Carrier VoIP

Gateway Controller Basics

NN10189-111

Document status: Standard
Document version: 08.02
Document date: 20 October 2006

Contents

Gateway Controller Basics

New in this release

The following sections detail what’s new in *Gateway Controller Basics* (NN10189-111) for (I)SN09U:

- "Features" (page 5)
- "Other changes" (page 6)

Features

See the following sections for information about feature changes:

- "H323 RAS-less Provisioning (A00009576)" (page 5)
- "Flex Large Line GWC prof (Ph1) (A00013275)" (page 5)
- "Provisioning of 2 Port Voice Services Processor 4e for MG 15000 (A00013555)" (page 6)

H323 RAS-less Provisioning (A00009576)

This feature provides the option to configure H.323 gateways and gatekeepers with the RAS-less functionality (no registration, admission, and status [RAS] messages are exchanged between a gateway and a GWC). The option is configured when associating an H.323 gateway with a GWC.

This feature adds protocol port value information for gateways in RAS-less mode to table "Media gateway profiles and characteristics" (page 43).

Flex Large Line GWC prof (Ph1) (A00013275)

This feature provides support for large line gateways supporting up to 2047 endpoints within a single virtual media gateway. Two new media gateway profiles are added to the GWC Manager: AUDIOCODES_6310_LINE (for Media Gateway 3500 using TP-6310 card and configured as a large line gateway) and AUDIOCODES_6310_TRUNK (for Media Gateway 3500 using TP-6310 card and configured as a trunk carrier gateway).

> ***Note:*** AUDIOCODES_6310_LINE profile is not supported in (I)SN09U release.

This feature adds profile AUDIOCODES_6310_TRUNK to table "Media gateway profiles and characteristics" (page 43).

Provisioning of 2 Port Voice Services Processor 4e for MG 15000 (A00013555)

This feature introduces the media gateway profile PVG_VSP4E to support a new Nortel Media Gateway 15000 called 2 Port VSP4e. The new profile is added to table "Media gateway profiles and characteristics" (page 43).

Other changes

See the following sections for information about changes that are not feature related:

- "New media gateway profiles: KEYMILE_UMUX and AUDCDSMG32LN" (page 6)
- "AFC media gateway profile" (page 6)

New media gateway profiles: KEYMILE_UMUX and AUDCDSMG32LN

The new profiles added to table "Media gateway profiles and characteristics" (page 43).

AFC media gateway profile

The AFC media gateway profile was removed from the GWC Manager GUI. All references to the AFC profile removed from the GWC documentation suite.

PVG naming

The following table lists the names used for certain gateways in Carrier Voice over IP (VoIP) documentation prior to (I)SN07 and provides the new brand names starting in (I)SN07.

The CS 2000 GWC Manager does not reflect these branding changes in (I)SN09U. As a result, the GWC customer documentation does not reflect these changes, as well. This table is being provided to map the names used in GWC documentation to other Carrier VoIP documentation.

Pre-SN07 name	Brand name starting in SN07
Passport Packet Voice Gateway (PVG)	Nortel Media Gateway 7480 or 15000
PVG 7400 or PVG 7K	Nortel Media Gateway 7480
PVG 15000 or PVG 15K	Nortel Media Gateway 15000

Gateway Controller customer documentation

The Gateway Controller documentation suite consists of the following NTPs:

- *Gateway Controller Basics* (NN10189-111)
- *Gateway Controller Configuration Management* (NN10205-511)
- *Gateway Controller Fault Management* (NN10202-911)
- *Gateway Controller Performance Management* (NN10208-711)
- *Gateway Controller Security and Administration* (NN10213-611)

Functional description

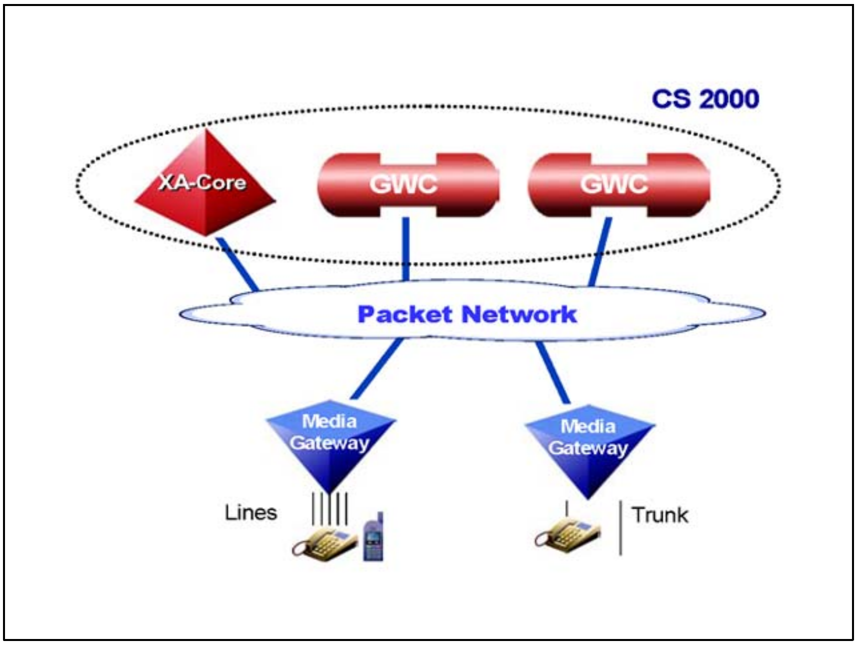
The Gateway Controller (GWC) is a network component in the Communication Server 2000 (CS 2000) and CS 2000 - Compact products. Its function is to manage and manipulate signaling and bearer paths on various types of media gateways. It receives instructions from the CS 2000 XA-Core or the Compact Call Agent (CCA) to perform various functions, such as: create or release a connection, collect in-band digits, and provide echo cancellation.

