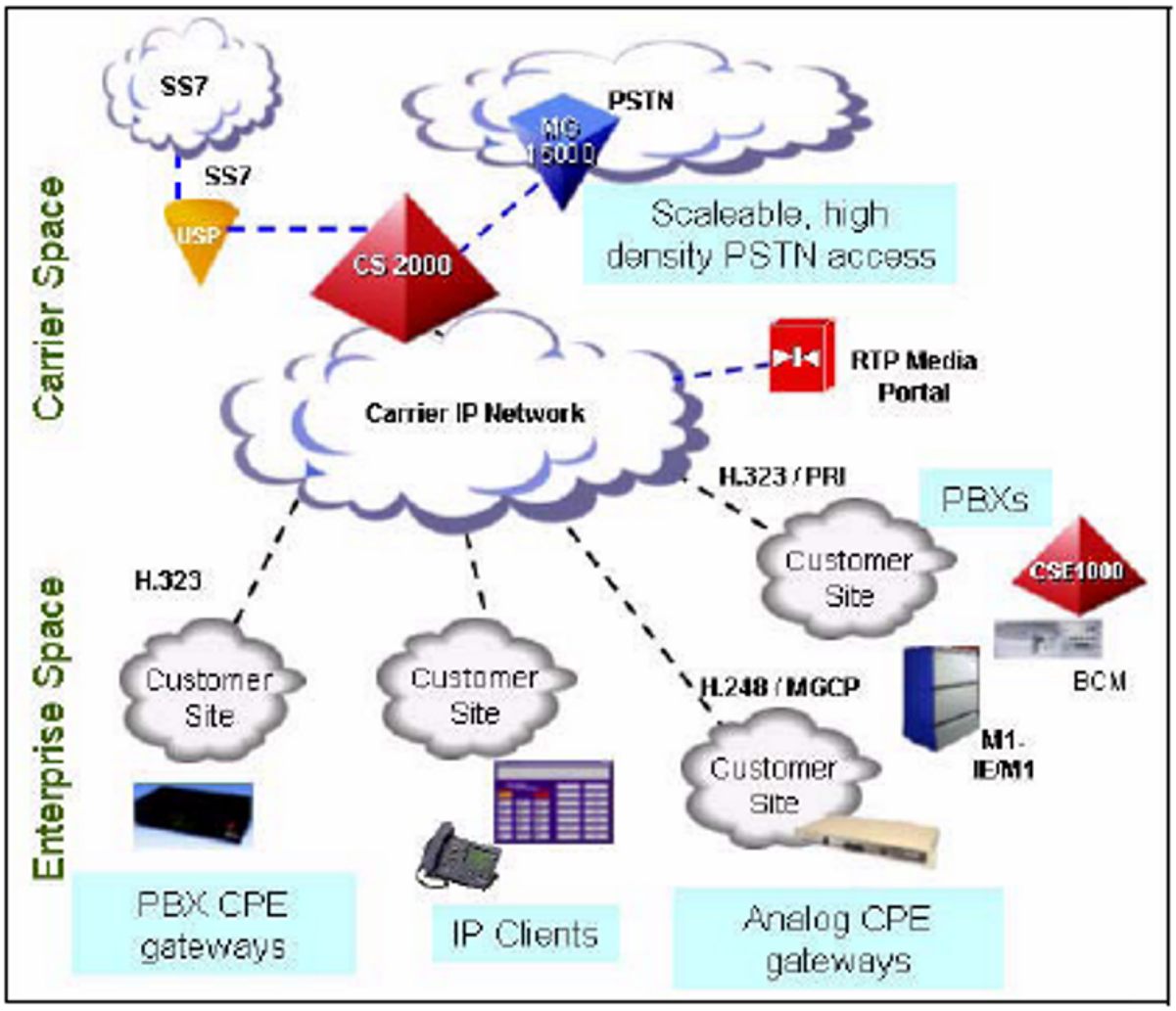
- network-level servicing
  - translations and routing
  - VPN services
  - Centrex groups
  - PSTN
- network access using H.323 specifications
  - IP-based networks
  - MCDN and DPNSS feature transparency
  - interoperability with Nortel and third-party H.323 CPE
  - multiple IP VPN
  - NAT/firewall traversal
  - interworking to trunks and lines

The VoIP VPN program offers the following benefits:

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

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

VoIP VPN architecture



Deployment

The VoIP VPN program is deployed in two primary applications:

- single Site Access for Small-Medium Enterprises, which supports integrated access and support of existing customer premise equipment (CPE)
- large Enterprise Multi-Site Hybrid VPN, which eliminates leased lines and provides a centrally-managed dial plan

Both the Communication Server 2000 (CS2000) and CS2000–Compact support VoIP VPN.

Call processing

- Signaling
  - — Registration, Admission, and Status Protocol (RAS) is an optional protocol only used with gatekeepers. RAS is a transactional protocol carried over User Datagram Protocol (UDP)
  - — H.225 is a call control protocol based on Q.931. H.225 is carried over Transmission Control Protocol (TCP). The connection channel can be dynamically established on call set-up
  - — H.245 is used for media channel negotiation and control. H.245 supports the dynamic allocation of ports on call setup and renegotiation. H.245 is transported over TCP

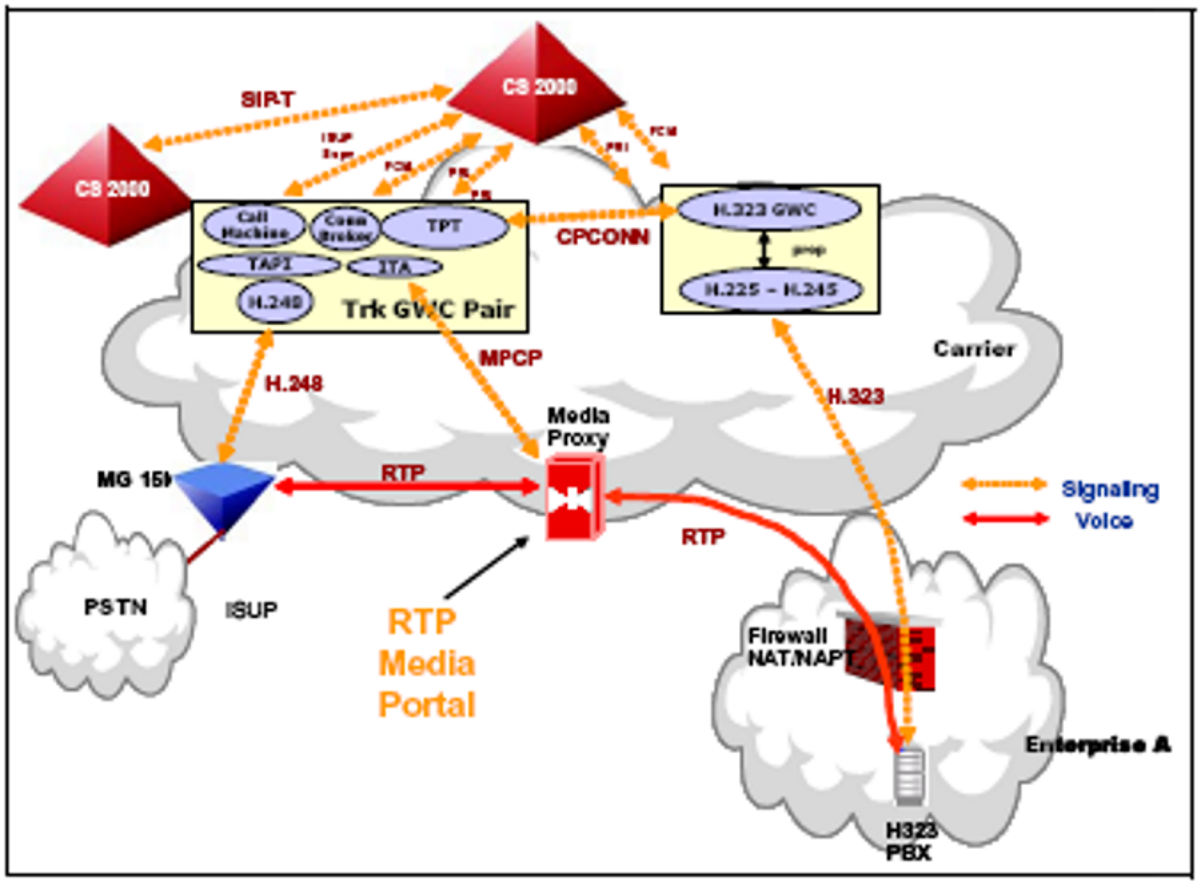
- Media or bearer traffic
  - — Real Time Protocol (RTP)
  - — Real Time Control Protocol (RTCP)

The VoIP VPN program uses the following components for call processing:

- The H.323 Gateway Controller supports signaling between the GWC and the H.323 network. The H.323 Gateway Controller performs the following functions:
  - — maps H.225 messages to either Primary Rate Interface (PRI) or SIP
  - — encapsulates the messages in SIP for transmission to the GWC
- A media proxy, such as the Border Control Point, transports the media stream between networks and end points if the endpoints are in different IP VPNs or different network address domains.

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



Platform

The H.323 GWC is the platform for the VoIP VPN program.

Centrex IP

Centrex IP is supported in TDM deployments and Carrier VoIP deployments. Unless indicated otherwise, this section describes Carrier VoIP deployments.

Overview

Centrex IP provides cost effective VoIP services for large and small businesses with seamless interworking between TDM, IP, and mobile workers. Enterprise workers can access over 200 business features, either through the Enterprise LAN or remotely through the Internet.

The following table lists the key components of a Centrex IP program.

Centrex IP components

Component	Function
Communications Server	Hosts Centrex features
Centrex IP Client Manager (CICM)	Allows clients to access Centrex features on the Communications Server
IP terminals	Provide end points on the IP network for subscriber access

Communications server

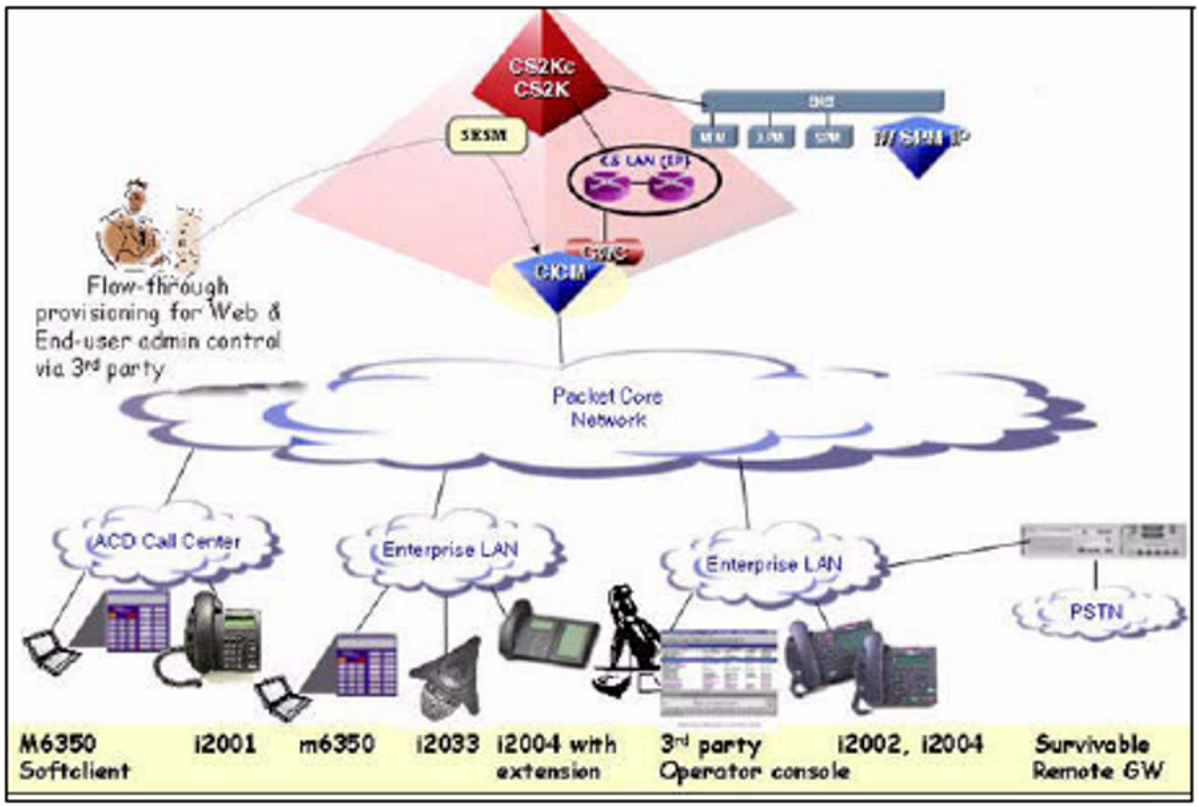
The Communication Server 2000 and the Communication Server 2000–Compact support Centrex IP.

Centrex IP Client Manager

This section briefly describes the function, hardware, and software of Centrex IP Client Manager (CICM).

Overview CICM provides the control interface between the Communication Server 2000 (CS2000) GWC and distributed IP clients on a managed IP network. This figure shows an example of a network topology with CICM.

Network topology with CICM



Centrex IP Client Manager (CICM) functions as a terminal server or signaling gateway in a Carrier VoIP network. CICM performs these functions:

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

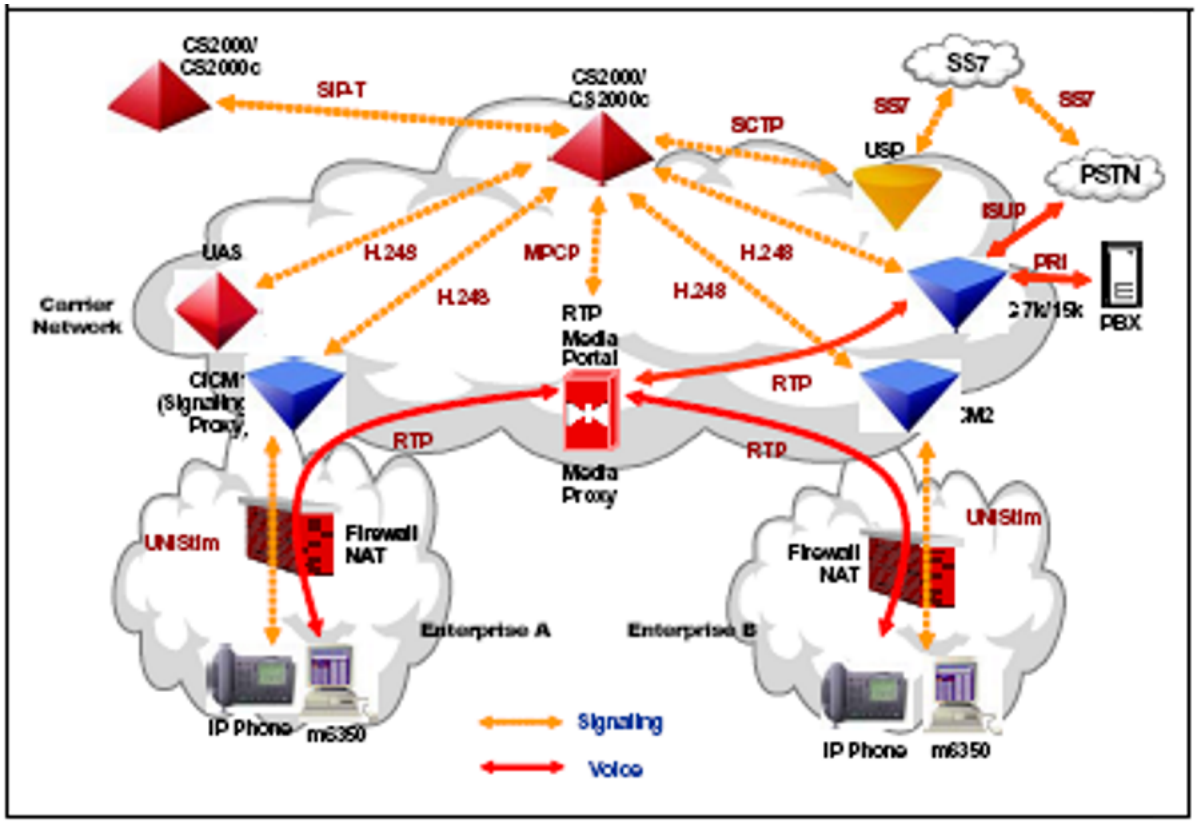
CICM does not transport media in the Carrier VoIP network:

- if the end points are in the same IP VPN or network address domain, the CS2000 GWC routes the media directly between the two endpoints.
- if the end points are in different IP VPNs or network address domains, media proxy, such as the Border Control Point, routes the media.

CICM uses H.248 to communicate with the CS2000 GWC. H.248/MEGACO is a joint ITU-T/IETF protocol defined in ITU-T recommendation H.248 and IETF RFC3015.

This figure shows the protocols used in a Carrier VoIP network with CICM.

CICM interfaces



The USP uses SCTP to connect to the ISUP GWC in the communication server complex.

