Configuration Management: Carrier Hosted Services

What’s new in this release?

PVG naming - The table below lists the names used for certain gateways in Carrier VoIP documentation prior to (i)SN07 and provides the new brand names starting in (i)SN07.

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

The Integrated Element Management System (EMS) supports Carrier Voice over IP (VoIP) components in (i)SN07.

The following table highlights the services and features in (I)SN07 Carrier Hosted Services(CHS).

H.323 service offering in (I)SN07 CHS

H.323 Service	
A00005822	AOC Support over H.323 AOC enables ISDN (BRI, PRI, and Q.SIG) subscribers to be informed of the number of charge units they incur for a call either during (using AOCD provisioning suboption) or at the end (using the AOCE provisioning) of a call. Refer to Provisioning Advice of Charge on page 15
A00002550	H.323 Gatekeeper to CS2000 Gatekeeper Interoperability This feature enables H.323 Gatekeepers in an external network (private, enterprise, other carrier's, etc.) to interop with a CS2000CS2000 H.323 Gatekeeper on a carrier network. For information on configuration procedures, refer to Configuring H.323 Gatekeeper to CS2000 Gatekeeper Interoperability on page 91
A00002739	Virtual Connections Admission Control (VCAC) This VCAC feature describes the functionality provided by VCAC, SOC requirements, CM datafill, and treatment. For provisioning information for VCAC SOC option, refer to Datafilling the CM for VCAC-SOC and treatment on page 105
A00003626	H.323 Support for Meridian Customer Defined Network (MCDN) Services (International CS2000 load) This feature • Allows the interconnection of MCDN based PBXs with certain line gateways for use in networked VPNs. • Supports MCDN interworking on nodal calls and via SIP-T (ETSI ISUP V2+ QFT) for inter-Call Server calls. • Implements and verifies a subset of MCDN services that are supported on P-phone agents or IBN lines agents. • Implements and verifies MCDN based services for the CS2000 international load. Support and verification for NA-load is provided by activity A00004096, NA Support for networked MCDN services. For more information, refer to Configuring H.323 support for MCDN Services on page 37
A00003627	T.38 FAX Support for International H.323

H.323 service offering in (I)SN07 CHS

H.323 Service	
	This activity provides “Call Server controlled switchover to T.38 (or G.711)” for Call Server routed H.323 calls. Fax interworking is supported on calls between H.323 GWs (e.g. Meridian, Cisco, BCM) and H.248 GWs (e.g. Media Gateway) or MGCP GWs (e.g. Mediatrix). At least one involved agent must be H.323. This activity builds on top of the SN06.1 activity A00001895 “H.323 Base Application” that included development to support basic call capabilities for H.323 GWs connected to the CS2000 (International CS2000 load). For more information, refer to the following • Configuring Call Server controlled switch over to T.38 on page 41 • Configuring H.248 for a T.38 fax call on page 45 • Configuring MGCP for a T.38 fax call on page 49
A00003628	Interworking Int’l H.323 to SIP MCS 5200 This International (i)SN07 activity verifies the interworking of various H323 gateways controlled by a CS 2000 and various SIP clients controlled by the Nortel Networks MCS 5200 system. The MCS 5200 is part of a carrier hosted voice VPN. The CS 2000 and MCS 5200 are interconnected through a SIP trunk. Refer to Interworking International H.323 to SIP MCS 5200 on page 53
A00004952	Interworking NA H.323 to SIP MCS 5200 The A00004952 North American (NA) activity verifies the interworking of various H323 gateways controlled by a CS 2000 and various SIP clients controlled by the Nortel Networks MCS 5200 system. Refer to Interworking North American H.323 to SIP MCS 5200 on page 69
A00003629	International H.323 MCDN Feature Transparency (Tunneling) for Multi Call-Server The scope of A00003629 is to ensure that the information to transact Meridian Customer Defined Network (MCDN) based services is tunneled for MCDN-capable gateways in inter-call server configurations using SIP-T (ETSI ISUP V2+ and QFT). For more information, refer to Configuring an International H.323 Network for a Multi-Call Server on page 77
A00003995	H.323 Gateway Change Capability

H.323 service offering in (I)SN07 CHS

H.323 Service	
	The H.323 gateway change capability, A00003995, is a service that allows the ability to change the initial provisioning of the H.323 gateway without affecting already provisioned GWs and EPGs. For more information, refer to Configuring H.323 Gateway Change Capability on page 35
A00004096	NA Support for Networked MCDN Services This feature allows interworking of MCDN based PBXs with certain hosted NA CS2000 centrex lines for use within the Enterprise network. Therefore, this feature addresses the development associated with providing the NA CS2000 switch the ability to support a specified set of MCDN services for its hosted centrex lines (i.e., CICM and Mediatrix 1104) within a carrier hosted H.323 network. For more information, refer to Configuring an NA H.323 for Networked MCDN services on page 87
A00004568	H.323 NA Networked CAS Tunneling This activity provides the functionality to support the tunneling of ANSI Call Associated (CAS) messages between 2 CS2000s via SIP-T, in support of the H.323 protocol. For more information, refer to Configuring H.323 NA Network CAS Tunneling on page 79
A00006495	H.323 Flexible Carriers The (i)SN07 activity A00006495 delivers the ability to add H.323 “virtual carriers” with “flexible” sizes to an H.323 gateway. For more information refer to Configuring an H.323 Flexible Carrier on page 85
A00006496	Multi D-Channel Support In (i)SN07, functionality for provisioning has been added or amended to exiting functionality. For more information, refer to Configuring multi D-channel support on page 95

SIP service offering in (I)SN07 CHS

SIP Service	
A00003933	SIP on SP2000 The Succession Communication Server 2000 Session Server Manager (SCS 2000) SIP gateway application delivers an RFC 3261 compliant interface for the CS 2000 that enables open operability with call servers, application servers, and proxy servers using Session Initiation Protocol (SIP). For location of information, Reference documentation on page 151
A00004005	Nortel Carrier Grade Linux (NCGL) platform “Session Server” The purpose of this design is to create a highly available base platform for delivery of multiple applications. The Session Server consists of a Network Equipment-Building System (NEBS) Level 3 compliant hardware platform plus a software framework and architecture for developing Carrier Grade applications and services. For related Session Server documentation, refer to Nortel Carrier Grade Linux (NCGL) platform Session Server on page 153
A00003653	Line Option of IPCM phones As part of the Nortel Networks Enterprise S2100 softswitch solution and the legacy SL-100, the IP Client Manager (IPCM) is a UNIStim phone gateway that hosts several models of IP phones. IPCM is the name for the Enterprise version of the Centrex IP Client Manager (CICM). For more information, refer to Configuring an IP Client line option for Centrex IP Service on page 149

VCAC service offering in (I)SN07 CHS

VCAC Service	
A00002512	GWCEM internet transparency VCAC provisioning. Refer to Provisioning GWCEM internet transparency for VCAC on page 99
A00004981	VCAC support for CICM gateways. Refer to Configuring VCAC support for CICM gateways on page 97
A00002644	Common Topology elements. Refer to Configuring Common Topology elements for VCAC on page 101

E911 service offering in (I)SN07 CHS

E911 Service	
A00003568	Emergency 911. Refer to Configuring E911 on page 103
A00003970	ECS VoIP Client Dynamic Discovery. Refer to Configuring E911 on page 103

Carrier Hosted Services

What’s new?

For the location of CHS-related documentation, refer to

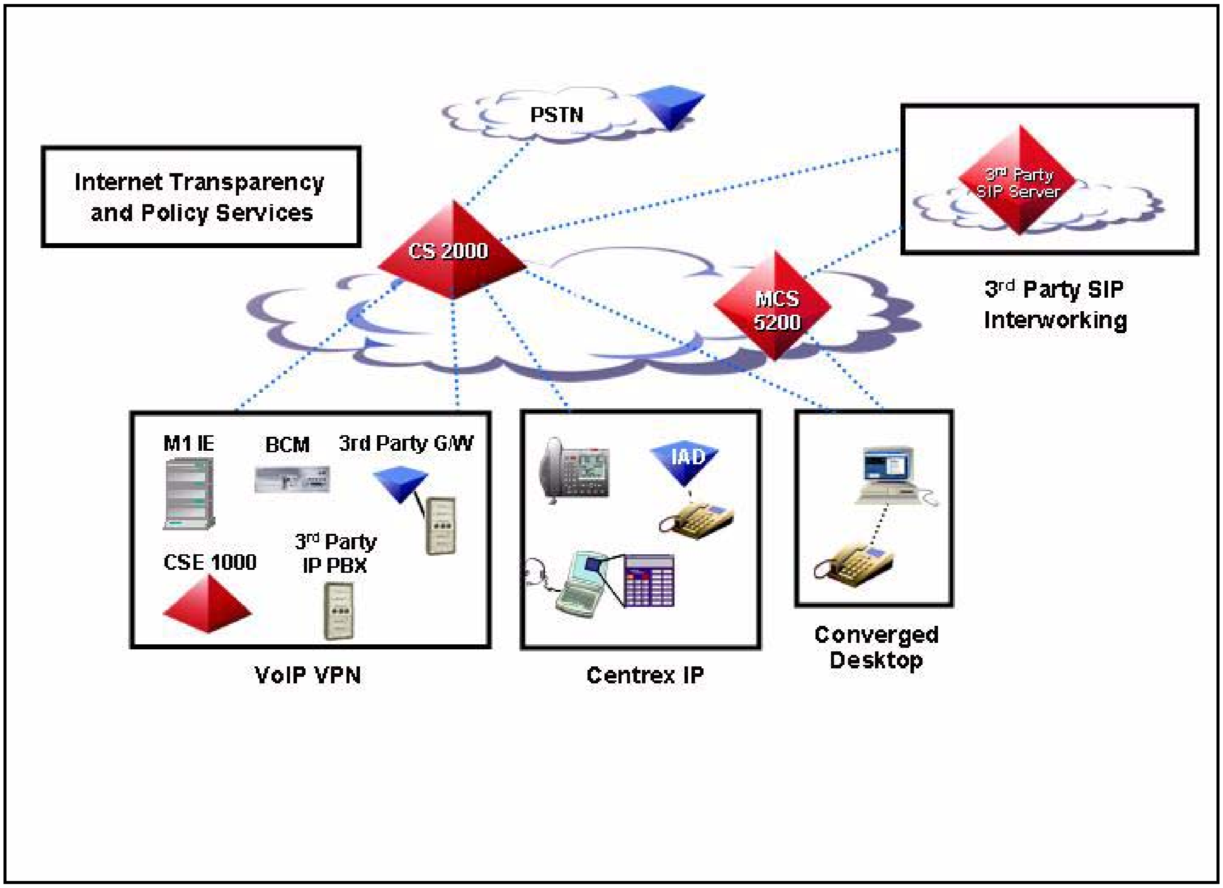
Where to get customer documentation on page 213

Overview

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

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

CHS architecture



VoIP technology enables voice to be carried over a data 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

Services

CHS includes the following services:

- VoIP VPN, which includes the following capabilities:
  - Network level servicing:
    - translations and routing
    - VPN services
    - Centrex groups
    - access to and from the Public Switch Telephone Network (PSTN)
  - Network access using H.323 specifications:
    - IP-based networks
    - feature transparency (Meridian Customer Defined Network [MCDN] and Digital Private Network Signaling System [DPNSS])
    - interworking to trunks and lines
  - Network interoperability supported
    - H.323 CS2000 Gatekeeper to Succession 1000 Gatekeeper
    - H.323 interworking to Cisco Call Manager
    - H.323 gateway media interoperability with MCS 5200 clients
    - H.323 to IP gateway interworking enhancements to support T.38 Fax and dual tone multifrequency (DTMF) interworking with an anchor packet gateway (APG)
- MCDN support

  CHS introduces enhanced Meridian customer defined networking (MCDN) support:
  - transparent tunneling of MCDN information between multiple CS 2000s with Succession 1000M/Business Communication Managers(BCM) connected at either end
  - interworking support that allows the CS 2000 to terminate MCDN functionality and interwork with Centrex lines, providing enhanced support for Enterprises with users split between IP-PBXs, integrated business network (IBN) Centrex lines, and Centrex IP lines of the CICM
- CICM, which includes the following capabilities:
  - H.248 connectivity with the CS 2000
  - support for NA and International markets

  - single-board gateway for 1000-user capacity
  - Real Time Protocol (RTP) Media Portal integration for Network Address Translation (NAT)/firewall traversal
  - multiple NAT domain support using virtual gateways
  - RFC2833 for inband tones
  - codec negotiation based on audio profile
  - DNR
- Internet Transparency and security-related products, which include the following capabilities:
  - Multiple IP-VPN and NAT/firewall traversal
  - Lawful Intercept (LI)
  - Emergency 911 (E911) enhanced support on the Enterprise network
- Multimedia Communication Server 5200 (MCS) to CS 2000 Interworking, which includes the following capabilities:
  - MCS 5200 3.0 interworking using IN-to-SIP
  - initial IN-to-SIP Blended User Agent between the MCS 5200 and the CS 2000:
    - Personal agent
    - Multimedia collaboration
    - Click to call to chosen device
    - Origination from telephone
- Third-party SIP interworking, which includes the following capabilities:
  - integration ready for third-party SIP application servers
  - integration ready for third-part SIP call servers

Carrier Hosted Services VoIP VPN

What’s new?

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

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

For location of documents, refer to the Reference information on page 14

BCM / CS 2000 upgrade

The upgrade procedure only pertains to customers already using the BCM 3.5 / SN06.2 load line-up. The subsequent releases of BCM and CS 2000 are BCM 3.6 and (i)SN07. This product combination has gone through full Product Verification (PV), and following successful achievement of both CS 2000 Verification Office (VO) and BCM Beta trial exit criteria, will be Nortel Networks preferred load line-up combination. The upgrade process should consist of first upgrading the CS 2000 to the SN07 load followed by upgrades of the customer equipment to BCM 3.6.

Note that during the BCM upgrade process, VoIP service will be disrupted until the BCM upgrade has been completed and three parameters on the BCM have been re-programmed through the BCM Unified Manager administration interface. The value of three parameters, the H.323 Call Signaling Port, the H.323 RAS port, and the H.245 Tunneling setting, do not get carried forward during the BCM 3.6 upgrade and need to be manually changed after the upgrade. After the upgrade the two RAS port settings are, by default, reversed from the required values. These parameters should be manually programmed through the Local Gateway IP Interface tab under the Services/IP Telephony/IP Trunks/H.323 Trunks section of the Unified Manager interface. The correct settings for these parameters are as follows:

After the BCM upgrade

- H.245 Tunneling: Enabled
- Call Signaling Port value: 0
- RAS Port value: 1719

All other BCM H.323 parameters associated with BCM/CS 2000 interoperability will be preserved during the BCM 3.6 upgrade process; the three parameters identified above will be preserved in any subsequent BCM upgrades beyond BCM 3.6, and no manual correction will be required.

Overview

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 Carrier Hosted Services VoIP VPN service offers the following benefits:

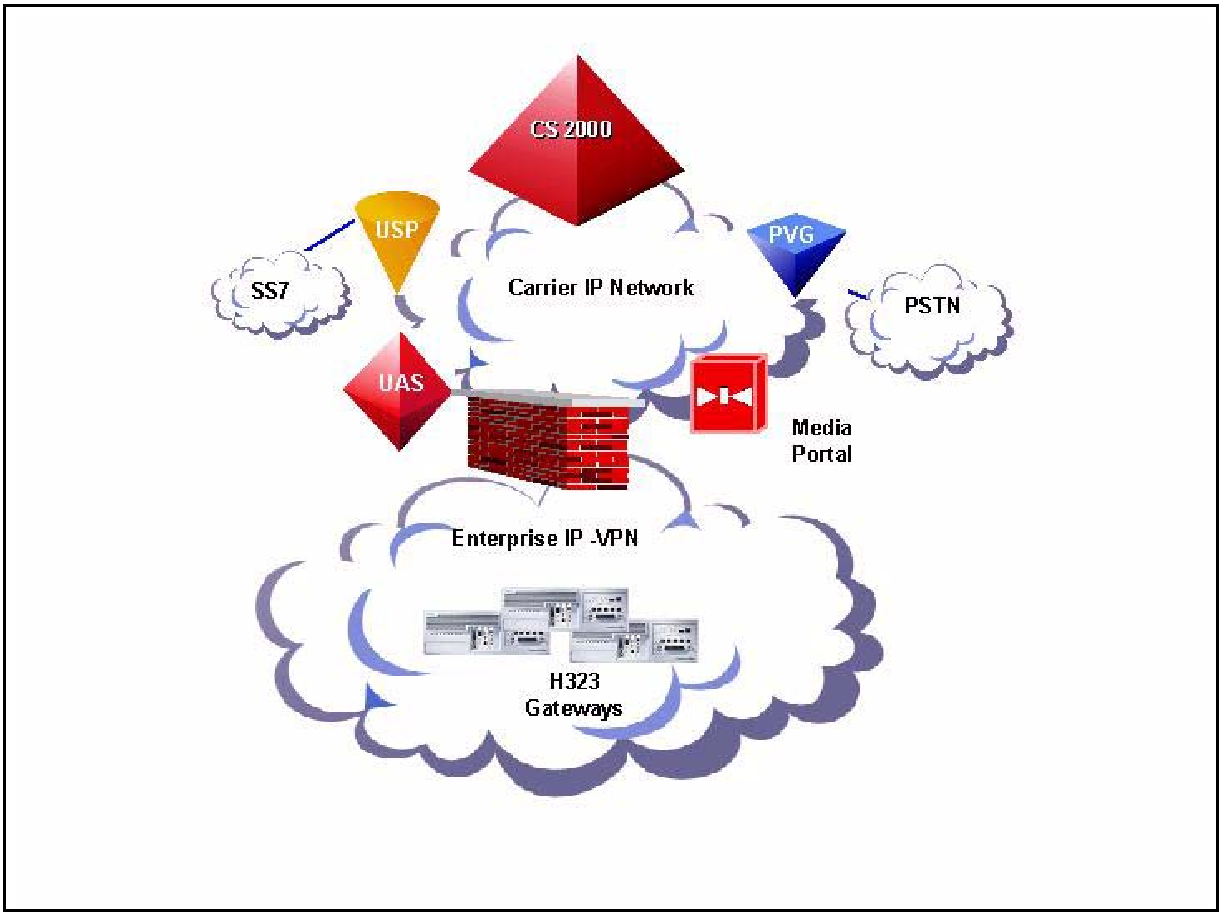
- reduced network connections
- simplified call routing
- seamless connections to remote locations
- streamlined network management
- increased network services and CPE revenue for carrier customers
- cost savings to enterprise customers through converged access and long-distance bypass

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

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

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

Carrier Hosted Services VoIP VPN architecture



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

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

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

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

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

Reference information

For a complete listing of all documentation associated with Carrier Hosted Services VoIP VPN refer to Where to get customer documentation on page 213

In particular, refer to the following sections:

- BCM on page 214
- CS1000 and CS 1000M on page 215
- Meridian 1 on page 215
- MCS 5100 on page 215

Provisioning Advice of Charge

What's new in this release?

For Advice of Charge (AOC) datafill considerations, refer to "Provisioning AOC through table TRKOPTS" on page 22

For APDU timing message considerations, refer to "Conditions for APDU timing messages" on page 26

Overview

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

The AOC service is delivered in three ways:

- **AOC-S** Advice of Charge at the call Setup
- **AOC-D** Advice of Charge During the call
- **AOC-E** Advice of Charge at the End of the call

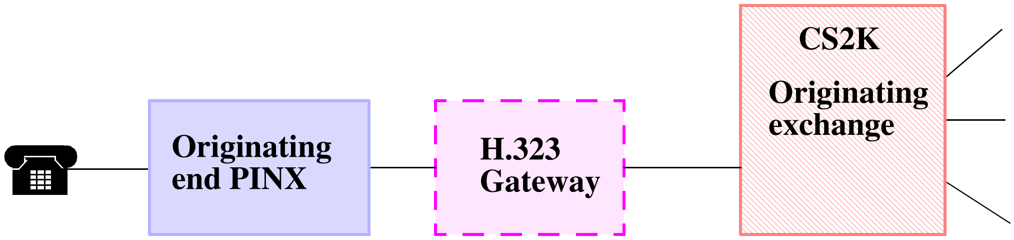
This activiy addresses two AOC services: AOC-D and AOC-E. These services are deployed for originating agents connected to the CS2000 over H.323. For the AOC calculation, the CS2K node has to be configured to determine and apply the tariffs (nodal configuration or combined CGP/CDP). Refer to "Combined CGP and CDP" on page 16

The overall solution includes a 3rd-party H.323 gateway capable of delivering AOC information to BRI subscribers in different national variants, for example in France:

- EURO-NUMBERIS (VN4, VN6)
- EURO-NUMBERIS+

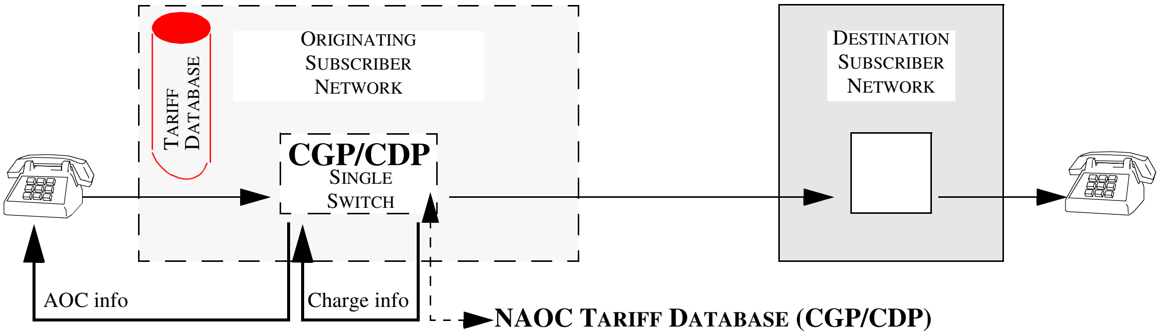
The following figure depicts a functional overview of AOC over H.323.

AOC over H.323 (functional overview)



The Network Advice of Charge (NAOC) service that is addressed in this activity is displayed in the following figure. The nodes involved in tariffing a call are the Charge Determination Point (CDP) and the Charge Generation Point (CGP). In the figure, the combined CDP/CGP are located on the same exchange. Tariff information is retrieved internally from the local tariff database and pulsed out to the subscriber.

Combined CGP and CDP


Tariff Database
Originating Subscriber Network
CGP/CDP
Single Switch
Destination Subscriber Network
AOC info
Charge info
NAOC Tariff Database (CGP/CDP)

NOAC interworking

A brief overview of the supported agent interworkings is given below. The combinations of supported interworkings are listed in the following table. Only the agents marked green and with an “X” are being supported. Other agents supported by AOC on QSIG that are not being covered by this activity are marked yellow and “N/A”

Platform	Originator	Terminating agents										
		H323 agents	IBN lines	ETSI PRI	QSIG (95)	ETSI ISUP V1	ETSI ISUP V2/V2+	SIP-T	SSURN2 (FTUP)	SPIROU	UK ISUP	ANSI ISUP
CS2K	H323	X							N/A			

The NOAC framework provides support for the following functionality:

- support for multiple carriers/resellers
    - Up to 16 carriers and 204 resellers can be handled by one CS2000 node.
- Enhanced Call Translations
    - The NAOC tariff determination process is initiated through new translation options cont/rte.
- Tariffing based on supported zoning information
    - local calls
    - national calls
    - international calls
    - service calls to premium rate services, non-geographical numbers, mobile subscribers, and other special destinations.
- Tariffing based on Type of Day / Time of Day System

  Up to 30 tariff changeovers (TCOs) and several datafillable day types are supported per CS2000 node. The CS2000 provides the ability to specify the zones that are applicable to each individual changeover time.
- Tariffing support for Discounts

  The Discount System is supported independently for each Carrier Identification Code (CIC) based carrier and simple reseller. Up to 511 discount levels can be assigned. Partial discounts can be given for service number.
- Enhanced Tariff tables include the following supported tariff definitions:
    - Block tariffing. This is simply a call setup charge, or a fixed amount to be applied at the beginning of a call.
    - Combination tariffing. This is a call setup charge along with a time dependent charge. A time dependant charge is an amount (in the Euro currency) to be applied on a per second basis.
    - Minimum communication charge. This is a call setup charge along with a “zero” first sub-tariff charge. In other words, the first sub-tariff is set to zero and there is a call setup charge. In this manner, regardless if the first tariff expires or not, the call will be charged at the minimum amount

Charging information

The following charging information applies to this activity.

- Charging Information at Call Set-up time (AOC-S)

  When the AOC-S supplementary service is activated, the network shall provide the user with call charging information at call establishment. In addition, the network shall inform the served user if a change in charging rates takes place during the call.

  The network shall provide the charging information during call establishment or at the latest at call connection. When there is a change in charging rate during the call, the network shall send information about the new charging rate to the served user.

- Charging Information During the Call (AOC-D)

  When the AOC-D supplementary service is activated, the network shall provide the user with call charging information during the active phase of a call. The network shall provide the charging information and transfer it to the user in an appropriate message. The supplied charging information shall be provided as a cumulative charge incurred so far for the call

  When the call is released, the network shall send the user the recorded charges for the call in one of the call control messages clearing the call.

  If the network has determined that the call is free of charge, the network shall send the user a free-of-charge indication. The network shall not send any further charging information during the call. When the call is released, the network shall send the free-of-charge indication in a call control message clearing the call.

  — Indication of Charge [télétaxe]

    This term is used in France to describe the supplementary service that informs the user of the charges attributed during the active phase of a call. Indication of Charge is another term for AOC-D.

- Charging Information at the End of the Call (AOC-E)

  When the AOC-E supplementary service is activated, the network shall provide the user with call charging information indicating the recorded chargeswhen the call is released. The network shall send the user the charging information in one of the call control messages clearing the call.

— Total Cost

This term is used in France in order to describe the supplementary service which informs the user of the call charges when the call is released. It is another term for AOC-E.