A GWC is commonly used to manage signaling and data paths or virtual connections between endpoints from one network component to another. A GWC mediates these virtual connections with other GWCs, inside or outside the network, through the internet or with local line or trunk access devices or other 3rd party peripherals. These devices are known as gateways or media gateways.

Role of the GWC in the network

The GWC inherits the role of the Extended Peripheral Module (XPM) from legacy DMS systems. That is, it interfaces between the call processing XA-Core or CCA and the line/trunk access devices, making the GWC appear to the XA-Core or CCA as an XPM.

Relationship of GWC to other CS 2000 network components



In a CS 2000 - Compact environment, the Compact Call Agent (CCA) provides the XA-Core functionality.

In a sense, the XA-Core or CCA views the GWC as another peripheral from a call processing, messaging, and control point of view. From a different perspective, media gateways and the XA-Core or CCA view the GWC as a media gateway controller (MGC). Therefore, the GWC connects the two views together providing:

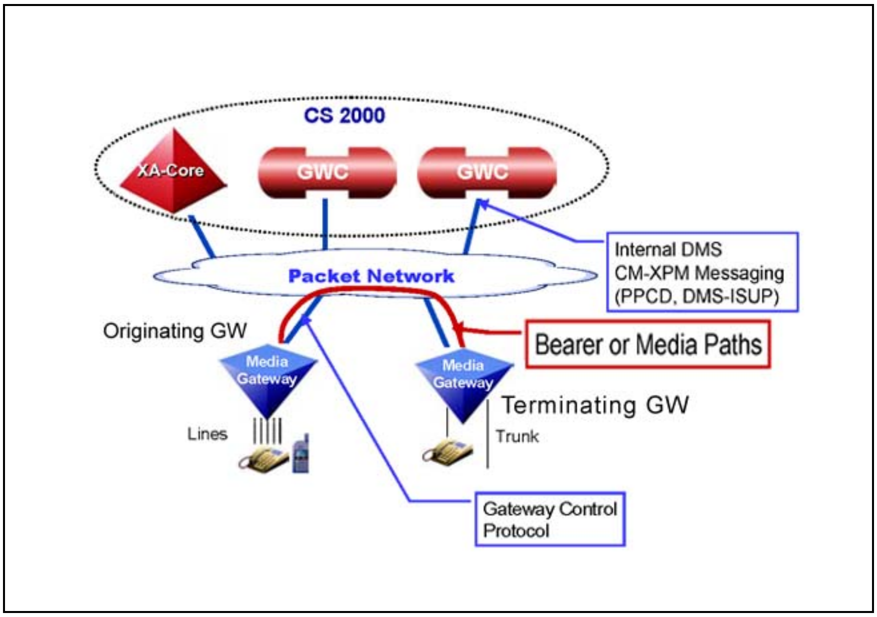
- inter-CS 2000 network calls using the Session Initiation Protocol for Telephony (SIP-T) messaging across the packet network to enable communication between CS 2000s
- intra-CS 2000 network calls using NCS, DSM-CC, MGCP, MEGACO/H.248, H.323 or TGCP signaling protocols to communicate with Nortel and third party gateways.

In order to perform its network role, a CS 2000 must be deployed with one or more media gateways for handling packet network bearer connections. A media gateway provides an interface for bearer connections to map a packet-based media stream onto a circuit-based media stream, seamlessly providing any required format conversion while maintaining content integrity. Depending on the telephony interface to be supported, a media gateway may also terminate legacy network signaling on one side and packet network signaling on the other. A gateway may also support signaling interpretation and conversion between the legacy network and the packet network.

Call flow and signaling in the GWC

The components of the CS 2000 use the packet network for signaling to each other and to the gateways. Because the components of the CS 2000 are connected through a packet network, they can be located close together at a single site or room, or spread far apart in distant locations. In an internet protocol (IP) network environment, the distance between network components is less of an issue than in a time division multiplexing (TDM) environment.