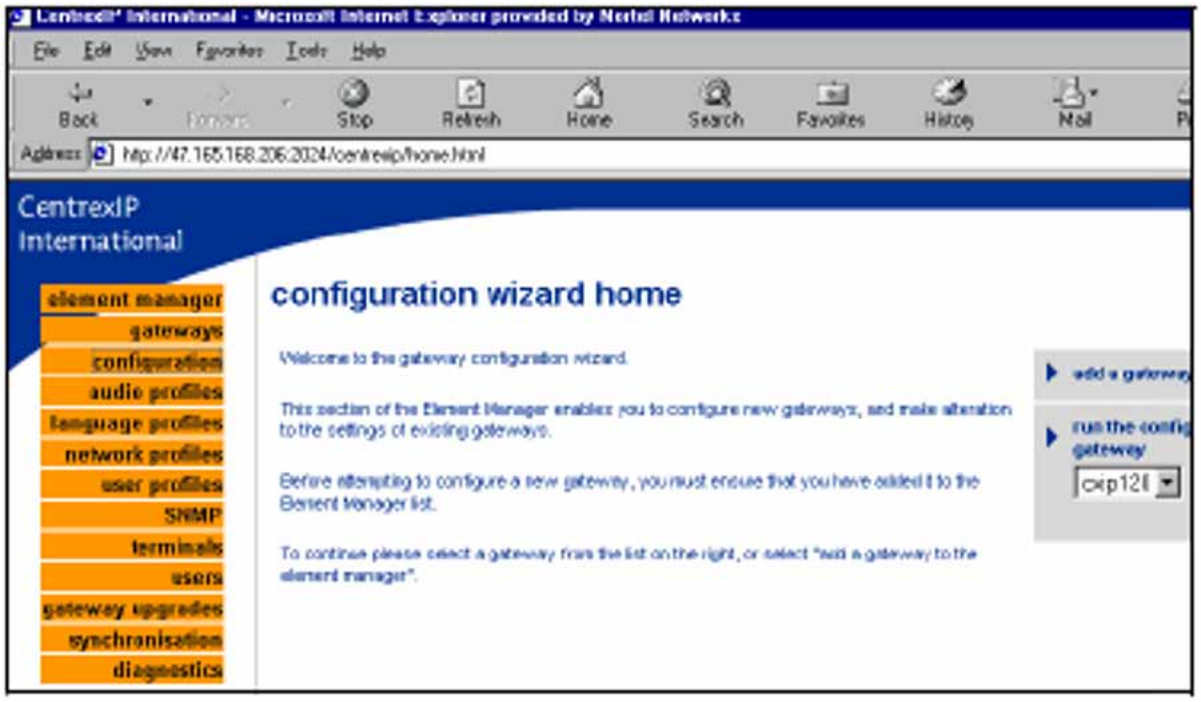
The CICM Element Manager (CICM EM) allows technicians to configure and maintain the CICM. CICM EM supports up to 100 CICM nodes in a Carrier VoIP or TDM deployment.

CICM EM provides these user interfaces:

- Web-based interface to configure and monitor the CICM
- Windows Terminal Server for access and management of the CICM hardware platform
- Telnet for recovery actions
- FTP to upload software upgrades and download log files

This figure shows an example of the CICM EM web-based user interface.

CICM EM web-based user interface



Hardware description The hardware platform for CICM depends on the Carrier VoIP release.

- For release SN06.2 and lower, CICM resides on the SAM16 platform.
- For release SN07 and higher, CICM resides on one of the following platforms:
  - SAM16 platform
  - SAM21 platform on a pair of CPN 5385 PIII processors. A single pair of processors can support up to 3200 ICM end users.

Software description

CICM and the CICM EM each have a separate software load. The following table lists the naming convention for each software load.

CICM software loads

Load	Naming convention	Example
CICM	CICM<release>	CICM0007
CICM EM	CICE<release>	CICE0007

IP terminal

An IP terminal provides an end point for subscriber access on the IP network. An IP terminal is a physical device comparable to a traditional telephone, or software that resides on a web server or the PC of a subscriber.

Centrex IP Client Manager (CICM) supports the following IP terminals:

- m6350 SoftClient
- IP Phone 2001
- IP Phone 2002
- IP Phone 2004
- Key Expansion Modules (KEM)
- IP Audio Conference Phone 2033
- IP Phone 2210 (wireless)
- IP Phone 2211 (wireless)
- IP Phone 2212 (wireless)

All terminals use the Unified Stimulus (UNIStim) protocol for signaling messages. UNIStim is a stimulus protocol that provides a command set that allows a host server to control the operations of a terminal. UNIStim is a Nortel proprietary protocol.

All terminals use Real-time Transport Protocol (RTP) for the media stream. The terminals perform these tasks:

- convert analog voice to digital Pulse Code Modulation (PCM)
- compress PCM
- insert PCM into IP packets
- encapsulate IP packets into Ethernet frames for transport over an IP network
- extract IP packets from Ethernet frames
- decompress PCM
- convert PCM to analog voice

For more information on Nortel IP Phones supported by CICM, see *CICM Basics (NN10044-111)*.

MCS 5200

The MCS 5200, part of Nortel Multimedia Communications Portfolio, seamlessly integrates voice with video, collaboration, and presence services to deliver next-generation communication services. It delivers a

tightly integrated set of innovative, Session Initiation Protocol-based (SIP) multimedia services bundles for both enterprises and consumers. The MCS 5200 integration with other Carrier Voice over IP Hosted Services of the Communication Server 2000 provides feature and support benefits to both the carrier and enterprise customers.

CHS components

This section describes the components of Carrier Hosted Services. Unless otherwise noted, the functionality applies to all CHS customers and markets.

Navigation

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 (CS2000) 		The CS2000 solution has evolved from the legacy DMS family of TDM CO switches. The CS2000 reuses much of the existing DMS TDM service software, as well as the carrier grade DMS hardware. CS2000 provides the following primary functions • call processing (including translations and routing) • Signaling System 7 (SS7) signaling • call feature processing (including features inherited from the DMS switch) • billing

Component	Sub-component	Function
CS2000	Extended Architecture Core (XA-Core)	The XA-Core is the computing engine of CS2000. The XA-Core provides maintenance, call processing, and billing functionality. The CS2000 also sends control messages (for connection set-up) to media gateways (such as the Media Gateway 15000, Multimedia Terminal Adapter, and MG 9000.) 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.
CS2000	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 CS2000 Core Manager.
CS2000	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 CS2000 to any legacy peripherals and is required for access to test trunk facilities.
CS2000	IOM	The IOM provides input/output (I/O) interface to the CS2000.
CS2000	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 CS2000 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 CS2000 configuration, the ISM houses IOMs. IOMs provide ports for serial input and output, enabling local and remote devices to communicate with the rest of CS2000 IOMs through the CS2000 message switch. The IOMs support datalinks that bring the CS2000 Core Manager or the CS2000 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.

Component	Sub-component	Function
	Office alarm unit (OAU)	The OAU connects a CS2000 with the office alarm system to provide notification of physical or electrical problems. An OAU consists of two main types of functional elements: • Scan points and monitoring devices for collecting environmental input (for example, temperature levels) and detecting state changes in peripheral equipment. • 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. 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.
CS2000	Service Application Module 21 (SAM21)	The SAM21 shelf houses the GWC cards. SAM 21 can contain CICM 7.0 cards. All tools and utilities for the SAM21 are provided by CS2000 SAM21 Manager.
CS2000	Gateway Controller (GWC) 	The GWCs provide protocol mediation between the CS2000 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. The CS2000 XA-Core and the CS2000–Compact also support the GWC. The GWCs support these protocols: • H.248 • H.323 • Automatic System for Performance Evaluation for the Network (ASPEN) • Session Initiation Protocol for Telephony (SIP-T) • ISDN 1.921-User Adaptation (IUA) • Simple Network Management Protocol (SNMP) • MTP3-User Adaptation Layer (M3UA) • packet cable NCS

Component	Sub-component	Function
		• packet cable Dynamic Quality of Service (DQoS) and Common Open Policy Services (COPS) • RTP Media Portal (MPCP) • PSTN trunk gateways and a PacketCable-compliant cable network (TGCP) Every GWC uses the same hardware and software. Profiles applied at the GWC Manager define the type of GWC.
CS2000	Session Server	The CS2000 Session Server is a software application that provides interoperability with third-party application servers and softswitches. The Session Server consists of a Network Equipment-Building System (NEBS) Level 3 compliant hardware platform plus a software framework and architecture for developing Carrier Grade applications and services. The Session Server is the platform for the following applications: • SIP gateway application • Policy Controller
	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 CS2000. FLPP uses SR 128 sub-rate fiber links to connect the CS2000 to the SS7 network.

Component	Sub-component	Function
CS2000	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 CS2000 and for OAM&P messaging between the UAS and the UAS manager.
CS2000	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.
CS2000	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: • 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) • high-speed link interface support to simple control transmission protocol (SCTP): IETF SIGTRAN SCTP/M2PA IP high-speed link (8-20 DS-0 equivalent) • DS0A, V.35, and channelized T1/E1 low-speed link support • direct messaging to the GWC using M3UA/UDP for TDM ISDN User Part (ISUP) trunking • load sharing between SS7 links • supports co-resident STP capability • support for American National Standards Institute (ANSI) and ETSI ISUP trunks • high service availability of 99.999% and in-service software upgrades during which no calls are lost • in-service LIU7 application upgrade from FLPP to USP • access to HMI through the Ethernet

Component	Sub-component	Function
		• support for up to 16 multipoint codes • support for up to 440 low-speed SS7 links
CS2000	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. The USP–Compact resides on two identical blades in a CS2000–Compact or SAM21 shelf and supports up to 16 channelized T1/E1 links and up to 8 multi-point codes.
CS2000	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 CS2000 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 CS2000, and consists of two Ethernet Routing Switch 8600s with 10/100 BaseT Ethernet or Gigabit Ethernet links to components.
CS2000–Compact 		The CS2000–Compact is a full-featured, small-footprint alternative to the CS2000, which is designed for new installations. The CS2000–Compact performs call processing, messaging, routing, translations, centralized systems delivery, and storage of office images and system data.
CS2000–Compact	Call Agent	The Call Agent is the computing engine of CS2000–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).
CS2000–Compact	STOrage Management (STORM)	The STORM card provides network file system (NFS) services to applications running in the CS2000–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.

Component	Sub-component	Function
Gateways		
Media Gateway 15000 		Media Gateway 15000 serves as a media gateway in the Voice over IP network. The Media Gateway 15000 supports the H.248 protocol for communication between the GWCs and Media Gateway 15000. The Media Gateway 15000 supports the following functions: • tone generation on the TDM side of the gateway, such as basic service tones, basic call progress tones, and expanded call progress tones • in-band DTMF digit collection for ISUP and primary rate interface (PRI) trunk agencies • clear channel data functionality for test trunk capability • modem and fax services over G.711 CODEC standard • software maintenance and release upgrade • 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 • T108 test trunk termination • interworking with TDM trunks through Interworking Spectrum Peripheral Module Internet Protocol (IW-SPM-IP) • two-port Gigabit Ethernet on the VSP3 card
RTP Media Portal 		The CS2000 uses the Real-time Transport Protocol media portal to establish media paths that span the address spaces of enterprise networks. The CS2000 uses the media portal as required to bridge the RTP paths between endpoints for CICM NAT traversal. RTP media portal is needed if the endpoints of the media path are not in the same IP address space, as is the case for calls between two enterprises, or calls from an enterprise H.323 gateway to a gateway on the carrier IP network.

Component	Sub-component	Function
Core Network		
Network management		
Integrated Element Management System (IEMS)		IEMS is a next generation element management system that provides a single point of data integration and network management for the Carrier VoIP network. At the central office level, IEMS provides the following functions: • provides graphical topology and inventory relationships between network elements and element management systems • aggregates all fault and performance data from network elements and element management systems • provides integrated fault and performance streams to the Network Management Layer • provides customer choice of operations support system (OSS) interfaces • provides extensible markup language (XML) aggregation of comma-separated value (CSV) files for performance • provides centralized fault and performance viewer with filtering capabilities • provides context-sensitive launching of network management interfaces • provides enhanced security features by improving the centralization of authentication, authorization, and administration, while also providing interfaces to external security databases • supports localization in many languages

Component	Sub-component	Function
IEMS	CS2000 Core Manager	The CS2000 Core Manager provides OAM&P functionality for the XA-Core and the subtending TDM components of the CS2000. It resides on the SuperNode Data Manager (SDM) platform and includes much of the SDM's existing OAM&P functionality. CS2000 Core Manager also provides access to logs for the MG 9000, GWC, UAS, Media Gateway 15000, SAM21 and XA-Core. In addition, the CS2000 Core Manager provides performance metrics for the XA-Core, MDM, and Media Gateway 15000. The CS2000 Core Manager provides access to logs, alarms, and performance monitoring data relating to call processing on the CS2000–Compact.
IEMS	Core and Billing Manager	The Core and Billing Manager (CBM) provides the OAM&P functionality of the CS2000 Core Manager. It resides on two Sun Netra 240 servers housed in the Cabinetized Operations Administration and Maintenance (COAM) cabinet. The CBM supports the following applications: • SuperNode Billing Application (SBA) • Operational Measurement (OM) delivery • Log streamer • Operations Systems Support (OSS) applications and communication services
IEMS	CS2000 Management Tools	CS2000 Management Tools is a suite of network management tools used in Voice over IP solutions. The CS2000 Management Tools suite consists of the following network management tools: • GWC Manager • UAS Manager • Audio Provisioning Server (APS) • APS Manager • SAM21 Manager • Network Patch Manager (NPM) • Nodes Configuration

Component	Sub-component	Function
		• Trunks Configuration • Carrier Endpoint Provisioning • Lines Configuration • Trunk Maintenance Manager (TMM) • Line Test Manager (LTM) • Lines Maintenance Manager (LMM) • V5.2 Configuration • V5.2 Maintenance • PM Poller • QoS Collector Application
IEMS	Call Agent Manager	The CS2000–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, Call Agent Manager is the primary interface for platform functions such as a cold switch of activity, routine, exercise text, jamming, and synchronization of the call processing application.
IEMS	CS2000 GWC Manager	The primary function of the CS2000 GWC Manager is to coordinate the configuration of the CS2000 GWCs. Also, the CS2000 GWC Manager is used for fault management of a CS2000 GWC node.
IEMS	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.
IEMS	Audio Provisionin g Server Manager (APS Manager)	The APS Manager provides a Web-based GUI that manages announcements from any workstation. The APS Manager client runs on a PC.

Component	Sub-component	Function
IEMS	CS2000 SAM21 Manager	The CS2000 SAM21 Manager is a GUI that provides access to OAM&P functions such as platform software load, platform diagnostics, platform upgrade, and Network File System (NSF)mount provisioning. In addition, the CS2000 SAM21 Manager for provisioning the hardware of a CS2000 GWC, for fault management of a CS2000 GWC card, and to upgrade the firmware of a CS2000 GWC. CS2000 SAM21 Manager has two components: the element manager server and the element manager client. The CS2000 SAM21 server resides on the same server that hosts the Succession Server Platform Foundation Software (SSPFS) NCL software package (part of the CS2000 Management Tools software). Currently, the SSPFS package runs on a Sun Netra t1400 or Netra 240. The CS2000 SAM21 element manager 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.
IEMS	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.
IEMS	Lines Maintenance Manager (LMM)	LMM provides an XML interface that allows you to use client applications (GUIs) to perform basic maintenance operations on GWC-managed lines, such as posting, busying, and returning to service.
IEMS	Session Server Manager	The Session Server Manager is a web-based interface residing on the Session Server to perform the provisioning and maintenance activities. This interface consists of a web system running on the Session Server Manager that provides provisioning web pages as well as maintenance related web pages. The Session Server can be configured to use IEMS between the customer operation LAN and the CS2000 LAN or it can be configured without IEMS.

Component	Sub-component	Function
IEMS	Universal Signaling Point (USP) Manager	USP Manger is a Windows 2000 workstation that provides a GUI for provisioning and monitoring SS7 interfaces. USP Manager also provides backup and software upgrade facilities for the USP.
IEMS	MG 9000 Manager	The Media Gateway 9000 Manager (MG 9000 Mgr) allows technicians to remotely manage all MG 9000 components in a CVoIP network. The MG 9000 is a client-server application that consists of the following components: • server software that resides on a central server • mid-tier database between the client and server for data storage The MG 9000 Mgr supports most common management operations, including the following: • network element discovery • equipment provisioning • carrier provisioning • service provisioning • fault handling and reporting • operational measurements
IEMS	STORage Management Manager (STORM Manager)	The STORM Manager is used with CS2000–Compact. The STORM Manager is a Web-server application that runs on the STORM card. The STORM Manager allows you to • provision and control application-level STORM functions • modify STORM file systems • view STORM logs
IEMS	Device Manager (for Ethernet Routing Switch 8600)	The Device Manager (for Ethernet Routing Switch 8600) is a suite of GUI applications that allows you to manage and configure an Ehternet Routing Switch 8600 chassis. It can be launched independently or as part of Optivity.

Component	Sub-component	Function
IEMS	Multiservice Device Manager (MDM)	MDM allows you to manage Media Gateway 15000. MDM allows you to perform fault management, configuration management, data collection, performance management, and security management. In addition, MDM forwards Media Gateway 15000 performance management, and fault management information to the CS2000 Core Manager. The MDM resides on a Sun-based workstation.
Centrex IP		
Centrex IP Client Manager (CICM)		CICM delivers Centrex capabilities to users connected to an IP network using VoIP technology. The CICM performs the following functions: • provides the interface between the Centrex feature set and an IP network • transcodes voice between IP data and the client network and PCM data from the XPM The CICM client allows a user to initiate and receive VoIP calls and to receive Centrex features from the CS2000. • the m6360 SoftClient application • the Nortel Networks IP Phone 200x Etherset telephones For more information on CICM, refer to *CICM Basics*, NN10044-111.