- Charging Units

  In this variant of AOC, the AOC charging information is presented to the terminal in form of a pulse count. The subscriber or terminal has to know the amount and currency equivalent to one pulse in order to calculate the cost of a call.

- Currency Units

  In this variant of AOC, the AOC charging information is presented to the terminal in form of amount and currency.

- AOC on request

  In this variant of AOC, charging information is not sent for every call that the user originates but only for calls where the subscriber explicitly requests AOC information by adding a respective Facility Information Element (FAC IE) into the Q.931 SETUP message.

Functional protocol

The functional protocol is based on the use of the Facility information element and the FACILITY message, as well as of other specific functional messages specified in clause 7 of Recommendation Q.932

This protocol is functional in the sense that it requires the knowledge of the related supplementary service by the user equipment supporting it. This facilitates user equipment operation without human intervention by defining semantics for the protocol elements which user equipment can process on its own.

The protocol is symmetrical and is applicable to both basic and primary rate interfaces.

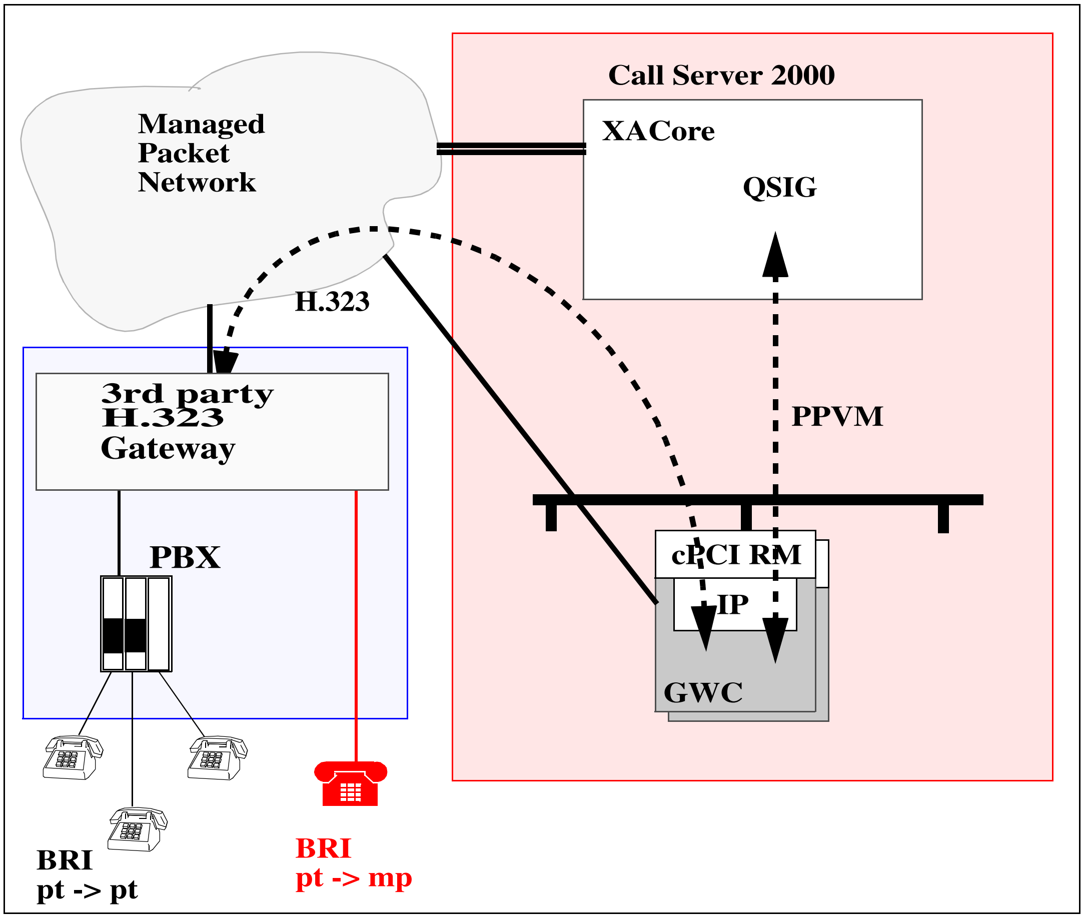
The key characteristic of the functional protocol is that it may operate end-to-end as contrasted with the Keypad Protocol that is local in nature.

AOC architecture

AOC is provided for ISDN agents connected via H.323 interface. From a CS2000 point of view, this interface is seen as a QSIG trunk. All related AOC messages are sent as Q.931 Facility Information

Elements, generated at the H.323 interface and tunneled in H.225[Q.931] messages to the H.323 gateway. At the gateway, the information is unpacked and applied to the originating ISDN agents. The following figure provides a high level view on the CS2000 architecture with regards to H.323.

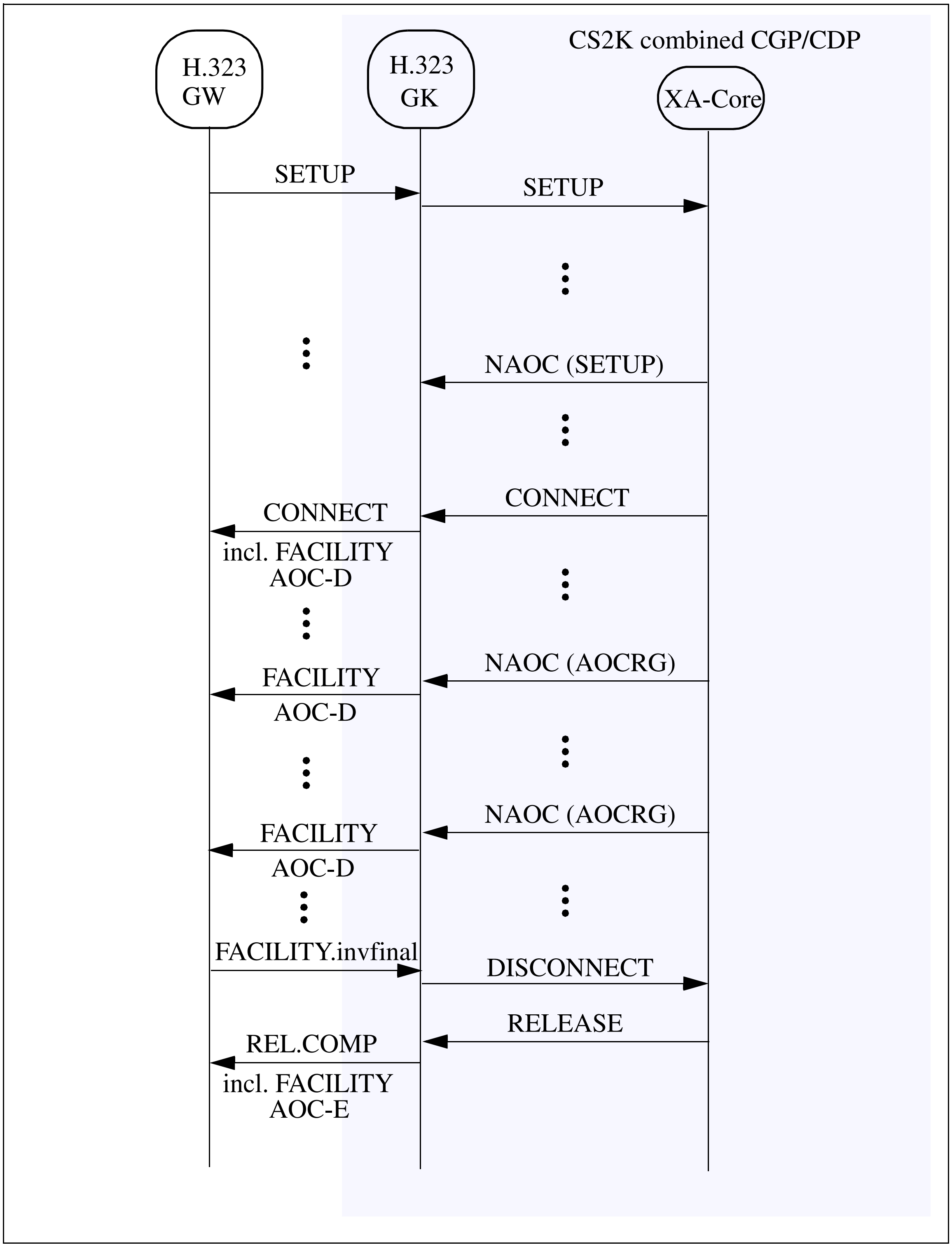
AOC over H.323



AOC message flow

The following figure depicts a sample AOC message flow on a combined CGP/CDP node.

AOC message flow on a combined CGP/CDP node



Provisioning AOC control

The AOC functionality can be provisioned through three components:

- Trunk group through table **TRKOPTS**
- GWC through table **SERVRINV**
- Call Server through Software Optionality Control (**SOC**) by using codes:
  - — **NETK0024**
  - — **NSUP0020**
  - — **NSUP0023**
  - — **PBXT0011**
  - — **PBXT0018**

Provisioning AOC through table TRKOPTS

at the H.323 gateway

1 For H323 trunks datafilled in table **TRKOPTS** for **AOC**, set the following fields:

- **AOCD**, to enable/disable the “AOC During call (AOC-D)” functionality.

  If set to **Y**, Facility messages are sent to provide the PBX subscriber with the charge unit count on a regular basis during a call.

- **AOCE**, to enable/disable the “AOC End of call (AOC-E)” functionality.

  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 customer belongs.
- **AOCREL** to enable/disable releasing a call if AOC is not available; that is, if the datafill on both CS2K and GW 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 might cause calls to be released.

If **AOCREL** is **TRUE**, the Q.931 **RELEASE COMPLETE** message contains no AOC information.

- **AOCCHGOV** to enable/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 specific 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 in the **SETUP** message (**REQUEST = ‘Y**’) or if it is invoked for every call (**REQUEST = ‘N**’).

  For H.323, **REQUEST** must be set to ‘**Y**’

Message protocols

The AOC message protocol is specified by the following three types of ETSI standards.

- AOC-S : Advice of Charge at the beginning of the call to advise the user about how the communication will be charged. Specified in ETS 300 178.
- AOC-D : Advice of Charge during a call. Information about the cost (units or currency) is delivered continuously during the call. Specified in ETS 300 179.
- AOC-E : Advice of Charge at the end of the call. Information about the total cost of the communication is delivered at disconnection. Specified in ETS 300 180.

The signalling protocol used for the AOC is defined in ETS 300 182 . For the purpose of this activity, the AOC information is mapped to H.323 / H.225 call signaling messages, using the Q.931 Facility Information Element to carry charging requests and charging information

The AOC Q.931 Facility Information Element is supported in the messages shown in the table below. The codeset change is done using a Q.931 Locking Shift information element.

MESSAGE TYPE	DIRECTION	COMMENTS
SETUP	user -> network	may be used to carry AOC-D and / or AOC-E invoke APDUs
FACILITY	user -> network	may be used to carry AOC-D and / or AOC-E invoke APDUs
FACILITY	network -> user	used to carry AOC-D (aocInterim) information
FACILITY	network -> user	also used to carry returnError and returnResult APDUs
CONNECT	network -> user	used to carry AOC-D returnError APDUs, reporting 'Service not Available' or 'supplementary Service Interaction Not Allowed'
RELEASE COMPLETE	network -> user	may be used for AOC-E (aocFinal) information

AOC requests

AOC requests from the originating H.323 gateway can be received in Facility IEs included in either **SETUP** or **FACILITY** messages. An AOC request in turn is a **ROSE** Invoke APDU with one of the operations defined for **AOC** in ISO 15049/ECMA-211 and ISO 15050/ECMA-212.

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

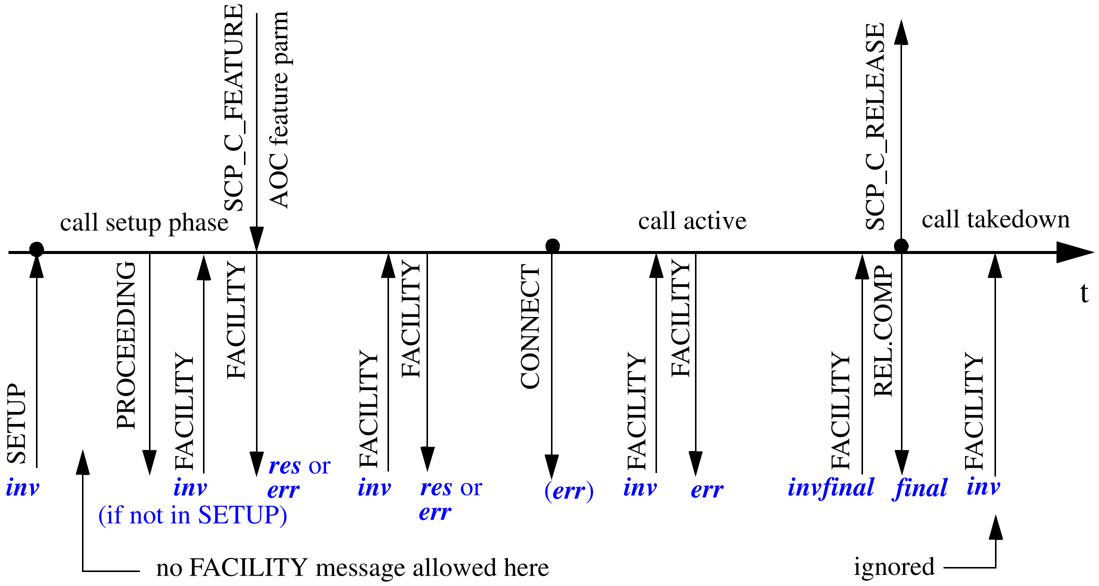
H.323 Gatekeeper should be imagined as being on the time axis. Messages above the time axis are from/to the CS2000 Core, and messages below the time axis are from/to the originating H.323 gateway.

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

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

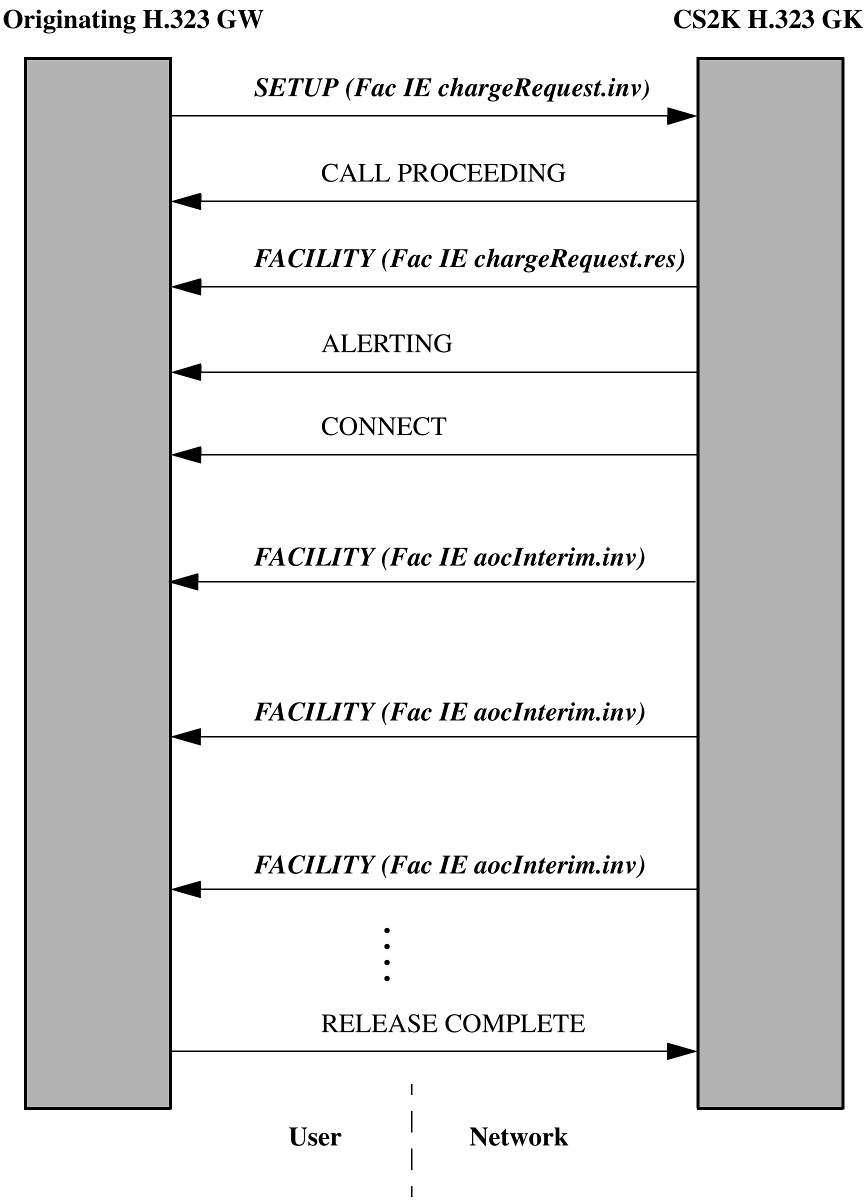
Charge information messages

The AOC charging information will be transported in a Facility Information Element as part of the FACILITY and RELEASE COMPLETE messages as defined in ISO 15049/ECMA-211 and ISO 15050/ECMA-212 .

The format of the AOC currency units messages for both AOC-D and AOC-E will be as defined in ISO 15049/ECMA-211 and ISO 15050/ECMA-212. If the originating GW offers AOC information in the ETSI format (ETS 300 179 and ETS 300 180) it would have to translate the ECMA encoded messages into ETSI format.

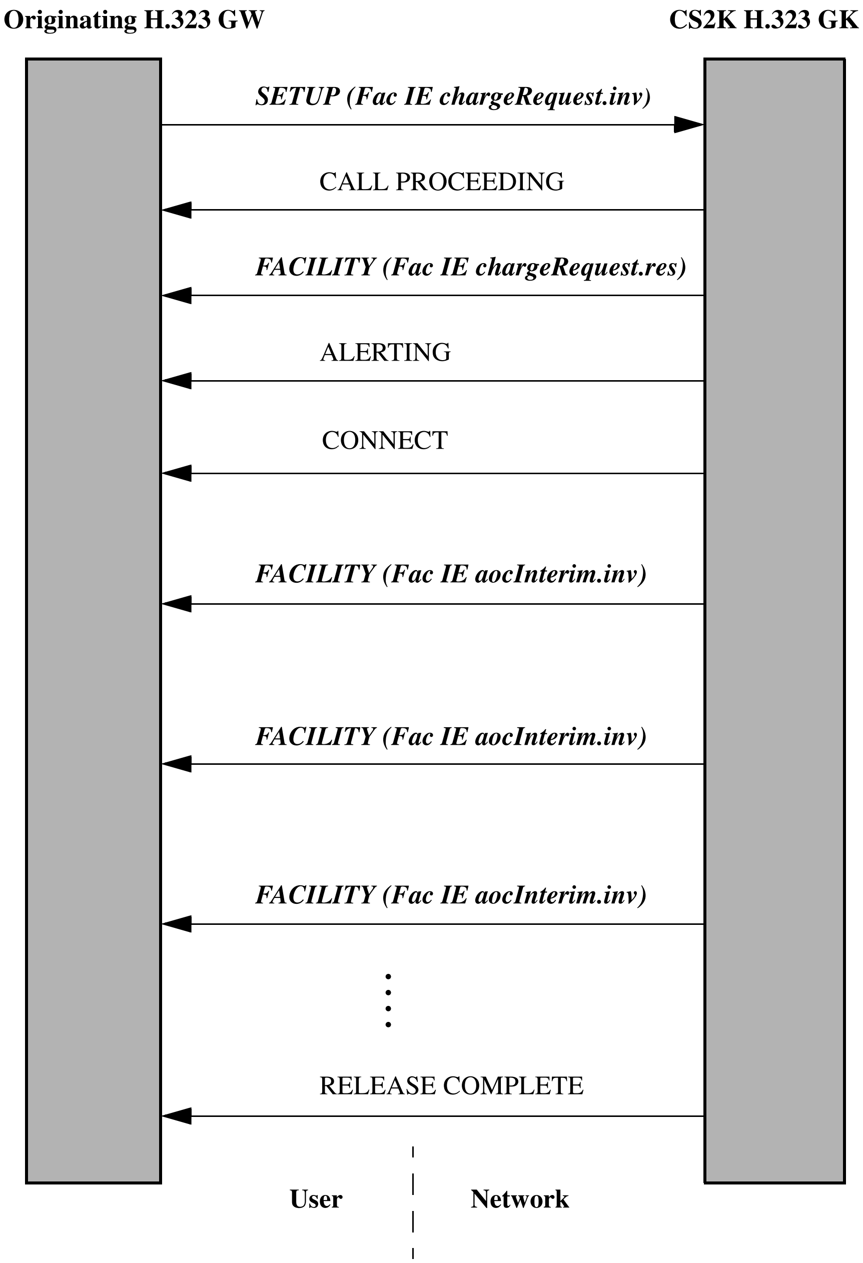
The following figures show the H.225[Q.931] (H.225 with embedded Q.931) message sequence charts relevant for the AOC functional protocol implementation of this activity

AOC-D message sequence (Clear Forward)


Originating H.323 GW
CS2K H.323 GK
SETUP (Fac IE chargeRequest.inv)
CALL PROCEEDING
FACILITY (Fac IE chargeRequest.res)
ALERTING
CONNECT
FACILITY (Fac IE aocInterim.inv)
FACILITY (Fac IE aocInterim.inv)
FACILITY (Fac IE aocInterim.inv)
RELEASE COMPLETE
User
Network

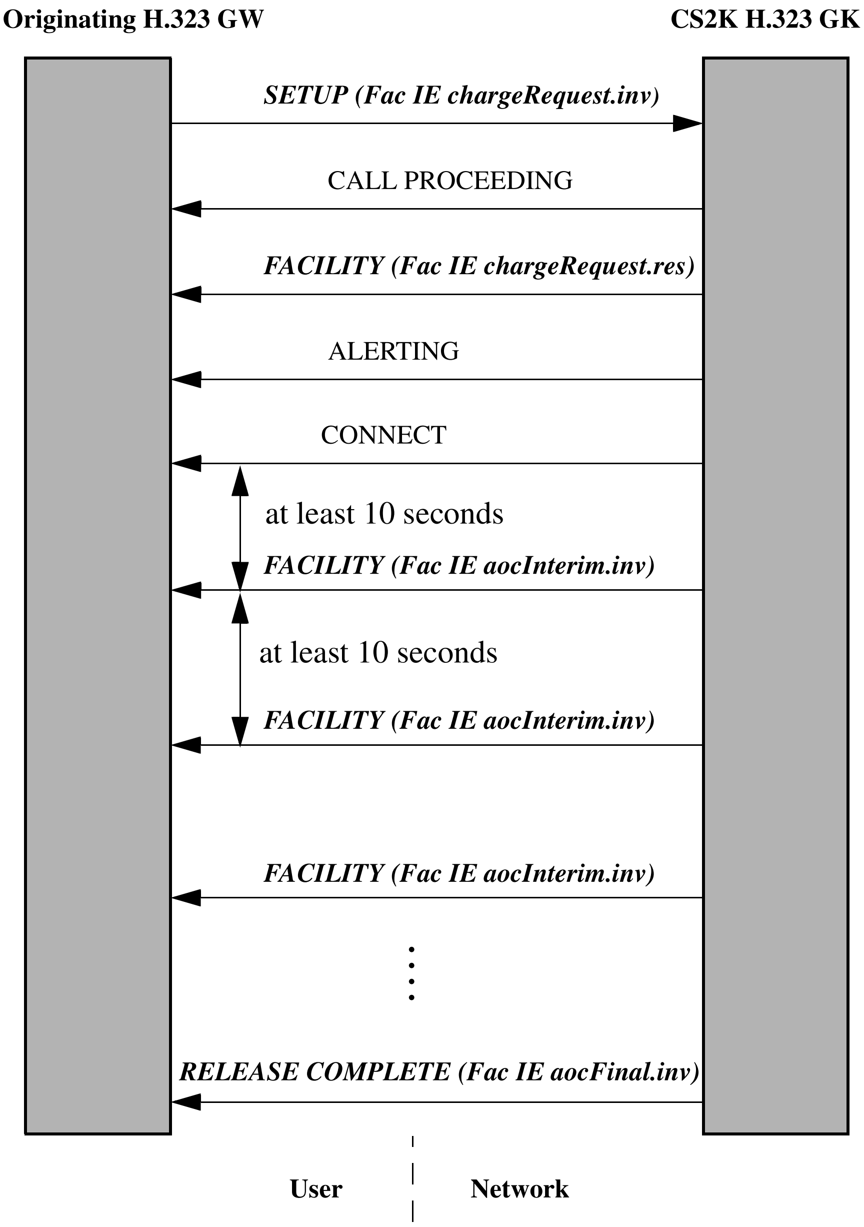
The following figure depicts a message sequence typical for AOC-D where the terminator takes down the call (Clear Backward).