Call flow, signaling and messaging with the GWC



In a CS 2000 - Compact environment, the Compact Call Agent (CCA) provides the XA-Core functionality.

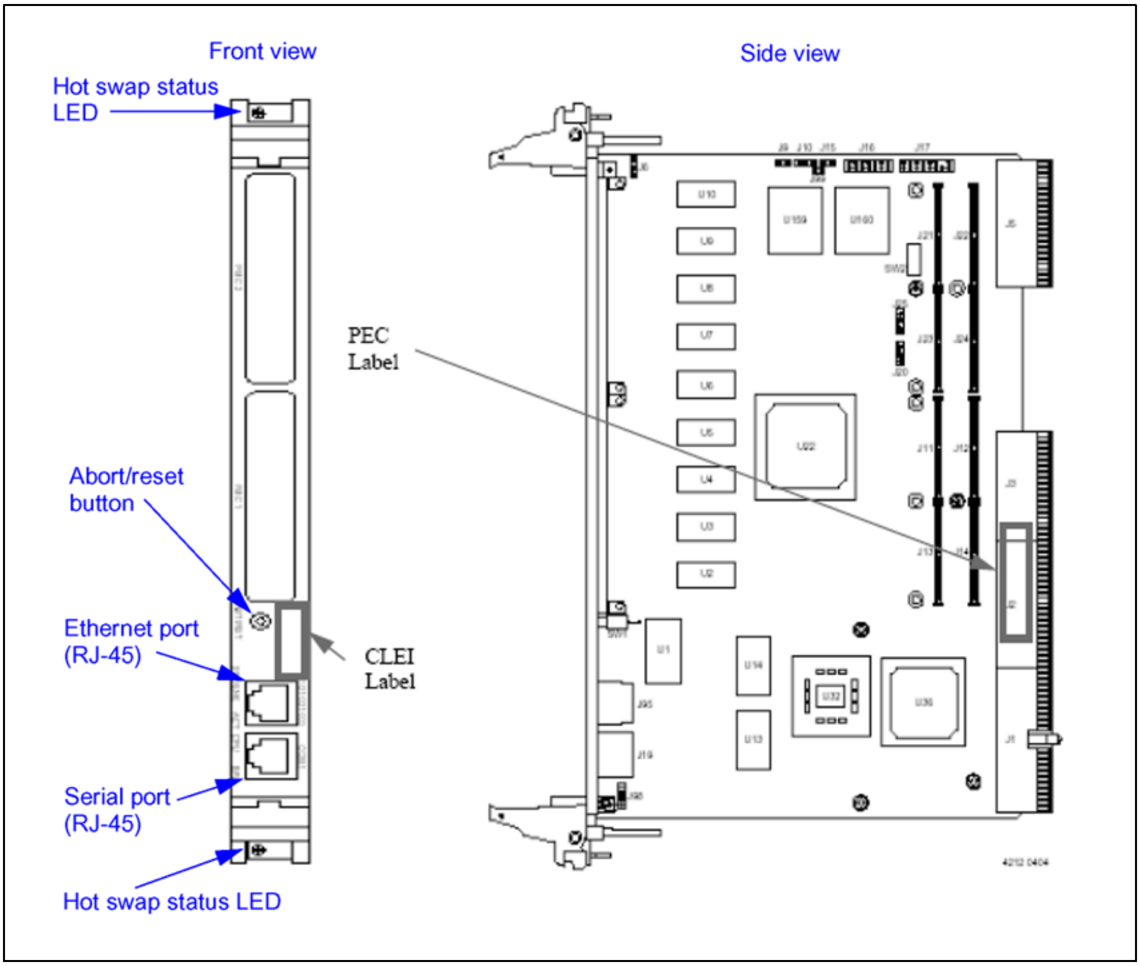
Call flow messages from the GWC to the gateways trigger the set up of the bearer path which carries the call content, whether voice or data. Using gateway control messages from the XA-Core or CCA, a GWC can then exchange connection information with another GWC allowing the two to handshake with the correct gateway control messaging so they can exchange IP addresses, media addresses, select codecs and simulate channel supervision messages (CSM). This allows the GWCs to create the appropriate gateway control messages that establish the bearer path through the packet network.

GWC hardware platform

The GWC card hardware runs on a Motorola N905 NSS board (MCPN905 card, introduced in SN08) or a Motorola N750 NSS board (MCPN750 card).