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 Communication Server 2000 (CS2000) utilize MCS RTP Media Portals for NAT/firewall transversal. There are two possible management system configurations for MCS RTP Portals associated with a CS2000: shared and dedicated.

In the shared configuration, the MCS RTP Media Portals associated with the CS2000 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 CS2000 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 Session Manager is the MCS 5200 service execution engine that provides the following software functionality: • SIP Proxy Server • Back-to-Back User Agent (BBUA) • SIP Registrar • CPL Interpreter • address resolution and routing capabilities The Session Manager is dual-homed. As an optional software feature of the Session Manager, the SIP Presence Module processes information for presence subscription and notification. For more information, refer to *MCS 5200 Session Manager Basics, NN10029-111*, and *MCS 5200 Presence Basics, NN10236-111*.
	The System Manager provides the services that support communication amongst the Multimedia Communication Server network elements and management requests issued from the System Management Console or the Open Management Interface (OMI). It provides the software functionality that: • manages the following functions for the MCS 5200 components, media server, and the gateways: — faults — configuration — performance • collects operations, administration, and maintenance (OAM) information for display on the System Management Console The System Manager is located in the private MCS 5200 network. The System Management Console is the administrator's interface to the Management Module. For information on the System Manager, refer to *MCS 5200 System Manager Basics, NN100030-111*. For information on the System Management Console, refer to *MCS 5200 System Management Console Basics, NN10247-111*.,

MCS 5200 components	Description
	For information on the System Manager in the dedicated configuration to support MCS RTP Media Portals associated with the CS2000, refer to the *CVoIP System Manager Basics, NN10369-111*. For information on the System Management Console in the dedicated configuration to support MCS RTP Media Portals associated with the CS2000, refer to the *CVoIP System Management Console User Guide, NN10370-111*.
	The Database functionality is comprised of several software components: Oracle database software, Database Manager component, and the Database Instance Monitor component. The Oracle database is accessed by some network components in order to provide storage and retrieval for: • subscriber location information • registration status based on information received with SIP client registration • routing and translation entries • system configuration data The Database functionality is located on the private MCS 5200 network. For more information, refer to *MCS 5200 Database Manager Basics, NN10031-111*. For information on the Database Manager in the dedicated configuration to support MCS RTP Portals associated with the CS2000, refer to the *CVoIP Database Manager Basics, NN10368-111*.
	The Accounting Manager provides a mechanism for receiving, storing, formatting, and transmitting accounting information for billing purposes. The Accounting Manager is located on the private MCS 5200 network. For more information, refer to *MCS 5200 Accounting Manager Basics, NN10037-111*.

MCS 5200 components	Description
	The Provisioning Manager 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: • service provider provisioning through the Provisioning Client • customer domain provisioning through the Provisioning Client • setting up network services functions, such as the network address book • enabling the administrator to do bulk provisioning either through an API or through a command line interface (CLI) Within the Provisioning Manager, 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. The Provisioning Manager is dual-homed. For more information about the Provisioning Manager, refer to *MCS 5200 Provisioning Manager Basics, NN10242-111*, and *Provisioning Client User Guide, NN10043-113*. For more information on provisioning tasks that the Provisioning Manager processes, refer to the following documents: • *Multimedia PC Client Manager User Guide, NN10041-113* • *IP Phone 2002 User Guide, NN10319-113* • *IP Phone 2004 User Guide, NN10042-113*
System Management Console 	The System Management Console is the element manager GUI for MCS 5200. With this GUI you can: • administer system, database, and service components • deploy and configure MCS 5200 system sites, servers, modules/components, and services • monitor the MCS 5200 system using alarms, logs, and performance measurements • manage collection of operations, administration, accounting, and maintenance information

MCS 5200 components	Description
	The System Management Console runs on a personal computer (PC) and communicates with the System Manager on the private MCS 5200 network. For more information about the System Management Console, refer to *MCS 5200 System Management Console Basics, NN10247-111*. For information on the System Management Console in the dedicated configuration to support MCS RTP Media Portals associated with the CS2000, refer to the *CVoIP System Management Console User Guide, NN10370-111*.

MCS 5200 optional functional components

This 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 IP Phone 200x and provides access to MCS 5200 SIP services. The IP Client Manager provides access to the following features: • instant messaging • information delivery services • session-handling services • call management services The IP Client Manager is dual-homed. It performs the SIP to UNIStim conversion that enables the interworking of IP Phone 200x with the SIP Application Module. For more information on the IP Client Manager, refer to the following documentation: • *MCS 5200 IP Client Manager Basics, NN10032-111* • *IP Phone 2002 User Guide, NN10319-113* • *IP Phone 2004 User Guide, NN10042-113*

MCS 5200 Media Servers

This 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: • support for up to 32 port audio conferences • independent Coder/Decoder (CODEC) negotiation for each conference call port • mid-session broadcast of SIP info signals to all conference parties (for example, a Web page URL) • hold/retrieve • round-robin resource allocation (for selecting media resources for conference calls) • long call service • call transfer • chaining conferences together (During a conference call on the SIP Audio Server, any client may add additional clients onto the conference call.) • authenticating SIP Application Module sending a request 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*.
	The RTP Media Portal is a network-distributed component that provides the following functions: • performs media-stream network address translation and network address port translation (NAT/NAPT) • provides a media firewall • provides third-party media controls • enables a client firewall/NAPT traversal mechanism

Media servers	Description
	The RTP Media Portal handles media streams using the Real-time Transport Protocol (RTP) and Real-time Transport Control Protocol (RTCP). 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. 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. The MAS supports the following services: • Ad hoc audio conferencing • Meet me audio conferencing 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

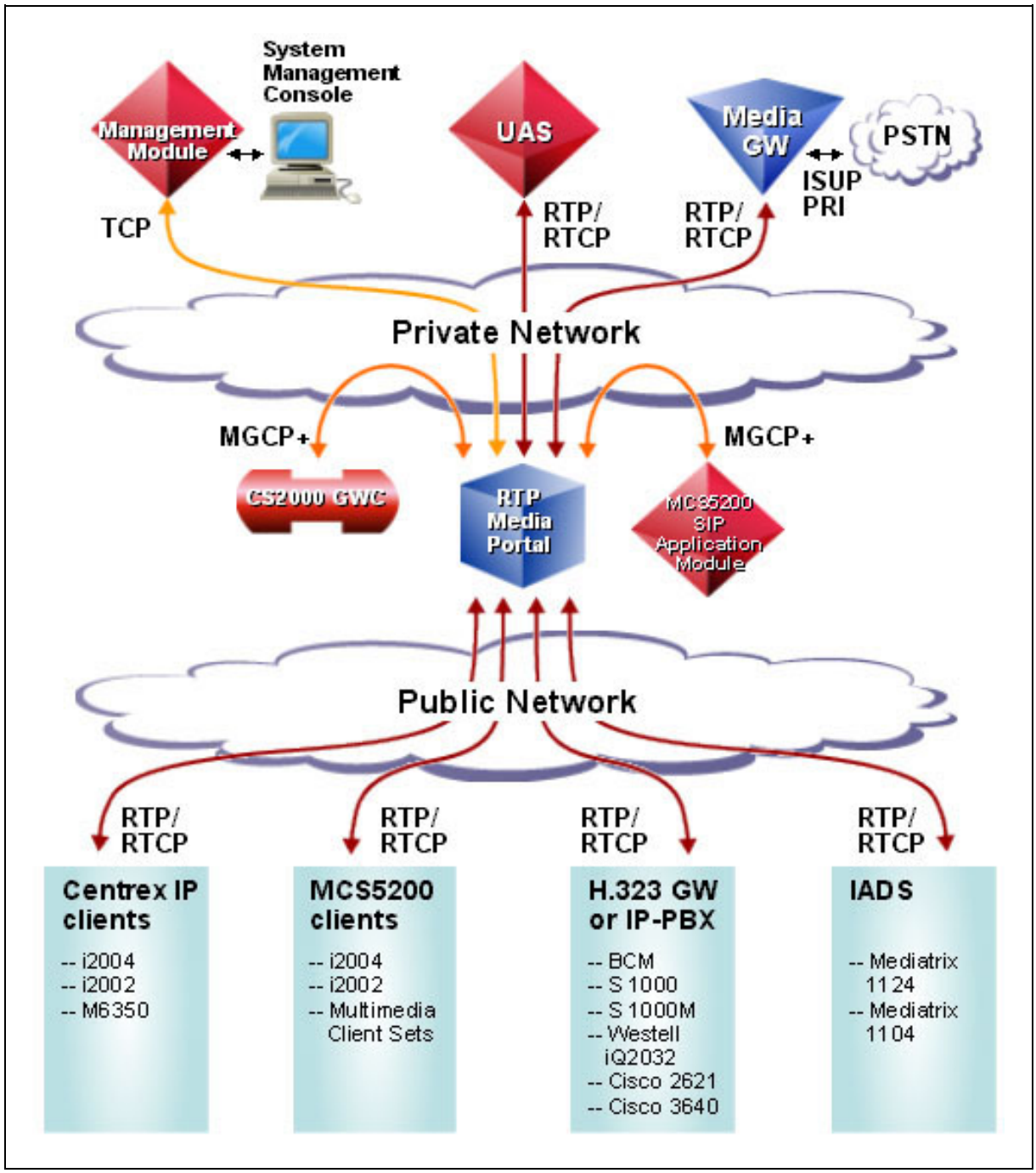
The RTP Media Portal service addresses media-specific issues with advanced service delivery, Internet addressing efficiencies, and system security. It functions as a media Network Address Port Translation (NAPT) point that shields private network components from external exposure through leaks in the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

This figure shows RTP Media Portal interworking among other components.

RTP Media Portal network interoperability



In the 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 Communication Server 2000 (CS2000). If the GW and the CS2000 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->CS2000 communication. Discovery provides another mechanism for GW->CS2000 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

This 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: • PRI call handling • CODEC negotiation • calling party name and number delivery to SIP • parameter mapping between SIP and PRI protocols 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.

This table lists brief descriptions of the MCS 5200 access clients.

MCS 5200 access clients

Access client	Description
Subscriber access to the SIP services network requires one of the following clients: Multimedia PC Client, IP Phone 2002 , IP Phone 2004 , 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: • traditional telephone services • multimedia communications — video calls — Instant Messaging — file sharing/file transferring — whiteboard session — Web page push • communication management — directory — call logs — Friends Online — address book 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*.

Access client	Description
	The IP Phone 2002 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 IP Phone 2002 advanced features include: • instant messaging • stock query • call forward • do not disturb • multiple user login (4 simultaneous users) • bulletins • Quality of Service (QoS) information The IP Phone 2002 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 IP Phone 2002, refer to the *IP Phone 2002 User Guide, NN10041-112*, and *MCS 5200 Feature Description Guide, NN10251-115*.
	The IP Phone 2004 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 IP Phone 2004 advanced features include: • instant messaging • stock query • call forward • do not disturb • multiple user login (6 simultaneous users) • bulletins • QoS information

Access client	Description
	The IP Phone 2004 is located on the managed public network and is managed by the IP Client Manager (IPCM). For more information on the IP Phone 2004, refer to the *IP Phone 2004 User Guide, NN10042-113*, and *MCS 5200 Feature Description Guide, NN10251-115*.
	The IP Phone 200x provides voice services, while the PC provides all other services. When the Multimedia PC Client is configured to control the IP Phone 200x, the configuration is known as the Multimedia Client Set. The Multimedia Client Set provides access to SIP features and services such as: • traditional telephone services • multimedia communications — video calls — Instant Messaging — file sharing/file transferring — whiteboard session — Web page push • communication management — global address book — call logs — Friends Online — personal address book For more information on the Multimedia Client Set, refer to the *Multimedia PC Client User Guide, NN10041-112; IP Phone 2002 User Guide, NN10319-113; IP Phone 2004 User Guide, NN10042-113;* and *MCS 5200 Feature Description Guide, NN10251-115*.

Access client	Description
	The Provisioning Client is a browser-based tool that allows service providers to provision: • administrators • domains • gateways • IP Client Managers • voice mail servers • service packages • telephony routing translations 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*.
	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: • Routes: to define call screening and routing behavior • Preference: to modify personal information and services • Directory: to manage key contact information; access personal and global address books • Click-to-call: to establish a call between two parties • Multimedia Web Client: to launch multimedia web client 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: • traditional telephone services

Access client	Description
	• multimedia services — video calls — Instant Messaging — Web page push • communication management — global address book — call logs — Friends Online — personal address book 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 functions. 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

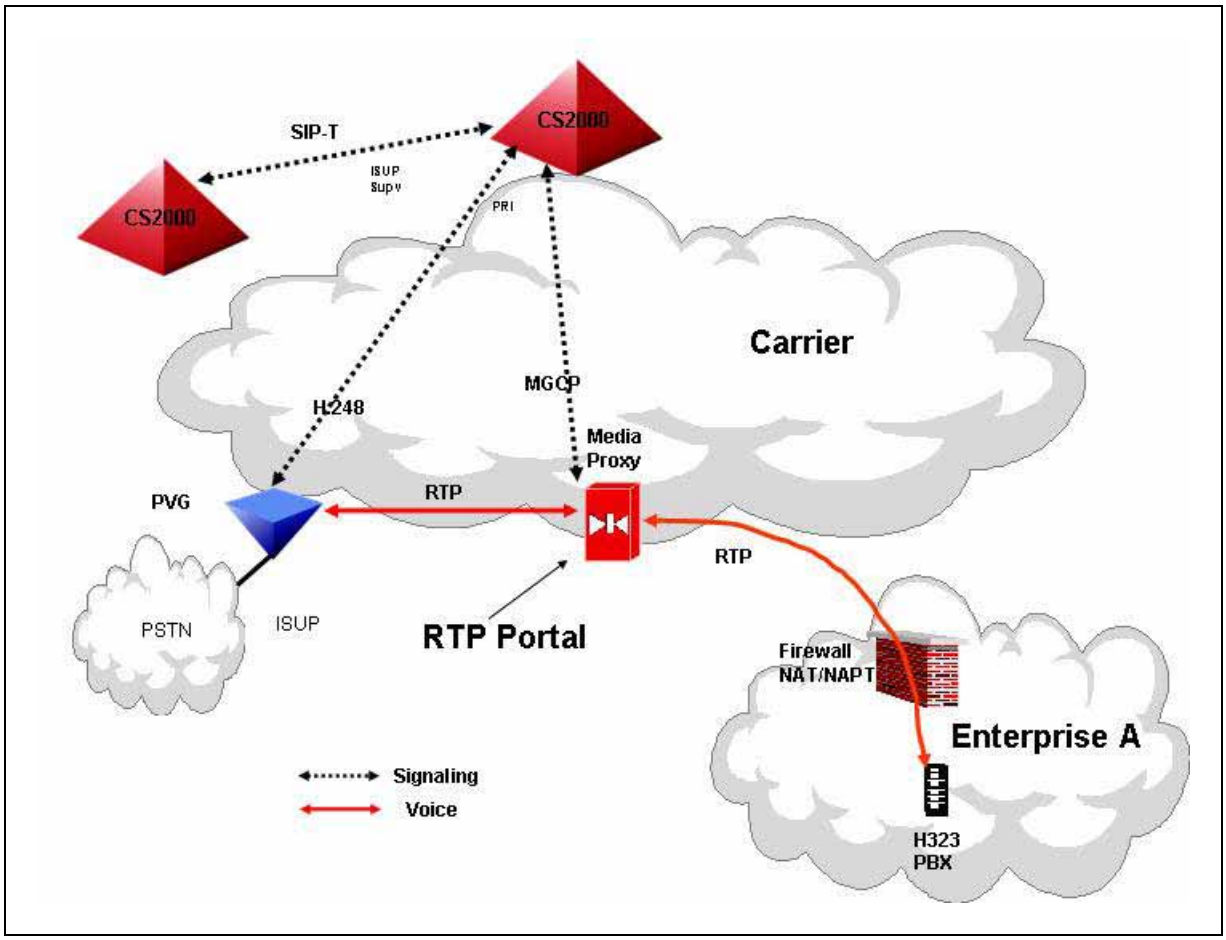
This section briefly describes the call processing flows for the products and applications associated with the Carrier Hosted Services. Unless otherwise noted, the functionality applies to all CHS customers and markets.