AOC-D message sequence (Clear Backward)


Originating H.323 GW
CS2K H.323 GK
SETUP (Fac IE chargeRequest.inv)
CALL PROCEEDING
FACILITY (Fac IE chargeRequest.res)
ALERTING
CONNECT
FACILITY (Fac IE aocInterim.inv)
FACILITY (Fac IE aocInterim.inv)
FACILITY (Fac IE aocInterim.inv)
RELEASE COMPLETE
User
Network

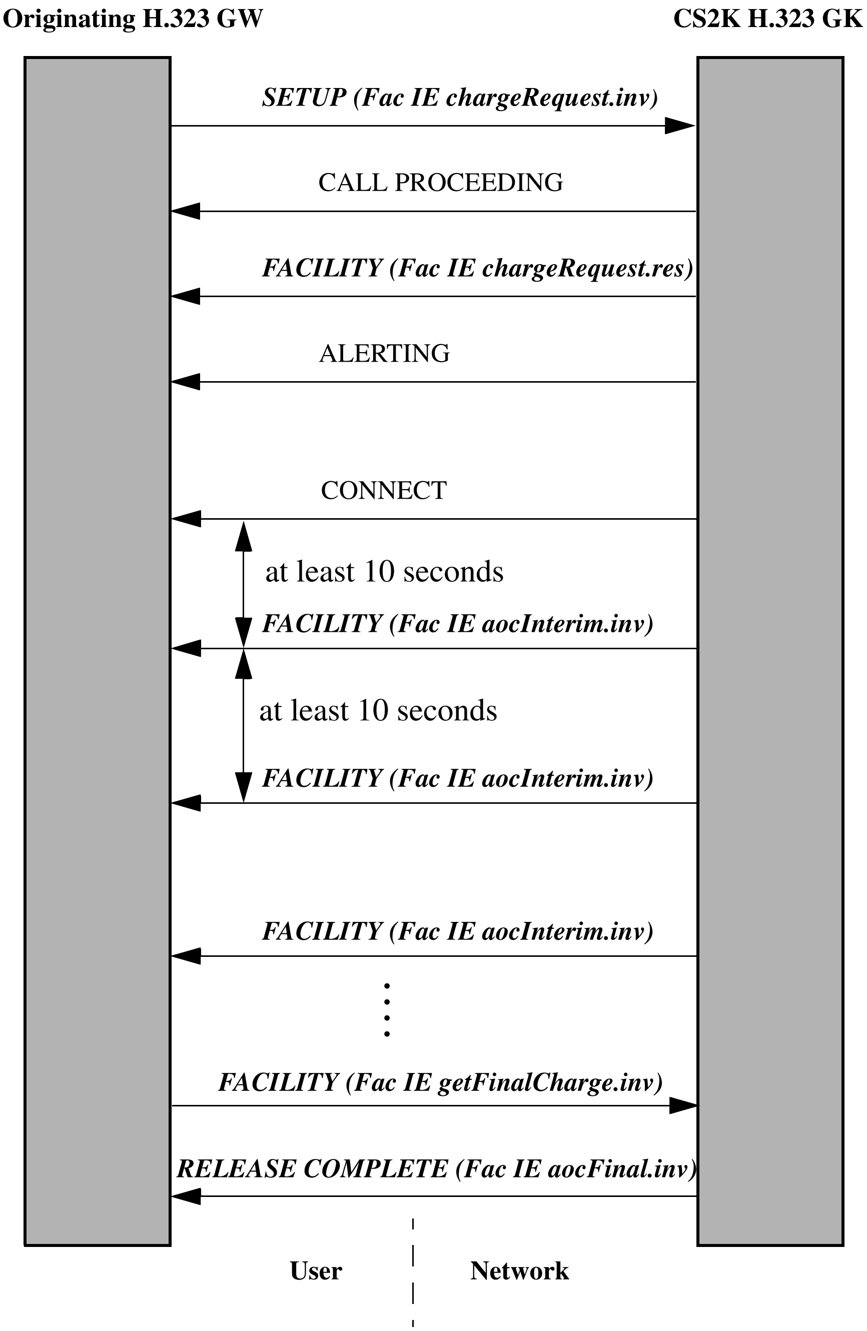
The following figures show the H.225[Q.931] message sequence charts for delivering both AOC-D and AOC-E information, considering two call take-down scenarios.

AOC-D/E message sequence (Clear Backward)


Originating H.323 GW
CS2K H.323 GK
SETUP (Fac IE chargeRequest.inv)
CALL PROCEEDING
FACILITY (Fac IE chargeRequest.res)
ALERTING
CONNECT
at least 10 seconds
FACILITY (Fac IE aocInterim.inv)
at least 10 seconds
FACILITY (Fac IE aocInterim.inv)
FACILITY (Fac IE aocInterim.inv)
RELEASE COMPLETE (Fac IE aocFinal.inv)
User
Network

The following figure depicts a typical AOC message sequence where initially only AOC-D is active. AOC-E is requested at call takedown. In this case call takedown from the originator (Clear Forward) is special in the way that it is not initiated by a RELEASE COMPLETE sent by the originating H.323 gateway, but by a FACILITY message with a getFinalCharge operation embedded.

AOC-D/E message sequence (Clear Forward)


Originating H.323 GW
CS2K H.323 GK
SETUP (Fac IE chargeRequest.inv)
CALL PROCEEDING
FACILITY (Fac IE chargeRequest.res)
ALERTING
CONNECT
at least 10 seconds
FACILITY (Fac IE aocInterim.inv)
at least 10 seconds
FACILITY (Fac IE aocInterim.inv)
FACILITY (Fac IE aocInterim.inv)
FACILITY (Fac IE getFinalCharge.inv)
RELEASE COMPLETE (Fac IE aocFinal.inv)
User
Network

For the format of the FACILITY message please refer to standards for H.225 and Q.931: ITU-T H.225.0 and ITU-T Q.931, respectively.

For the format of the AOC Facility IE, please refer to ISO 15049/ECMA-211 and ISO 15050/ECMA-212. If the originating GW offers AOC information in the ETSI format (ETS 300 179 and ETS 300 180), the ECMA encoded messages would need to be translated into ESTI format.

The encoding used for sending the charge units in the AOC Facility IE is ASN.1 and is done according to ITU-T Recommendations.

If a call is free of charge, this is indicated by sending an indication “free of charge”.

In the case of AOC-D, the “free of charge” indication is sent twice: after CONNECT and at the end of the call.

In case of AOC-E the “free of charge” indication is sent once at the end of the call. Sending of “free of charge” as a response to an AOC request is not supported. Note that this does not lead to a non-compliance to ETS 300 179 and ETS 300 180.

Hardware requirements or dependencies

An appropriate H.323 GW from a 3rd party vendor being able to convert Facility messages from ECMA format ISO 15049/ECMA-211 and ISO 15050/ECMA-212 into ETSI format ETS 300 179 and ETS 300 180 is needed.

Software requirements or dependencies

The AOC feature requires the following features be activated by SOC:

- NETK0024 Network AOC Tariff
- NSUP0020 NAOC/PCA Supp Svcs
- NSUP0023 PCA SW Metering Support for Billing
- PBXT0011 ETSI PRI Info
- PBXT0018 QSIG AOC

NAOC tariff information is required, since this feature reuses the NAOC framework. If no NAOC information is provided, the payment ceiling counter cannot be updated for that call. NAOC datafill including the NAOC tables and translation options have to be set up in an appropriate way. Please refer to the following standards for additional information:

- ETS 300 178 - ISDN
- ETS 300 178 - ISDN
- ETS 300 178 - ISDN
- ETS 300 178 - ISDN

- ITU-T H.225.0
- ITU-T Q.931
- ITU-T Q.932

Restrictions or Limitations

The following restrictions or limitations are introduced by this activity:

- Sending of AOC charge information as currency units is not supported for H.323 trunks
- AOC calculation based on the charging interval introduced with A00002625 [39] is not supported
- A delta may exist between the number of charge units saved in the AMA record by the CM feature A00002638 [38] 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 GWC calculation of the AOC does not influence or change AMA records extension introduced with A00002638 [38]. 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 calls. AOC on H.323 for non-bearer calls is not supported. Facility IEs with AOC operations for these calls are transparently passed through the CS2000.

Configuring H.323 Gateway Change Capability

Overview

The H.323 gateway change capability is a service that allows the ability to change the initial provisioning of the H.323 gateway without affecting already provisioned GWs and EPGs.

The following procedures enable this H.323 gateway change capability service.

- Change the capacity of an H.323 GW after initial provisioning.
- Change the IP address of an H.323 GW after initial provisioning.
- Change the Port of an H.323 GW after initial provisioning.
- Specify the TID location of EPGs.
- Provide modified GUI display capabilities for H.323 EPGs.

Note: To realize greater flexibility when adding EPGs, in (i)SN07, EPGs are no longer automatically added when an H.323 GW is added.

Reference documentation

For configuration information for this feature, refer to the following procedures located in the document **GWC Configuration Management** , NN10205-511

- **Associate an H.323 media gateway**
- **Add carriers to a GWC**
- **Delete carriers from a GWC**
- **View carrier provisioning data for a GWC node**
- **Change gateway attributes**
- **Disassociate a media gateway**

Configuring H.323 support for MCDN Services

Overview

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

- the interconnection of MCDN based PBXs with certain line gateways for use in networked VPNs.
- MCDN interworking on nodal calls and via SIP-T (ETSI ISUP V2+ QFT) for inter-Call Server calls.
- MCDN based service interworking between the Nortel Networks Media Gateway 1000 or BCM (H.323 GWs) on one call leg and CICM (H.248 GW) or Mediatrix IAD (MGCP GW) on the other call leg.
- MCDN services which are supported on P-phone agents or IBN lines agents.
- MCDN based services for the CS2K international load.

MCDN interworking includes:

- H.323 GW (BCM) <--> H.248 GW (CICM, P-phone)
- H.323 GW (BCM) <--> MGCP GW (Mediatrix, IBN lines)
- H.323 GW (Nortel Networks Media Gateway 1000) <--> H.248 GW (CICM, P-phone)
- H.323 GW (Nortel Networks Media Gateway 1000) <--> MGCP GW (Mediatrix, IBN lines)

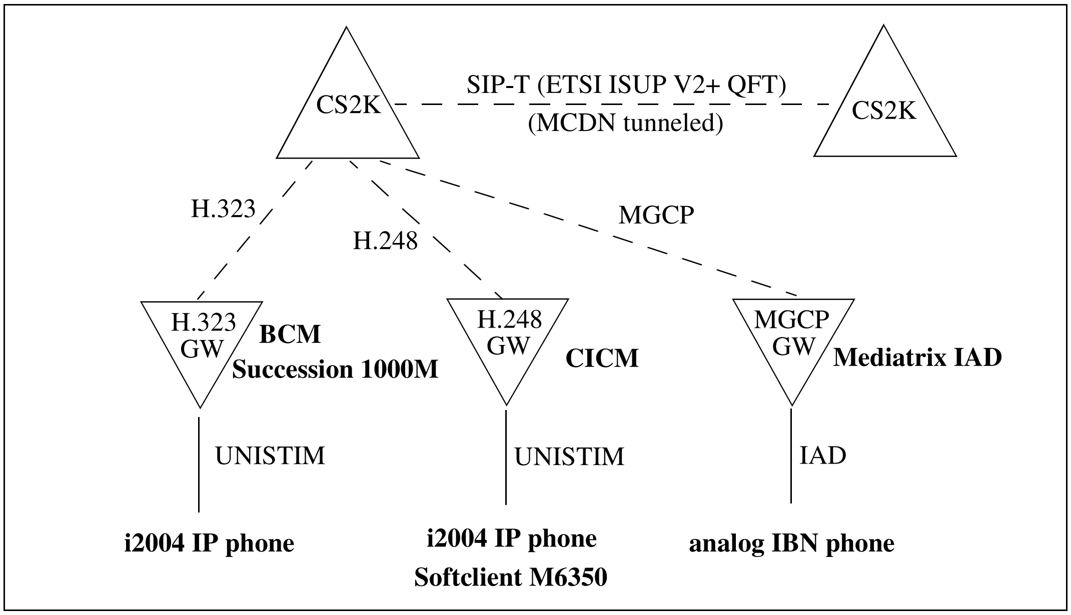
Prerequisites

H.323 support verifies a subset of MCDN services that are supported on P-phone agents or IBN line agents.

H.323 support implements and verifies MCDN based services for the CS 2000 international load.

Associated network drawing

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



Limitations and Restrictions

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

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

  For supported MCDN services, refer to “Features and services” on page 185
- 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.
- Verification of MCDN services is done using the Nortel Networks Media 1000 Gateway. Omitting verification on the Media 1000 GW is acceptable since both GWs use the same software load.
- Testing is done on the international CS 2000 load only.
- Limitation on Connected Number Delivery: In the software load of the Nortel Networks Media 1000 Gateway and BCM gateways, which this feature will be based upon (see section 2.4 Software Requirements and Dependencies), 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 Nortel Networks Media 1000 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 (see section 2.4 Software Requirements and Dependencies), 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.

References

For a complete list of MCDN services, refer to “Features and services” on page 185.

Configuring Call Server controlled switch over to T.38

Overview

This activity provides “Call Server controlled switch over to T.38 (or G.711)” for Call Server routed H.323 calls. Fax interworking over Session Initiation Protocol (SIP-T) is supported on calls between H.323 GWs (e.g. Meridian, Cisco, BCM) and H.248 GWs (e.g. Media Gateway) or MGCP GWs (e.g. Mediatrix). At least one involved agent must be H.323.

Prerequisites

To switch successfully to T.38, each side of the gateway must know the T.38 capabilities of the other gateway.

To verify that Call Server controlled switch over to T.38 is supported and can be used in SDP, the GW indicates the T.38 capability by including the line "a=cdsc: 1 image udptl t38".

Call Server controlled switchover to T.38 (or G.711) depends on the T.38 network option:

- If Netopt is set to “T.38” and both GW support T.38, then upon fax detection, switchover is done from G.729 (or G.711) to T.38 codec.
- If Netopt is not set to “T.38”, or a GW does not support T.38, then switchover to T.38 does not apply. If the call was set up with G.729 codec, switching is done from G.729 to G.711 codec. If the call was set up with G.711, no switchover occurs.

Sequence of SIP-T messages

- The H.323 GWC requests the remote H.248 or MGCP side to detect a fax tone and to notify the H.343 GWC about a fax event.
- The H.323 GWC receives a fax event notification from remote H.248 or MGCP side.
- H.323 GWC controls switching to T.38 mode.
- The logical voice channel is cleared.
- A T.38 fax channel is opened.
- The SDP(T.38) data is sent to the remote side.
- An invite to switch over to T.38 is sent to remote side.
-

A remote H.248 or MGCP GW may send an SDP indicating the simultaneous support of

— the voice media stream indicated by the line: "m=audio ..”

— the T.38 media stream indicated by the line: "m=image..."

> ***Note:*** The “m=image 1 udptl t38” line in SDP means that T.38 codec is supported and “autonomous switchover to T.38” can be used.

- A H.323 GW that does not support a voice media stream and T.38 media stream at the same time, removes/rejects the “m=image 1 udptl t38” line. This rejection means that “autonomous switchover to T.38” can not be used for this call.

Associated SDP coding example for configuring an H.323 fax call

The following table gives and SDP coding example for interworking an H.248 GW supporting "autononomous switching to T.38" and an H.323 GW supporting "Call Server controlled T.38 switching". Fast start (FS) applies to to the H.323 side of the gateway.

SDP example for H.248 (Fast start) to H.323 interworking over SIP-T

H.248 > H.323: INVITE (SDP)	H.248 < H.323: 200 OK (SDP)
v=0	v=0
c=IN IP4 128.96.41.1	c=IN IP4 128.96.41.1
m=audio 1111 RTP/AVP 18 (Note 1)	a=sqn: 0
a=ptime:20	a=cdsc: 1 image udptl t38 (Note 3)
m=image 1112 udptl t38 (Note 2)	m=audio 2222 RTP/AVP 18 (Note 1)
	a=ptime:20

SDP example for H.248 (Fast start) to H.323 interworking over SIP-T

H.248 > H.323: INVITE (SDP)	H.248 < H.323: 200 OK (SDP)
	~~m=image 0 udptl t38~~ (Note 4)

Note 1: Both sides supports G.729 codec. The voice call is set up with G.729 codec.

Note 2: Originating H.248 side commits simultaneous support for T.38 and indicates usage of “autonomous T.38 switching”.

Note 3: Terminating H.323 side indicates T.38 capability (not simultaneous to G.729).

Note 4: Terminating H.323 does not support “autonomous T.38 switching”. Current ISN07 implementation does not send “m=image 0 udptl t38” back. Omitting “m=image ...” indicates, that “autonomous T.38 switching” is not supported by terminating side.

Configuring H.248 for a T.38 fax call

Overview

The implementation of the Call Server controlled switchover to T.38 mode makes use of the Call Type Discriminator package (ctyp) with the event Discriminating Tone detected (dtone).

Prerequisites

To verify that Call Server controlled switch over to T.38 is supported and can be used in SDP, the GW indicates the T.38 capability by including the line "a=cdsc: 1 image udptl t38".

Note: If the remote SDP indicates T.38 capability (a=cdsc: 1 image udptl t38), then “Call Server controlled switchover to T.38 mode” applies.

Sequence of SIP-T messages

- The GWC checks the GW capability to support T.38 by means of the H.248 command, Audit Value.
- To verify that Call Server controlled switch over to T.38 is supported with the H.248 package, the H.248 GW replies with the H.248 package "ctyp-1". Refer to the “Coding example: Check supported H.248 packages” on page 46

  Note: If Netopt = “T.38”, the H.248 GWC adds the ephemeral termination with voice and T.38 codec. Refer to the “Coding example: Add ephemeral with G.729 and T.38 codec” on page 47
- Once the remote SDP is received, the H.248 GW can switch over to T.38.
  - — If the remote SDP indicates T.38 codec (m=image 1 udptl t38), then “autonomous switchover to T.38" applies.
  - — If the remote SDP indicates T.38 codapability (a=cdsc: 1image udptl t38), then “Call Server controlled switchover to T.38 mode" applies.

H.248 Coding examples

The following H.248 coding examples display H.248 messages as used in the call flow.

Coding example: Check supported H.248 packages

Transaction (GWC > MG)	Reply (GWC < MG)
MEGACO/1 [47.174.66.80]:2944	MEGACO/1 [47.166.34.20]:2944
Transaction=62 {	Reply=62 {
Context=-{	Context=-{
AuditValue=Root {	AuditValue=Root {
Audit { Packages }	Audit { Packages {...,ctyp-1, ..} }
}}}	}}}

Coding example: Request fax event detection

Transaction (GWC > MG)	Reply (GWC < MG)
MEGACO/1 [47.174.66.80]:2944	MEGACO/1 [47.166.34.20]:2944
Transaction=63 {	Reply=63 {
Context=$ {	Context=1234{
Add=e1/03/05/1 {	Add=e1/03/05/1
M{O{MO=RC, tdmc/ec=ON }},	}}
Events = 234 {ctyp/dtone}	
}}}	

Coding example: Notify fax event V.21 flag

Transaction (GWC < MG)	Reply (GWC > MG)
MEGACO/1 [47.166.34.20]:2944	MEGACO/1 [47.174.66.80]:2944
Transaction=64 {	Reply=64 {

Coding example: Notify fax event V.21 flag

Transaction (GWC < MG)	Reply (GWC > MG)
Context=1234 { {	Context=1234{
Notify=e1/03/05/1 {	Notify=e1/03/05/1
ObservedEvents = 234 {	}}
20030924T14001201:ctyp/dtone{dtt=V21flag}	
}}}	

Coding example: Add ephemeral with G.729 and T.38 codec

Transaction (GWC > MG)	Reply (GWC < MG)
MEGACO/1 [47.166.34.20]:2944	MEGACO/1 [47.174.66.80]:2944
Transaction=64 {	Reply=64 {
Context=1234 {	Context=1234{
Add = $ {	Add = rtp/34 {
Media { LocalControl {	Media {Local {
v=0	v=0
c=IN IP4 $	c=IN IP4 47.174.66.14
m=audio$ RTP/AVP 18	m=audio 1111 RTP/AVP 18 13 19
a=ptime:20	a=ptime:20
m=image $ udptl t38	m=image 2222 udptl t38
...	a=T38Fax ...
}}}}}	a=T38Fax ...
	...
	}}}}}

Coding example: Add ephemeral with G.729 and T.38 codec

Transaction (GWC > MG)	Reply (GWC < MG)
Note 1: The ephemeral termination is added with T.38 codec, to support “autonomous switchover to T.38” for e.g. Media Gateway to Media Gateway calls. At this point the remote GW type is unknown. If the remote side is H.323, then the T.38 codec is removed by the H.323 GW (codec negotiation). Note 2: This example shows 2 media lines in one session descriptor, as implemented in ISN06.2. This example will be updated at end of this feature to display real used SDP syntax.	

Configuring MGCP for a T.38 fax call

Overview

The implementation of "Call Server controlled switchover to T.38 mode" makes use of the Fax tone (ft).

Sequence of SIP-T messages

- Once the remote SDP is received, the MGCP GW switches over to T.38 mode.
  - If the remote SDP contains T.38 codec (m=image 1 udptl t38), then “autonomaous switchover to T.38” applies.
  - If the remote SDP indicates T.38 capability (a=cdsc: 1 image udptl t38), then “Call Server controlled switchover to T.38 mode” applies.

Note: the MGCP GW detects a fax call by detecting the V.21 fax preamble. The fax tone event must also be generated when the T.30 CNG tone is detected.

H.248 Coding examples

The following H.248 coding examples display H.248 messages as used in the call flow.

Coding example: Check supported H.248 packages

Transaction (GWC > MG)	Reply (GWC < MG)
MEGACO/1 [47.174.66.80]:2944	MEGACO/1 [47.166.34.20]:2944
Transaction=62 {	Reply=62 {
Context=-{	Context=-{
AuditValue=Root {	AuditValue=Root {
Audit { Packages }	Audit { Packages {...,ctyp-1, ..} }
}}}	}}}

Coding example: Request fax event detection

Transaction (GWC > MG)	Reply (GWC < MG)
MEGACO/1 [47.174.66.80]:2944	MEGACO/1 [47.166.34.20]:2944
Transaction=63 {	Reply=63 {
Context=$ {	Context=1234{
Add=e1/03/05/1 {	Add=e1/03/05/1
M{O{MO=RC, tdmc/ec=ON }},	}}
Events = 234 {ctyp/dtone}	
}}}	

Coding example: Notify fax event V.21 flag

Transaction (GWC < MG)	Reply (GWC > MG)
MEGACO/1 [47.166.34.20]:2944	MEGACO/1 [47.174.66.80]:2944
Transaction=64 {	Reply=64 {
Context=1234 { {	Context=1234{
Notify=e1/03/05/1 {	Notify=e1/03/05/1
ObservedEvents = 234 {	}}
20030924T14001201:ctyp/dtone{dtt=V21flag}	
}}}	

Coding example: Add ephemeral with G.729 and T.38 codec

Transaction (GWC > MG)	Reply (GWC < MG)
MEGACO/1 [47.166.34.20]:2944	MEGACO/1 [47.174.66.80]:2944
Transaction=64 {	Reply=64 {
Context=1234 {	Context=1234{

Coding example: Add ephemeral with G.729 and T.38 codec

Transaction (GWC > MG)	Reply (GWC < MG)
Add = $ {	Add = rtp/34 {
Media { LocalControl {	Media {Local {
v=0	v=0
c=IN IP4 $	c=IN IP4 47.174.66.14
m=audio$ RTP/AVP 18	m=audio 1111 RTP/AVP 18 13 19
a=ptime:20	a=ptime:20
m=image $ udptl t38	m=image 2222 udptl t38
...	a=T38Fax ...
}}}}}	a=T38Fax ...
	...
	}}}}}

Note 1: The ephemeral termination is added with T.38 codec, to support “autonomous switchover to T.38” for e.g. Media Gateway to Media Gateway calls. At this point the remote GW type is unknown. If the remote side is H.323, then the T.38 codec is removed by the H.323 GW (codec negotiation).

Note 2: This example shows 2 media lines in one session descriptor, as implemented in ISN06.2. This example will be updated at end of this feature to display real used SDP syntax.

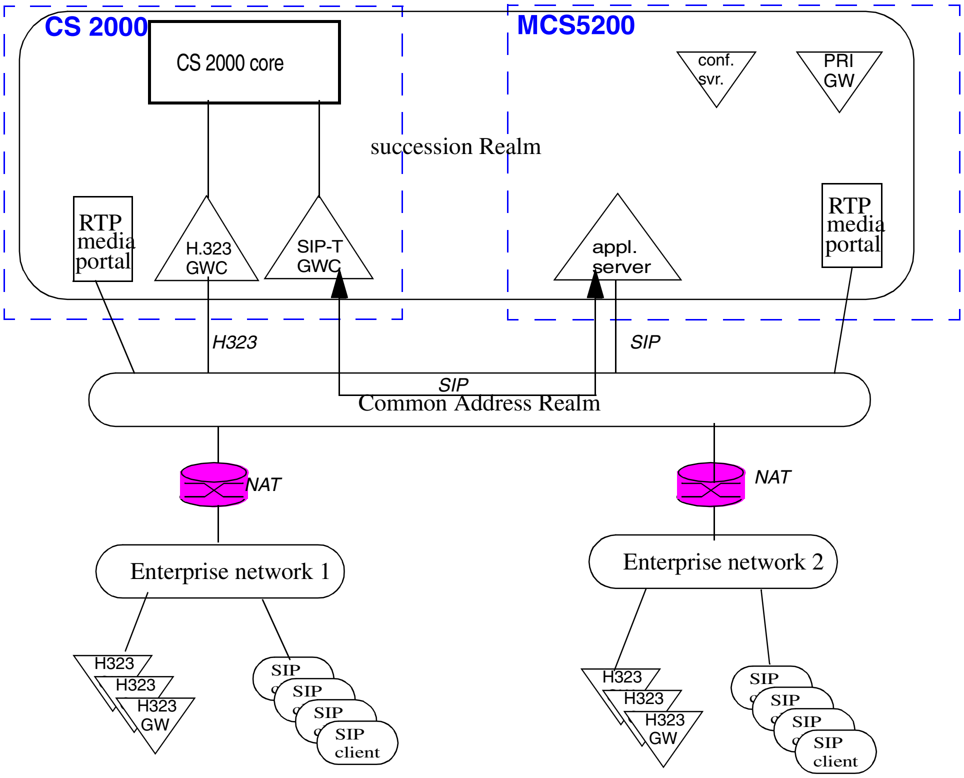
Interworking International H.323 to SIP MCS 5200

Overview

This SN07 activity verifies the interworking of various H323 gateways controlled by a CS 2000 and various SIP clients controlled by the Nortel Networks MCS 5200 system. The MCS 5200 is part of a carrier hosted voice VPN. The CS 2000 and MCS 5200 are interconnected through a SIP trunk.

The interworking configuration follows:

H.323 to MCS 5200 interworking configuration



The following table indicates the compliance of the interworking requirements between the CS 2000 H.323 gateway and the MCS 5200.