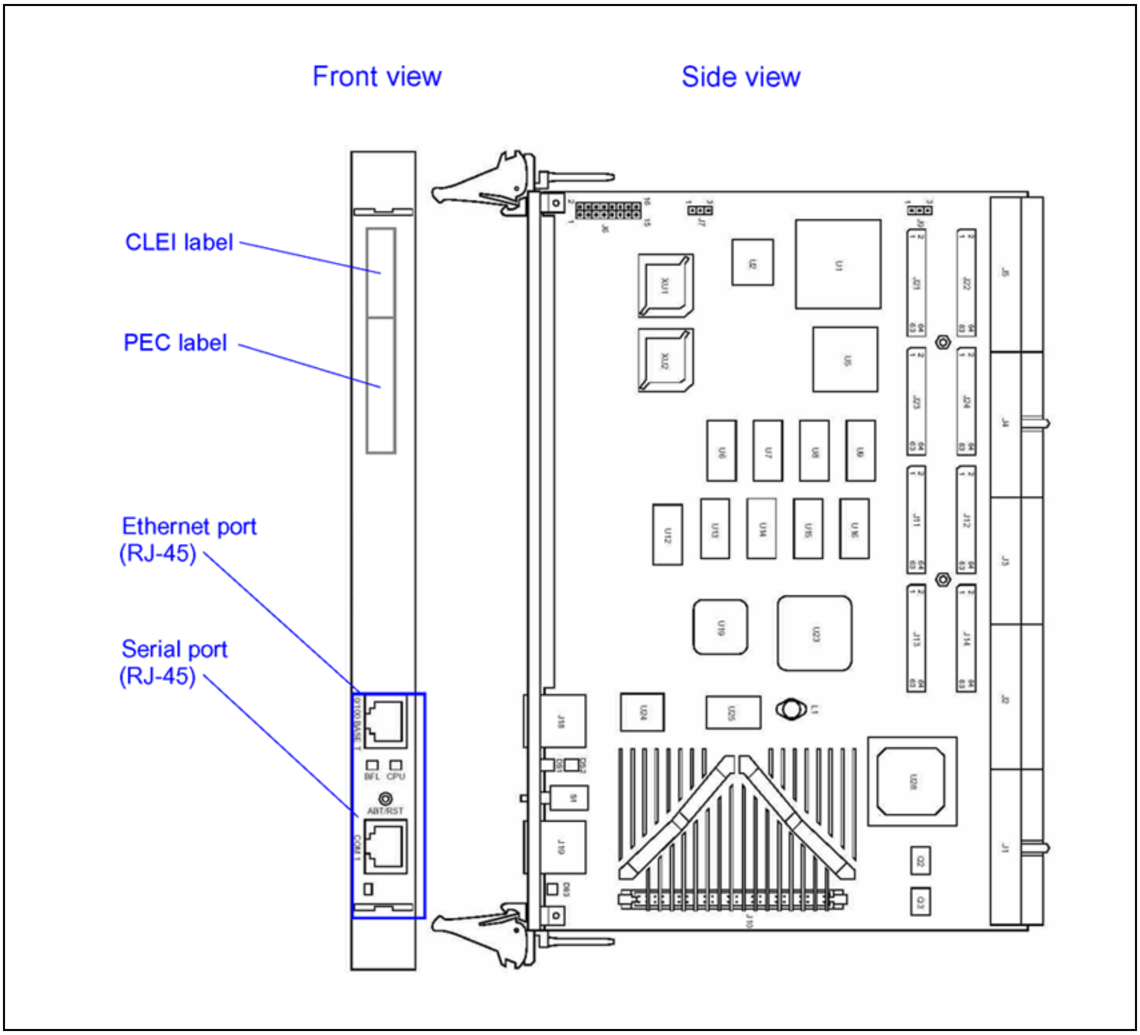
The following two figures highlight some physical attributes of the GWC cards.

Motorola N905 NSS board



For card identification, see the product engineering code (PEC) bar code label near the right edge of the card (side view), and the common language equipment identifier (CLEI) label near the bottom of the card edge (front view).