Navigation

VoIP VPN

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

VoIP VPN call flow



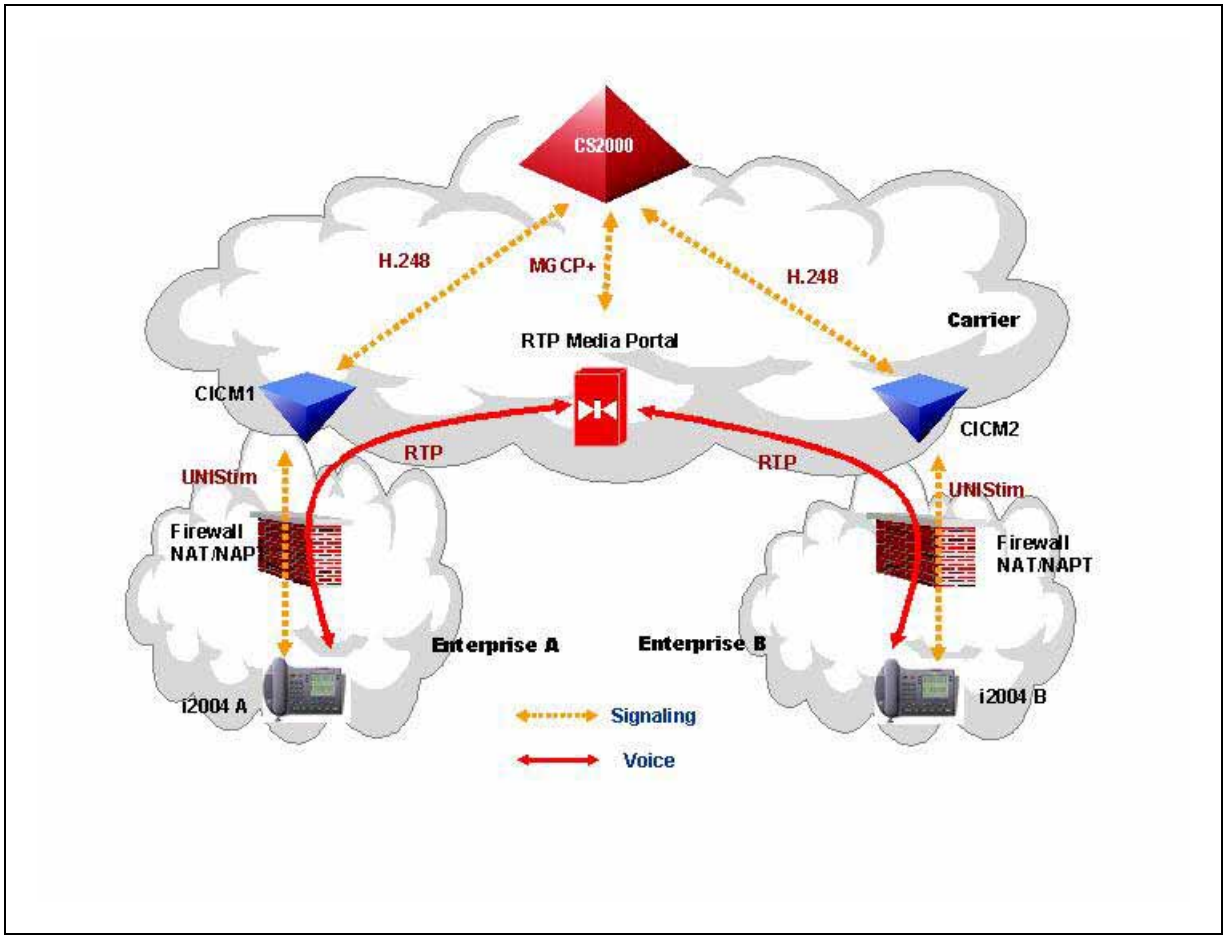
CICM

Centrex IP Client Manager (CICM) converts UNIStim messages between the CICM and the Centrex IP clients to H.248 messages to the Communication Server.

Unlike TDM deployments, the 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.)

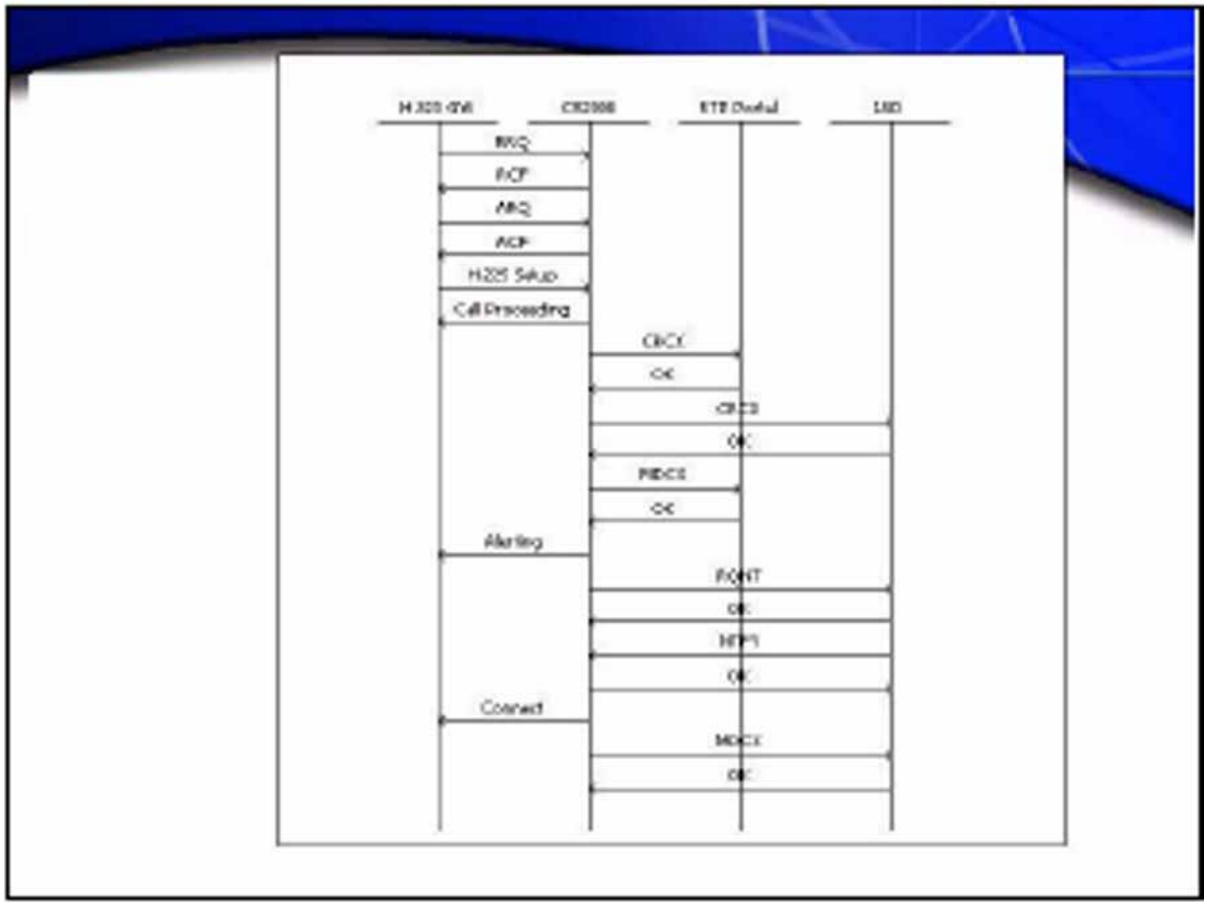
The following figure shows a call flow using Centrex IP and CICM.

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" (page 68) 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.

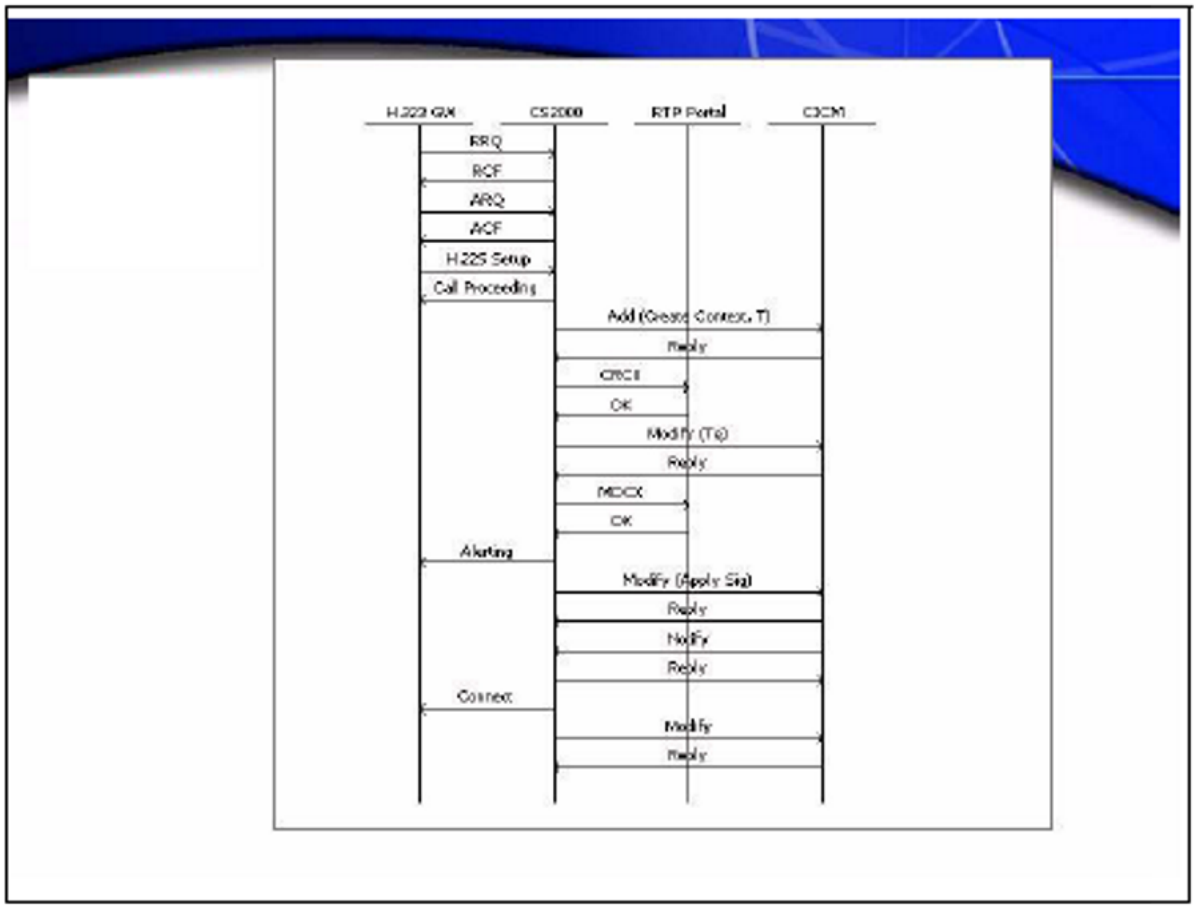
The communication server sends the Alerting message to the originating H.323 gateway, including the RTP port that should be used on the RTP Media Portal. The communication server then sends a Request Notification (RQNT) to the terminating IAD, directing it to apply ringing and provide notification when 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" (page 69) 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 CS2000 refer to *CVoIP RTP Media Portal Basics, NN10367-111*.

CHS services

Unless otherwise noted, the functionality applies to all CHS customers and markets. CHS includes these 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 Communication Server 2000 (CS2000) through PRI and H.323:

- CS1000 and CS1000M (Release 4.5)
- Business Communications Manager (BCM) (Releases 3.6 and 3.7)

The following functionality is new to VoIP VPN in CHS Solutions release (I)SN09FF:

- H.323 Clear Channel Data (UDI) support

  Unrestricted Digital Information (UDI) provides the ability to pass bit-transparent 64Kbit/s channel data. This functionality is required to support some services such as video conferencing.

- Release Link Trunking (RLT) H.323 support

  Frees unused call signaling paths that result from call path changes, for example call forwarding and call transfers. RLT allows for more efficient use of network resources.

- Q.SIG feature mapping into H.323 (Phase 1).

  This functionality provides mapping between the H.323 and the following Q.SG Supplementary Services:

  — COnnected Line Identification Presentation (COLP)— allows the calling party to receive the number of the called party

  — COnnected Line Identification Restriction (COLR)—allows the called party to prevent the presentation of its number to the calling party

- H.323 RAS-less functionality on the GWC.

  The H.323 Gatekeeper uses Registration, Admission and Status (RAS) messages and procedures to control access to the network. In certain H.323 VPN configurations, for instance carrier-to-carrier interconnect, there is a need to provide H.225/H.245 call signalling between entities without the use of RAS messages. “RAS-less” is the term used to describe this H.323 configuration.

- integration with up-versions of VoIP VPN endpoint software loads

CHS VoIP VPN benefits

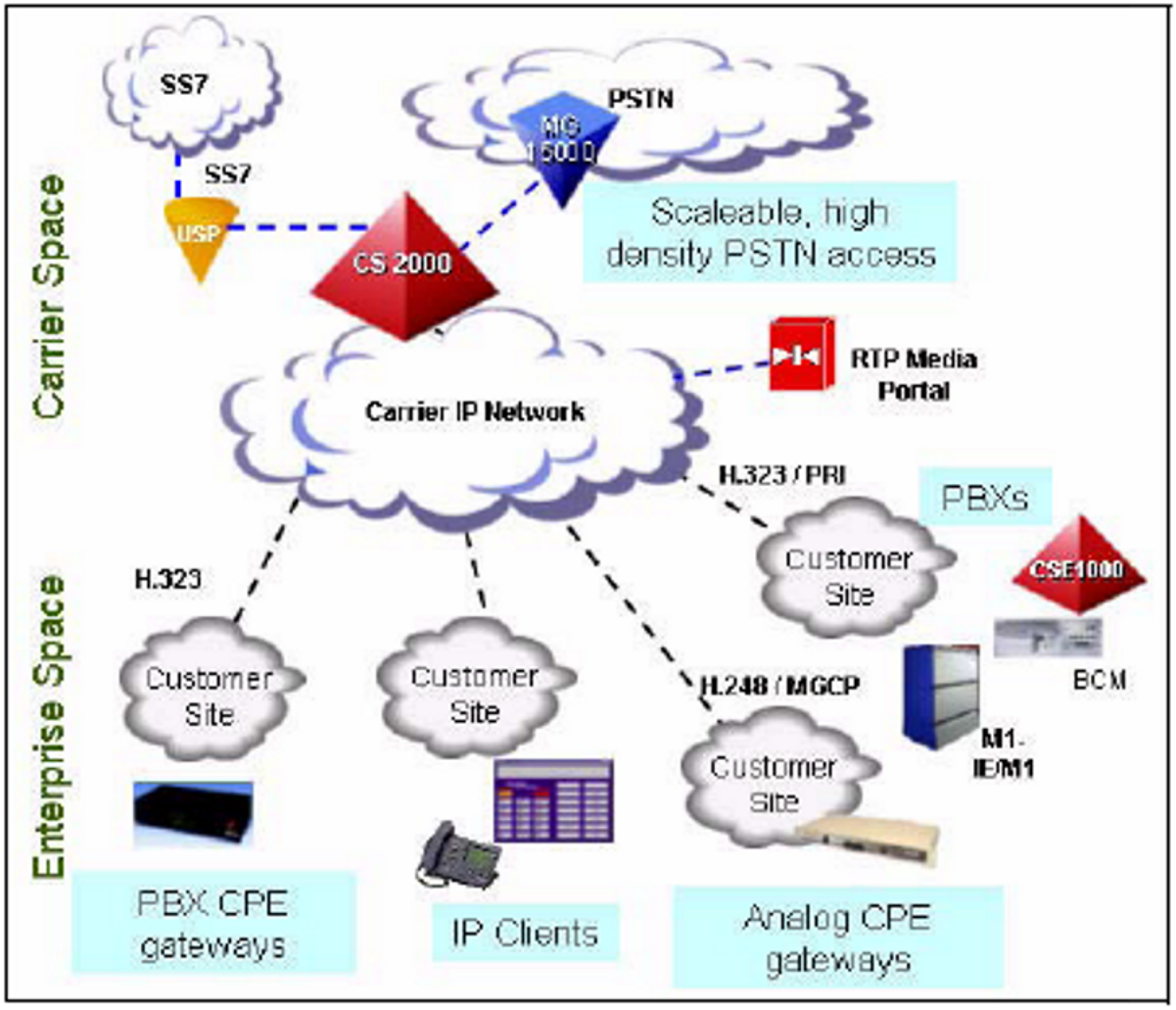
The Carrier Hosted Services VoIP VPN service offers the following benefits:

- 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
- available on the CS2000 and the Communication Server 2000–Compact (CS2000–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 H.323 gateways are supported in release (I)SN09FF including:

- Meridian 1
- Business Communications Manager (BCM) release 3.7
- Nortel Communication Server 1000 Media Gateway (CS 1000M) release 4.5
- third-party gateways (Westell, Cisco)

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 CS2000 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 functions for the hosted Communication Server 2000 (CS2000). Therefore, any originating or end-node functions that relate to DPNSS features are not supported by the host CS2000. Any support for originating/terminating DFT as end-node functions on CS2000 IAD gateway lines, require DFT (IBN7 TDM/SIP-T) looparounds.
- Direct BTUP interworking for PSTN breakout calls from the CS2000 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 CS2000, 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 CS2000 to apply the RingBack tone after connection, the CS2000 will not be able to apply the tone.

For a list of supported DPNSS/Centrex features, refer to "Features and services" (page 120).

For a complete listing of all documentation associated with Carrier Hosted Services VoIP VPN refer to "Where to get customer documentation" (page 149) .

In particular, refer to the following sections:

- "BCM" (page 150)
- "CS1000 and CS 1000M" (page 150)
- "Meridian 1" (page 150)
- "MCS 5100" (page 150)

MCDN

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

- transparent tunneling of MCDN information between multiple Communication Server 2000s (CS2000) with Communication Server 1000M/Business Communication Managers (BCM) connected at either end
- interworking support that allows the CS2000 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 Centrex IP Client Manager (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 Communication Server 2000 (CS2000) 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 node 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 CS2000 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 CS2000 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" (page 120):

- BCM interworking to CICM and Mediatrix for nodal calls and through SIP-T
- S1000 and S1000M interworking to Centrex IP Client Manager (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, CS2000 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 Communication Server 2000 (CS2000) 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" (page 120).