Req	Requirement text	Comments
201-1	Support interop between the CS2K H.323 GK and the MCS for Intl markets	Compliant It is assumed that this is a general requirement and the supported topology is specified in requirements 201-2, 201-3, 201-6, 201-7.
201-2	Support media and signaling interop between a CS2K H.323 endpoint and an MCS SIP client that are both connected to the same call server.	Compliant Assumption: MCS5200, not the MCS SIP client, is connected to the call server.
201-3	Support media and signaling interop between a CS2K H.323 endpoint and an MCS SIP client when they are connected to different call servers. SIP-T between the CS2K call servers should be able to carry ETSI ISUPv2	Partially-Compliant Private DN information needs to be tunneled through the public network, currently this functionality is not implemented on the CS2K. Calls that are originated by the MCS are treated as public calls. Assumption: MCS5200, not the MCS SIP client, is connected to the call server.

Req	Requirement text	Comments
201-4	Support for interoperability between the following H.323 gateways and MCS SIP clients: **H.323 gateways** • Westell — liQ2031 supporting 1 E1 with DPNSS — ilQ2032 supporting 2 E1 with DPNSS • Cisco IOS gateways • SBC (Cisco IOS GK, S1K/S1KM) • S1K/S1KM • BCM • Cisco Call Manager **MCS SIP clients** • SIP PRI gateway (UAS based) • PC Client • Web Client • i2004/i2002 • Conference Server (UAS based)	Partially-Compliant Excluded H.323 GWs • Session Border Controller (SBC) is not available in FDH lab • Cisco Call Manager is not available in FDH lab. • Cisco 3725 GW is used as Cisco IOS GW Excluded MCS SIP Clients • i2002 (assume i2004 phone is identical)
201-5	Support MCS SIP clients as subscribers in a CS2K hosted VoIP VPN.	Compliant Assumes MCS clients will be treated as a single NCOS, specifically the NCOS assigned to the IBN SIP-T trunk. Note, there are no specific test cases for this requirement.
201-6	Support for MCS hosted users in the same Enterprise/IP address space as the H.323 gateways. (Understand that based on the current MCS implementation that both the MCS and CS2K would insert RTP media portals into the call).	Compliant

Req	Requirement text	Comments
201-7	Support for MCS hosted users and CS2K controlled H.323 gateways being in different Enterprises/IP Address spaces. (Understand that based on the current MCS implementation that both the MCS and CS2K would insert RTP media portals into the call).	Compliant
201-8	Support for service interactions:	Partially-Compliant No supplementary services on Cisco 3725 available.
	Call Forward	Only available on H323 GW, on MCS the ROUTES functionality was tested
	Conference	On MCS only ad hoc conferencing was tested. On H323 GWs, only three-way calls were tested.
	Call Transfer	
	Caller ID	Only calling number displayed, no calling name.
	Decline and Reject Reasons	Reject reason will not be displayed.
	Codec Selection	
	Hotline	Only available on MCS i2004 client, not on H323 GW.
	Redirect	Only available on MCS, not on H323 GW.
201-9	Support DTMF interworking between H.323 endpoints (S1K/S1KM, BCM, Cisco Call Manager, SBC, Cisco IOS (RFC2833), Westell (RFC 2833)) and MCS clients (SIP INFO - SIP PRI gw (UAS based), RFC 2833 - i2004, i2002, PC Client, Web Client, Conference Server (UAS based)	Non-Compliant The current implementation does not support the transmission of OOB DTMF between MCS and CS2K.
201-10	Support for G.711 and G.729 codecs	Compliant
201-11	Support for 10 and 20 msec packetization rates. The H.323 GWC must handle the fact that the MCS doesn’t send the PTIME parameter.	Compliant

Supported markets

This feature only covers markets supported by the international version of CS 2000.

VPN topology

The MCS 5200 is interconnected to the CS 2000 by a SIP trunk.

The activity supports VPN networks with the following topology:

- VPNs hosted by one CS 2000
- VPNs hosted by several CS 2000 interconnected by a SIP-T[ETSI ISUPv2] trunk

Limitation:

Calls originated by an MCS client that terminate on an H323 client that is not connected to the same CS2K as the MCS cannot be treated as private calls, i.e. private information will be lost.
This limitation is caused by the fact that the private information is not tunnelled through the SIPT trunk between the different call servers.

Supported H323 gateways and SIP clients

On the CS 2000 the following H323 gateways will be supported:

- S 1000
- S 1000M
- BCM
- Westell
  - liQ2031 supporting 1 E1 with DPNSS
  - ilQ2032 supporting 2 E1 with DPNSS
- Cisco router 3600 (Cisco IOS GW)
- Cisco router 3725 (Cisco IOS GW)

> ***Note:*** The Cisco call manager and the Cisco router 2600 will not be supported.

The following MCS clients are supported:

- PC client
- Web client
- i2004 internet telephone

- PRI gateway (UAS based)
- Conference server (UAS based)

VPN support on the MCS

In order to create a VPN spanning the CS 2000 and the MCS 5200 each customer group on the CS 2000 will be mapped onto one domain on the MCS 5200. For each VoIP VPN/domain there is exactly one SIP trunk between the CS 2000 and the MCS.

Thus, several VoIP VPNs may exist in a configuration consisting of a CS 2000 and an MCS.

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

Media portal insertion

The media portal will always be inserted on both the MCS 5200 and the CS 2000 independent of the fact, if the MCS 5200 clients and the H323 gateway reside in the same enterprise network or not.

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

Supplementary services

For the indicated served users: MCS, BCM, S 1000/S 1000M, Westell, and Cisco 3600/Cisco 2725, the following table describes the supported services on the various H323 gateways and the SIP clients.

Here is brief explanation of terms used in the table:

- n/a - not applicable. Calls between H.323 agents are not in the scope of this feature. However, it is possible that in a multi-party call, different H.323 agents can be involved in the call.
- served user - party that requests a supplementary service. It can be the call originator, e.g. in case of the ‘hotline’ service, the call terminator, e.g. in case of the ‘caller ID’ service or it can be a party not being involved in a call, e.g. in case of service

activation/deactivation.
This definition is also used in ITU-T recommendations.

- other party - party that is involved in a call in which a served user invokes a supplementary service.

		served user: **MCS**	**served user:** **BCM**	**served user:** **S 1000/S 1000M**	**served user:** **Westell**	**served user:** **Cisco 3600/ Cisco 3725**
other party	MCS	n/a	• Call Forward	• Call Forward	• Call Forward ***Note:*** If Westell does CFU/CFB to the MCS PRI GW, no audible ringing is provided on the originator's side. This result is due to a restriction on the Westell GW.	-
			• 3WC	• 3WC	• 3WC	
			• Call Transfer w/ consultation	• Call Transfer w/ consultation	• Call Transfer w/ consultation	
			• Blind transfer	• Blind transfer	• Blind transfer	

		served user: **MCS**	**served user:** **BCM**	**served user:** **S 1000/S 1000M**	**served user:** **Westell**	**served user:** **Cisco 3600/ Cisco 3725**
			- Caller ID ***Note:*** Only calling number is displayed; calling number is **not** displayed.	- Caller ID ***Note:*** Only calling number is displayed; calling number is **not** displayed.	- Caller ID ***Note:*** Only calling number is displayed; calling number is **not** displayed.	
other party	BCM	- Conference ***Note:*** Only statio controlled conference is considered, no meet-me conference.	n/a	n/a	n/a	n/a
		- Call Transfer w/ consultation				
		- Blind Transfer				
		- Caller ID				

		served user: MCS	served user: BCM	served user: S 1000/S 1000M	served user: Westell	served user: Cisco 3600/ Cisco 3725
		• Decline & Reject Reason ***Note:*** The reject reason will not be displayed on the H323 GW				
		• Hotline				
		• Redirection				
other party	S 1000M	• Conference ***Note:*** Only statio controlled conference is considered, no meet-me conference.	n/a	n/a	n/a	n/a
		• Call Transfer w/ consultation				
		• Blind Transfer				
		• Caller ID				

		served user: **MCS**	**served user:** **BCM**	**served user:** **S 1000/S 1000M**	**served user:** **Westell**	**served user:** **Cisco 3600/ Cisco 3725**
		• Decline & Reject Reason ***Note:*** The reject reason will not be displayed on the H323 GW				
		• Hotline				
		• Redirection				
other party	Cisco 3600/ Cisco 3725	• Conference ***Note:*** Only station controlled conference is considered; no meet-me conference	n/a	n/a	n/a	n/a
		• Call Transfer w/ consultation				
		• Blind Transfer				
		• Caller ID				

		served user: **MCS**	**served user:** **BCM**	**served user:** **S 1000/S 1000M**	**served user:** **Westell**	**served user:** **Cisco 3600/ Cisco 3725**
		• Decline & Reject Reason ***Note:*** The reject reason will not be displayed on the H323 GW				
		• Hotline				
		• Redirection				
	BCM	• Conference ***Note:*** Only station controlled conference is considered; no meet-me conference	n/a	n/a	n/a	n/a
		• Call Transfer w/ consultation				
		• Blind Transfer				
		• Caller ID				

		served user: **MCS**	**served user:** **BCM**	**served user:** **S 1000/S 1000M**	**served user:** **Westell**	**served user:** **Cisco 3600/ Cisco 3725**
		• Decline & Reject Reason ***Note:*** The reject reason will not be displayed on the H323 GW				
		• Hotline				
		• Redirection				

Support to DTMF

Out of Band DTMF transmission between MCS clients and H323 clients hosted by the CS2K is not possible with the current implementation.

S1000/S1000M, BCM and Westell H323 GWs are only capable to send OOB DTMF signals. So, DTMF transmission from these GWs to the MCS is not possible.

Inband DTMF (non RCF 2833) transmission was verified as described in the following table.

The terms used in the table are explained as follows:

- **n/a** - not applicable. Calls between H.323 agents are not in the scope of this feature.
- **+** functionality supported.
- **-** functionality not supported.

		DTMF receiver				
		MCS client	**S 1000/ S 1000M**	**BCM**	**Westell**	**Cisco 3600/ Cisco 3725**
DTFM Sender	**MCS client**	n/a	+	+	+	+
	S 1000/ S 1000M	-	n/a	n/a	n/a	n/a
	BCM	-	n/a	n/a	n/a	n/a
	Westell	-	n/a	n/a	n/a	n/a
	Cisco 3600/ Cisco 3725	+	n/a	n/a	n/a	n/a

Codecs supported

This activity supports G.711 and G.729 codecs. This activity will verify packetization rates of 10 and 20 ms.

The following table shows the supported codecs/packetization rates on the different gateways.

	MCS clients					
	G711-a		**G729**		**G729a/b**	
	10ms	**20ms**	**10ms**	**20ms**	**10ms**	**20ms**

	MCS clients					
S 1000/ S 1000M	+	+	+	+	- ***Note:*** S 1000/S 1000M considers G729a and G729a/b as different codecs. CS2K never sends a codec of G729a/b to S 1000/S 1000M. So, S 1000M refuses a call from the CS2K that only offers G729 or G729a.	- ***Note:*** S 1000/S 1000M considers G729a and G729a/b as different codecs. CS2K never sends a codec of G729a/b to S 1000/S 1000M. So, S 1000M refuses a call from the CS2K that only offers G729 or G729a.
BCM	+	+	+	+	codec not supported by H323 GW	
Westell	+	+	+	+		
Cisco 3600/ 3725	+	+	+	+		

Software requirements or dependencies

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

- S 1000: release 3.5
- S 1000M: release 3.5
- BCM: release 3.6
- Westell liQ 2031, IPH-DP 1-6-11, supporting 1 E1 with DPNSS
- Westell liQ 2032, IPH-DP 1-6-11, supporting 2 E1 with DPNSS
- Cisco router 3600/3725 (Cisco IOS GW):release 12.3
- MCS 5200: release 3.0

Note: Testing will be done with the newest available load.

Limitations and restrictions

The S 1000 gateway is not explicitely tested, but it is assumed that the functional behaviour is the same as for the S 1000M.

The Cisco IOS GW 3600 is not explicitely tested, but it is assumed that the functional behaviour is the same as for the Cisco IOS GW 3725

This feature is restricted by the availability of supplementary services as specified in the section “Supplementary services” on page 58

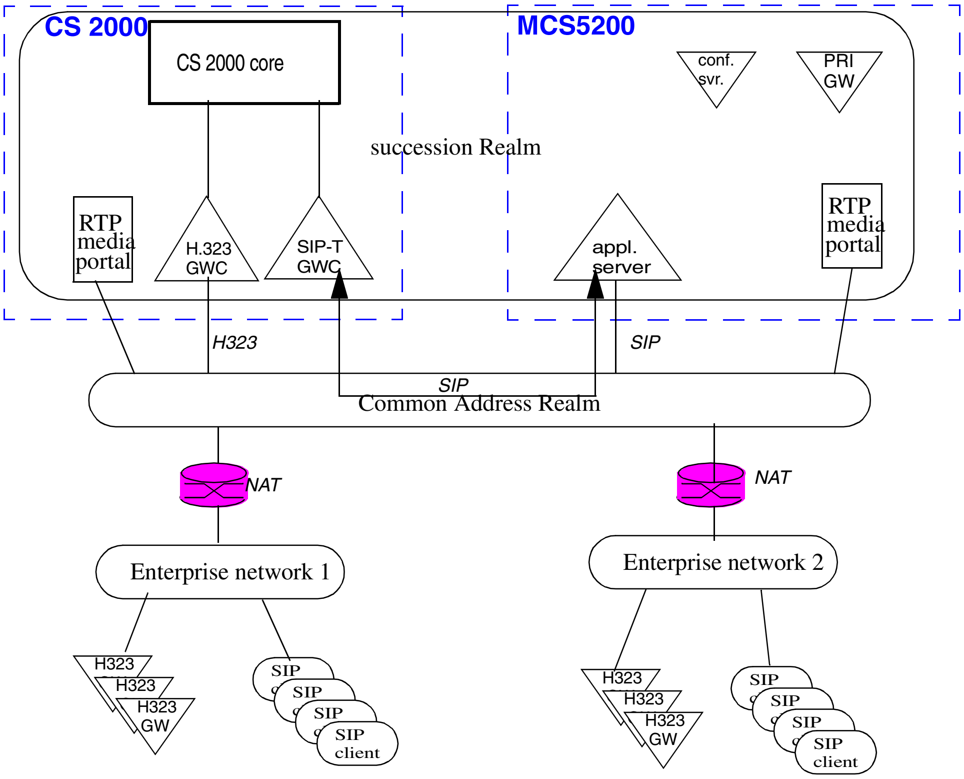
The VPN is realized by a UDP dial plan consisting of location code and extention, e.g. 740 1234.

Interworking North American H.323 to SIP MCS 5200

Overview

The following figure is an example H.323 to MCS 5200 interworking configuration for North America (NA).

H.323 to MCS 5200 interworking configuration



The following table indicates the compliance of the interworking requirements between the CS 2000 H.323 gateway and the MCS 5200.

Req	Requirement text	Comments
201-1	Support interop between the CS2K H.323 GK and the MCS for NA markets	Compliant It is assumed that this is a general requirement and the supported topology is specified in requirements 201-2, 201-3, 201-6, 201-7.

Req	Requirement text	Comments
201-2	Support media and signaling interop between a CS2K H.323 endpoint and an MCS SIP client that are both connected to the same call server.	Compliant Assumption: MCS5200, not the MCS SIP client, is connected to the call server.
201-3	Support media and signaling interop between a CS2K H.323 endpoint and an MCS SIP client when they are connected to different call servers. SIP-T between the CS2K call servers should be able to carry ANSI ISUPv2.	Partially-Compliant Private DN information needs to be tunneled through the public network, currently this functionality is not implemented on the CS2K. Calls that are originated by the MCS are treated as public calls. Assumption: MCS5200, not the MCS SIP client, is connected to the call server.
201-4	Support for interoperability between the following H.323 gateways and MCS SIP clients: **H.323 gateways** • Westell — liQ2031 supporting 1 E1 with DPNSS — ilQ2032 supporting 2 E1 with DPNSS • Cisco IOS gateways • SBC (Cisco IOS GK, S1K/S1KM) • S1K/S1KM • BCM • Cisco Call Manager **MCS SIP clients** • SIP PRI gateway • PC Client • Web Client • i2004/i2002 • Conference Server	Partially-Compliant Excluded H.323 GWs • Session Border Controller (SBC) is not available for test • Westell • Cisco Call Manager is not available for test. • Cisco 3745 GW is used as Cisco IOS GW. Excluded MCS SIP Clients • i2002 (assume i2004 phone is identical) • SIP PRI gateway • MCS Conference server not available for test.

Req	Requirement text	Comments
201-5	Support MCS SIP clients as subscribers in a CS2K hosted VoIP VPN.	Compliant Assumes MCS clients will be treated as a single NCOS, specifically the NCOS assigned to the IBN SIP-T trunk. Note, there are no specific test cases for this requirement.
201-6	Support for MCS hosted users in the same Enterprise/IP address space as the H.323 gateways. (Understand that based on the current MCS implementation that both the MCS and CS2K would insert RTP media portals into the call).	Partially-Compliant Media will not remain on the Enterprise VPN since both MCS and CS2K will insert a Media Portal.
201-7	Support for MCS hosted users and CS2K controlled H.323 gateways being in different Enterprises/IP Address spaces. (Understand that based on the current MCS implementation that both the MCS and CS2K would insert RTP media portals into the call).	Compliant
201-8	Support for service interactions:	Partially-Compliant No supplementary services on Cisco 3745 available.
	Call Forward	
	Conference	On H323 GWs, only three-way calls were tested.
	Call Transfer	
	Caller ID	Only calling number displayed, no calling name.
	Decline and Reject Reasons	Reject reason will not be displayed.
	Codec Selection	
	Hotline	Only available on MCS i2004 client, not on H323 GW.
	Redirect	Only available on MCS, not on H323 GW.

Req	Requirement text	Comments
201-9	Support DTMF interworking between H.323 endpoints (S1K/S1KM, BCM, Cisco Call Manager, SBC, Cisco IOS (RFC2833), Westell (RFC 2833)) and MCS clients (SIP INFO - SIP PRI gw, RFC 2833 - i2004, i2002, PC Client, Web Client, Conference Server	Non-Compliant DTMF is not being supported in this release.
201-10	Support for G.711 and G.729 codecs	Compliant
201-11	Support for 10 and 20 msec packetization rates. The H.323 GWC must handle the fact that the MCS doesn't send the PTIME parameter.	Compliant

Supported markets

This feature only covers markets supported by the NA version of CS 2000.

VPN topology

The MCS 5200 is interconnected to the CS 2000 by a SIP trunk.

The activity supports VPN networks with the following topology:

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

Limitation:

Calls originated by an MCS client that terminate on an H.323 client that is not connected to the same CS2K as the MCS cannot be treated as private calls; i.e., private information will be lost.

Supported H323 gateways and SIP clients

On the CS 2000 the following H.323 gateways will be supported:

- S 1000
- S 1000M
- BCM
- Cisco IOS GW

The following MCS clients are supported:

- PC client
- Web client
- i2004 internet telephone
- Conference server

VPN support on the MCS

In order to create a VPN spanning the CS 2000 and the MCS 5200 each customer group on the CS 2000 will be mapped onto one domain on the MCS 5200. For each VoIP VPN/domain there is exactly one SIP trunk between the CS 2000 and the MCS.

Thus, several VoIP VPNs may exist in a configuration consisting of a CS 2000 and an MCS.

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

Media portal insertion

The media portal will always be inserted on both the MCS 5200 and the CS 2000 independent of the fact, if the MCS 5200 clients and the H323 gateway reside in the same enterprise network or not.

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

Supplementary services

The following table describes the services on the various H.323 gateways and SIP clients.

> ***Note 1:*** A Served User is a party that requests a service. It can be the call originator, as in the case of the hotline service, or the call terminator, as in the case of the caller ID service.
>
> ***Note 2:*** Call Forward does not interact across the MCS 5200 CS2K domains except to deliver a call between the two domains.

Note 3: For Ad Hoc Audio Conference, the client that starts the conference, controls where the conference bridge is allocated (MCS 5200 or CS2000).

Services for MCS/H.323 Clients

Served User				
MCS	**BCM**	**S1000M (aka M1)**	**S1000**	**Cisco 3745**
Conferencing ***Note:*** Only station controlled conference is considered, no meet-me conference (MCS 5200 3.0 in RTPG does not support meet-me conferencing).	Call Forward	Call Forward	Call Forward	Call Forward
Call Transfer	Conferencing ***Note:*** Depending on the capabilities of the gateway, the conference bridge may be located on the GW or on the CS2K.	Conferencing ***Note:*** Depending on the capabilities of the gateway, the conference bridge may be located on the GW or on the CS2K.	Conferencing ***Note:*** Depending on the capabilities of the gateway, the conference bridge may be located on the GW or on the CS2K.	Conferencing ***Note:*** Depending on the capabilities of the gateway, the conference bridge may be located on the GW or on the CS2K.
Caller ID	Call Transfer ***Note:*** Each platform views the other as just initiating a new call.	Call Transfer ***Note:*** Each platform views the other as just initiating a new call.	Call Transfer ***Note:*** Each platform views the other as just initiating a new call.	Call Transfer ***Note:*** Each platform views the other as just initiating a new call.
Decline & Reject Reason				
Hotline	Caller ID	Caller ID	Caller ID	Caller ID

Services for MCS/H.323 Clients

Served User				
MCS	**BCM**	**S1000M (aka M1)**	**S1000**	**Cisco 3745**
Redirection				

Codecs supported

This activity supports G.711 and G.729 codecs. This activity will verify packetization rates of 10 and 20 ms.

The following table indicates with a plus sign (+) the supported codecs/packetization rates on the different gateways.

MCS Clients				
	G711u		G729	
	10ms	20ms	10ms	20ms
S 1000/ S 1000M	+	+	+	+
BCM	+	+	+	+
Cisco IOS Gateway	+	+	+	+

Software requirements or dependencies

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

- S 1000: SSE-2.11.03
- S 1000M: SSE-2.11.03
- BCM: release 3.6
- Cisco 3745 : 12.2
- MCS 5200: release 3.0
- CS2000: SN07

Limitations and restrictions

The Cisco IOS GW 3745 is assumed that the functional behavior is the same as for the Cisco IOS GW product line.

This feature is restricted by the availability of supplementary services as specified in the section “Supplementary services” on page 73

Configuring an International H.323 Network for a Multi-Call Server

Overview

In SN07, Meridian Customer Defined Network (MCDN) based services are tunneled for MCDN capable gateways in inter-call server configurations using SIP-T (ETSI ISUPV2+ and QFT).

Pre-requisites

SIP-T (ETSI ISUPV2+) is used as the transport mechanism for MCDN based service information in inter-call server configurations and requires the activation of the QSIG Feature Transparency option (QFT).

Limitations and Restrictions

The limitations and restrictions for configuring an international H.323 for multi Call Servers include the following:

- Only the tunneling mechanism for MCDN based services is verified.
- Tunneling of MCDN data between enterprises (different customer groups) is out of scope of this activity.
- Service interaction between MCDN based services is not verified within this activity.

Configuring H.323 NA Network CAS Tunneling

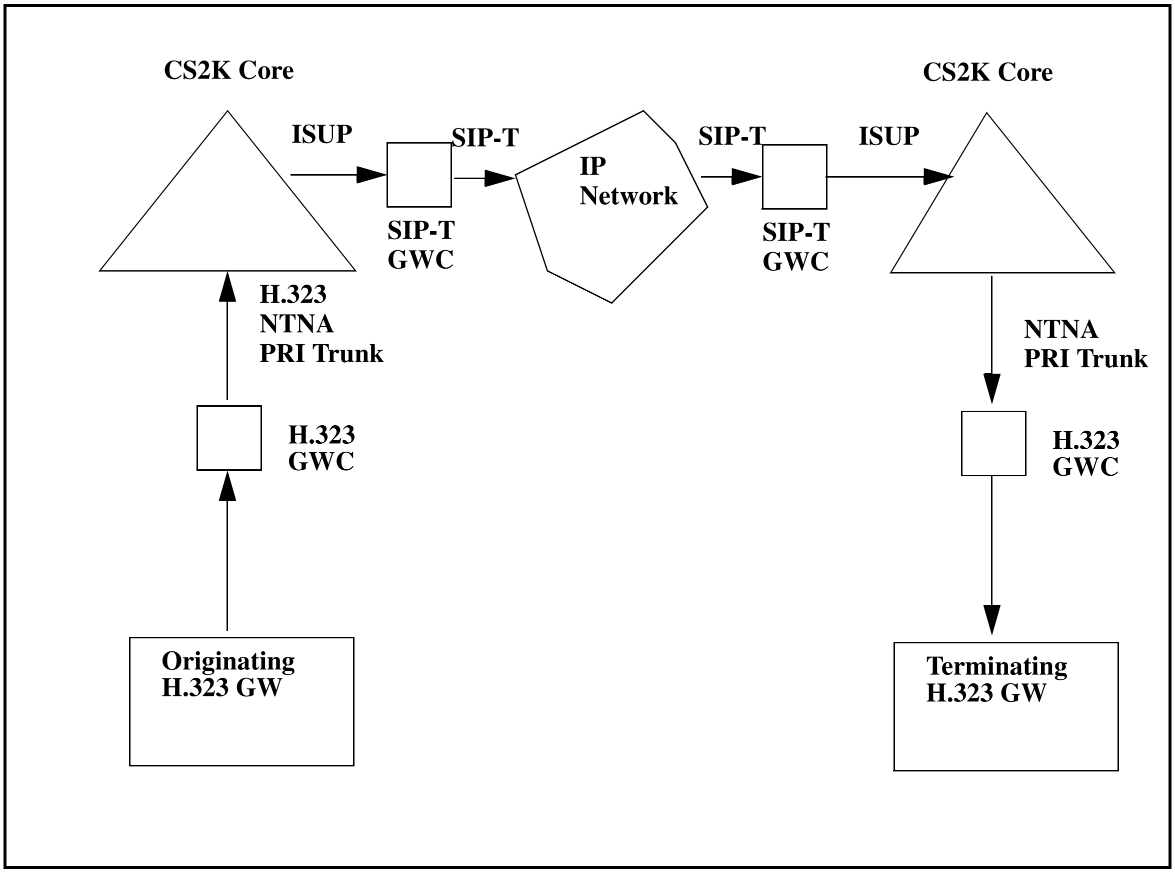
Overview

This activity provides the functionality to support the tunneling of ANSI Call Associated (CAS) messages between two CS 2000s over SIP-T in support of the H.323 protocol.