Motorola N750 NSS board

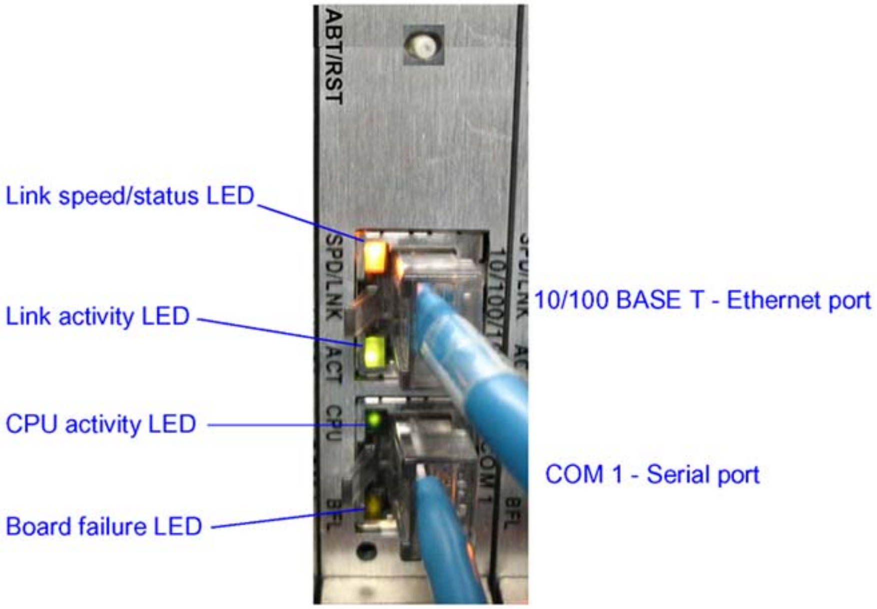


For card identification, see the CLEI label and the PEC bar code label, both near the top of the card edge (front view).

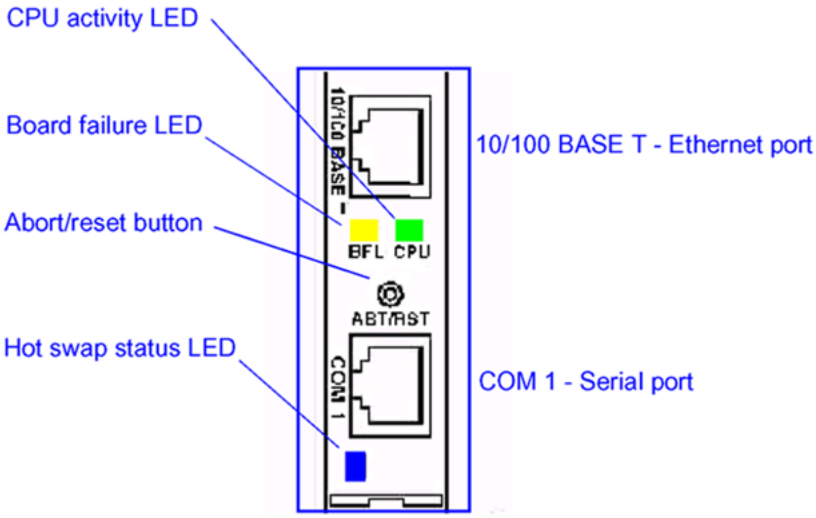
The CS 2000 SAM21 Manager displays the card name (MCPN750, MCPN905) and the corresponding memory size in the Equip tab of the card view. For details, see the CS 2000 SAM21 Manager section in the *Basics* NTP for your solution.

The following two figures show details of the Ethernet and serial ports of the GWC cards.

Ethernet port and serial port details (N905 NSS board)



Ethernet port and serial port details (N750 NSS board)



The Ethernet port is an RJ-45 connector labeled 10/100 Base-T, located on the front panel above the connector labeled COM1. This connection is used to communicate with:

- Computing module (CM) - for static data, and call processing information
- CS 2000 GWC Manager - for maintenance and configuration
- media gateways - for call processing functions
- mate GWC - for data sync and fault tolerance
- other GWCs - for call processing functions
- CS 2000 Core Manager or Core and Billing Manager (CBM) - bootp/load server (same subnet)

  GWC cards are normally located on the same subnet as the CS 2000 Core Manager or Core and Billing Manager (CBM), and the Ethernet or High Speed Input/Output Processor (EIOP/HIOP) XA-Core components. For more information, see "GWC hardware platform" (page 9).

The RJ-45 connector labeled COM1 located at the bottom of the front panel is used as an emergency access serial port.

The following LEDs appear on the front of the GWC cards:

- SPD/LNK (green/yellow; MCPN905 only) - Ethernet link speed and status; lights green to show 1000-Preliminary link, lights yellow to show 10/100-Mbit link, off if no valid link.

  As the GWC link uses only 100Base-T, the normal operating condition of this LED is yellow.
- ACT (green; MCPN905 only) - Ethernet link activity; lights when the Ethernet link is active
- CPU (green) - CPU activity; lights when the card’s processor is active
- BFL (yellow) - Board failure; lights when a system failure occurs on the card
- Hot swap status (blue; in handles of MCPN905 card) - Lights when it is permissible to remove the card from the shelf

In addition to the LEDs, there is also an ABT/RST (abort/reset) button on the front of GWC card. To abort the CPU’s current process, press this button briefly (for less than three seconds). To reset the card, press and hold this button for more than three seconds.

The GWC node and carrier grade reliability

A Gateway Controller node consists of a pair of redundant GWC cards usually housed in two different SAM21 shelves within the same frame. One card (unit 0) is active while the other card (unit 1) is in warm standby mode. The standby card is ready to take over should the active card fail, or when a manual action such as a call processing switch activity (SWACT) is performed. If a warm SWACT occurs, either automatically or by manual intervention, stable calls (calls that have been answered) will survive, but calls being set up are not guaranteed to survive. A manual SWACT may be either warm or cold. If a cold SWACT occurs, all calls are dropped.