- 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 CS2000 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 (such as CND - Calling Number Delivery, CNAMD–Calling Name Delivery.).
- In the Centrex IP Client Manager (CICM) (CS2000) to S1000M direction, only private Numbering Plan Indication (NPI) calls contain this privately built MCDN tunneled data.Public calls do not contain MCDN tunneled data.

  In the CICM (CS2000) to S1000M direction, private NPI with Local Type of Number (TON) is coded as an UIPE ESN CDP TON.

- CS2000 Core Calling Name Delivery remains unchanged by this activity to either line agents or trunk agents; therefore, existing functions, 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:

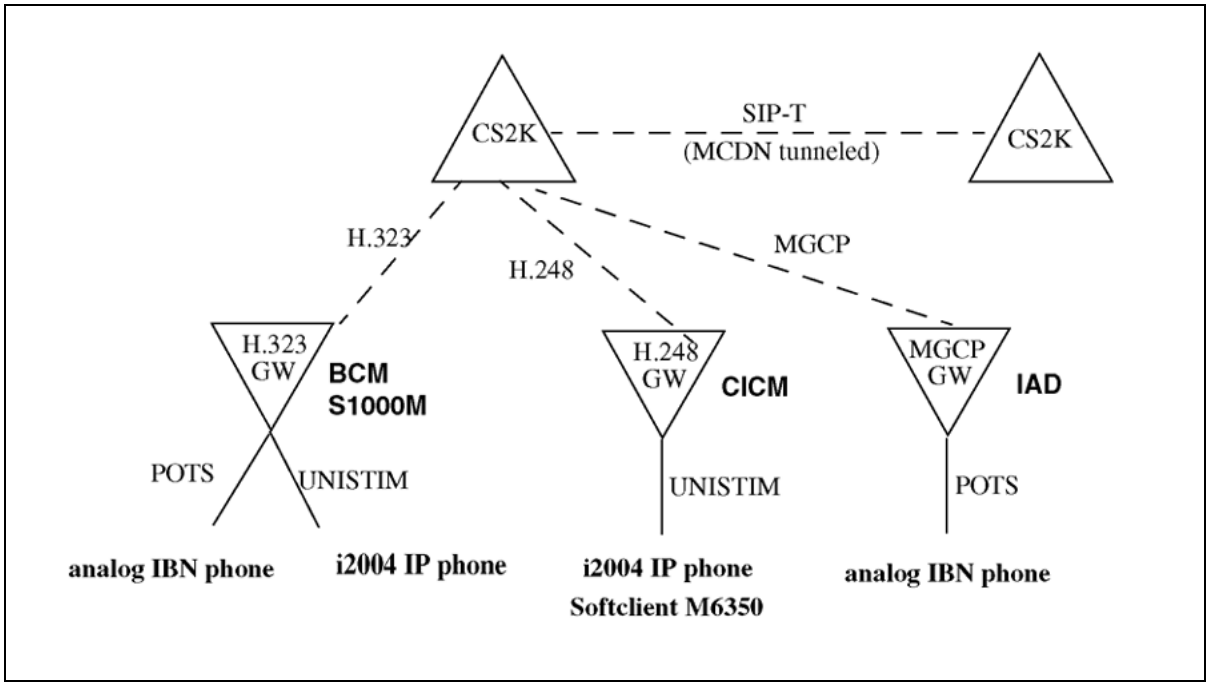
- MCDN interworking on nodal calls and via SIP-T (ETSI ISUP V2+ QFT) for inter-Call Server calls.
- MCDN based service interworking between the S1000M or BCM (H.323 GWs) on one call leg and Centrex IP Client Manager (CICM) (H.248 GW) or Mediatrix IAD (MGCP GW) on the other call leg.
- MCDN services which 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)

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

Associated network drawing



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" (page 120).

- 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" (page 120).

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 Communication Server 2000 (CS2000) through 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 CS2000. 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 user ID
- 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 CS2000 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 manager 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

Centrex IP Client Manager (CICM) allows for transparent access to 200-plus, Centrex-featured voice services.

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 four versions of the physical etherset: the i2001, i2002, i2004 or i2033. 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

Centrex IP Client Manager (CICM) has the following capacity limits:

- For each CICM Motorola CPN 5385 resource card pair:
  - 3,069 subscriber line—provisioning capacity
  - 21,600 busy hour half-call attempts (BHHCA)
  - 3,069 active calls
- CICM is scalable by adding more CICM processors
- One pair of CICM-EM cards is needed for each Communication Server 2000 (CS2000)
  - Able to support up to 100 CICM resource pair cards
- Per GWC resource card pair:

— 6,400 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" (page 151).

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

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.

Internet Transparency and security-related products

The Internet Transparency and security products deliver the following capabilities:

- Multiple IP VPN
- Enhanced support for emergency services on an Enterprise network.
- 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 CS2000 Interworking

Multimedia Communication Server 5200 (MCS) to Communication Swever2000 (CS2000) Interworking includes the following capabilities:

- MCS 5200 4.0 interworking in (I)SN08.
- North American market support for Converged Desktop between the MCS 5200 and CS2000 via IN-to-SIP signaling gateway:
  - Personal agent
  - Multimedia collaboration
  - Click to call to chosen device
  - Origination from telephone

MCS 5200 to CS2000 interworking supports the CS2000 and various H.323 gateways controlled by a CS2000, 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 CS2000 and MCS 5200 are interconnected through a SIP trunk.

Interoperability between MCS hosted users and CS2000-hosted H.323 gateways is supported in the same or different Enterprise/IP address spaces.

In order to create a VPN spanning the CS2000 and the MCS 5200, each customer group on the CS2000 is mapped onto one domain on the MCS 5200. For each VoIP VPN/domain, there is exactly one SIP trunk between the CS2000 and the MCS. Several VoIP VPNs may exist in a configuration consisting of a CS2000 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.

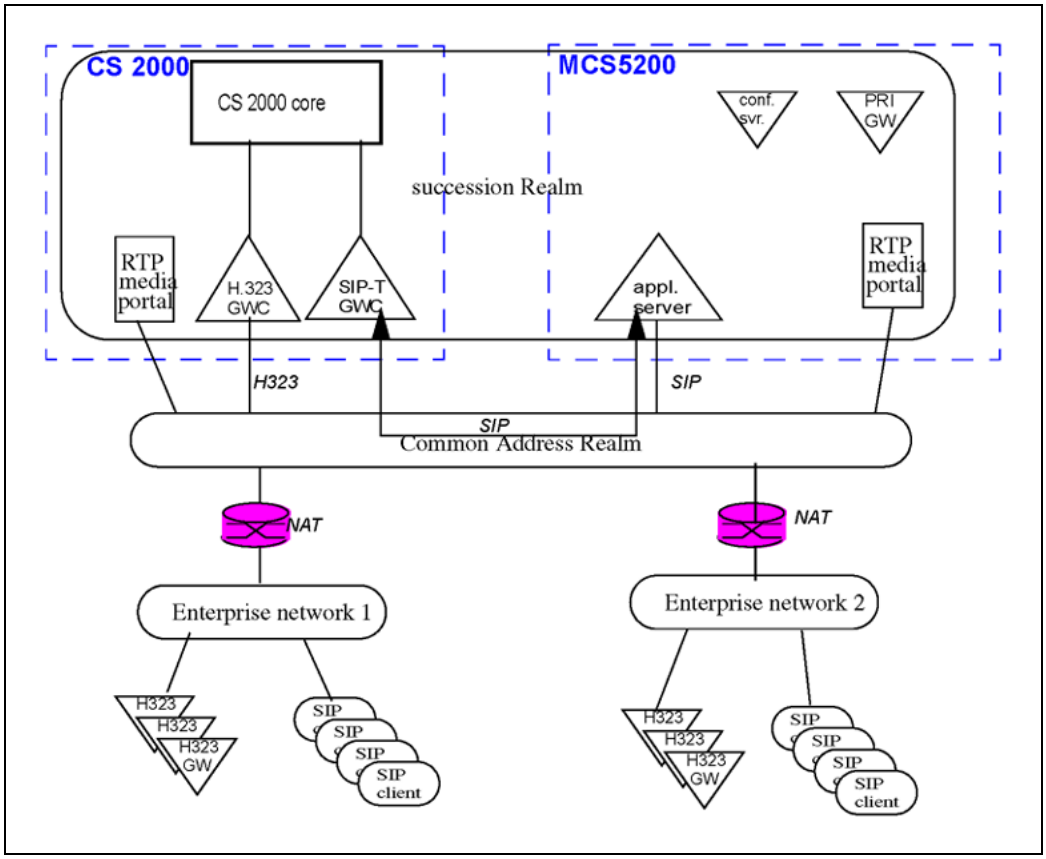
This feature supports G.711 and G.729 codecs at packetization rates of 10 and 20 ms.

The following MCS 5200 clients are supported:

- PC client
- Web client
- Nortel IP Phone 2004 and IP Phone 2002 internet telephones

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 CS2000
- VPNs hosted by several CS2000 interconnected by a SIP-T trunk

On the CS2000, the following H.323 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)

Media portal insertion

The media portal must be inserted on both the MCS 5200 and the Communication Server 2000 (CS2000) regardless of whether the MCS 5200 clients and the H.323 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 always perform a public/public NAT. That is, the Media streams between the MCS and the CS2000 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.)

  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 Nortel IP Phone 2002 or IP Phone 2004 Internet Telephone such that a specific hotline number is called when the subscribed user that is registered on the IP Phone 2002 or IP Phone 2004 Internet Telephone goes off hook.

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

- *Provisioning Client User Guide, NN10043-113*
- *IP Phone 2004 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 Communication Server 2000 (CS2000) 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 CS2000 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 CS2000 would insert RTP media portals on both the MCS 5200 and the CS2000.

This feature is restricted by the availability of supplementary services specified in the section "Supplementary services" (page 85).

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 CS2000 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-party SIP call servers
- Converged Desktop functionality through SIP for CS2000

The Session Server 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)SN08, refer to the documents on the component, "Session Server" (page 151).

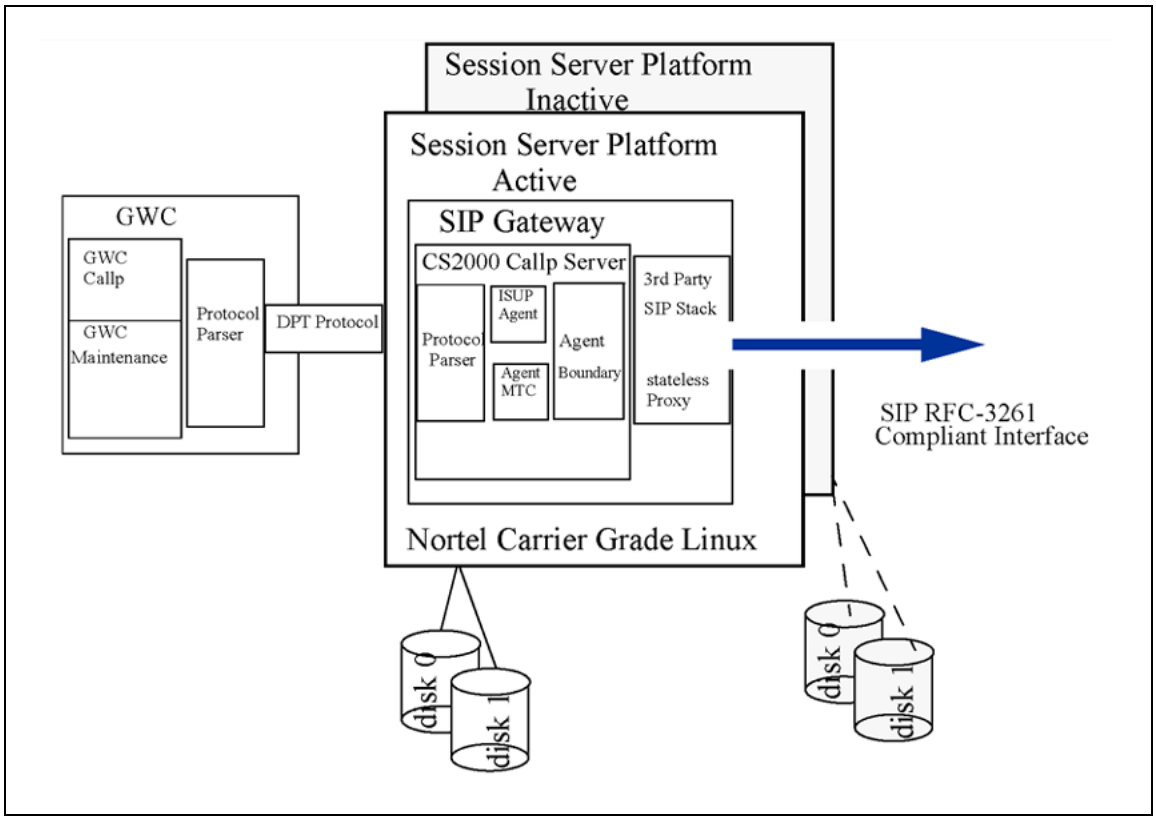
Session Server

The Session Server is a high-capacity, carrier-grade platform introduced in SN07. The Session Server is part of the Communication Server 2000 (CS2000) or CS2000–Compact and serves as a platform for the following applications:

- SIP Gateway Application
- Policy Controller

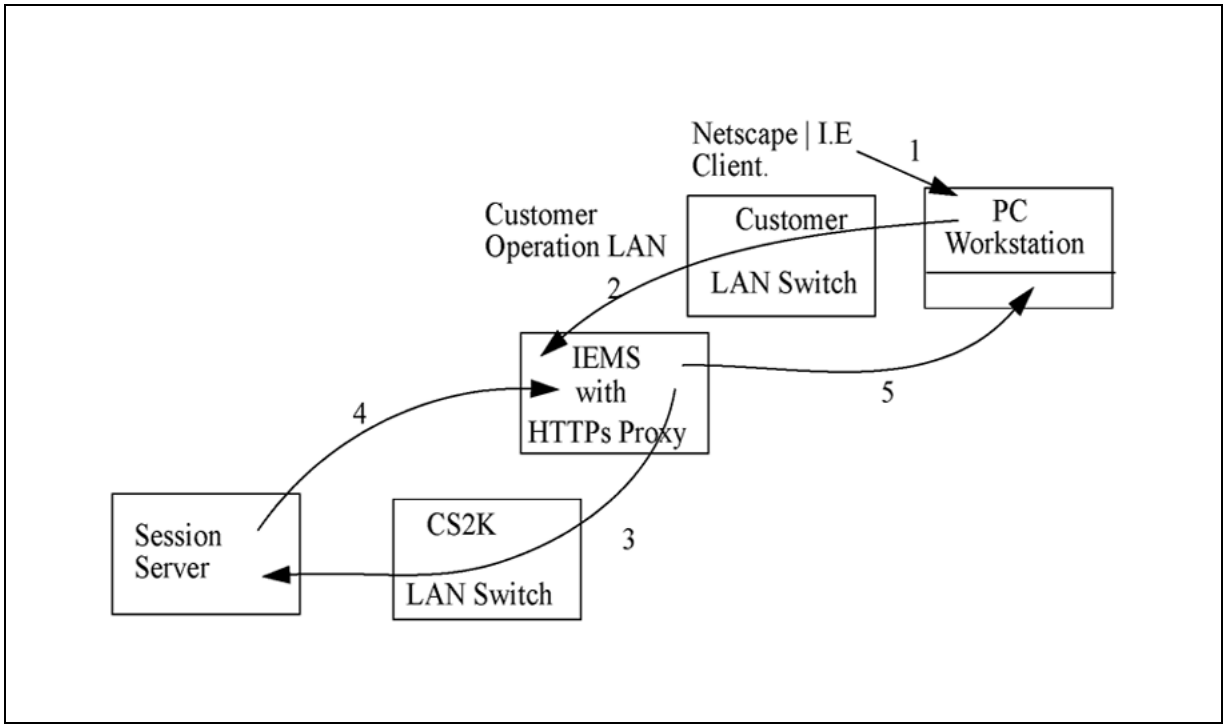
The architecture for the Session Server consists of a mated pair of Services Application Module- eXtreme Thin Servers (SAM-XTS) with a configuration similar to that of a gateway controller. Each unit is interconnected through a gigabit ethernet link as shown in the "Mated pair Session Server" (page 88). 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 CS2000 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.

SIP Gateway Application

The SIP Gateway Application supports call processing interoperability between the communication server, third-party call server, and application servers. Support includes the following functionality:

- set-up and take-down of SIP calls
- messaging to the DPT Gateway Controllers
- Messaging to remote SIP servers

The Session Server captures and stores all SIP messages related to call processing, including protocol events.

In release (I)SN08, The Session Server pegs OM counts for the SIP Gateway application on a more granular basis, such as per SIP link, to provide more details on the operations and performance of the Session Server

For more information about the Session Server, refer to the documents located in the CHS Solution collection in Helmsman Express. For a listing of documents, refer to "Session Server" (page 151).