The following network configuration displays how a CAS message is

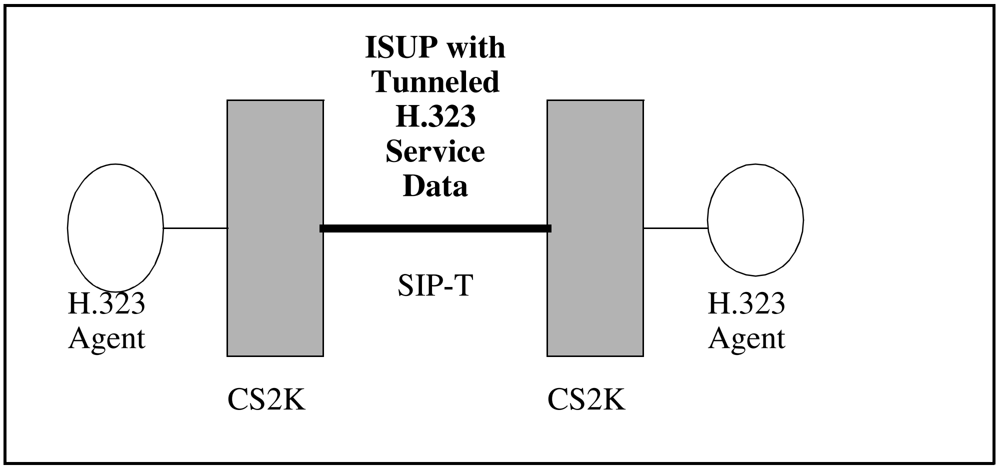
- routed from the originating GW through a GWC to the core a the originating node
- tunneled across the network by SIP-T to the terminating node
- tunneled in a PRI facility message to the terminating GW

Network CAS H.323 tunneling over SIP-T



Even though SIP-T is the only network protocol supported, the H.323 payload is tunneled within ISUP messages through the SIP-T messages, hence the references to ISUP as shown in the following figure.

Functional behavior



H.323 call processing

This activity covers the development within the CS2000 core to enhance the PRI/ISUP interworking to tunnel the H.323 payload within an appropriate ISUP parameter to the destination CS2000 where the payload is extracted and presented in such a way that the existing PRI functionality will tunnel that payload and route it to the terminating GW.

ANSI call processing

The H.323 message is

- received from an H.323 gateway (GW) by the Gateway Controller (GWC)
- mapped to an NTNA PRI Q.931 message
- sent over an H.323 NTNA PRI trunk signaling channel to the CS 2000 for processing

CAS call processing

The GWC processes H.323 data from the originating switch:

- extracts the tunneled payload from the UUIE in the H.323 message
- includes the message in the Facility Informaton Element (FAC IE) of a corresponding NTNA PRI message

- if the payload is destined for a local CS 2000,
  - routes the message to the appropriate NTNA PRI trunk
- If the payload is destined for a gateway at a remote CS 2000,
  - extracts PRI message from payload
  - tunnels H.323 message within an ISUP message to the destination switch using SIP-T protocol over the IP network

The terminating CS 2000

- receives payload within the ISUP message
- tunnels received ISUP message within the FAC IE of an NTNA PRI message
- sends ISUP message to the GWC over an NTNA PRI H.323 trunk signaling channel
  - The GWC tunnels the payload with the UUIE of an H.323 message through the appropriate gateway.

Tunneling of H.323 data

The tunneling of H.323 data within an ISUP message can be divided into two components

- Mapping PRI Fac IE's to ISUP Parameters
- Segmenting Large Payloads

Mapping PRI Fac IE's to ISUP Parameters

At the originating GWC, this component determines that there is H.323 data to tunnel, creates the appropriate ISUP parameter, and adds the H.323 data.

At the terminating CS 2000, this component determines there is H.323 data tunneled. Existing PRI functionality ensures the data is tunneled to the destination gateway.

The following list shows the mapping of PRI to ISUP messages that can tunnel the data. The SC_X messages are sent from the GWC. The SCP_C messages are sent to the GWC.

- Setup (maps to SCP_X_Origination/SCP_C_Origination) -> ISUP IAM
- Alerting (maps to SCP_X_Alerting/SCP_C_Alerting or SCP_X_Progress/SCP_C_Progress) -> ISUP ACM
- FAC (maps to SCP_X_FAC/SCP_C_FAC) -> ISUP FAC

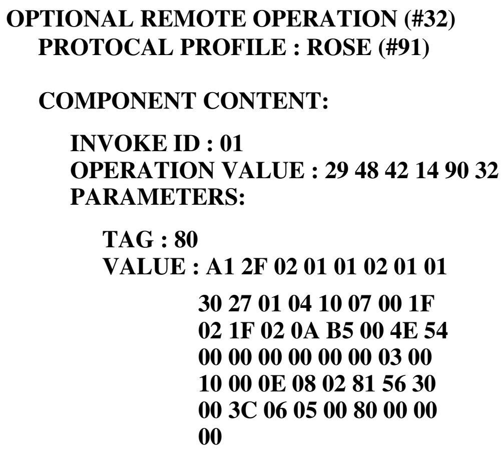
- Connect (maps to SCP_X_Progress ppi=Connect/SCP_C_Progress ppi=Connect) -> ISUP ANM
- Release (maps to SCP_X_Release/SCP_C_Release) -> ISUP REL

Associated data table for configuring Remote Operation (RO) parameter

In each of the listed ISUP messages the H.323 payload is tunneled in the ISUP Remote Operation (RO) parameter. The H.323 payload is tunneled within the Value field of the RO.

The following figure shows the structure of an RO parm containing an H.323 payload.

Format of an ISUP RO parameter for H.323 tunneling



```
OPTIONAL REMOTE OPERATION (#32)
    PROTOCAL PROFILE : ROSE (#91)

    COMPONENT CONTENT:

        INVOKE ID : 01
        OPERATION VALUE : 29 48 42 14 90 32
        PARAMETERS:

            TAG : 80
            VALUE : A1 2F 02 01 01 02 01 01
                        30 27 01 04 10 07 00 1F
                        02 1F 02 0A B5 00 4E 54
                        00 00 00 00 00 00 03 00
                        10 00 0E 08 02 81 56 30
                        00 3C 06 05 00 80 00 00
                        00
```

Segmenting large payloads

The originating H.323 GWC controls segmenting the payload and restoring it at the remote office. The GWC

- segments the payload based on a preset maximum, currently 180 bytes from the GW. The first 180 bytes is sent in the applicable PRI message.
- tunnels data in the RO of the appropriate ISUP message
- sends the remainder of the data in a PRI FAC message
  - — Data is tunneled in the RO of the ISUP FAC.
- restores the payload data at the remote office

The CS 2000 controls segmenting the payload and restoring it at the terminating office.

- For the PRI SETUP message, the first 100 bytes is tunneled in the RO of the ISUP IAM. The remainder of the data is tunneled in the RO of the ISUP FAC.
- For all other PRI messages with greater than 115 bytes, the data is tunneled in multiple ROs of the applicable ISUP message.

Configuring an H.323 Flexible Carrier

Overview

This SN07 activity will enable the addition of H.323 virtual carriers with a size within the range of 4 to 672. The current implementation allocates H.323 virtual carriers in blocks of 24 or 32, based on the market. The new capability will only effect carriers that are defined as the type H.323.

The H.323 Flexible Carrier feature will enable our customers to allocate small and large groups of endpoints for H.323 gateways. By allowing variable size blocks of endpoints/TIDs (Terminal Identifiers), customers can manage the TID range of a H.323 GWC (Gateway Controller) more efficiently.

The new capability is targeted to customers who don't have OSS (Operations Support System) requirements to provision blocks of endpoints in (24 or 32) increments and support small H.323 systems.

Reference documentation

For configuration information, refer to the following procedure in the document: **GWC Configuration Management**, NN10205-511

- **Add carriers to a GWC**

Configuring an NA H.323 for Networked MCDN services

Overview

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

- Interworking on a per nodal basis. These specific set of MCDN services are supported and interworked over a PRIH323 Trunk facility between either a Nortel Network Media Gateway 1000 or BCM, and a hosted centrex line on a NA CS2K switch.
- Interworking on a per inter-Call Server basis. These specific set of MCDN services are supported and interworked over a SIP-T Trunk facility between either a Nortel Network Media Gateway 1000 or BCM, and a hosted centrex line on a NA CS2K switch.

The following H.323 intereworkings 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 (Nortel Network Media Gateway 1000) <--> H.248 GW (CICM, P-phone)
- H.323 GW (Nortel Network Media Gateway 1000) <--> MGCP GW (Mediatrix, IBN lines)

The following supported MCDN services are listed in the “Features and services” on page 185

- BCM interworking to CICM and Mediatrix for nodal calls and through SIP-T
- Nortel Networks Media Gateway 1000 interworking to CICM and Mediatrix GW for nodal calls and through SIP-T.

Pre-requisites

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

A SIP_T H.323 Trunk tunnels ANSI ISUP data through a SIP-T Trunk for support of the H.323 protocol on an NA CM load.

Sequence of datafill

The PRI$_{H.323}$ trunk type is provisioned on the CS 2000 within the LTDATA table with the PRI_IP_PROT option, and the H.323 VOIP_PROTOCOL_TYPE.

The SIP_TH.323 trunk type will be provisioned on the CS2K within the following existing CS2K Tables:

- CLLI
- TRKGRP
- TRKSGRP
- MGCINV
- TELEPROF
- VRINV
- TRKOPTS
- DPTRKMEM

Associated data tables for configuring trunks for PRI$_{H.323}$

The following example is of PRI$_{H.323}$ datafill.

PRI$_{H.323}$ datafill trunk type example

```
TABLE: LTDATA
LTDKEY LTDRSLT
--------------
ISDN 867 SERV SERV Y Y ALWAYS ALWAYS (PRI_IP_PROT H323) $
```

Limitations and Restrictions

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

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

  For supported MCDN services, refer to “Features and services” on page 185
- Line side development (P-phone, IBN lines) is not part of this feature.
- Development on the H.323 agents (BCM, Nortel Networks Media Gateway 1000) is not part of this feature.
- MCDN Services which are not supported either by an H.323 agent or the line agent, will not be supported by this feature

- Tunneling of MCDN data between Enterprises is outside of scope of this feature.
- Verification of MCDN services is done using Nortel Networks Media Gateway 1000M. Omitting verification on Succession1000 GW is acceptable, because both GWs use the same software load.
- Testing is done on the North American CS2K load only.
- For Calling Name and Number delivery, the appropriate feature must be provisioned against the subscriber (i.e., CND - Calling Number Delivery, CNAMD - Calling Name Delivery, etc.)
- In the Mediatrix/CICM (CS2K) to Succession-1000M direction, only private Numbering Plan Indication (NPI) calls will contain this privately built MCDN tunneled data - public calls will not contain MCDN tunneled data.
- In the Mediatrix/CICM (CS2K) to Succession-1000M direction, private NPI with Local Type of Number (TON) is coded as an UIPE ESN CDP TON.
- CS2K Core Calling Name Delivery remains unchanged by this activity to either line agents or trunk agents; therefore, existing functionalities, restrictions or limitations of Calling Name Delivery remain applicable.

Configuring H.323 Gatekeeper to CS2000 Gatekeeper Interoperability

Overview

This feature enables H.323 Gatekeepers in an external network (private, enterprise, other carrier's, etc.) to interop with a CS2000 H.323 Gatekeeper on a carrier network.

Reference documentation

For configuration information, refer to the following procedure in the document: **GWC Configuration Management**, NN10205-511

- **Associate an H.323 media gateway**

VCAC, Internet Transparency, Security

What's new?

In CHS (i)SN06.2, Media Proxies were datafilled on every Gateway Controller (GWC).

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

To provision the VCAC SOC option, refer to the following procedures in the section:Provisioning VCAC SOC on page 105:

- Enabling the VCAC SOC option on the CM on page 105
- Datafilling the CM for VCAC-SOC and treatment on page 105
- Disabling the VCAC SOC option on the CM on page 105

Virtual Call Admissions Control

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

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

Internet Transparency and security-related products

The Internet Transparency and security products deliver the following capabilities:

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

Reference information

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

Configuring multi D-channel support

Overview

In (i)SN07, functionality for provisioning has been added or amended to exiting functionality to include:

- changing the capacity of an H.323 GW after initial provisioning
- changing the IP address of an H.323 GW after initial provisioning
- changing the port of an H.323 GW after initial provisioning
- allowing users to specify the TID location of EPGs
- providing modified GUI display capabilities for H.323 EPGs

An important change to point out as a consequence of this feature is that EPGs are no longer automatically added when a H.323 GW is added. This change was implemented so that greater flexibility could be realized when adding EPGs. It gives the users the ability to specify the location of the EPs in the system so that Terminal Space can be controlled, and therefore fragmentation can be better managed.

This (i)SN07 activity will enable the addition of H.323 virtual carriers with a size within the range of 4 to 672. The current implementation allocates H.323 virtual carriers in blocks of 24 or 32, based on the market. The new capability will only effect carriers that are defined as the type H.323.

Reference documentation

For configuration information, refer to the following procedure in the document: **GWC Configuration Management**, NN10205-511

- **Add carriers to a GWC**

Configuring VCAC support for CICM gateways

Reference documentation

For configuration information for this feature, refer to the following procedures located in the NTP: **GWC Configuration Management**, NN10205-511

- Associate a line media gateway with middlebox
- View gateway provisioning data for a GWC node
- Change gateway attributes

Provisioning GWCEM internet transparency for VCAC

Reference documentation

For configuration information for this feature, refer to the following procedures located in NTP: **GWC Configuration Management** , NN10205-511

- **General GWC procedures**
- **Associate a line media gateway with middlebox**
- **Change gateway attributes**
- **Add a network address translator (NAT) device**
- **Delete a network address translator (NAT) device**
- **Change attributes of a network address translator (NAT) device**
- **Configure resource usage data for limited bandwidth links (LBLs)**
- **Add a limited bandwidth link (LBL)**
- **Change attributes of a limited bandwidth link (LBL)**

Configuring Common Topology elements for VCAC

Reference documentation

For configuration information for this feature, refer to the following procedures located inthe NTP: **GWC Configuration Management**, NN10205-511

- **General GWC procedures**
- **Set the call agent identifier**
- **View a network address translator (NAT) middlebox**
- **Add a network address translator (NAT) device**
- **Delete a network address translator (NAT) device**

Configuring E911

Reference documentation

For configuration information for this feature, refer to the following procedures in the NTP: **GWC Configuration Management** , NN10205-511

- **General GWC configuration procedures**
- **Configure a destination for CICM location information**
- **Enable/disable CICM location change reporting**

Provisioning VCAC SOC

Overview

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

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

Datafilling the CM for VCAC-SOC and treatment

at the command line

1 Datafill the NBLN treatment in table TMTCNTL:OFFTREAT

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

Example: NBLN Y S CONGESTION

Enabling the VCAC SOC option on the CM

at the command line

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

ASSIGN RTU <keycode> TO CS2Q0002

Note: The RTU flag is set to Y.

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

ASSIGN STATE ON TO CS2Q0002

Disabling the VCAC SOC option on the CM

at the command line

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

REMOVE RTU <keycode> FROM CS2Q0002

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

ASSIGN STATE IDLE TO CS2Q0002

Third-party SIP interworking

What’s new?

In (i)SN07, the following enhancements are made to CHS interworking:

- Configuring an IP Client line option for Centrex IP Service on page 149
- SIP on SP2000 on page 151
- Nortel Carrier Grade Linux (NCGL) platform Session Server on page 153

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

For more information about SIP-T in (i)SN07, refer to the documents on the component, Session Server on page 216

Overview

The Third-Party SIP Interworking product allows the CS 2000 to use SIP to interwork with third-party call servers and application servers.

SIP is a service-enabling protocol used for real-time, multimedia sessions to integrate voice, data and video. The SIP Application Module uses SIP to communicate with the following MCS 5200 components:

- SIP Audio Server
- SIP PRI Gateway
- Provisioning Module
- Web Client Manager
- IP Client Manager

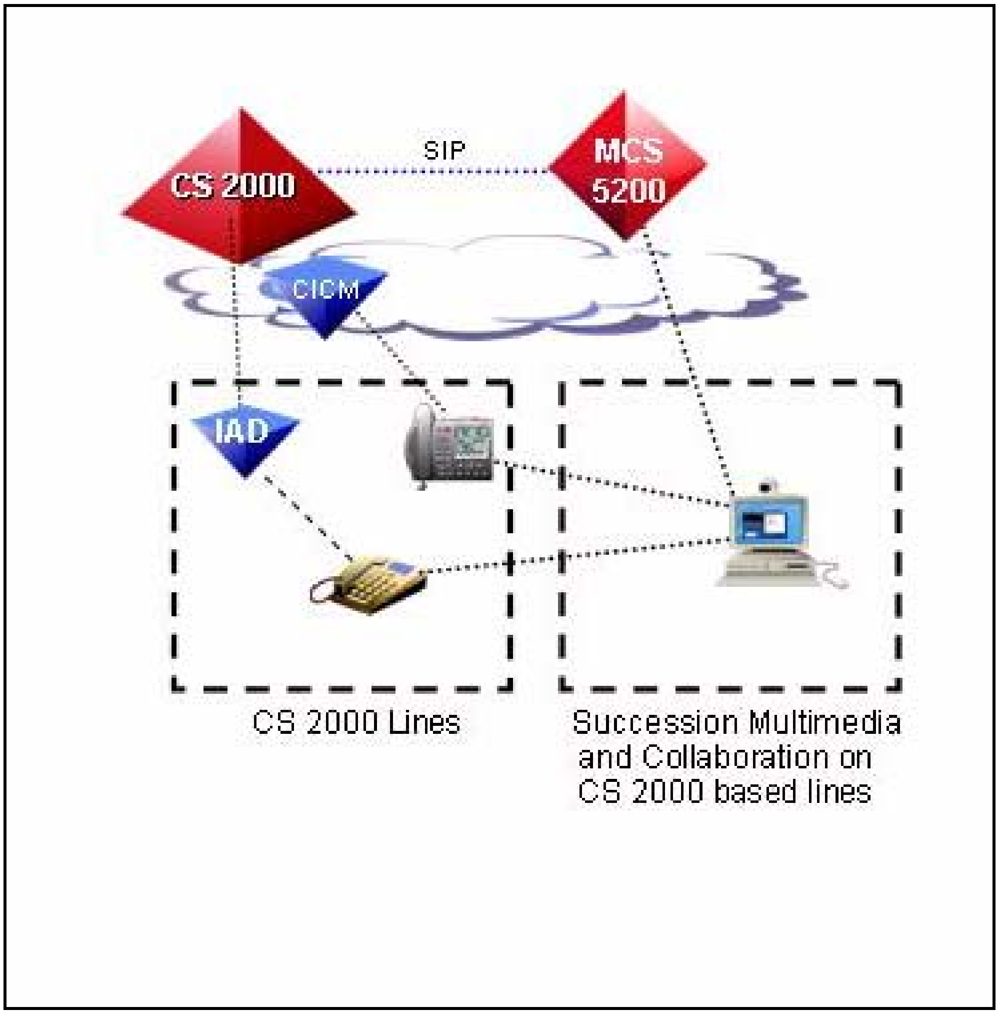
- Multimedia PC Client
- Multimedia Client Set
- Media Application Server (MAS)

MCS 5200 to CS 2000 Interworking

The MCS 5200 to CS 2000 Interworking product supports interworking between user agents on a CS 2000 and an MCS 5200 network to create a converged network.

The following figure shows the architecture of the MCS 5200 to CS 2000 Interworking product to create a converged desktop.

MCS 5200/CS 2000 Interworking architecture


SIP
CS 2000
MCS 5200
CICM
IAD
CS 2000 Lines
Succession Multimedia and Collaboration on CS 2000 based lines

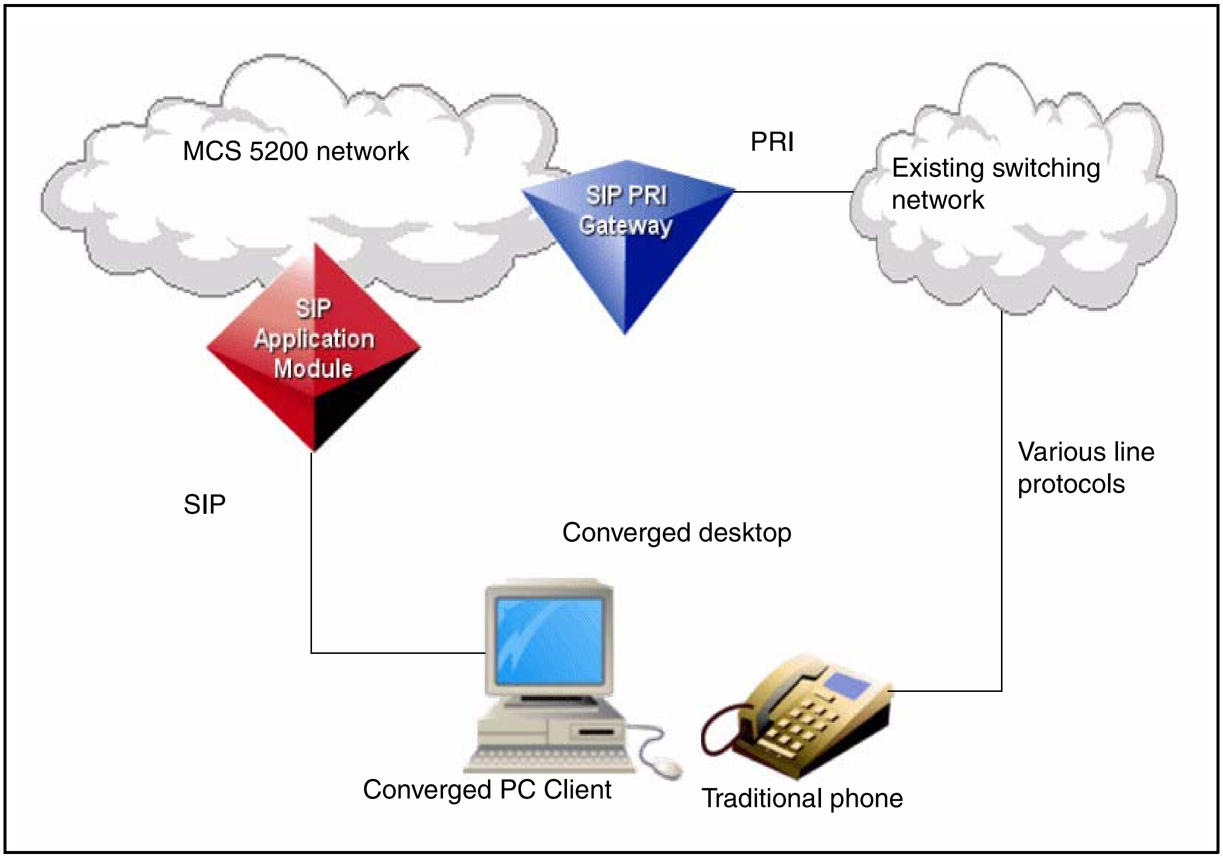
In a converged desktop, end users can use their existing desktop telephone for voice calls and the Multimedia PC Client for multimedia communication.

The Multimedia PC Client is a software application that transforms a PC into a powerful telephony and multimedia communication tool. This software application runs on a PC and provides access to SIP features and multimedia services, including the following:

- the ability to set up automated enhanced routing and screening of incoming calls based on time of date or on the calling party's identity
- a call log of all incoming calls
- the ability to send instant messages (IM) to the party on the other end of the call
- the ability to start collaborative applications:
  - shared whiteboard
  - file transfer
  - web browsing
  - clipboard transfer with the party on the other end of the call
- the ability to receive a picture ID of the party on the other end of the call

A converged desktop consists of a TDM telephone and a multimedia PC client software positioned as a Converged PC Client. The following figure shows how the Converged PC Client connects with the network.

Converged desktop services network diagram



The Converged Desktop Services (CDS) includes the following features:

- Advanced call handling – The user can use the MCS 5200 Personal Agent web pages to control the user's availability. By providing this ability to CDS users, features not easily accessible on existing TDM switching system become viable. (For example, a user can activate MCS 5200-based forking using the Personal Agent so that when the user's desktop telephone is called, the user's cell phone also rings. Once one leg of the forked call is answered, the other leg stops ringing.
- Inbound call log – The user can see who has called and when the call occurred.
- Video calling line identification – The user can see who is calling. The picture is retrieved from the network-based address book accessible on the Converged PC Client.
- Redirection of incoming calls at the Converged PC Client – Upon arrival of an incoming call, the user can click on the "Redirect" button

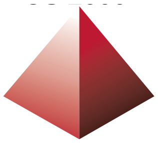
to send the incoming call to another address. Once the user answers the call, the redirect function is no longer available.

- File transfer – If both the originator and terminator support the MCS 5200 file transfer collaboration application, then files can be transferred back and forth between the two users.
- Whiteboard sharing – If both the originator and terminator support the MCS 5200 whiteboard collaboration application, then a whiteboard session can be set up between the two users.
- Clipboard transfer – If both the originator and terminator support the MCS 5200 clipboard transfer collaboration application, then the Windows System Clipboard can be transferred between the two users. The clipboard transfer application allows a user to copy items such as PowerPoint slides or sections of Excel spreadsheets to the clipboard, and to send them to another party.
- Web co-browsing – If both the originator and terminator have access to this functionality, one user can automatically drive the other's web browser. (The Web Client supports reception of web pages, but cannot send web pages to a Converged PC Client.
- Instant Messaging (IM) – The Converged PC Client can send and receive messages from any client that supports the Nortel Networks IM format. All MCS 5200 clients support sending and receiving of IMs with each other.
- Presence state indications – The Converged PC Client enables the user to select a presence state in the MCS 5200 network. The user can then see the presence states for "Friends" in his or her network-based address book.