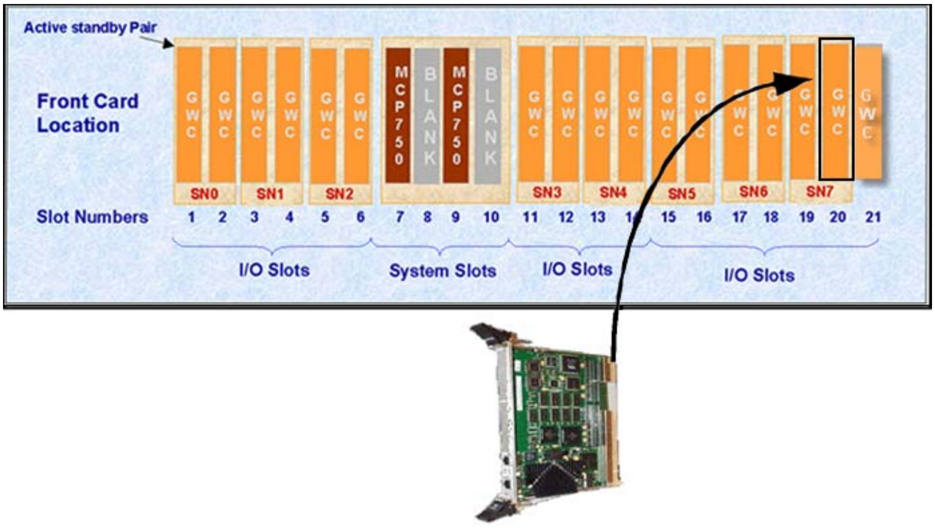
Redundant card pairs, bound together as a node in separate SAM21 shelves, help ensure carrier grade reliability within the Nortel Carrier Voice over IP (VoIP) network.

GWC cards and the SAM21 shelf

The CS 2000 SAM21 shelf accommodates a maximum of 17 GWC cards. Other devices have different shelf capacity limits and configurations.

The SAM21 Shelf Controller provides physical management of the SAM21 shelf and supports the resident GWCs (or other cards). Depending on the customer's network requirements, all 17 I/O slots in the SAM21 shelf can be filled with GWC cards. The following figure shows an example of GWC card positions in SAM21 shelf.

Example of GWC card positions in SAM21 shelf



In the CS 2000 - Compact, the CS 2000 Compact Call Agent shelf is used to house the GWC cards. It provides the same support for the GWC card as does the SAM21 shelf, although configurations and GWC card positions may vary.

Software architecture

The software used on the GWC is based on the XPM peripheral loads used in the DMS-100 family, with some modifications. The software architecture of the GWC can be extended to support multiple media gateway control protocols (such as H.248, H.323 and NCS).

The GWC software is loaded over the network from the CS 2000 Core Manager or Core and Billing Manager (CBM) when a GWC card is booted and provisioned using the CS 2000 SAM21 Manager. Patching is performed using the Network Patch Manager (NPM), a component in the CS 2000 Management Tools suite of applications.

Software loads and provisioning

Each GWC card is provisioned separately using the CS 2000 SAM21 Manager. The following software loads are required:

- GWC Flash file (for manual firmware upgrades)
- GWC NA or Intl Software Load for a specific release

Software ordering and delivery

For more information about ordering software and support options, see the *Basics* NTP applicable to your solution.

Upgrade and patch system

A GWC’s firmware is upgraded using the CS 2000 SAM21 Manager when the GWC card is assigned service, or when a new firmware load is available.

The Network Patch Manager (NPM) is used to support the patching of GWC software loads. Patches can be customized to apply to selected GWC cards or to all cards in the SAM21 shelf.

The CS 2000 GWC Manager software is upgraded as part of a CS 2000 Management Tools application upgrade. For more information about upgrades, see *Nortel Carrier Voice over IP Upgrades and Patches* (NN10440-450).

The CS 2000 GWC Manager is designed to handle backward compatibility for up to two (2) major GWC releases.

For information about the contents of the CS 2000 Management Tools software packages, including CS2M and SESM, see the *Basics* NTP applicable to your solution.

Working with the Gateway Controller

GWC fault, configuration, performance and security management activities, as well as upgrades, are all performed using tools that are part of the CS 2000 network.

Tools, utilities and user interfaces

The CS 2000 SAM21 Manager and the CS 2000 GWC Manager are the GWC's principal user interfaces. Otherwise, there are no special software tools required to install or maintain the GWC in a Nortel Carrier VoIP network.

The GWC uses the following tools to perform FCAPS activities:

- The CS 2000 SAM21 Manager is used to provision a GWC card's hardware and is also used for fault management of a GWC card.