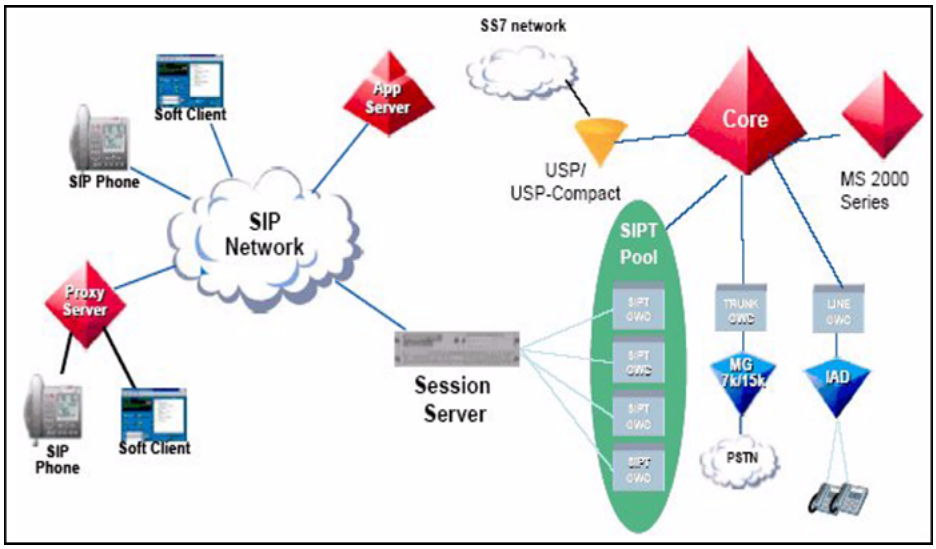
Policy Controller

The Policy Controller (PC) is a software application that resides on the Session Server. The Policy Controller provides network admission control for the clients and devices served from the CS2000 in CHS.

The focus of the Policy Controller is enforcement of resource control plane policies such as QoS policies in CHS. The Policy Controller combines awareness of subscribers with awareness of network resources to assure reliable network handling of media flows. Policy-based call admission control decisions in the Policy Controller take into account the requester's resource reservation request and available capacity to determine whether or not to accept the request.

The Policy Controller provides facilities for general application maintenance and network topology provisioning.

Policy Controller architecture



In release (I)SN08, VCAC Bandwidth Policy is the only policy supported. This policy carries out network resource reservation functions.

The Policy Controller applies the default policy to all requests for network resources to enforce call admission control. Resource requests can be in the form of a flow specification or an amount of bandwidth requested. The VCAC Bandwidth usage calculations are used to monitor the bandwidth usage status, and ensure there are enough resources for call requests.

The Policy Controller functions as its own element manager. Provisioning and maintenance activities for a Policy Controller take place on the Policy Controller itself. The provision framework provides a web based interface to configure Policy Controller system parameters, provision network topology, perform application management, and display Policy Controller-specific OMs, alarms, and logs.

Limitations and Restrictions

The release (I)SN08 deployment of Policy Controller has these limitations:

- each Policy Controller only supports one Communication Server 2000 (CS2000)
- if migrating from basic VCAC to network VCAC, initial commissioning requires a transfer of topology data from the SESM. The transfer requires the customer to perform these following tasks:
  - query the data from the OSS to the SESM
  - add the data to the Policy Controller
- The base platform does not support centralized authentication of passwords.
- The Policy Controller cannot co-run with other applications that reside on the Session Server.

VCAC

Virtual Call Admissions Control (VCAC) is a Quality of Service (QoS) mechanism that allows the Communication Server 2000 (CS2000) to cancel post-dial, pre-ringing calls that would overload a segment of the packet network.VCAC is used to provide Network Resource Based Admission Control by setting service class bandwidth limits based on the bandwidth available on the subscriber's access link. VCAC is virtual because it does not require interaction with real network elements. It models network elements and tracks the amount of bandwidth consumed by the application flows. When the model indicates that bandwidth is fully utilized and any additional flows would exceed link capacities, no additional flows are authorized.

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.

In release (I)SN08, the Policy Controller extends the VCAC functionality on the CS2000 Gateway Controller across the network. A network-wide VCAC allows the bandwidth resource through-links in an access network to be shared by all gateways and endpoints on a CS2000. Network VCAC removes the critical restrictions on deploying VCAC on sites with a mix of gateway types. Network VCAC also removes the limitation of an LBL and the gateway behind it having to be on the same GWC.

If the Policy Controller application is not available or the TCP connection between the GWC and the Policy Controller is down, the call will be allowed to go through without doing any checks on bandwidth availability. Should Policy Controller topology not know about any particular link it is queried on, it will reply with an error and the GWC allows the call to proceed without any QoS.

Network VCAC also supports composite middleboxes (a middlebox that is a NAT and LBL at the same time).

The SOC option must be in the ON state for Network VCAC to be usable. For information on enabling SOC, see "Enabling the VCAC SOC option on the CM" (page 114). For information on upgrading, see...

Limitations and Restrictions

The limitations and restrictions for Network VCAC are:

- network VCAC supports a single Communication Server 2000 (CS2000). It does not support multiple CS2000s or MCS.
- a maximum of five network links between a GW and the service provider’s core network
- only uses the negotiated values for a call
- requires that voice traffic is prioritized over data traffic

  VCAC does not model voice and non-SPC controlled data traffic on the same LBL. Careful modeling of the logical network is required.
- interactions with CODEC negotiation

  In a network configured to use G729 as the preferred CODEC and G711 as the default, the originator offers a list of CODECs to the terminator who chooses which one the call will use. Initially, the NVCAC application assumes the worst case (G711) at the originator until the negotiated SDP is returned by the terminator. However, this means that it is not

always possible to get the expected number of G729 on a link. This is difficult to detect as it is difficult to guarantee that all calls will negotiate G729.

CHS Limitations and Restrictions

The following limitations apply to release (I)SN08 and higher:

- Centrex IP Client Manager (CICM) Active Call Failover
- VCAC
- AOC over H.323

CICM Active Call Fail over limitations and restrictions

The following limitations apply to the Centrex IP Client Manager (CICM) Active Call Fail over function:

- During the switch of activity of the VMG component, only stable calls are guaranteed to survive. Unstable calls may or may not survive.
- Performing a stop or restart of a node from the element manager will not automatically initiate a switch of activity (SWACT) even if one may be desirable. It is the operator's responsibility to ensure the node is in the desired state before performing the stop. The element manager will however provide warnings of proceeding with any potentially service affecting actions.
- After it is initiated, a SWACT cannot be cancelled despite its possibly long duration. To return the system to its original pre-SWACT state, a second SWACT must be carried out once the first one completes.
- The only supported upgrade path to 8.10 is from 7.20 for both the CICM and EM. The 8.10 Element Manager may be used to manage release SN06.2, SN07, and SN08 CICMs.
- With 8.10, the CICM ceases to support a load-sharing mode. Active Call Fail over's goal is to shift the role of the secondary node from providing a load-sharing capability to providing full fail over redundancy.
- Because of the amount of processing work involved in the terminal recovery process, some real-time impact on call processing may arise during a SWACT.
- The terminal recovery process does not currently prioritize terminals in active calls over idle terminals. The recovery process aims to recover all terminals sequentially and without prejudice. However, the recovery process does give immediate priority to a terminal that experiences user interaction.
- During a SWACT, incoming events (state change requests) from the GWC will not be immediately presented to a non recovered terminal. Only at the point that the terminal is recovered is it presented the updates.

- In the rare case that the new master node should experience an outage while a switch of activity is in progress, it cannot be guaranteed that some terminals won't reboot and that calls won't be lost as a result.

VCAC limitations and restrictions

The VCAC architecture has some provisioning limits that are enforced by the provisioning system. These are:

- There is a maximum of 5 network links between a GW and the Service Provider's core network.
- VCAC only uses the negotiated values for a call. This means that fax and modem bespeaking to G711 from G729 will not be modeled. Similarly, T.38 fax calls will not change the modeled bandwidth for the call.
- There is a requirement that voice traffic is prioritized over the data traffic. VCAC does not model voice and non-PC controlled data traffic on the same LBL. This has to be done by careful modeling of the logical network as part of the system engineering.

AOC over H.323 limitations and restrictions

The following limitations apply to the AOC over H.323 functionality.

- Sending of AOC charge information as currency units is not supported for H.323 QSIG trunks at this time.
- AOC calculation based on the charging interval introduced with A00002625 is not supported.
- A delta may exist between the number of charge units saved in the AMA record by the CM feature 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 calculation done in the CM.
- The GW calculation of the AOC does not influence or change AMA records extension introduced with A00002638. There are no direct interactions between the AMA billing system and the AOC functionality in the GWC.
- AOC on H.323 QSIG is only supported for bearer calls. AOC on H.323 QSIG for non-bearer calls is not supported. Facility IEs with AOC operations for these calls are transparently passed through the CS2000.
- AOC-S (AOC at call setup) is not supporte.
- Provisioning of AOC can only be per trunk group and per GWC. AOC request is always on a per call basis.
- Out of the support AOC modes, only those will be delivered which are requested and provisioned at the same time.

- Only connection-oriented charging information is transmitted to the user (charges for supplementary services are not included).
- In case no system resources are available in the GWC, a FACILITY message with a Facility IE coded “chargeNot Available” is sent towards the originating H.323 gateway. If the AOCREL boolean is set in table TRKOPTS, the call is released; otherwise, it is not released.
- Race condition: If a call has AOC-D activated, the originating H.323 gateway might receive a FACILITY message after it sent out a ’getFinalCharge’ request. This message should not cause an erroneous charge display because it will be received before the release complete message with the final charge.
- The feature is supported over GWC Warm SWACTs. No errors are expected for Swacts with both units InSv. If the inactive unit is returned to service and then a Swact happens, there can be errors for the calls that were in talking state at RTS.
- The calculation of the charging rate time interval can produce a result which is not an exact multiple of 100ms. The result is therefore rounded up to the next 0.1 sec. multiple.
- Basic Service discounts are not supported on H.323 QSIG because there is not formal definition of Basic Service for H.323 QSIG, even though Bearer Capability and High Layer Compatibility are both defined. This means that table AOCBSDSC will not be used by AOC on H.323 QSIG.
- When changes are done in the table SERVINV, these are not dynamically reported to the GWC. After adding the AOC option, the GWC has to be double swacted in order for the changes to take effect.
- The SESM interface for table SERVINV does not support the AOC option. This option has to be manually added to the table SERVINV.
- The currency name can only consist of up to 10 capital letters (no lower case and blanks supported).
- Currency name changes affect calls in progress as well as new calls.
- It is possibly to define only 16 currency names and 16 currency units conversion factor per Call Server.
- A conversion factor change does not affect calls in progress; it only affects calls established after the changes.
- AOC charge requests arriving at the CS2000 after CONNECT are always rejected by the CS2000. This means that no AOC service will be provided for any charge requests received after CoNNECT.
- According to the AOC specification it does not make sense to send more than one AOC APDU per message. If an incoming message or

Facility IE contains more AOC InvokePDUs, only the first APDU per message is considered. The remaining APDUs are passed through towards the terminating party.

- If an AOC charge request is received in a FACILITY message during the overlap sending phase and before enough digits were received to route, the following situation may lead to failure to provide the service: the reception of the remaining digits necessary to find a reroute takes longer than 15 seconds. The reason is timer T1>=15 seconds running in the originating PINX, waiting for a reply to the request. This timer may time out, because CS2000 can send the reply only when it found the route. As a result, the PINX displays a not available message to the user and ignores the AOC information received from Communication Server 2000 (CS2000).
- Table TRKOPTS, AOC option, AOCREL = Yes datafill does not have an effect in the following situations (calls are not released):
  - No AOC service is provisioned, but a request is received. The request is replied with 'notAvailable' and the call continues. No CS2000 log is generated.
  - QSIG AOC is provisioned with protocol type KEYPAD or with charging type CHARGING (units). In these situations the system does not display a not available message, so no GWC Swerrs and CS2000 PM189 logs are generated, and no AOC information is sent out.
- The content of the Interpretation APDU in the AOC requests is not checked by CS2000. But the actions taken (which would depend on it) are always according to the AOC standard.
- AOC tariff determination is supported only for the combined CGP/CDP scenario. Support for the French NAOC trunk metering functionality (ITX/TAX messages) is not part of this activity. The translations table xxHEAD/xxCODE will therefor have to use the keyword (NAOCxxxx).
- The following restrictions already exist for the NAOC tariff database:
  - only 220 operators (16 carrier and 204 reseller) are available per CS2000 node
  - a pool of up to 30 TCOs is available for all operators (carrier and reseller) on a single CS2000 node. TCOs can be shared between operators
  - every carrier can address up to 1022 zones and up to 1022 tariffs. Zones cannot be shared between incompatible zone classes
  - a pool of up to 30 TCOs is available for all operators (arrier and reseller) on a single CS2000 node. TCOs can be shared between operators

- zoning for international calls is not available on a reseller basis
- only 10,000 ONDCs can be used for zoning national calls
- only 511 discounts are available per single CS2000 node
- all exceptions have to be zones as SERVice calls
- up to 4 million SERVice DNs can be datafilled in table SERVZONE

CS2000 H.323 limitations and restrictions

The following limitations apply to the Communication Server 2000 (CS2000) H.323 network.

- The CS2000 H323 system does not support silence suppression codecs: G.729b or G.729ab, G.723.
- Comfort noise on the CS2000 H.323 system is not supported.
- 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 timeout in the router should be set high enough to keep those long duration calls active, situations where the user tries to invoke a feature after talking for a long period of time. See "Configuration notes" (page 103).
- DISA Services:
  - For CS2000 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 CS2000, 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 CS2000, 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 CS2000 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 CS2000 marked as private. Instead, those fields are sent to the CS2000 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 release (I)SN08 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 audible ringback tone during the Call Setup (at the time of ALERTing).

- The BCM GW does not support SlowStart signaling on origination.
- The Communication Server 2000 (CS2000) H.323 System currently interoperates with Cisco's H.323 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-recvto
    ```

- 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 CS2000 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.
- Automatic Call Back (ACB) is supported in release (I)SN09FF; Network Ring Again is supported for calls within the same customer group.
- The following are a few features that are not currently supported on the CS2000 H.323 IPPBX.
  - Executive Busy Override (EBO)
  - Release Link Trunk (RLT)
  - 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 default 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.

- M1 Conference Keys only work after the conference party answers the call.
- H.323 GWs do not send any packets till the CONNECT. So you need to change to the loss timer on the Media Gateway 15000 to 0, see the third bullet of "Configuration notes" (page 103).
- 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.

This table lists ways to carry DTMF digits between different GWs:

Carrying DTMF digits between gateways

Termination 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
From the 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 plays the tone. DTMF digits pressed on the phone off Media Gateway 15000: –G.711 CODEC H.323 does not request to collect DTMF digits; so, DTMF from the Media Gateway 15000 is delivered as an in-band tone. –G.729 CODEC H.323 GWs do request the Media Gateway 15000 to collect DTMF digits; so, the DTMF from the Media Gateway 15000 is 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 does not play the tone. H.323 does not request Mediatrix to collect DTMF digits; so, DTMF pressed on Mediatrix is 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 hears 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 added to a conference call while still alerting, the H.323 subscriber does not receive audible ringback.

  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 Communication Server 2000 (CS2000) 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. You must change the loss timer on the Media Gateway 15000 (PVG) to 0.

Changing the loss timer on the Media Gateway 15000 to zero

Step	Action

At the command line

1 Open a Telnet session with the Nortel Networks Media Gateway 15000, and check the card slot you are using on the Media Gateway 15000.

2 Type this command:

```
St prov
```

3 Type this command:

```
set nsta/13 vgs brag/1 loss 0
```

4 Type this command:

```
set nsta/13 vgs brag/2 loss 0
```

5 Type this command:

```
set nsta/13 vgs brag/16 loss 0
```

6 Type this command:

```
act prov
```

7 Type this command:

```
confirm prov
```

—End—

- If RFC 2833 support is required for the in-band DTMF tones, make sure that RFC 2833 is checked on the Configure Network window of the Communication Server 2000 (CS2000) Mgmt GUI.
- CODECs are added to the CS2000 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 CS2000 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** variable is in the TABLE TRKOPTS for the SIP-T Trunks should be set as follows

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

  — **INTER DOMAIN** variable 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 timeout value of 35 minutes is recommended.

Configuration Management

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

Navigation

Integrated Element Management System

You can perform many fault, configuration, accounting, performance, and security activities in release (I)SN07 using the Integrated Element Management System (IEMS). For more information, refer to the *Integrated EMS Basics NTP, NN10329-111.*

To launch the Communication Server 2000 (CS2000) GWC Manager or the CS2000 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

Advice of Charge (AOC) gives the Communication Server 2000 (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" (page 108).

For APDU timing message considerations, refer to "Conditions for APDU timing messages" (page 109).

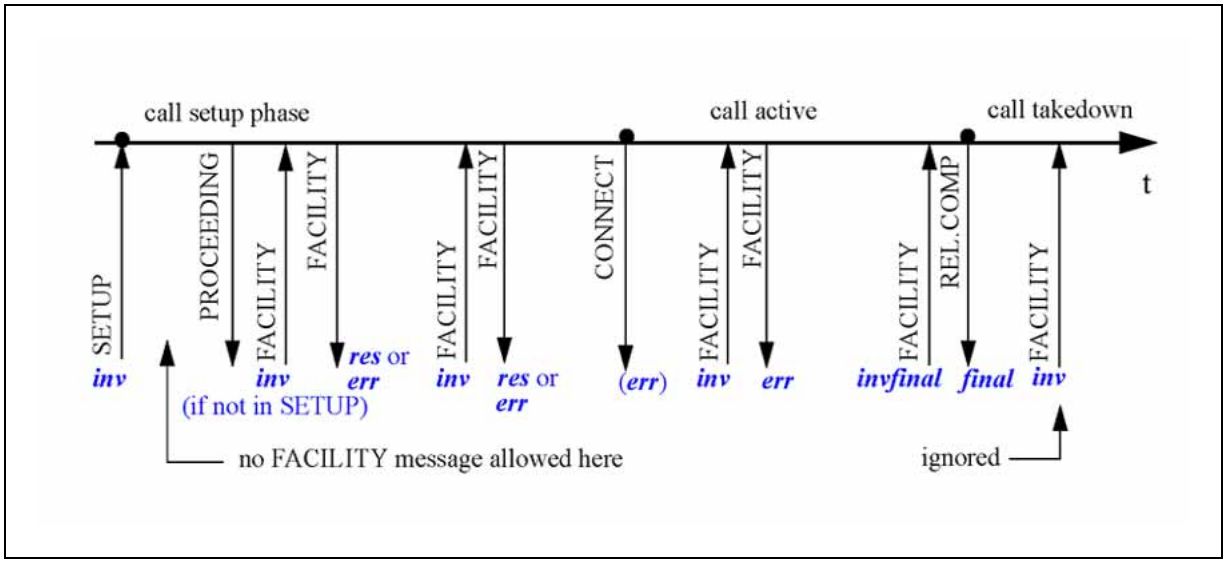
The following figure shows the per-call sequence of AOC requests and responses on a relative time scale, as supported by this activity.