CHS components

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

CHS components and their functions

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

CHS components and their functions

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

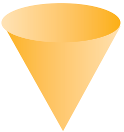
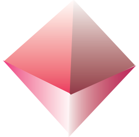
CHS components and their functions

Component	Sub-component	Function
	Office alarm unit (OAU)	The OAU connects a CS 2000 with the office alarm system to provide notification of physical or electrical problems. An OAU consists of two main types of functional elements: • 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.
CS 2000	Service Application Module 21 (SAM21)	The SAM21 shelf houses the GWC cards. All tools and utilities for the SAM21 are provided by CS 2000 SAM21 Manager.

CHS components and their functions

Component	Sub-component	Function
CS 2000	Gateway Controller (GWC)	The GWCs provide protocol mediation between the XA-Core and media gateways such as the Media Gateway 15000, MG 9000, and the RTP Media Portal. In other words, the GWCs convert proprietary supervision messages from the XA-Core to protocols recognized by the media gateways. The CS 2000 XA-Core and the CS 2000 - 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 • packet cable Dynamic Quality of Service (DQoS) and Common Open Policy Services (COPS) • Media Gateway Control Protocol (MGCP) Every GWC uses the same hardware and software. Profiles applied at the GWC Manager define the type of GWC.

CHS components and their functions

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

CHS components and their functions

Component	Sub-component	Function
CS 2000	Audio Provisioning Server (APS)	The APS is a subcomponent of UAS. The APS is required whenever the UAS is used as the announcement server. The APS assures that all UASs in the network use the same announcements. The APS is a non-call processing component. It uses a user-friendly web interface to provision audio services and to set up distribution of announcements to UASs in the network.

CHS components and their functions

Component	Sub-component	Function
CS 2000	Universal Signaling Point (USP) and USP Compact	The USP is the default SS7 signaling server for new installations (greenfield). The USP supports a redundant 10/100BaseT IP interface. This release provides the following capabilities: • 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 • support for up to 16 multi-point codes • support for up to 440 low-speed SS7 links

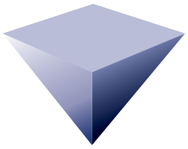
CHS components and their functions

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

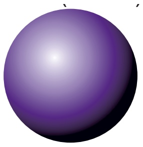
CHS components and their functions

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

CHS components and their functions

Component	Sub-component	Function
Gateways		
Media Gateway 15000 		Media Gateway 15000 serves as a media gateway in the Succession Network. It 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

CHS components and their functions

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

CHS components and their functions

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

CHS components and their functions

Component	Sub-component	Function
Nortel Networks Multiservice Switch (MSS)	CS 2000 Management Tools	CS 2000 Management Tools is a suite of network management tools used in Succession solutions. The CS 2000 Management Tools suite consists of the following network management tools: • GWC Manager • UAS Manager • APS • APS Manager • SAM21 Manager • Network Patch Manager (NPM) • Nodes Configuration • 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 • Batch Provisioning Tool (BPT) • Batch Configuration Monitor • OSSGate • USP Bootp Server

CHS components and their functions

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

CHS components and their functions

Component	Sub-component	Function
Nortel Networks Multiservice Switch (MSS)	CS 2000 SAM21 Manager	The CS 2000 SAM21 Manager is a graphical user interface (GUI) that provides access to OAM&P functions such as platform software load, platform diagnostics, platform upgrade, and NFS mount provisioning. In addition, the CS 2000 SAM21 Manager provisions the hardware of a CS 2000 GWC, for fault management of a CS 2000 GWC card, and to upgrade the firmware of a CS 2000 GWC. CS 2000 SAM21 Manager has two components: the EM server and the EM client. The CS 2000 SAM21 EM server resides on the same server that hosts the Succession Server Platform Foundation Software (SSPFS) non-CM load (NCL) software package (part of the CS 2000 Management Tools software). Currently, the SSPFS package runs on a Netra t1400. Note that CS 2000 SAM21 EM server does not have a GUI. The CS 2000 SAM21 EM client runs on either a PC or Sun Solaris machine and provides a GUI of the physical layout of the SAM 21 shelf for fault management and configuration management of the SAM21 shelf.
Nortel Networks Multiservice Switch (MSS)	Network Patch Manager (NPM)	The NPM is used to support individual patching of software loads for the following components: • CS 2000 GWC • MG 9000 • MG 9000 Manager • Network Patch Manager (NPM) • Patching Server Element (PSE) • SAM21 EM • CS 2000 Management Server

CHS components and their functions

Component	Sub-component	Function
Nortel Networks Multiservice Switch (MSS)	Trunk Maintenance Manager (TMM)	The TMM provides an XML interface that allows client applications (GUIs) to perform basic maintenance operations on GWC-managed trunks, such as posting, busying, and returning to service.
Nortel Networks Multiservice Switch (MSS)	Lines Maintenance Manager (LMM)	The LMM application is used to post lines and perform maintenance activities on them.
Nortel Networks Multiservice Switch (MSS)	V5.2 Configuration and Maintenance	The V5.2 Configuration and Maintenance applications are used to manage v5.2 interfaces within a Succession Network. ***Note:*** These applications are available only in the International version of the software.

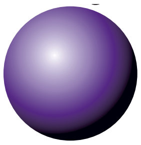
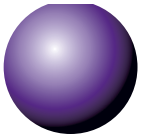
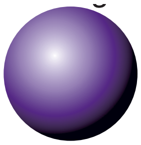
CHS components and their functions

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

CHS components and their functions

Component	Sub-component	Function
Nortel Networks Multiservice Switch (MSS)	Batch Configuration Monitor	The Batch Configuration Monitor is a web-browser interface to view provisioning output files in a readable format.
Nortel Networks Multiservice Switch (MSS)	OSSGate	OSSGate is a GUI application that provides a machine interface for provisioning components in Succession. The main functionality of OSSGate is to act as a gateway to the Node, Carrier, Trunk, Line, ADSL Provisioning applications and the Trunk Maintenance application.
Nortel Networks Multiservice Switch (MSS)	Trunk Maintenance Manager (TMM)	The TMM provides an XML interface that allows client applications (GUIs) to perform basic maintenance operations on GWC-managed trunks, such as posting, busying, and returning to service.

CHS components and their functions

Component	Sub-component	Function
Nortel Networks Multiservice Switch (MSS)	Call Agent Manager 	The CS 2000 - Compact Call Agent Manager is a menu-driven console application that provides access to SAM21 platform alarms, platform performance monitoring, platform logs, platform connectivity, and platform patching. In addition, Call Agent Manager is the primary interface for platform functions such as a cold SWACT, routine exercise text, jamming and synchronization of the call processing application.
Nortel Networks Multiservice Switch (MSS)	STORM Manager 	The STORM Manager is used with CS 2000 - Compact. The STORM Manager is a Web-server application that runs on the STORM card. STORM Manager allows you to: • provision and control application-level STORM functions • modify STORM file systems • view STORM logs
Nortel Networks Multiservice Switch (MSS)	Universal Signaling Point (USP) Manager 	USP Manager is a Windows 2000 workstation that provides a GUI for provisioning and monitoring SS7 interfaces. The bootp server for the USP is part of the CS 2000 Management Tools server.

CHS components and their functions

Component	Sub-component	Function
Nortel Networks Multiservice Switch (MSS)	Nortel Networks Multiservice Switch 8600 Device Manager	The Device Manager (for Nortel Networks Multiservice Switch 8600) is a suite of GUI applications that manages and configures a Nortel Networks Multiservice Switch 8600 chassis. It can be launched independently or as part of Optivity.
Nortel Networks Multiservice Switch (MSS)	RTP Media Portal Manager	For the RTP Media Port, the System Management Console is used to perform fault and configuration management. The RTP Media Portal management data is stored on the Management Module and the Database Module. The Management Module stores alarm, log, and OM data. The Database Module stores configuration data.
Nortel Networks Multiservice Switch (MSS)	Preside MDM	Preside MDM manages the Media Gateway 15000. Nortel Networks MDM performs fault management, configuration management, data collection, performance management, and security management. In addition, Nortel Networks MDM forwards Media Gateway 15000 performance management, and fault management information to the CS 2000 Core Manager. Nortel Networks MDM resides on a Sun-based workstation.
Centrex IP		
Centrex IP Client Manager		The CICM delivers Centrex capabilities to users connected to an IP network using VoIP technology on a PC SoftClient or an IP P-phone.

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

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

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

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

MCS 5200 functional components (required)

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

MCS 5200 functional components (required)

MCS 5200 components	Description
	The Management Module enables communication between the System Management Console and other network components. It provides the software functionality that: • 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 Management Module is located in the private MCS 5200 network. The System Management Console is the administrators interface to the Management Module. For information on the Management Module, refer to *MCS 5200 Management Module Basics,* NN100030-111. For information on the System Management Console, refer to *MCS 5200 System Management Console Basics*, NN10247-111. For information on the Management Module in the dedicated configuration to support MCS RTP Media Portals associated with the CS 2000, refer to the *CVoIP Management Module Basics,* NN10369-111. For information on the System Management Console in the dedicated configuration to support MCS RTP Media Portals associated with the CS 2000, refer to the *CVoIP System Management Console User Guide*, NN10370-111.

MCS 5200 functional components (required)

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

MCS 5200 functional components (required)

MCS 5200 components	Description
	The Provisioning Module provides the interface for the access clients (Multimedia PC Client, Multimedia Client Set, Provisioning Client, and Personal Agent) to securely access the data stored in the Oracle Database. It supports the following tasks: • 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 Module, a Sun ONE Web Server* processes HTTP requests from the Multimedia Web Client, Personal Agent, and Provisioning Client to support self provisioning and network-based services. The Provisioning Module is dual-homed. For more information about the Provisioning Module, refer to *MCS 5200 Provisioning Module Basics,* NN10242-111*,* and *Provisioning Client User Guide,* NN10043-113. For more information on provisioning tasks that the Provisioning Module processes, refer to the following documents: • *Provisioning Client User Guide*, NN10043-113 • *Multimedia PC Client User Guide,* NN10041-113 • *Multimedia Web Client User Guide*, NN10040-113 • i2002 Internet Telephone User Guide, NN10319-113 • *i2004 Internet Telephone User Guide*, NN10042-113

MCS 5200 functional components (required)

MCS 5200 components	Description
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 • 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 The System Management Console runs on a personal computer (PC) and communicates with the Management Module on the private MCS 5200 network. For more information about the System Management Console, refer to *MCS 5200 System Management Console Basics*, NN10247-111. For information on the System Management Console in the dedicated configuration to support MCS RTP Media Portals associated with the CS 2000, refer to the *CVoIP System Management Console User Guide*, NN10370-111.

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

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

MCS 5200 component	Description
	The IP Client Manager manages the i2002 and i2004 Internet Telephones. It provides them access to MCS 5200 SIP services. The IP Client Manager provides access to the following features: • 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 i2002 and i2004 Internet Telephones 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 • i2002 Internet Telephone User Guide, NN10319-113 • *i2004 Internet Telephone User Guide,* NN10042-113
	The Web Client Manager manages the Multimedia Web Client and enables subscribers to access the MCS 5200 SIP services from a Web browser. The Web Client Manager also provides the Multimedia Web Client feature set and enables the interworking of the Multimedia Web Client and the SIP Application Module. The Web Client Manager is deployed from the System Management Console. For more information on the Web Client Manager, refer to *MCS 5200 Web Client Manager Basics,* NN10277-111.

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

MCS 5200 media servers

Media servers	Description
SIP Audio Server	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.

MCS 5200 media servers

Media servers	Description
	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 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.

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

MCS 5200 Gateway

Gateway	Description
	The SIP PRI Gateway converts packet-based voice streams to circuit-based voice streams to allow SIP endpoints the ability to connect to PSTN devices. Some of its functions include: • 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.

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

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

Table 0-1 MCS 5200 access clients (Sheet 1 of 5)

Access client	Description
Note: Subscriber access to the SIP services network requires one of the following clients: Multimedia PC Client, i2002 Internet Telephone, i2004 Internet Telephone, Multimedia Web Client, or Multimedia Client Set.	
	The Multimedia PC Client is a stand-alone SIP-enabled user agent installed on a Personal Computer (PC) that provides access to SIP features and services such as: • 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.*

Table 0-1 MCS 5200 access clients (Sheet 2 of 5)

Access client	Description
	The i2002 and i2004 Internet Telephones provide voice services, while the PC provides all other services. When the Multimedia PC Client is configured to control the i2002 and i2004 Internet Telephones, the configuration is known as the Multimedia Client Set. The Multimedia Client Set provides access to SIP features and services such as: • 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; *i2002 Internet Telephone User Guide,* NN10319-113; *i2004 Internet Telephone User Guide,* NN10042-113; and MCS 5200 *Feature Description Guide*.

Table 0-1 MCS 5200 access clients (Sheet 3 of 5)

Access client	Description
	The i2002 Internet Telephone is a MCS 5200 hard client device that provides a traditional looking telephone set enhanced with multimedia features for accessing IP-based MCS 5200 SIP services. It provides a two line display to enable multimedia services. Some of the i2002 Internet Telephone advanced features include: • Instant Messaging • stock query • call forward • do not disturb • multiple user login (4 simultaneous users) • bulletins • Quality of Service (QoS) information The IP-based i2002 Internet Telephone is located on the managed public network and is managed by the IP Client Manager (IPCM). For a complete list of features, refer to of this chapter. For more information on the i2002 Internet Telephone, refer to the *i2002 Internet Telephone User Guide,* NN10041-112, and MCS 5200 *Feature Description Guide*.
	The i2004 Internet Telephone is a Nortel Networks MCS 5200 hard client device that provides a traditional looking telephone set enhanced with multimedia features for accessing IP-based MCS 5200 SIP services. It provides a large, multiple line display to enable multimedia services. Some of the i2004 Internet Telephone advanced features include: • Instant Messaging • stock query • call forward • do not disturb • multiple user login (6 simultaneous users) • bulletins • QoS information The IP-based i2004 Internet Telephone is located on the managed public network and is managed by the IP Client Manager (IPCM). For more information on the i2004 Internet Telephone, refer to the *i2004 Internet Telephone User Guide,* NN10042-113, and MCS 5200 *Feature Description Guide*.

Table 0-1 MCS 5200 access clients (Sheet 4 of 5)

Access client	Description
 Provisioning Client	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.

Table 0-1 MCS 5200 access clients (Sheet 5 of 5)

Access client	Description
	The Personal Agent is a browser-based client that allows users to perform network-based management with their own MCS 5200 services and communication preferences. Features include: • 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.*
	The Multimedia Web Client is a Web-based access client that provides various multimedia and telephony features such as: • traditional telephone services • 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 functionalities. For more information on the Multimedia Web Client, refer to the *Multimedia Web Client User Guide,* NN10040-112, and *MCS 5200 Feature Description Guide*.

Configuring an IP Client line option for Centrex IP Service

Overview

For SN07/SE07, Nortel Networks Enterprise S2100 softswitch solution and the legacy SL-100 delivers the IPCLIENT line option. This option distinguishes lines with actual M5216 phones from IPCM lines that have the UNIStim phones. IPCM lines are provisioned using the M5216 Line Class Code (LCC). Currently, there is no indication of a line being an IPCM line in the core (such as in a QLEN or QDN output). The option is provisioned using Servord, and lines assigned the IPCLIENT option indicates that they are IPCM lines.

The IPCLIENT option may be assigned or removed from a line using the following Servord commands: NEW, NEWACD, ADO, EST, ADD, DEO. It is supported in the COPYSET, CKLN, and CHF commands.

An end-user has the capability to “hot-desk” from IPCM phone to IPCM phone. However, hot-desking may not be all that frequent, and there may be a phone that is the end-user’s primary phone. Therefore, when IPCLIENT is entered as an option, the provisioner is prompted for the primary set type. The available selections will be

- I2001
- I2002
- I2004
- SOFTCLIENT
- OTHER

Lines assigned the IPCLIENT option will be indicated as IP Clients in the output of query commands such as QLEN, QDN, QLENWRK, QDNWRK, and QCUST.

The count of M5216 lines with the IPCLIENT option assigned will appear in the COUNTALL OPT output. For DMSMON and ALMSTAT line output and COUNTALL output by LCC, IPCM lines will continue to be counted as M5216 lines.

Pre-requisites

This service is offered through the SN07 CHS load. The following information summarizes upgrade activities for CHS in SN07.

- All SN06.1 solutions must be upgraded to SN06.2 before going to SN07.
- CHS will not support upgrades from SN06.1 to SN07.
- CHS is configured to interwork with other non-CHS solution. For example, other non-CHS solutions could be upgraded to SN07 and then have additional equipment configured on them such as the CICM or H.323 devices, which would then make use of CHS capabilities.

Upgrade document

Refer to the following NTP for upgrade information and procedures: **IP Solution Upgrades Vol. 1 of 2**, NN10344-450 v1.

SIP on SP2000

Overview

The Succession Communication Server 2000 Session Server Manager (SCS 2000) SIP gateway application delivers an RFC 3261 compliant interface for the CS 2000 that enables open operability with call servers, application servers, and proxy servers using Session Initiation Protocol (SIP).

Reference documentation

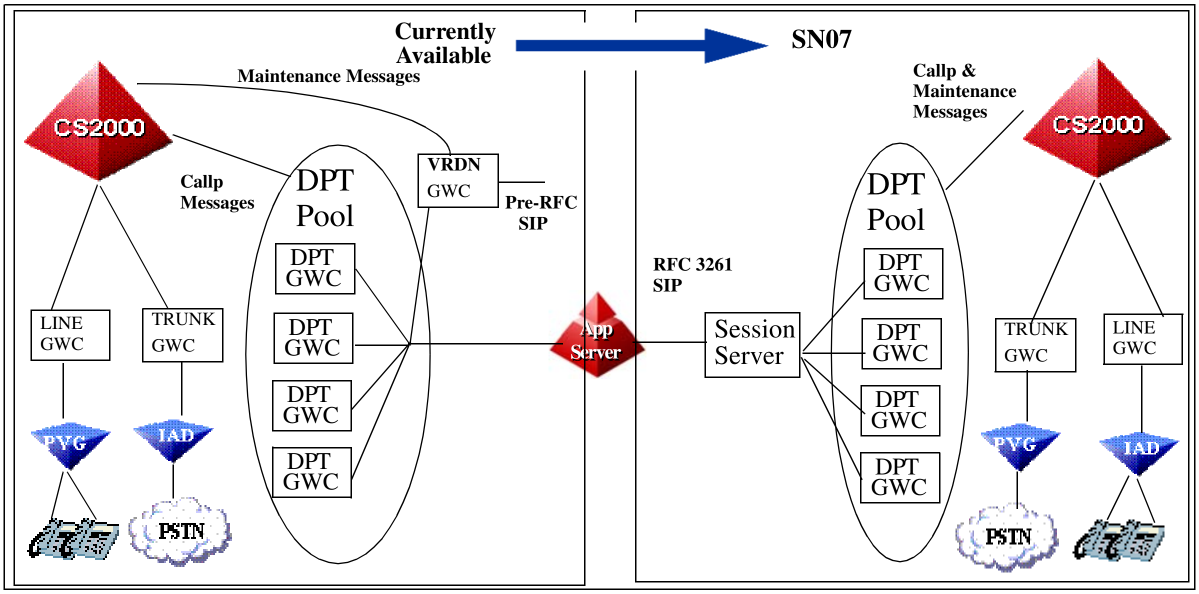
For configuration information, refer to the following procedure in the document: **NA PT-IP Basics,** NN10300-100

Nortel Carrier Grade Linux (NCGL) platform Session Server

Overview

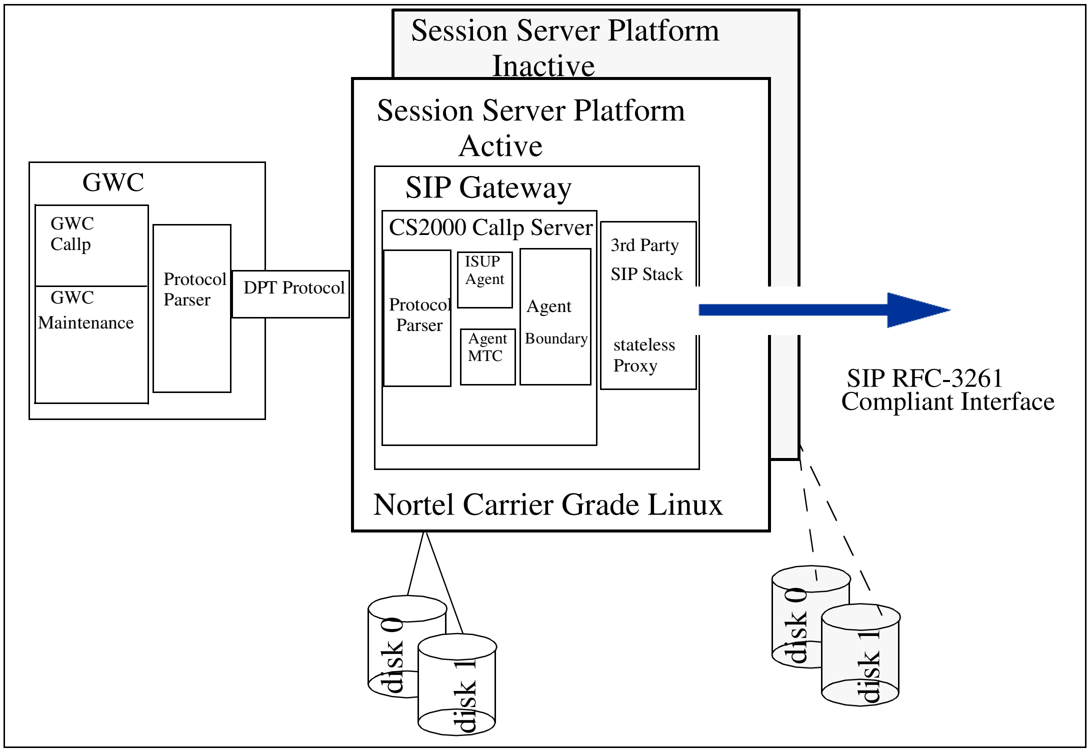
The purpose of this design is to create a highly available base platform for delivery of multiple applications. The Session Server consists of a Network Equipment-Building System (NEBS) Level 3 compliant hardware platform plus a software framework and architecture for developing Carrier Grade applications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

Design intent of Session Server platform



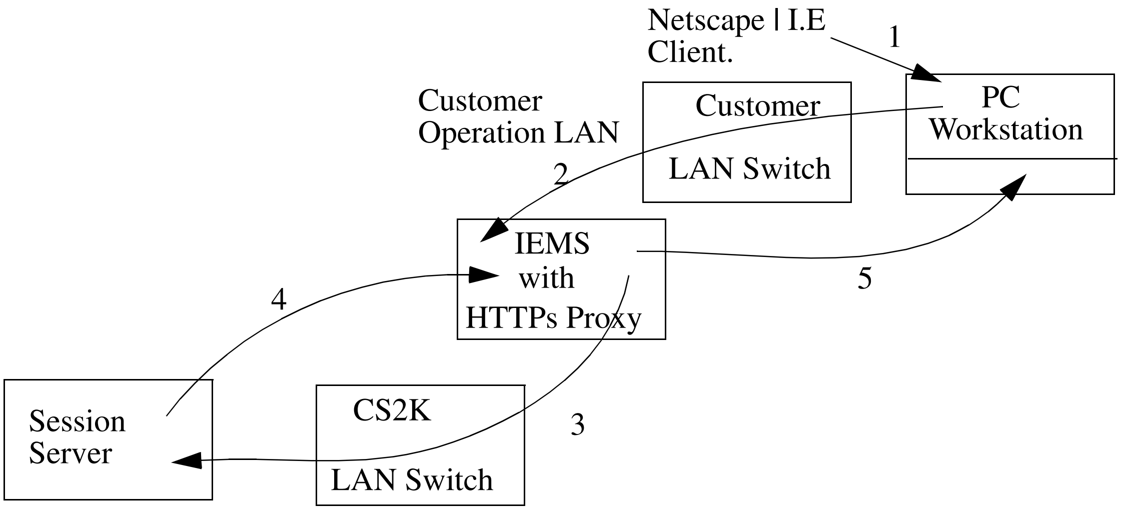
In the SN07 release, the architecture for the Session Server will consist of a mated pair of Services Application Module- eXtreme Thin Server (SAM-XTS) with a configuration similar to that of gateway controller. The units consists of an active and inactive unit. Each unit is in reality a fully functional Session Server that is interconnected via a gigabit ethernet LAN as shown in “Mated pair Session Server” on page 154. Each server provides processor capacity, local disk storage, and high-bandwidth network connectivity.

Mated pair Session Server



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

Configure Session Server with IEMS



An overview of the configuration steps include:

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

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

Session Server documents

For more information about

For more information about the Session Server, refer to the following documents located in the CHS Solution collection in Helmsman Express: “Session Server” on page 216

RTP Media Portal service

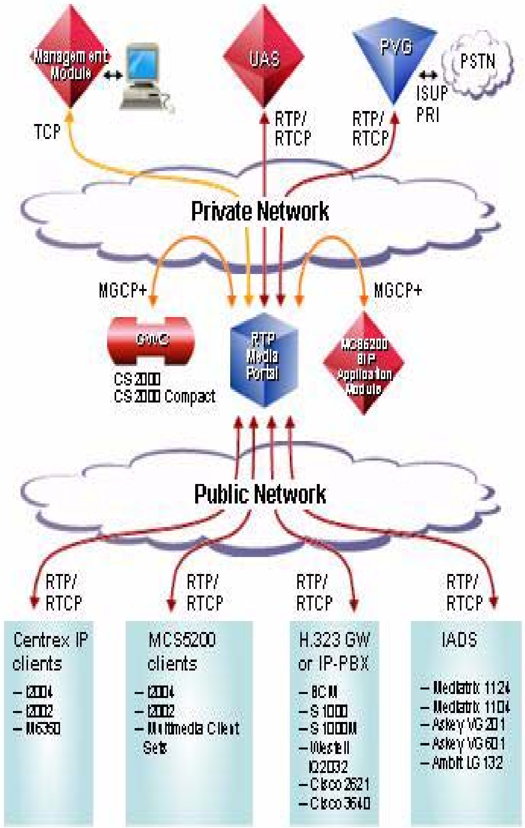
Overview

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

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

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

RTP Media Portal network interoperability



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

A call control signaling channel is established between the H.323 gateway and the CS 2000. If the GW and the CS 2000 reside in separate IP-VPNs (different IP address domains that cannot route directly to one another), dynamic discovery and keepalive are supported on the gateways and GWCs to provide another mechanism for GW->CS2K communication. Discovery provides another mechanism for GW->CS2K communication.