  The SAM21 platform provides fault and configuration management on the SAM21 shelf hardware using its two Shelf Controllers. The CS 2000 SAM21 Manager handles all provisioning information and for delivering that information to the SAM21 platform. The SAM21 Manager also receives all alarm information from the platform.
- The CS 2000 GWC Manager is used to configure a GWC node's call processing services and is also used for fault management of a GWC node.

  The CS 2000 GWC Manager provides application status and configuration management of the GWC application cards residing in the SAM21 shelf hardware. The CS 2000 GWC Manager handles all configuration information and delivers that information to the GWC application cards. The GWC Manager also receives all alarm information from the GWC application.
- The Network Patch Manager (NPM) is used to perform patching and software upgrade activities on the GWC.
- The Line Maintenance Manager (LMM) and Trunk Maintenance Manager (TMM), components of the CS 2000 Management Tools suite, are used to manage lines and trunks that operate over a GWC.
- The MAP interface on the XA-Core (or the Call Agent Manager in the CS 2000 - Compact environment) and the CS 2000 GWC Manager are used for performance monitoring.

For information about how to access the CS 2000 GWC Manager and the CS 2000 SAM21 Manager, see the CS 2000 Management Tools sections in *Nortel ATM/IP Solution-level Administration and Security* (NN10402-600).

Integrated Element Management System

Many FCAPS activities may now be performed using the Integrated Element Management System (IEMS). In addition, access to the tools in the preceding list, including the CS 2000 GWC Manager and the CS 2000 SAM21 Manager, is now provided using the IEMS. For more information, see *IEMS Overview* (NN10329-111).

For information about how to launch the CS 2000 GWC Manager or the CS 2000 SAM21 Manager, see the following procedures in *IEMS Overview* (NN10329-111):

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

Configuration

Initial configuration of Gateway Controllers is completed by Nortel installation personnel. Customers can re-configure GWCs and increase GWC capacity in a network as well as configuring packet network connections between the GWC and the different gateway types.

Provisioning of GWC card base parameters is completed using the CS 2000 SAM21 Manager. Associating GWC nodes with a gateway service type and provisioning endpoints that enable the GWC node to mediate the bearer path for a call is done using the CS 2000 GWC Manager. In general, the process of configuring a GWC and associating the node with a media gateway is similar for all GWC service types and media gateways. Differences in configuration scenarios occur due to the type of gateway used (lines, trunks, VRDN, H.323) and if network address translator (NAT), policy enforcement point (PEP), or application layer gateway (ALG) devices are required.

Fault management

The GWC uses self-testing, automated diagnostics and reporting systems for maintenance and faults management. These systems raise alarms and generate logs when the following types of hardware or software events occur:

- a fault or failure condition
- correction of a fault or failure
- a threshold is crossed and the GWC is operating at a degraded level or has exceeded a defined operating capacity level
- a condition occurs that is transient or cannot be repaired.

For information about alarms and logs on the CS 2000 Management Tools server, see *Nortel ATM/IP Solution-level Fault Management* (NN10408-900).

Alarms

Alarms provide notification that a system hardware or software-related event has occurred that requires attention. Alarms are generated by the GWC or a related component, such as a gateway, when problems or conditions are detected that change the performance or operating state of a GWC node and its connections. Administration of the network elements requires monitoring for alarms and checking that functions continue without interruption.

The GWC is installed and provisioned with a set of pre-defined alarms. You cannot remove or modify these alarms; however, you can disable them. By default, all system alarms are enabled.

Alarm management for the GWC is separated into two categories: hardware faults and service and application faults. Hardware fault management activities are carried out using the CS 2000 SAM21 Manager. Service and application fault management activities are carried out using the CS 2000 GWC Manager.

Alarm severity codes indicate the impact of events on the GWC or other network elements. There are four levels of alarm listed here in order of severity:

- Critical alarm
- Major alarm
- Minor alarm
- Warning Alarm

Each alarm has a specific color based on the alarm severity. Critical and major alarms are red, minor alarms are orange and warnings are yellow.

Alarm information may be sent to the following:

- the alarm browser in the CS 2000 GWC Manager
- the Operations Support System (OSS) interface
- the CS 2000 Management Tool server syslog storage for logs.
- the Integrated Element Management System (IEMS)

For information about GWC alarms and for procedures about viewing alarms, see *Gateway Controller Fault Management* (NN10202-911).

Logs

Log reports are generated whenever a significant event has occurred on the GWC. Log reports include status and activity details, as well as reports on hardware or software faults, test results, changes in state, and other temporary events that may affect system performance. GWC logs can help when troubleshooting a problem.

GWC log information is stored in syslog log files in the /var/log directory on the CS 2000 Management Tool server. The same information may also be forwarded to the customer's OSS interface and to the IEMS.