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 is sent only 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 is replied to with an err APDU in FACILITY (supplementary Service Interaction Not Allowed).
- An inv APDU received after RELEASE COMPLETE is discarded by the CS2000 without reply.
- An invfinal APDU may be sent in a FACILITY message up to the beginning of the call take-down phase.

  Please note that H.323 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 "DCAM-1353602" (page 110).

- 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" (page 112).

Restrictions and limitations

The following restrictions and limitations apply to AOC:

- Sending of Advice of Charge (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 Communication Server 2000 (CS2000).

Provisioning AOC through table TRKOPTS

Use "DCAM-1353602" (page 110) to provision Advice of Charge (AOC) using the TRKOPTS table.

Step	Action

At the MAP terminal

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

```
> TABLE TRKOPTS
```

2 Press the **Enter** key.

Example response:

```
TABLE: TRKOPTS
```

3 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 Communication Server 2000 (CS2000) 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.

4 Exit the table editor.

—End—

Provisioning AOC through SOC

Step	Action

At the MAP terminal

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

```
> ASSIGN RTU <keycode> TO <SOC>
```

where

keycode is the keycode provided by Nortel
SOC is the SOC code (NETK0024, NSUP0020, NSUP0023, PBXT0011, PBXT0018)

2 Press the Enter key.

3 Activate the SOC code by typing

```
> ASSIGN STATE ON TO <SOC>
```

where

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

4 Press the Enter key.

—End—

Enabling VCAC SOC

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 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

Step Action

At the command line

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

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

Sample datafill for TABLE: TMTMAP

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

—End—

Datafilling the CM for VCAC-SOC and treatment

Step Action

ATTENTION

For line gateways using VCAC, you must datafill 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.

For example, NBLN Y S CONGESTION.

—End—

Enabling the VCAC SOC option on the CM

Step	Action

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

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
```

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
```