Pre-requisites

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.

Reference document

RTP Portal information:

- For more information on the MCS RTP Media Portal when in association with a CS 2000 refer to the following document located in the Multimedia Communication Portfolio collection in Helmsman Express. on page 217
- For more information on the RTP Media Portal, refer to the following document located in the Multimedia Communication Portfolio collection in Helmsman Express. on page 217
- For more information on the MCS 5200 documentation suite, refer to the Multimedia Communication Portfolio collection in Helmsman Express. on page 217

Call processing in Carrier Hosted Services

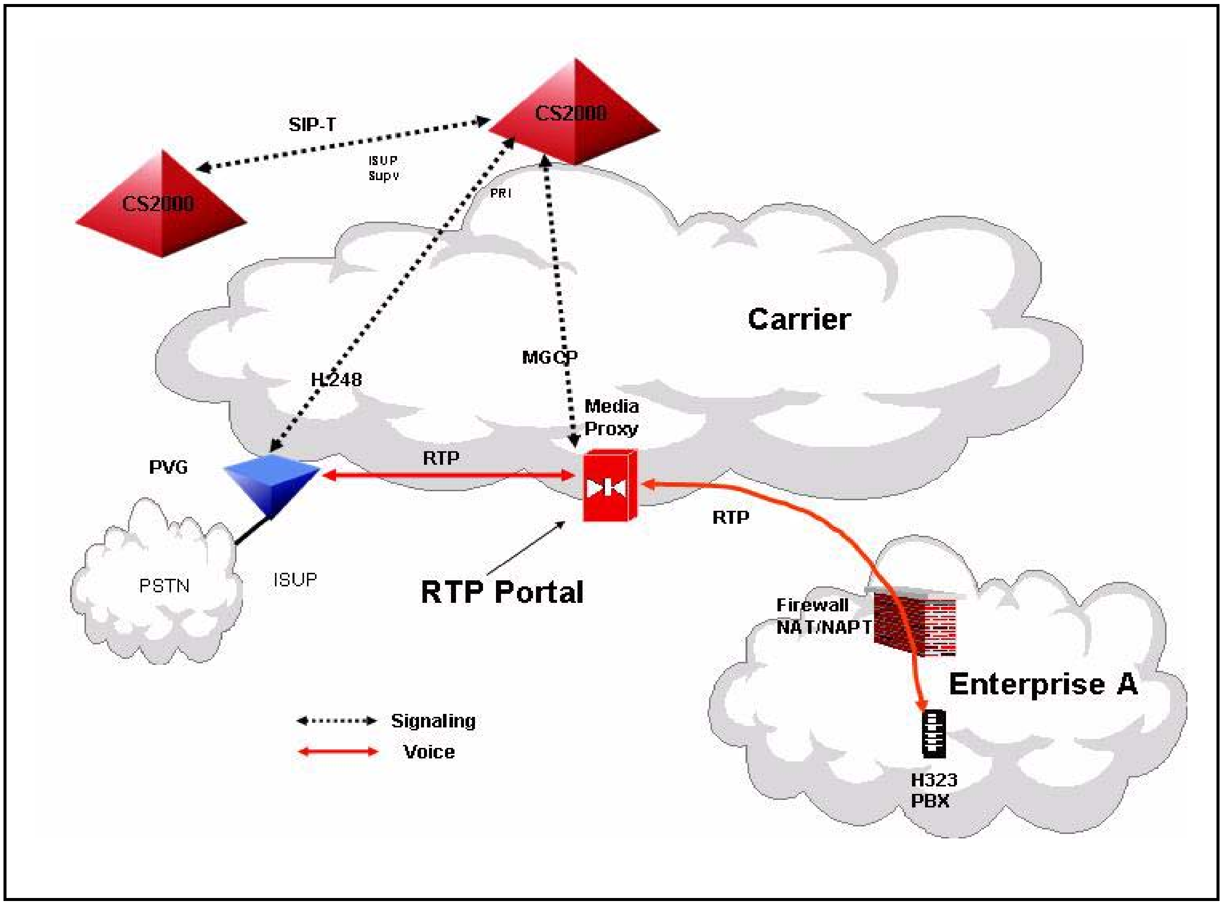
Overview

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

VoIP VPN

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

VoIP VPN call flow



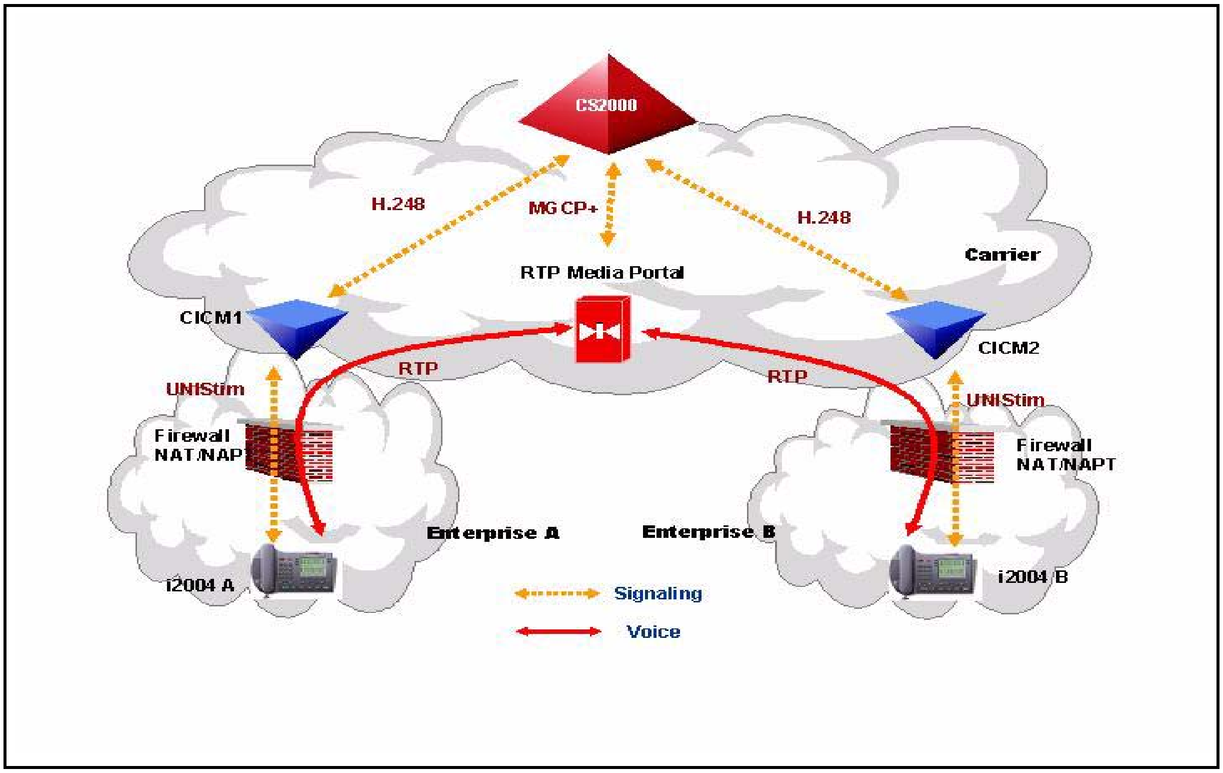
CICM

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

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

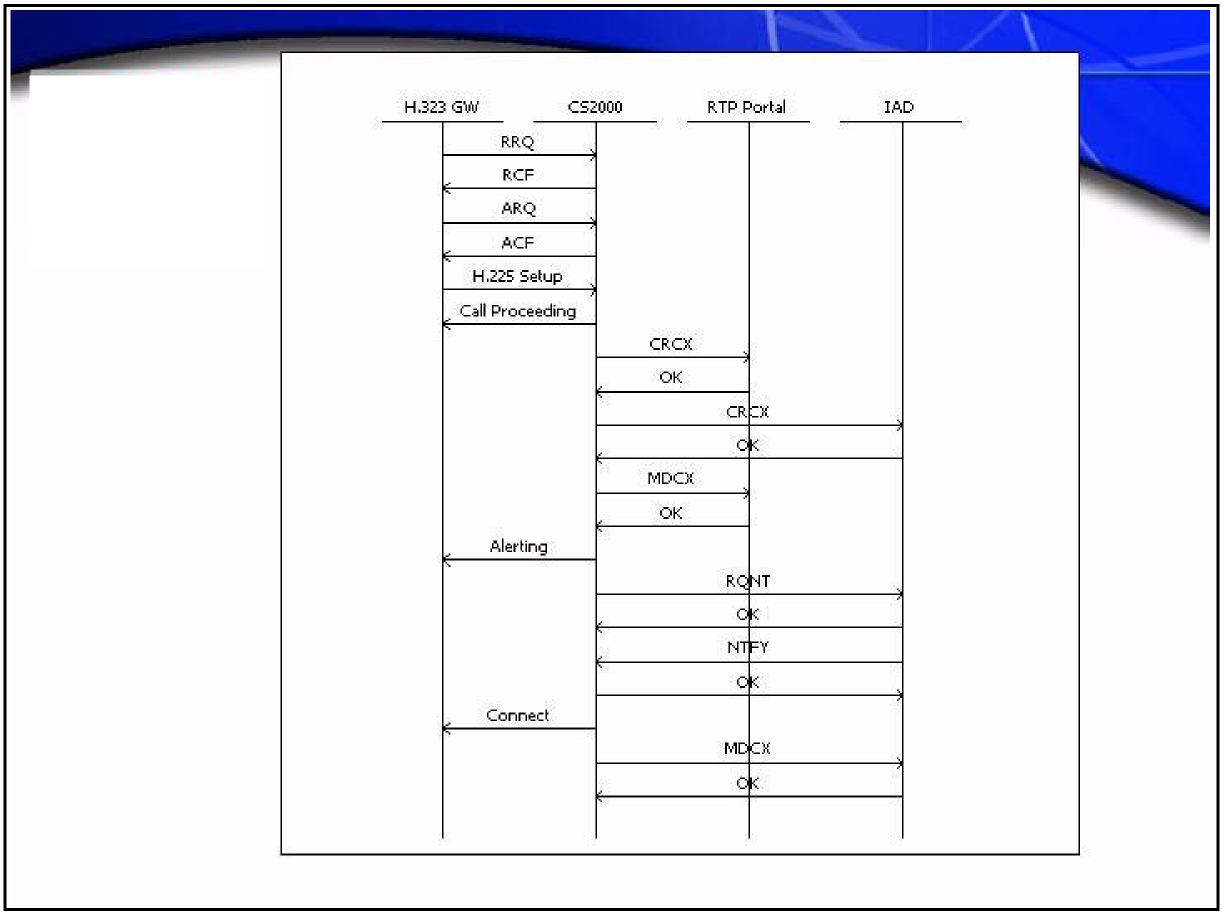
The following figure shows a call flow using Succession Centrex IP and the Succession CICM.

Succession Centrex IP call flow



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

VoIP VPN-to-MGCP IAD call setup



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

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

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

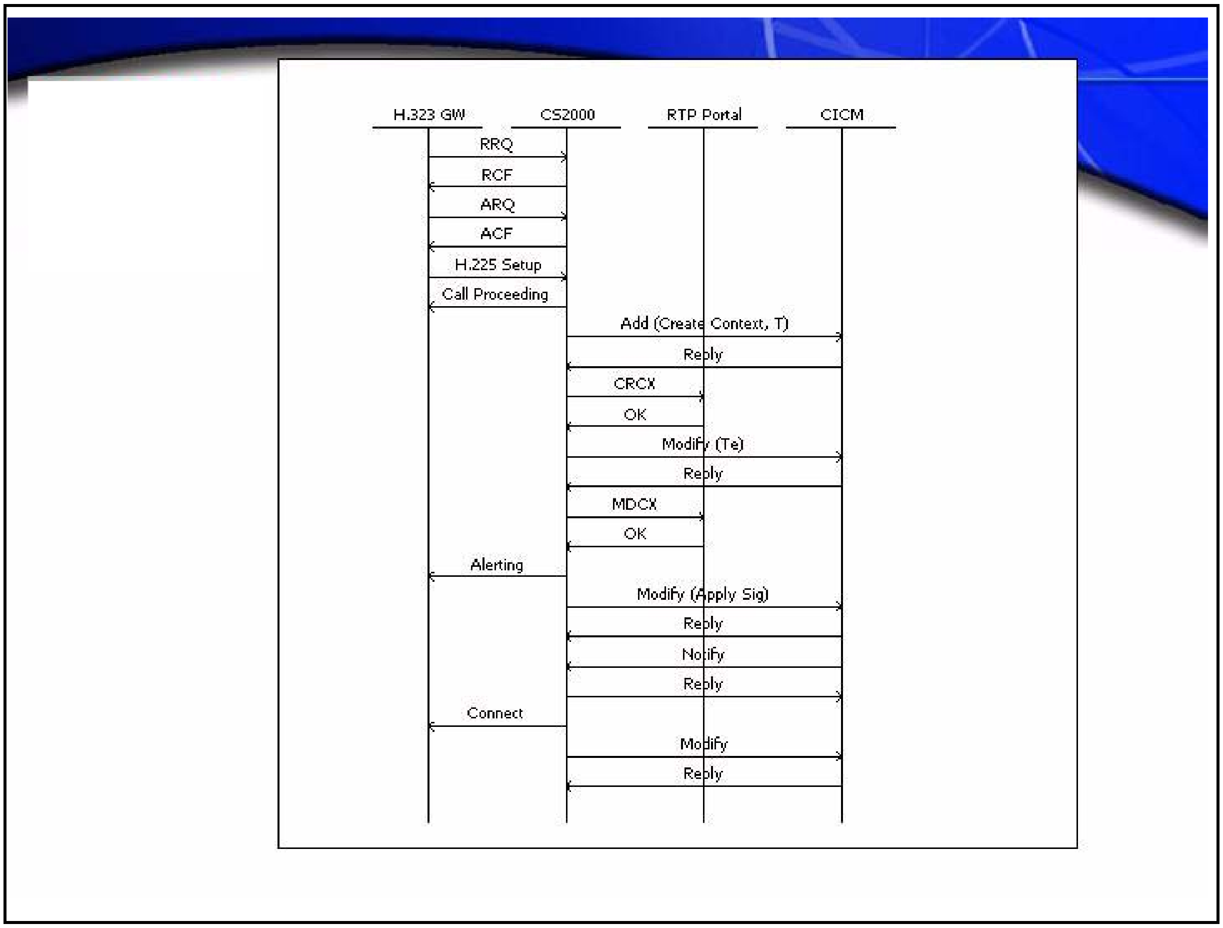
The communication server sends the Alerting message to the originating H.323 gateway, including the RTP port that should be used on the RTP Media Portal. The communication server then sends a Request Notification (RQNT) to the terminating IAD, directing it to apply ringing and provide notification when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

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

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

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

VoIP VPN-to-H.248 CICM call setup



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

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

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

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

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

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

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

Reference documentation

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

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

Centrex IP Call Manager

What's new?

For information about what's new in the current CICM release, refer to the suite of documentation listed in Where to get customer documentation on page 213

CICM

The CICM delivers Centrex capabilities to users connected to an IP network using VoIP technology on a PC SoftClient or an IP P-phone.

The CICM performs the following functions:

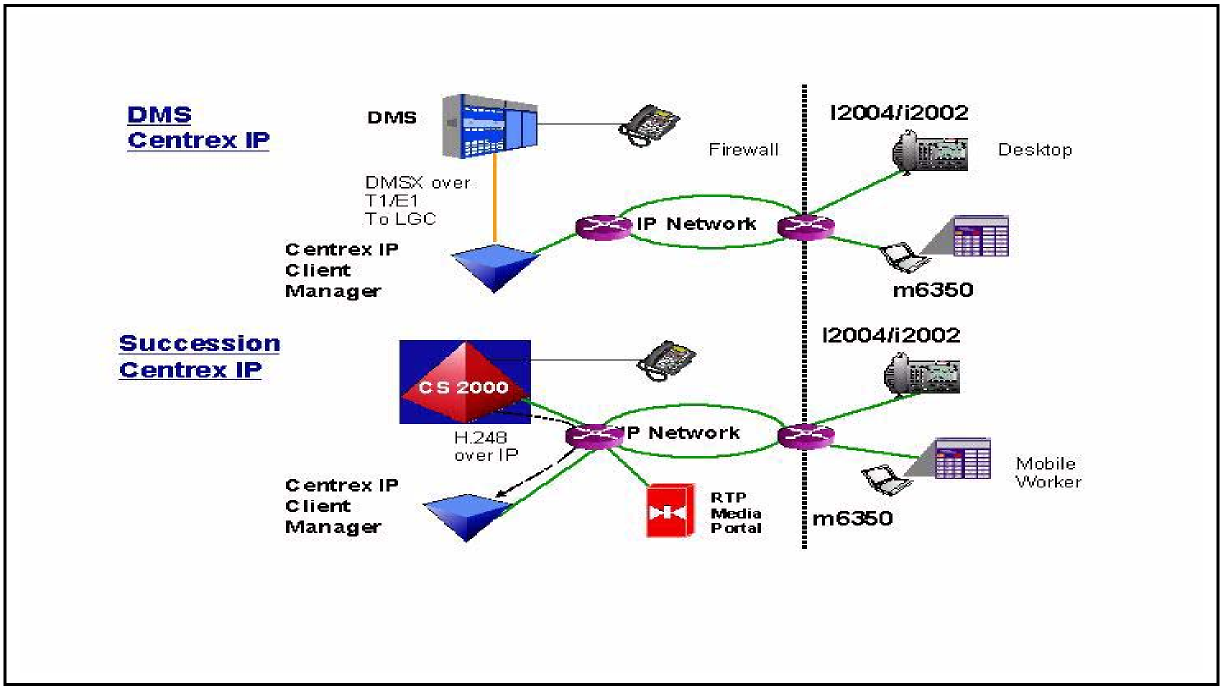
- provides the interface between the CS 2000 Centrex feature set and an IP network
- transcodes voice between IP data from the client network and pulse code modulation (PCM) data from the DMS/SL XMS-based peripheral module (XPM), or any of the following
  - — PCM-30 line group controller (PLGC), or
  - — line trunk controller (LTC)/line group controller (LGC)/remote cluster controller (RCC)

The Succession Centrex IP program uses Nortel Networks Succession product portfolio to provide transparent featured Centrex services over the converged IP/packet infrastructure.

> ***Note:*** In a carrier-hosted deployment, the Succession communication server can be either a CS 2000, which is based on the XA-Core hardware platform, or a CS 2000 - Compact, which is based on the third-party core (call agent) hardware platform.

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

Figure 0-1 Centrex IP architecture



The CICM connects to a PLGC using an E1 link for international customers. North American customers use a T1 link to connect the CICM to an LGC/ LTC/RCC.

The CICM acts as a “lights out” server. That is, it has no monitor, keyboard, or mouse. Once it is connected and powered up, all maintenance is performed remotely from a PC on the Administration LAN.

From a functional perspective, the CICM 7.0 gateway acts as a signaling proxy that converts Unified Network IP Stimulus (UNIStim) signaling and control messages between the CICM gateway and Centrex IP clients to H.248 messages for interface to the communication server. With the Succession CICM, the RTP media stream does not go through the CICM gateway.

In the SAM21-based CICM 7.0, the CICM-EM becomes a pair of Motorola CPN5385 resource cards, one active and the other hot stand-by, providing 1+1 redundancy. Only one pair of the CICM-EM resource cards is required per CS 2000, capable of supporting up to 100 pairs of the CICM resource cards. The hot stand-by CICM-EM resource card is equivalent to the Secondary Element Manager (SEM) chassis in the SAM16-based CICM releases.

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

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

Optionally, a redundant pair of EMs can be deployed – one primary and another secondary EM – for loadsharing. Each EM is located in a different central office (CO) for diversity. One EM processor board has two 10/100 BaseT ports.

The Centrex IP clients allow end users to initiate and receive VoIP calls, and receive Centrex features from a Succession communication server. Centrex IP supports the following clients:

- i200x (either an i2002 or i2004) Etherset, which connects directly to a LAN through built-in integrated three-port Internet Telephony Switch Module
- m6350 SoftClient, which is an IP telephony software client installed on a PC attached to a LAN. The SoftClient requires a headset and adaptor that plugs into a universal serial bus (USB) port on the PC.

> ***Note:*** Centrex IP clients are also called clients, terminals, or client terminals.

Shelf configuration

The CICM performs as a terminal server or a signaling gateway.

CICM and the CICM element manager reside on blades in the SAM 21 chassis, which reduces the footprint and cost of CICM.

- CICM resides on a pair of Motorola 5385 processors. A single pair of processors can support 3200 CICM end users.
- CICM EM resides on a single processor

The SAM21 CICM/GWC chassis can be housed on one of the two PI tested, NEBS-2 compliant frames: the SAM21 frame (SAMF) and the Call Control Frame (CCF). One SAMF frame may house (a) (b)

- up to three SAM21 CICM/GWC chassis; or
- up to two SAM21 CICM/GWC chassis, plus up to six Media Server chassis (AudioCodes MS2010 IP chassis).

The CCF frame supports one of the following two configurations:

- up to two SAM21 CICM/GWC chassis, or
- up to two SAM21 CICM/GWC chassis, up to six MS2010 IP chassis, plus one STORM chassis for STORM storage systems.

Deployment

The Centrex IP program can be deployed in a Succession network and a legacy DMS network.

The legacy DMS Centrex IP program uses DMS-X protocol and existing time division multiplex (TDM)-based peripherals. The TDM CICM supports the following functions:

- allows terminals to access Centrex services hosted on the Communication Server
- acts as a bridge between the TDM switching network and the IP network

The Succession Centrex IP program supports Succession networks using H.248 protocol. The Succession CICM allows IP terminals to access Centrex services hosted on the communication server.

Dual node redundancy (DNR)

Pairs of CPU cards provide hardware redundancy for CICM applications. Dual node redundancy enables both nodes of the CICM gateway to process H.248 messages and behave in a master and slave capacity.

TDM CICM configuration

In a TDM CICM configuration, both halves of the peripheral operate in a full load sharing mode with the Core (DMS CM) communicating with both nodes equally. Each CICM node appears to the DMS switch as a remote line concentrating module (RLCM). One CICM virtual line concentrating module (VLCM) appears to the DMS switch as a complete RLCM.

A client initially can log on to either CICM node and receive service. With one unit busied, the DMS switch sends messages only to one side of the CICM.

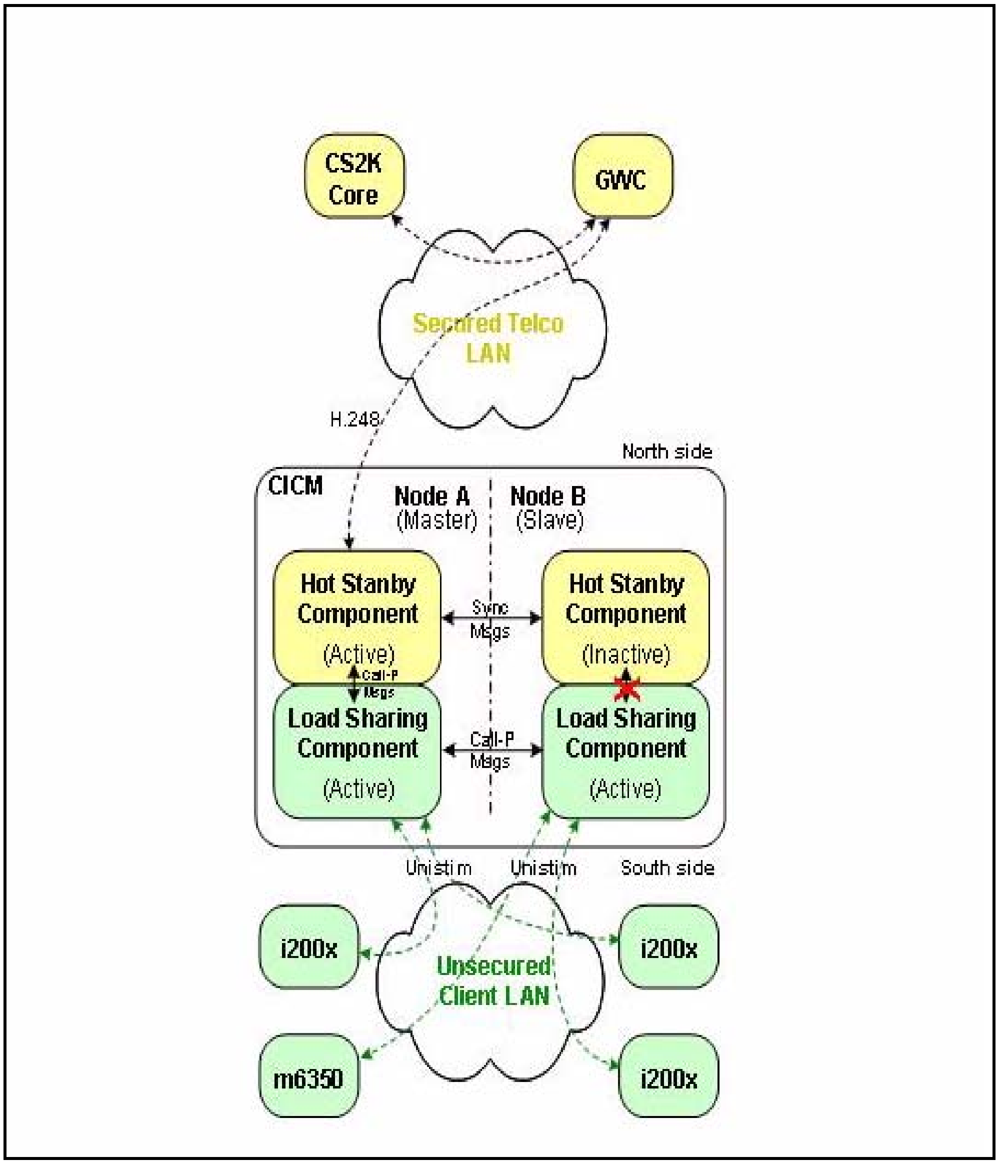
If one of the CICM nodes becomes unusable (due to a hardware failure or during an upgrade), the non-failing node can still provide service. When one node becomes unusable, all current calls on the failed node are dropped, and client could have to log in again to regain service.