—End—

Disabling the VCAC SOC option on the CM

Step	Action

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
```

—End—

Migrating from Basic VCAC to Network VCAC on the Policy Controller

Purpose of this procedure

In release (I)SN08, the Policy Controller supports the Network Resource Reservation Policy using Network Virtual Call Admissions Control (VCAC) as the enforcement mechanism. Network VCAC enhances Basic VCAC and moves call admissions control from the Communication Server 2000 (CS2000) system to the Policy Controller.

Use procedure "DCAM-1353632" (page 116) to migrate from Basic VCAC to Network VCAC on the Policy Controller.

Limitations and restrictions

This procedure has the following limitations and restrictions:

- This procedure is only for offices that are already operating with Basic VCAC on their Communication Server 2000 (CS2000) system and are upgrading to Network VCAC.
- This procedure does not apply to offices with new installations that contain (I)SN08 Network VCAC or to offices upgrading to release (I)SN08 Basic VCAC.
- During the migration from Basic VCAC to Network VCAC, do not perform any Network zone provisioning until you activate Network VCAC on the Policy Controller.
- Activating Network VCAC is network-wide. You cannot operate both Basic VCAC and Network VCAC on your CS2000 network.
- There is no provisioning connection between the Policy Controller and the CS2000 system in release (I)SN08. You must provision all network zone topology information first into CS2000 system and then into the Policy Controller.

Prerequisites

This procedure has the following prerequisites:

- You must upgrade all Communication Server 2000 (CS2000) components to the (I)SN08 release before you begin this procedure. The CS2000 system continues to support Basic VCAC over the upgrade from the SN07 release to the (I)SN08 release until you activate Network VCAC.
- For upgrade procedures on CS2000 components, refer to *Upgrading a Carrier Voice over IP Network* (NN10440-450).

- You must already be operating Basic VCAC on your CS2000 network. The Basic VCAC value is set to ON.

Migrating from Basic VCAC to Network VCAC on the Policy Controller

ATTENTION

All NAT, LBL, and composite NAT-LBL zones must be configured identically and in the same order first on the CS2000 system and then on the Policy Controller. If you change a network zone attribute on the CS2000 system, you must immediately change it on the Policy Controller. Otherwise, Network VCAC will not function correctly.

For the CS2000 system network zone GUI configuration information, refer to NTP *Gateway Controller Configuration Management* (NN10205-511). For the CS2000, refer to NTP *Policy Controller Configuration Management* (NN10432-511).

Step	Action

At the SESM/OSSGate interface/Policy Controller

1 After the CS2000 components are upgraded to release (I)SN08, do not make any changes to the network zones (NAT, LBL, and composite NAT-LBL zones) on the CS2000 system until the switch to Network VCAC on the Policy Controller is complete. This restriction maintains consistency of the topology data on the CS2000 system and the Policy Controller and ensures Network VCAC will work properly.

2 Ensure that you have the network zone details (all NAT, LBL, and composite NAT-LBL zones) available from the CS2000 system.

Get a detailed list of network zones (NAT, LBL, or composite NAT-LBL zones) currently provisioned in the CS2000 system by querying all network zones names, IDs and network zone parents.

For the GUI procedure, refer to *View available network devices* in *Gateway Controller Configuration Management* (NN10205-511). For the XML procedure, use the XML command query **`NetworkZone`** in *OSSGate User's Guide* (NN10004-512).

3 Install and commission the Policy Controller with release (I)SN08.

For Policy Controller installation and commissioning procedures, refer to Installation Method *Policy Controller Installation and Commissioning* (IM 24-0493) and *Policy Controller Configuration Management* (NN10432-511).

4 Use the network zone data that you obtained from the CS2000 system to provision network zones on the Policy Controller. The

network zone data that you enter on the Policy Controller must be identical and in the same order as the network zone data currently on CS2000 system. You must add a network parent zone before its network child zone. To ensure a network zone match between the systems, you must manually verify that the network zone data is identical to both.

You can use either the GUI or XML procedure to add a network zone on the Policy Controller. Refer to the procedure *Add Network Zone* in *Policy Controller Configuration Management* (NN10432-511).

5 Add and provision the Policy Controller into the CS2000 system, which allows the CS2000 system to establish connection to the Policy Controller. Confirm that the Policy Controller is functioning correctly, that its TCP links to the CS2000 system are working, and no alarms have been generated.

For the GUI procedure, refer to *Add a Policy Controller* in the latest version of *Gateway Controller Configuration Management* (NN10205-511). For the XML procedure and the commands, refer to *OSSGate User's Guide* (NN10004-512).

ATTENTION

To minimize disruption to the network, perform the switch to Network VCAC during a period when there are fewer calls.

6 Using the GUI procedure or the XML command, switch ON Network VCAC. When Network VCAC is activated, the CS2000 system stops running Basic VCAC, and switches to using the Policy Controller for Network VCAC policy decisions.

For the GUI procedure, refer to the latest version of *Gateway Controller Configuration Management* (NN10205-511). For the XML procedure, refer to *OSSGate User's Guide* (NN10004-512).

When the Network VCAC is activated, all calls trigger bandwidth management through the Policy Controller. There is no current bandwidth status between Basic and Network VCAC so the Policy Controller will have no knowledge of existing calls that were set up under Basic VCAC. This condition can lead to temporary degradation of voice quality on some calls.

ATTENTION

The provisioning restrictions changed with release (I)SN08. Beginning with this release, it is possible to mix agent types (IAD, CICM, H323) behind a common link. Changes to agent types will not survive a rollback, so do not make any changes to the network zone topology until Network VCAC has had sufficient time to soak and be tested.

7 Verify call processing to confirm Network VCAC on the Policy Controller is functioning properly. Monitor the Policy Controller, Gateway Controller, and Core logs that indicate a problem. Before making any network zone topology changes, allow the system to soak for a period of time so potential errors can appear and be corrected.

8 When the system is functioning correctly, you can then make changes to the network zone data in the CS2000 system and the Policy Controller. Ensure that all network zone changes are entered identically first on the CS2000 system and then on the Policy Controller to manually keep them in synchronization doing forward. Otherwise, there will be a network zone topology mismatch and calls will fail.

For GUI procedures to add network zones and change network zone attributes for the CS2000 system and the Policy Controller, refer to the latest version of *Gateway Controller Configuration Management* (NN10205-511). For the XML procedures, refer to *OSSGate User's Guide* (NN10004-512).

—End—

Network VCAC rollback

ATTENTION

Only perform a rollback from Network VCAC to Basic VCAC during the period when you are preventing changes to the network zone topology in the CS2000 system (up to step 8). Otherwise, network zone topology mismatches can occur between the CS2000 system and the Policy Controller, causing Basic VCAC to work incorrectly.

Use procedure "DCAM-1353633" (page 118) to abort the switch to Network VCAC and rollback to Basic VCAC.

Step	Action

At the SESM/OSSGate interface

1 Deactivate Network VCAC in the CS2000 system. For the GUI procedure, refer to *Change the Network VCAC status* in the latest version of *Gateway Controller Configuration Management* (NN10205-511). For the XML procedure, refer to *OSSGate User's Guide* (NN10004-512).

After Network VCAC is deactivated, the CS2000 system manages bandwidth. The bandwidth status does not transfer from the Policy Controller to the CS2000, which can lead to temporary degradation of voice quality on calls. As existing calls clear, potential problems are removed.

—End—

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 Centrex IP Client Manager (CICM) clients.

Not all services are supported by both North American and international markets.

North American and international services supported by CICM clients

Option	Service	IP Phone 2004	IP Phone 2002	IP Phone 2033	m6350 SoftClient
3WC	Three Way Calling	x	x	x	x
AAB	Automatic Answer Back	x	x	x	x
ACB	Automatic Call Back	x	x	x	x
ACD	Automatic Call Distribution	x	x	x	x
ACD - AAK	ACD–Answer Agent Key	x	x	x	x
ACD - ACDNR	ACD–Automatic Call Distribution Not Ready	x	x	x	x
ACD - ASL	ACD–Agent Status Lamp	x	x	x	x
ACD - CAG	ACD–Call Agent	x	x	x	x
ACD - CIF	ACD–Controlled Interflow	x	x	x	x
ACD - CLSUP	ACD–Call Supervisor	x	x	x	x
ACD - DASK	ACD–Display Agent Status	x	x	x	x
ACD - DQS	ACD–Display Queue Status	x	x	x	x
ACD - DQT	ACD–Display Queue Threshold	x	x	x	x
ACD - ECM / ICM	ACD–Extended Call Management	x	x	x	x
ACD - EMK	ACD–Emergency Key	x	x	x	x
ACD - FAA	ACD–Forced Agent Availability	x	x	x	x
ACD - LOB	ACD–Line of Business	x	x	x	x
ACD - NGTSRVCE	ACD–Night Service	x	x	x	x
ACD - OBS	ACD–Observe Agent	x	x	x	x

Option	Service	IP Phone 2004	IP Phone 2002	IP Phone 2033	m6350 SoftClient
ACD - SUPR	ACD–Supervisor	x	x	x	x
ACRJ	Anonymous Caller Rejection	x	x	x	x
AIN	Advanced Intelligent Network	x	x	x	x
AINDN	AIN Directory Number	x	x	x	x
AINMWT	AIN Message Waiting	x	x	x	x
AMATEST	Automatic Message Accounting Test Call Capability	x	x	x	x
AMSGDENY	Access to Messaging Deny	x	x	x	x
AR	Automatic Recall	x	x	x	x
ARDDN	Automatic Recall Dialable DN	x	x	x	x
ATC	Automatic Time and Charges	x	x	x	x
AUD	Automatic Dial	x	x	x	x
AUL	Automatic Line	x	x	x	x
AUTODISP	Automatic Display	x	x	x	x
AVT	AUTOVON Termination	x	x	x	x
BLF	Busy Lamp Field for Meridian Business Sets	x	x	x	x
BNN	Bridged Night Number	x	x	x	x
CBE	Call Forwarding Busy Internal Calls Only	x	x	x	x
CBI	Call Busy Intragroup (or Channel Bus Interface)	x	x	x	x
CBU	Call Forwarding Busy Unrestricted	x	x	x	x
CCW	Cancel Call Waiting	x	x	x	x
CDC	Customer Data Change	x	x	x	x
CDE	Exclude External Calls from Call Forwarding	x	x	x	x
CDI	Exclude Intragroup Calls from Call Forwarding	x	x	x	x

Option	Service	IP Phone 2004	IP Phone 2002	IP Phone 2033	m6350 SoftClient
CDU	Call Forwarding Do Not Answer Unrestricted	x	x	x	x
CFB	Call Forwarding Busy	x	x	x	x
CFCW	Call Forward Call Waiting	x	x	x	x
CFD	Call Forwarding Do Not Answer (Business sets)	x	x	x	x
CFDVT	Call Forwarding Do Not Answer Variable Timer	x	x	x	x
CFF	Call Forwarding Fixed	x	x	x	x
CFGD	Call Forwarding Do Not Answer for Hunt Group	x	x	x	x
CFI	Call Forwarding Intragroup	x	x	x	x
CFK	Call Forwarding on a per Key Basis	x	x	x	x
CFMDN	Call Forwarding MADN Secondary Member	x	x	x	x
CFRA	Call Forwarding Remote Access	x	x	x	x
CFS	Call Forwarding Simultaneous Screening	x	x	x	x
CFTB	Call Forward Timed for CFB	x	x	x	x
CFTD	Call Forward Timed for CFD	x	x	x	x
CFU	Call Forwarding Universal	x	x	x	x
CFWVAL	Call Forwarding Validation	x	x	x	x
CID (NTS_CID)	Calling Party Identification	x	x	x	x
CIR	Circular Hunt	x	x	x	x
CLI	Calling Line Identification	x	x	x	x
CMCF	Control Multiple Call Forwarding	x	x	x	x
CNDBO	Calling Number Delivery Blocking Override	x	x	x	x
CNF	Station Controlled Conference	x	x	x	x
COT	Customer Originated Trace	x	x	x	x

Option	Service	IP Phone 2004	IP Phone 2002	IP Phone 2033	m6350 SoftClient
COTAMA	Customer Originated Trace with AMA	x	x	x	x
CPU	Call Pickup	x	x	x	x
CTD	Carrier Toll Denied	x	x	x	x
CTW	Call Transfer Warning	x	x	x	x
CWD	Dial Call Waiting	x	x	x	x
CWI	Call Waiting Intragroup	x	x	x	x
CWO	Call Waiting Originating	x	x	x	x
CWR	Call Waiting Ringback	x	x	x	x
CWT	Call Waiting	x	x	x	x
CWX	Call Waiting Exempt	x	x	x	x
CXR	Call Transfer	x	x	x	x
DCBI	Directed Call Pickup Barge-In	x	x	x	x
DCBX	Directed Call Pickup Barge-In Exempt	x	x	x	x
DCF	Denied Call Forwarding	x	x	x	x
DCPK	Directed Call Park	x	x	x	x
DCPU	Directed Call Pickup	x	x	x	x
DCPX	Directed Call Pickup Exempt	x	x	x	x
DENYCTFP	Deny Call Transfer Fraud Prevention	x	x	x	x
DENYISA	Deny In-Session Activation	x	x	x	x
DID	Direct Inward Dialing	x	x	x	x
DIN	Denied Incoming	x	x	x	x
DISA	Direct System Inward Access	x	x	x	x
DISP	Display	x	x	x	x
DLH	Distributed Line Hunt	x	x	x	x
DND	Do Not Disturb	x	x	x	x
DNH	Directory Number Hunt	x	x	x	x
DMCT	Deny Malicious Call Termination	x	x	x	x

Option	Service	IP Phone 2004	IP Phone 2002	IP Phone 2033	m6350 SoftClient
DNID (NTS_DNID)	Dialed Number Identification Delivery	x	x	x	x
DOD	Direct Outward Dialing	x	x	x	x
DOR	Denied Origination	x	x	x	x
DRCW	Distinctive Ringing/Call Waiting	—	—	x	—
DRING	Distinctive Ringing	x	x	x	x
DTM	Denied Termination	x	x	x	x
E911	Emergency Services (interaction support)	x	x	x	x
EBO	Executive Busy Override	x	x	x	x
EBX	Executive Busy Override Exempt	x	x	x	x
ELN	Essential Line	x	x	x	x
Int'l Emergency Call	International Emergency Call Routing	x	x	x	x
EMW	Executive Message Waiting	x	x	x	x
EXT	Extensiopossible Issued-On	x	x	x	x
FCTDINT	Full Carrier Toll Deny for International Carriers	x	x	x	x
FCTDNTER	InterLATA Full Carrier Toll Denied	x	x	x	x
FCTDNTRA	IntraLATA Full Carrier Toll Denied	x	x	x	x
FGA	Feature Group A	x	x	x	x
FNT	Free Number Terminating	x	x	x	x
FTRGRP	Feature Group	x	x	x	x
FTRKEYS	Feature Keys	x	x	x	x
FXR	Fast Transfer	x	x	x	x
ICSDEACT	In Call Service Deactivation	x	x	x	x
IECFB	Internal/External Call Forwarding Busy	x	x	x	x
IECFD	Internal/External Call Forwarding Do Not Answer	x	x	x	x
ILB	Inhibit Line Busy	x	x	x	x

Option	Service	IP Phone 2004	IP Phone 2002	IP Phone 2033	m6350 SoftClient
IN (CS-X)	Intelligent Networks (CS-X)	x	x	x	x
INSPECT	Inspect Key	x	x	x	x
INTPIC	International Primary Carrier	x	x	x	x
IRR	Inhibit Ring Reminder	x	x	x	x
JOIN	Conference Join	x	x	x	x
KSH	Key Short Hunt	x	x	x	x
KSMOH	Key Set Music on Hold	x	x	x	x
LCDR	Local Call Detail Recording	x	x	x	x
LI	Lawful Intercept	x	x	x	x
LMOH	Line Music on Hold	x	x	x	x
LNP	Local Number Portability (LRN based)	x	x	x	x
LNR	Last Number Redial	x	x	x	x
LNRA	Last Number Redial Associated with Set	x	x	x	x
LOD	Line Overflow to DN	x	x	x	x
LOR	Line Overflow to Route	x	x	x	x
LPIC	IntraLATA PIC	x	x	x	x
LVM	Leave Message	x	x	x	x
MBK	Make Busy Key	x	x	x	x
MBSCAMP	Meridian Business Set Station Camp-On	x	x	x	x
MCH	Malicious Call Hold	x	x	x	x
MDN MCA	Multiple Appearance Directory Number (MADN) Multiple Call Arrangement	x	x	x	x
MDN SCA	MADN Single Call Arrangement	x	x	x	x
MDNNAME	MADN Member Name	x	x	x	x
MEETME	Meet Me Conference	x	x	x	x
MEMDISP	MADN Member Display	x	x	x	x
MLAMP	MADN Lamp	x	x	x	x
MLH	Multi-line Hunt	x	x	x	x

Option	Service	IP Phone 2004	IP Phone 2002	IP Phone 2033	m6350 SoftClient
MREL	MADN Release	x	x	x	x
MRF	MADN Ring Forwarding	x	x	x	x
MRFM	MADN Ring Forwarding Manual	x	x	x	x
MSB	Make Set Busy	x	x	x	x
MSBI	Make Set Busy Intragroup	x	x	x	x
MWIDC	Message Waiting Indication	x	x	x	x
MWINK	MADN Message Waiting Indicator	x	x	x	x
MWQRY	Message Waiting Query	x	x	x	x
MWT	Message Waiting	x	x	x	x
NAME	Name Display	x	x	x	x
NOH	No Receiver Off-Hook Tone	x	x	x	x
OLS	Originating Line Select	x	x	x	x
ONI	Operator Number Identification	x	x	x	x
OP	Operator Services Access	x	x	x	x
PBL	Private Business Line	x	x	x	x
PCWT	Precedence Call Waiting Termination	x	x	x	x
PDO	Prevent Delete Option	x	x	x	x
PF	Power Features	x	x	x	x
PIC	Primary InterLATA Carrier	x	x	x	x
PILOT	Pilot DN Billing	x	x	x	x
PLP	Plug-up (Trouble Intercept)	x	x	x	x
PORT	10-digit unconditional LNP trigger	x	x	x	x
PPL	PVN Priority Line	x	x	x	x
PREMTBL	Call Pre-emption	x	x	x	x
PRESET CONF	Preset Conference	x	x	x	x
PRH	Preferential Hunting	x	x	x	x
PPK	Call Park	x	x	x	x
PRL	Privacy Release	x	x	x	x
PRV	Privacy for MADN	x	x	x	x

Option	Service	IP Phone 2004	IP Phone 2002	IP Phone 2033	m6350 SoftClient
QBS	Query Busy Station	x	x	x	x
QCK	Quick Conference Key	x	x	x	x
QTD	Query Time and Date	x	x	x	x
RAG	Ring Again	x	x	x	x
RCF/RCFEA	Remote Call Forwarding (Access to)	x	x	x	x
RCVD	Received Digits Billing	x	x	x	x
REASDSP	Reason Display	x	x	x	x
RPA	Repeated Alert	x	x	x	x
RSP	Restricted Sent Paid	x	x	x	x
RSUS	Requested Suspension	x	x	x	x
SACB	Subscriber Activated Call Blocking	x	x	x	x
SBLF	Set Based Lamp Field	x	x	x	x
SCA	Selective Call Acceptance	x	x	x	x
SCF	Selective Call Forwarding	x	x	x	x
SCL	Speed Calling Long	x	x	x	x
SCMP	Series Completion	x	x	x	x
SCRJ	Selective Call Rejection	x	x	x	x
SCS	Speed Calling Short	x	x	x	x
SCU	Speed Calling User	x	x	x	x
SDSDENY	Special Delivery Service Deny	x	x	x	x
SDY	Line Study	x	x	x	x
SEC	Security	x	x	x	x
SETMODEL	Set Model	x	x	x	x
SIMRING	Simultaneous Ringing	x	x	x	x
SL	Secondary Language	x	x	x	x
SLQ	Single Line Queuing	x	x	x	x
SLU	Subscriber Line Usage	x	x	x	x
SMDI	Simplified Message Desk Interface	x	x	x	x
SMDR	Station Message Detail Recording	x	x	x	x

Option	Service	IP Phone 2004	IP Phone 2002	IP Phone 2033	m6350 SoftClient
SOR	Station Origination Restriction	x	x	x	x
SORC	Station Origination Restrictions Controller	x	x	x	x
SPB	Special Billing	x	x	x	x
SPR	Selective Suppression of MDCR/SMDR	x	x	x	x
SSAC	Station Specific Authorization Codes	x	x	x	x
SUPPRESS	Suppress Line Identification Information	x	x	x	x
SUS	Suspended Service	x	x	x	x
SVCGRP	Service Group	x	x	x	x
TBO	Terminating Billing Option	x	x	x	x
TERM	Terminating DN Billing	x	x	x	x
TES	Toll Essential	x	x	x	x
TFO	Terminating Fault Option	x	x	x	x
TLS	Terminating Line Select	x	x	x	x
TollFree	Toll Free Services	x	x	x	x
UCD	Uniform Call Distribution	x	x	x	x
UCDLG	Uniform Call Distribution Login	x	x	x	x
WML	Warm Line	x	x	x	x
WUCR	Wake Up Call Ring Timeout	x	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.

North American and international services supported by H.323 for VoIP VPN

Service	H.323 Access	Media Gateway 15000 PRI	Media Gateway 1500 ISUP	DPT Access

		Access	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
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
BAS Offnet Access Services	x	x	x	x
BAS Flex Bellcore AMA	x	x	x	x
BAS SDM Table Access	x	x	x	x

a. Does not apply to North American markets.

Service	H.323 Access	Media Gateway 15000 PRI Access	Media Gateway 1500 ISUP Access	DPT Access
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
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
a. Does not apply to North American markets.				

Service	H.323 Access	Media Gateway 15000 PRI Access	Media Gateway 1500 ISUP Access	DPT Access
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
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	—	—

a. Does not apply to North American markets.

Service	H.323 Access	Media Gateway 15000 PRI Access	Media Gateway 1500 ISUP Access	DPT Access
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
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
NTS 800+CID DID Display/ CMS	x	x	x	x

a. Does not apply to North American markets.

Service	H.323 Access	Media Gateway 15000 PRI Access	Media Gateway 1500 ISUP Access	DPT Access
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.

North American services supported by H.323 for BCM interworking

	BCM interworking to			
Service	**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			
Called Number Delivery	x	x	x	x
Network Call Party Name Display				
Calling Party Name Delivery	x	x	x Note 3	x 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

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 CS2000 to S1000M direction, only private calls contain the MCDN private data (for displaying Calling Name). For CS2000 to S1000M direction, public calls do noy contain private MCDN data. Therefore, the public CS2000 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 functions, restrictions, or limitations of Calling Name Delivery are applicable.

	BCM interworking to			
Service	**CICM (nodal)**	**CICM (SIP-T)**	**IAD gateway (nodal)**	**IAD gateway (SIP-T)**
Network Hunting	—	—	—	—
Call Transfer	x	x	x	x
Call Pickup	—	-—	—	—
Network message services				
Message Waiting Indication	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 CS2000 to S1000M direction, only private calls contain the MCDN private data (for displaying Calling Name). For CS2000 to S1000M direction, public calls do noy contain private MCDN data. Therefore, the public CS2000 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 functions, restrictions, or limitations of Calling Name Delivery are 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.

International services supported by H.323 for BCM interworking

	BCM interworking to			
Service	**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 Centrex IP Client Manager (CICM) and IAD gateway for nodal calls, and calls through SIP-T.

North American (NA) services supported by H.323 for S1000M

	S1000M interworking to			
Service	**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			
Called Number Delivery	x	x		
Network Call Party Name Display				
Calling Party Name Delivery	x	x	x Note 3	x 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				

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 CS2000.

Note 3: Communication Server 1000M requires Calling Name to be tunneled within an H.323 Setup message. In addition, for the CS2000 to CS1000M direction, only private calls contain the MCDN private data for displaying Calling Name; public calls do NOT contain private MCDN data. Therefore, for public CS2000 to CS1000M direction, Calling Display is not displayed.

Note 4: Calling Name Delivery within the Core remains unchanged to either line agents or trunk agents; therefor, existing functions, restrictions, or limitations of Calling Name Delivery remain applicable.

	S1000M interworking to			
Service	**CICM (nodal)**	**CICM (SIP-T)**	**IAD gateway (nodal)**	**IAD gateway (SIP-T)**
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	—	x	x	x
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	—	—	—	—

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 CS2000.

Note 3: Communication Server 1000M requires Calling Name to be tunneled within an H.323 Setup message. In addition, for the CS2000 to CS1000M direction, only private calls contain the MCDN private data for displaying Calling Name; public calls do NOT contain private MCDN data. Therefore, for public CS2000 to CS1000M direction, Calling Display is not displayed.

Note 4: Calling Name Delivery within the Core remains unchanged to either line agents or trunk agents; therefor, existing functions, restrictions, or limitations of Calling Name Delivery remain applicable.

	S1000M interworking to			
Service	**CICM (nodal)**	**CICM (SIP-T)**	**IAD gateway (nodal)**	**IAD gateway (SIP-T)**
Network Wide Calling Party Privacy	—	—	—	—
Display of Calling Party Denied	—	—	—	—
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	—	—	—	—

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 CS2000.

Note 3: Communication Server 1000M requires Calling Name to be tunneled within an H.323 Setup message. In addition, for the CS2000 to CS1000M direction, only private calls contain the MCDN private data for displaying Calling Name; public calls do NOT contain private MCDN data. Therefore, for public CS2000 to CS1000M direction, Calling Display is not displayed.

Note 4: Calling Name Delivery within the Core remains unchanged to either line agents or trunk agents; therefor, existing functions, restrictions, or limitations of Calling Name Delivery remain applicable.

	S1000M interworking to			
Service	**CICM (nodal)**	**CICM (SIP-T)**	**IAD gateway (nodal)**	**IAD gateway (SIP-T)**
Electronic Tandem Network	—	—	—	—
Meridian Switched Network Variable Types of Outpulsing on Same Call	—	—	—	—
Network CLID and NCOS Display Interaction with 3WC	—	x	—	—
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 CS2000.

Note 3: Communication Server 1000M requires Calling Name to be tunneled within an H.323 Setup message. In addition, for the CS2000 to CS1000M direction, only private calls contain the MCDN private data for displaying Calling Name; public calls do NOT contain private MCDN data. Therefore, for public CS2000 to CS1000M direction, Calling Display is not displayed.

Note 4: Calling Name Delivery within the Core remains unchanged to either line agents or trunk agents; therefor, existing functions, 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 Centrex IP Client Manager (CICM) and IAD gateway for nodal calls, and calls through SIP-T.

International services supported by H.323 interworking

	BCM interworking to			
Service	**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 CS2000

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

Release (I)SN07 DPNSS international services

DPNSS Service	Nodal Transit (Note 1)	Network 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 CS2000.
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	—	—

Note 1: Nodal Transit refers to a transit configuration where Communication Server 2000 (CS2000) 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.

DPNSS Service	Nodal Transit (Note 1)	Network 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	—	—
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	—	—

Note 1: Nodal Transit refers to a transit configuration where Communication Server 2000 (CS2000) 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.

DPNSS Service	Nodal Transit (Note 1)	Network Transit (Note 2)	End Node Calling/ Called	Comment
Traveling Class of Service	X	X	—	—
Number Presentation Restriction	X	X	—	—

Note 1: Nodal Transit refers to a transit configuration where Communication Server 2000 (CS2000) 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 release (I)SN07.

Release (I)SN07 international DPNSS/Centrex services

DPNSS Service	Nodal Transit	Network Transit	End Node Calling/ Called	Comment
Meet Me Conference (Flash only)	X	X	X	—
Station Controlled Conference	X	X	X	—
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 call is forwarded over UKISUP.

DPNSS Service	Nodal Transit	Network Transit	End Node Calling/ Called	Comment
Call Forward Immediate	X	X	X	The call is forwarded over UKISUP.
Call Forward Busy	X	X	X	The call is forwarded over UKISUP.

Customer support

Solution and customer support

Nortel 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 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

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

Customer information

Software release and support policy

A 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 software release.

Ordering and support overview

A 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 does not recommend using retired (unsupported) software releases in existing offices and does not deploy a retired release to an initial (new) installation or an extension. Therefore, each individual 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 for 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, software releases reach FVS status every 6 months. Thus, 6 months after FVS of a software release, another new release becomes available for ordering and loading. The network provider can choose either to deploy this next 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.

ATTENTION

Any updates or exceptions to the Software Release and Support Policy must be made through Solution/Service Update and/or Solution/Service Information publications. Contact your Nortel representative for more information about Nortel 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
VPN Router 600	Software support is available for the last published software release and one release back (including their associated patches, fixes, and workarounds).
Ethernet Routing Switch 8600/Device Manager	Software support is available for the last published software release and one release back (including their associated patches, fixes and workarounds).
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.

In addition to the optional support packages, Nortel 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 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 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.

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

Access from the Nortel 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 electronic software delivery server to the customer LAN/WAN, the security algorithm is used. For Nortel Multiservice Data Manager software loads, the Nortel 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 for help on customer information

Contact the Nortel account prime for help on customer information.

Customer information

Nortel 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 Voice over IP Network solution is delivered on a CD ROM.

For valuable customer information, refer to Nortel 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:

- CS2000
- CS2000–Compact
- CS2000 Management Tools
- Gateway Controller
- Nortel Multiservice Switch 15000 and 20000
- Nortel Multiservice Data Manager
- MDM
- UAS
- USP
- USP–Compact

- XA–Core

BCM

BCM information is located in the Business Communications Manager 3.7 collection in Helmsman. In particular, refer to:

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

Business Communication Manager (BCM) documentation

BCM documents	Title
N0008589	Programming Operations Guide
N0008591	IP Telephony Configuration Guide

CS1000 and CS 1000M

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

Communication Server 1000 and CS1000M documentation

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
555-3001-363	IP Trunk: Description, Installation and Operation
553-3001-365	IP Line: Description, Installation and Operation
553-3031-258	Nortel Communication Server 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.

Centrex IP Client Manager (CICM) documentation

CICM	Title
NN10027-113	CICM Etherset Installation Guide and User Manual
NN10182-113	m6350 Softclient Installation Guide
NN10183-114	m6350 Softclient Branding Kit
297-5551-901	m6350 TAPI Service Provider Installation and Troubleshooting Guide
NN10044-111	CICM Basics
NN10230-461	CICM Upgrades
NN10027-111	CICM Fault Management
NN10240-511	CICM Configuration Management
NN10244-811	CICM Accounting Management
NN10248-711	CICM Performance Management
NN10252-611	CICM Security and Administration

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 documentation

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 Communicatin Server 2000 (CS2000), refer to the following table of documents located in the **Multimedia Communication Portfolio** collection in Helmsman Express.

RTP Media Portal dedicated documentation sources

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

For more information on the MCS RTP Media Portal when in association with a CS2000 refer to the following document located in the **Multimedia Communication Portfolio** collection in Helmsman Express.

MCS RTP Media Portal with CS2000 documentation

RTP Media Portal interop with CS2000	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 Basics

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 Basics

MCS interworking	Title
NN10372-111	MCS 5200 Interworking Basics

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.

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

Acme Packet training

Course descriptions, locations and information specific to Acme Packet products can be found at www.acmepacket.com. Select Training from the Support menu for a list of courses currently available, or contact training@acmepacket.com for further inquiries and registration.

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 Communication Server 2000 (CS2000) and for Nortel 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" (page 147) section.

Operations support services

Nortel 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 business hours or as scheduled with a TAS supervisor
- response from Nortel 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 onsite 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 VoIP

Carrier Hosted Services Basics

Publication: NN10234-100
Document status: Standard
Document version: 06.02
Document date: 20 October 2006

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

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