Succession CICM

In a Succession CICM configuration, only one side of the peripheral can communicate with the Core (the CS 2000). Therefore, a master-slave relationship exists between the two nodes of the Succession CICM configuration.

The following figure shows how DNR can affect the software components that comprise CICM in a Succession configuration.

Figure 0-2 CICM DNR in Succession



Each CICM node (that is each half of the gateway) executes an identical software load. The gateway controller (GWC)-facing side (or north side) of the CICM operates in a hot standby mode. This component communicates with the GWC using H.248 over UDP/IP. As the GWC recognizes only one entity, it does not expect to communicate with another component. Therefore, only one half of the CICM can communicate with the GWC at any time (that is, the master node).

The inactive hot standby component must keep completely synchronized with the active side. (Note the double headed arrows in the previous figure connecting both hot standby components.) Total synchronization ensures that both nodes retain an accurate view of the state of call processing at a given time. Therefore, the inactive side can take control of these functions if needed.

The terminal-facing side (or south side) of the CICM operates in a load sharing mode. For this software component, each node hosts approximately half of the terminals connected to the CICM to balance the load.

> ***Note:*** In the previous figure, the Call-P arrows show the messaging path between the components in a standard call scenarios. Although both load sharing components host terminals, the message path ensures that all terminal events from either side are routed to the master hot standby component as only it communicates with the GWC.

Key aspects

The following list briefly describes the key aspects surrounding the DNR feature.

- In the TDM configuration, both nodes communicate equally with the PLGC (using DMS-X over TDM links). However, in the Succession configuration, only one node assumes the master role and communicates with the GWC.
- Only a single node, the master, can communicate with the CICM GWC at any time. (The CICM ensures that the IP and port are moved to the appropriate interface, as needed.)
- In a failure scenario on the active node, the CICM automatically initiates a switch of activity (SWACT) to maintain service.
- The CICM differentiates between failure scenarios in which a SWACT is required. For example, if a communication loss occurs with the GWC, the CICM only initiates a SWACT if it determines that the failure has occurred with the H.248 link or with an interface on the active node. The SWACT occurs only if such action is likely to resolve the loss of communication.
- All stable calls survive a SWACT.

  A stable call is a call that is in the “talking” state. In this state, CODEC negotiation has been completed and the voice path has been set up. No further action is required. No call processing feature is active in a stable call. (An idle terminal is also considered a stable call.)
- Unstable calls can survive a SWACT.
- Only one side of the CICM supports hot-swap takeovers. The other side of the CICM continues to operate in a load-sharing mode as

with the CICM TDM version. That is, even stable calls mainly hosted on the recently out-of-service master node can be lost in a failure scenario.

- A facility is available for the operator to determine which node is currently the active node.
- An operator can initiate a SWACT at any time. Once started, an operator-initiated SWACT cannot be canceled. A second SWACT must be initiated to return the system to its original pre-SWACT state.

Limitations and Restrictions

What's new?

The following limitations are included in the section (i)SN07 CS 2000 H.323 limitations and restrictions on page 175 and are new to both SN06.2 and (i)SN07:

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

(i)SN07 CS 2000 H.323 limitations and restrictions

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

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

  If the GW is behind the NAT, then the trunks must be Bsy/INB in order to change the capacity or IP address.

- The NAT dynamic mapping time-out in the router should be set high enough to keep those long duration calls active - where the user tries to invoke a feature after talking for a long period of time. (See Configuration notes on page 181.)
- DISA Services :
  - — For CS2K H.323, DISA DN hosted off of BCM is NOT supported.
  - — When a Carrier Based Line (CICM, MediaTrix, etc.) dials a DISA DN hosted on the CS2K, the DISA DN grants access to a Hosted IPPBX Enterprise (that is an S1000) without a work-around requirement of going over the ISUP loop-around first.
  - — DISA is NOT supported when a Carrier Based Line (CICM, MediaTrix, etc.) dials a DISA DN hosted on the S1000/S1000M/BCM.
  - — When an H.323 IPPBX Line (BCM, S1000, S1000M, etc.) dials a DISA DN hosted on the S1000/S1000M, DISA calls work without any work around.
  - — When an H.323 IPPBX Line (BCM, S1000, S1000M, etc.) dials a DISA DN hosted on the CS2K, the call should route to ISUP looparounds (on a Media Gateway 15000) before terminating to DISA.
- To preserve DPNSS VPN network capabilities, calls between the Westell LIQ 2032/2016 GW DPNSS trunks and other agents (line or Media Gateway 15000) must be routed through SIP-T IBN7(DFT) loop-around trunks to preserve DPNSS VPN network capabilities. Also trunks and lines should be in the same network (i.e. the customer groups of the line and trunk have the same NETNAME value) and the CLID option for the line’s customer group are set to ONNET to get a CLI display for all VPN calls (or OFFNET if you want CLI display for all calls).
- Currently, the CS2K H.323 system uses H.450 for DPNSS tunneling only and does not support any H.450 based supplementary features.
- The TCP keepalive is disabled by default to prevent the active calls after the warm swact from dropping (except when the call involves Cisco 2600 and 3620 GW, in which case the call drops after the warm swact).
- Inter-working between H.323 and the IW SPM is not supported. A loop-around trunk should be used instead.
- Slow start calls are supported with G.711 only.

- The CNDB (Calling Number Delivery Blocking) and CNNB (Calling Name and Number Delivery Blocking) features work with the following datafill.

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

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

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

H.323 Gateway limitations and restrictions

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

- For the calls terminating on the S1000M1 and S1000, the NET_RINGBACK_ON option must be provisioned in the TABLE LTDATA for all S1000M1 and S1000 trunk CLLIs in order to get the audiable ringback tone during the Call Setup (at the time of ALERTing).
- The BCM GW does not support SlowStart signaling on origination.
- The CS2K H323 System currently interoperates with Cisco's H323 IOS- version 12.2(24) 2600 and 3620 GWs; however, there are a number of restrictions to be addressed in a future load release from Cisco:
  - — Cisco calls are terminated by the GW 1 minute after a GWC warm SWACT.
  - — Cisco 2600 and 3620 GWs must be configured in a 1:1 static bind NAT configuration
  - — For call scenarios where the 2600 or 3620 Cisco GW is to connect to the UAS (in SN06.2) and the UAS/AMS [in (i)SN07],

and the Media Portal is present in the call topology due to NAT/FW traversal, the Cisco GW must be configured to transmit/receive immediately from the Cisco configuration level: `voice rtp send-recv`to

- For Core Cold and Reload restarts and for GWC Cold SWACT, H.323 calls may not get dropped in the H.323 GWs and will be dropped in the Core. The audit system in the CS2K will clear such calls.
- After a warm SWACT on the GWC, any attempted tcp messaging caused by a feature activation or dtmf key press (if it is conveyed by out of bandmsgs) will cause a warm swacted call to drop.
- The following are a few features that are not currently supported on the CS2K H.323 IPPBX.
  - Executive Busy Override (EBO)
  - Automatic Call Back (ACB); however, Network Ring Again is supported for calls within the same customer group.
  - Release Link Trunk (RLT)
  - Malicious Call Hold (MCH); however, MCH is supported on the Carrier Based Lines (CICM, MediaTrix, etc).
  - Network ACD
- Codec Provisioning: If an H.323 GW can support both G.711 and G.729, then G.711 should be provisioned as a defualt codec and G.729 should be provisioned as a preferred codec. No GW should be configured as having only a G.729 codec. Configure BCM3.5 to have no preferred codec and to have G711 as the default codec. For the BCM3.5 Unified Manager, there is a need to set G711 as the default codec for the Nortel IP terminal. Configure BCM 3.6 gateways to have G.711 as default and G.729 preferred.
- H.323 calls with only a Symmetric codec and ptime are supported (the H.323 GW must receive what is sent; that is, if a GW sends G711, then the H.323 GW must receive G711; if a GW sends 20ms, then the GW must receive 20ms).
- M1 Conference Keys only work after the conference party answers the call.
- H.323 GWs do not send any packets till the CONNECT. So we need to change to the loss timer on the Media Gateway 15000 to 0 - see the third bullet of the Configuration notes on page 181.

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

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

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

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

H.323 Protocol limitations

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

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

These scenarios include:

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

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

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

Configuration notes

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

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

  Examples include:

  — ISDN 13 SERV

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

  — ISDN 14 SERV

  — SERV Y Y ALWAYS ALWAYS (NET_RINGBACK_ON) (PRI_IP_PROT H323) $
- The Media proxy (RTP Portal) must be associated in CS 2000 Mgmt. Server -> GWC# ->Provisioning -> Media Proxies -> for those GWCs that have at least one GW behind the NAT.
- Most of the H.323 GWs do not send any packets till the CONNECT. So we need to change the loss timer on the Media Gateway 15000 (PVG) to 0.

Procedure 0-1 Changing the loss timer on the Media Gateway

15000 to zero

at the command line te

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

2 **St prov**

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

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

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

6 **act prov**

7 **confirm prov**

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

  Examples include:

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

  — 10.19.199.195(NAT Router IPAddress):7001(port on the NAT router)<-> 10.88.88.55(H.323 GW IP address):1720(Call Sig. port on the GW)
- For gateways such as Cisco GWs that do not provide a static RAS port, N:1 addressing is not an option as mapping the port must be done dynamically. This is a NAT 1:1 configuration and is supported by giving port 0 in the CS 2000 Mgmt. Server for the Cisco GW.
- If a H323 gateway in the International market does not support overlap signaling for termination, then the translation in the core should be set to do en-bloc signaling by using the TABLE PXCODE and minmax mm option to control for the en-bloc sending.

- The “INTER DOMAIN" bool is in the TABLE TRKOPTS for the SIP-T Trunks should be set as follows
  - "INTER DOMAIN" bool should be set to Y (that is, inter-domain) for all SIP-T trunks except loop-around trunks.
  - "INTER DOMAIN" bool should be set to N (that is, intra-domain) for SIP-T loop-around trunks.
- Do not enable e.164 registration in the H.323 GW as this kind of registration is not supported by GWC.
- For NATs with per-protocol time-outs, the recommended timer values are
  - For TCP (for Call Signaling), a bind time-out of 35 minutes.
  - For UDP (for RAS), a bind time-out of 3 minutes.

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

Features and services

Overview

This section lists the services that CHS support.

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

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

CICM supported services

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

CICM supported services

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

CICM supported services

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

CICM supported services

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

CICM supported services

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

CICM supported services

Option	Service	i2004	i2002	m6350 SoftClient
DRCW	Distinctive Ringing/Call Waiting			
DRING	Distinctive Ringing	x	x	x
DTM	Denied Termination	x	x	x
E911	Emergency Services (interaction support)	x	x	x
EBO	Executive Busy Override	x	x	x
EBX	Executive Busy Override Exempt	x	x	x
ELN	Essential Line	x	x	x
Int’l Emergency Call	International Emergency Call Routing	x	x	x
EMW	Executive Message Waiting	x	x	x
EXT	Extensiopossible Issued-On	x	x	x
FCTDINT	Full Carrier Toll Deny for International Carriers	x	x	x
FCTDNTER	InterLATA Full Carrier Toll Denied	x	x	x
FCTDNTRA	IntraLATA Full Carrier Toll Denied	x	x	x
FGA	Feature Group A	x	x	x
FNT	Free Number Terminating	x	x	x
FTRGRP	Feature Group	x	x	x
FTRKEYS	Feature Keys	x	x	x
FXR	Fast Transfer	x	x	x
ICSDEACT	In Call Service Deactivation	x	x	x
IECFB	Internal/External Call Forwarding Busy	x	x	x

CICM supported services

Option	Service	i2004	i2002	m6350 SoftClient
IECFD	Internal/External Call Forwarding Do Not Answer	x	x	x
ILB	Inhibit Line Busy	x	x	x
IN (CS-X)	Intelligent Networks (CS-X)	x	x	x
INSPECT	Inspect Key	x	x	x
INTPIC	International Primary Carrier	x	x	x
IRR	Inhibit Ring Reminder	x	x	x
JOIN	Conference Join	x	x	x
KSH	Key Short Hunt	x	x	x
KSMOH	Key Set Music on Hold	x	x	x
LCDR	Local Call Detail Recording	x	x	x
LI	Lawful Intercept	x	x	x
LMOH	Line Music on Hold	x	x	x
LNP	Local Number Portability (LRN based)	x	x	x
LNR	Last Number Redial	x	x	x
LNRA	Last Number Redial Associated with Set	x	x	x
LOD	Line Overflow to DN	x	x	x
LOR	Line Overflow to Route	x	x	x
LPIC	IntraLATA PIC	x	x	x
LVM	Leave Message	x	x	x
MBK	Make Busy Key	x	x	x
MBSCAMP	Meridian Business Set Station Camp-On	x	x	x

CICM supported services

Option	Service	i2004	i2002	m6350 SoftClient
MCH	Malicious Call Hold	x	x	x
MDN MCA	Multiple Appearance Directory Number (MADN) Multiple Call Arrangement	x	x	x
MDN SCA	MADN Single Call Arrangement	x	x	x
MDNNAME	MADN Member Name	x	x	x
MEETME	Meet Me Conference	x	x	x
MEMDISP	MADN Member Display	x	x	x
MLAMP	MADN Lamp	x	x	x
MLH	Multi-line Hunt	x	x	x
MREL	MADN Release	x	x	x
MRF	MADN Ring Forwarding	x	x	x
MRFM	MADN Ring Forwarding Manual	x	x	x
MSB	Make Set Busy	x	x	x
MSBI	Make Set Busy Intragroup	x	x	x
MWIDC	Message Waiting Indication	x	x	x
MWINK	MADN Message Waiting Indicator	x	x	x
MWQRY	Message Waiting Query	x	x	x
MWT	Message Waiting	x	x	x
NAME	Name Display	x	x	x
NOH	No Receiver Off-Hook Tone	x	x	x
OLS	Originating Line Select	x	x	x
ONI	Operator Number Identification	x	x	x
OP	Operator Services Access	x	x	x

CICM supported services

Option	Service	i2004	i2002	m6350 SoftClient
PBL	Private Business Line	x	x	x
PCWT	Precedence Call Waiting Termination	x	x	x
PDO	Prevent Delete Option	x	x	x
PF	Power Features	x	x	x
PIC	Primary InterLATA Carrier	x	x	x
PILOT	Pilot DN Billing	x	x	x
PLP	Plug-up (Trouble Intercept)	x	x	x
PORT	10-digit unconditional LNP trigger	x	x	x
PPL	PVN Priority Line	x	x	x
PREMTBL	Call Pre-emption	x	x	x
PRESET CONF	Preset Conference	x	x	x
PRH	Preferential Hunting	x	x	x
PPK	Call Park	x	x	x
PRL	Privacy Release	x	x	x
PRV	Privacy for MADN	x	x	x
QBS	Query Busy Station	x	x	x
QCK	Quick Conference Key	x	x	x
QTD	Query Time and Date	x	x	x
RAG	Ring Again	x	x	x
RCF/RCFEA	Remote Call Forwarding (Access to)	x	x	x
RCVD	Received Digits Billing	x	x	x

CICM supported services

Option	Service	i2004	i2002	m6350 SoftClient
REASDSP	Reason Display	x	x	x
RPA	Repeated Alert	x	x	x
RSP	Restricted Sent Paid	x	x	x
RSUS	Requested Suspension	x	x	x
SACB	Subscriber Activated Call Blocking	x	x	x
SBLF	Set Based Lamp Field	x	x	x
SCA	Selective Call Acceptance	x	x	x
SCF	Selective Call Forwarding	x	x	x
SCL	Speed Calling Long	x	x	x
SCMP	Series Completion	x	x	x
SCRJ	Selective Call Rejection	x	x	x
SCS	Speed Calling Short	x	x	x
SCU	Speed Calling User	x	x	x
SDSDENY	Special Delivery Service Deny	x	x	x
SDY	Line Study	x	x	x
SEC	Security	x	x	x
SETMODEL	Set Model	x	x	x
SIMRING	Simultaneous Ringing	x	x	x
SL	Secondary Language	x	x	x
SLQ	Single Line Queuing	x	x	x
SLU	Subscriber LIne Usage	x	x	x
SMDI	Simplified Message Desk Interface	x	x	x

CICM supported services

Option	Service	i2004	i2002	m6350 SoftClient
SMDR	Station Message Detail Recording	x	x	x
SOR	Station Origination Restriction	x	x	x
SORC	Station Origination Restrictions Controller	x	x	x
SPB	Special Billing	x	x	x
SPR	Selective Suppression of MDCR/SMDR	x	x	x
SSAC	Station Specific Authorization Codes	x	x	x
SUPPRESS	Suppress Line Identification Information	x	x	x
SUS	Suspended Service	x	x	x
SVCGRP	Service Group	x	x	x
TBO	Terminating Billing Option	x	x	x
TERM	Terminating DN Billing	x	x	x
TES	Toll Essential	x	x	x
TFO	Terminating Fault Option	x	x	x
TLS	Terminating Line Select	x	x	x
TollFree	Toll Free Services	x	x	x
UCD	Uniform Call Distribution	x	x	x
UCDLG	Uniform Call Distribution Login	x	x	x
WML	Warm Line	x	x	x
WUCR	Wake Up Call Ring Timeout	x	x	x

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

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

Service	H.323 Access	Media Gateway 15000 PRI Access	Media Gateway 1500 ISUP Access	DPT Access
AIN SE R5 - International PFX	x	x	x	x
AIN SE R5 - OperSvcs PFX	x	x	x	x
Alternate 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
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

Service	H.323 Access	Media Gateway 15000 PRI Access	Media Gateway 1500 ISUP Access	DPT Access
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 C7ISUPIerLta Conn AT	x	x	x	x
EQA ISUP Intermed. Tandem	x	x	x	x
EQA Intermediate Tandem	x	x	x	x
EQA Tandem AMA Control	x	x	x	x
Expensive Route Warning	x	x	x	x
Forced On-net	x	x	x	x
Government Emergency Telephony System (GETS)	x	x	x	x
Head-end Break-in	x	x	x	x
IDDD via ARS	x	x	x	x

Service	H.323 Access	Media Gateway 15000 PRI Access	Media Gateway 1500 ISUP Access	DPT Access
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
MCDN Interworked services (interworked to CS2K-based Centrex lines)				
Network Class of Service (NCOS)	x	x	x	x
Calling Number Delivery	x	x	x	x
Connected Number Delivery	x	x	x	x
Called Number Delivery	x	x	x	x
Network Name Delivery (NND)	x	x	x	x
Calling Party Name Delivery	x	x	x	x
Connected Party Name Delivery	x	x	x	x

Service	H.323 Access	Media Gateway 15000 PRI Access	Media Gateway 1500 ISUP Access	DPT Access
Original Called Party Name Delivery	x	x	x	x
Called Party Name Delivery	x	x	x	x
Redirecting Party Name Delivery	x	x	x	x
Redirection Party Name Delivery	x	x	x	x
Network Call Redirection	x	x	x	x
Call Forwarding	x	x	x	x
Call Transfer	x	x	x	x
Call Pickup	x	x	x	x
Network Wide Ring Again (RAG)	x	x	x	x
Network Speed Calling	x	x	x	x
Network Authorization Code	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 (ARS)	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

Service	H.323 Access	Media Gateway 15000 PRI Access	Media Gateway 1500 ISUP Access	DPT Access
NI0 Circular Hunt - NA	x	x		
NI0 Circular Hunt - NI	x	x		
NI0 ISDN Base	x	x		
NI0 ISDN PRI Base	x	x		
NI0 ISDN PRI CNAM	x	x		
NI0 PRI Hotel/Motel	x	x		
NI0 PRI NI-1 Base	x	x		
NI0 PRI NI-2 Base	x	x		
NI0 E911 Scrn NI-2	x	x		
NI0 PRI Message Services	x	x		
NI0 Message Services SMDI Replacement	x	x		
NI0 CFW I/F Busy	x	x		
NI0 CFW I/F Busy NI-2	x	x		
OAM EADAS DC and HW Inv.	x	x	x	x
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

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

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

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

Service	BCM interworking to			
	CICM (nodal)	CICM (SIP-T)	Mediatrix (nodal)	Mediatrix (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		

Service	BCM interworking to			
	CICM (nodal)	CICM (SIP-T)	Mediatrix (nodal)	Mediatrix (SIP-T)
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

The following table lists the International services that are currently supported by H.323 for Nortel Networks Media Gateway 1000 interworking to CICM and Mediatrix GW for nodal calls and calls through SIP-T.

Service	BCM interworking to			
	CICM (nodal)	CICM (SIP-T)	Mediatrix (nodal)	Mediatrix (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

Service	BCM interworking to			
	CICM (nodal)	CICM (SIP-T)	Mediatrix (nodal)	Mediatrix (SIP-T)
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

Customer support

Overview

This section describes the range of services Nortel Networks offers:

Solution and customer support

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

Corrective action can include the following:

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

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

Customer information

Software release and support policy

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

Ordering and support overview

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

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

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

Software upgrade path overview

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

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

Optional support package overview

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

Standard software support policy

Components	Standard software support policy
Contivity 600	Software support is available for the last published software release and one release back (including their associated patches, fixes, and workarounds).
Passport 8600/Device Manager	Software support is available for the last published software release and one release back (including their associated patches, fixes and workarounds).
Nortel Networks Multiservice Switch (formerly Passport) 15000	Software releases are supported for 2 years (24 months) after declaration of General Availability (GA). This policy applies to PCR 3.0 and later software releases.
Nortel Networks Multiservice Data Manager (formerly Preside MDM)	Software releases are supported for 2 years (24 months) after declaration of GA. This policy applies to MDM 13.3 and later software releases.

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

Service bundling

Customers can purchase the following additional services:

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

- electronic software delivery
- mentoring services

Web site information

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

Customer responsibilities

The information in this section is intended for use by Nortel Networks Sales, Business and Development, and Marketing personnel who are responsible for ensuring that customers are aware of and agree with their responsibilities when discussing the solution. Additionally, these responsibilities must be written into any subsequent contracts which result from such discussions or negotiations.

This section includes the following:

- Hardware baseline
- Electronic software delivery requirements

Hardware baseline

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

Electronic software delivery requirements

Information on electronic software delivery (ESD) patches is included in the document *Upgrading the Succession Network*, NN10261450. Succession solution electronic software delivery requirements include:

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

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

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

- DMS and SPM software delivery

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

  There are two main ways to employ electronic software delivery.

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

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

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

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

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

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

The following table lists the approximate comparative download times for throughput over selected dedicated connection links. The customer must consider what transmission time is acceptable to their operations in order to determine the throughput requirements for their network.

Comparative transmission times for 100 Mbytes

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

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

In summary, requirements for electronic software delivery are:

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

Security requirements for DMS and SPM based-equipment software loads

Access from the Nortel Networks electronic software delivery server to a customer's server is over a switched circuit, and user identification and password provide security. To log in from the Nortel Networks electronic software delivery server to the customer LAN/WAN, the security algorithm is used. For Nortel Networks Multiservice Switch (formerly Passport 15000), and Nortel Networks Multiservice Data Manager (formerly Preside MDM) software loads, the Nortel Networks electronic software delivery system uses a secure-access system. The customer login ID and passwords are managed as part of the POL suite.

Training and documentation

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

Contacting Nortel Networks for help on customer information

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

Customer information

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

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

Legacy information

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

Where to get customer documentation

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

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

www.nortelnetworks.com

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

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

- CS 2000
- CS 2000 - Compact
- CS 2000 Management Tools
- Gateway Controller
- Nortel Networks Multiservice Switch 15000 and 20000 (formerly Passport)
- Notel Networks Multiservice Data Manager (formerly Preside MDM)
- Preside MSS
- UAS
- USP
- USP - Compact
- XA-Core

BCM

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

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

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

CS1000 and CS 1000M

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

CS 1000 / CS 1000M	Title
555-3001-000	Library Navigator (contains a description of all NTPs in the collection)
555-3001-213	IP Peer Networking
555-3001-363	IP Trunk: Description, Installation and Operation
553-3001-365	IP Line: Description, Installation and Operation
553-3031-258	Succession 1000 System: Upgrade Procedures

Meridian 1

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

MCS 5100

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

CICM documentation

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

CICM	Title
NN10027-111	CICM Series 2.5 Product and Technology Fundamentals
NN10027-113	CICM Series 2.5 Etherset Installation Guide and User Manual
NN10182-113	CICM Series 2.5 m6350 SoftClient Installation Guide
NN10183-114	CICM Series 2.4 m6350 SoftClient Branding Kit
972-5551-901	m6350 TAPI Service Provider Installation and Troubleshooting Guide
NN10234-100	CICM Basics

CICM	Title
NN10230-461	CICM Upgrades
NN10233-911	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

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

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

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

RTP Portal

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

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

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

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

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

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

MCS 5200 interworking

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

MCS interworking	Title
NN10033111	MCS 5200 Interworking

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

Where to get training information

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

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

Professional services

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

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

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

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

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

Operations support services

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

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

Routine TAS, S1 and S2

The service provides the following help for customers:

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

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

ETAS, E1 and E2

This service provides the following help for customers:

- Coverage 24 hours a day, 7 days a week
- Immediate assistance through telephone and/or remote access
- Diagnosis of cause and recommended actions to restore operational stability
- ETAS-initiated on-site assistance made necessary by emergency conditions and covered by the S&SP
- Customer-initiated on-side assistance, available through mutual agreement and dispatched within 4 hours of mutual agreement

Additional charges are billed for travel and per diem expense, plus the current hourly rate.

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

Escalation procedure

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

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