For procedures about viewing logs, see*Gateway Controller Fault Management* (NN10202-911).

For the description of the GWC logs, see *Carrier Voice over IP Fault Management Logs Reference* (NN10275-909).

Performance management

CS 2000 captures performance metrics through operational measurement (OM) registers. The OMs collect operational statistics that are reported to the XA-Core or the CCA, and stored in the XA-Core or the CCA for future retrieval. Performance is measured and reported by event peg counts and state usage counts. Some OMs originate from the gateways and are reported to the GWC, which then forwards them to the CS 2000. For information about how to retrieve these gateways OM statistics, see *Communication Server 2000 Performance Management* (NN10149-711).

In addition to OMs, the GWC also uses Management Information Base (MIB) based performance measurements (PM) to collect statistics. Some PMs are polled by the simple network management protocol (SNMP) PM poller, a utility on the CS 2000 Management Tools server. PM poller collects performance attributes from several network components, including the GWC.

Performance data from devices, including the GWC, is collected using one of the following applications:

- Integrated Element Management System (IEMS)

  From (I)SN08 onwards, this is the recommended method.

- SNMP PM poller

  This application is available, but is no longer supported.

Operational administration

GWC card administration is managed using the CS 2000 SAM21 Manager client. GWC node service management is available through the CS 2000 GWC Manager.

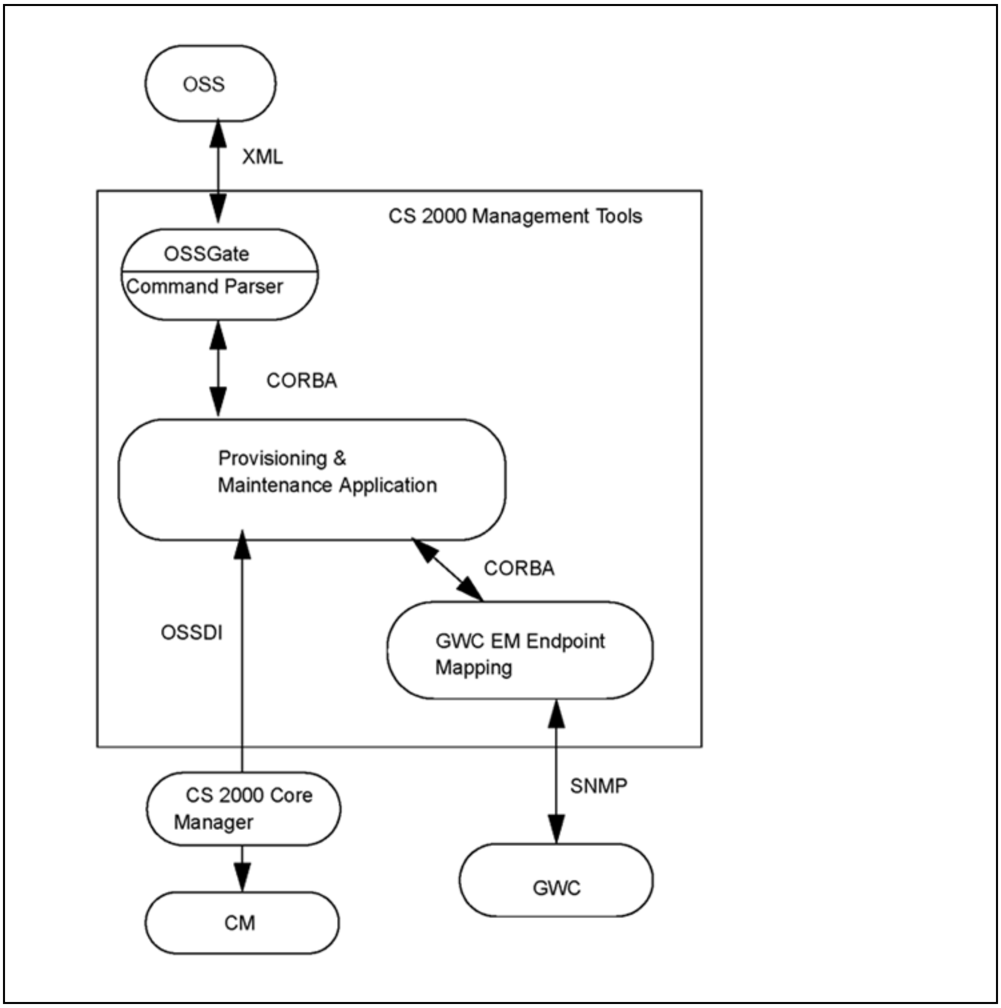
V5.2 line and interface administration is not supported using the CS 2000 GWC Manager. V5.2 line administration is performed using the CS 2000 XA-Core MAPCI interface.

Bulk provisioning using OSSGate

Bulk provisioning (configuration) of GWCs in a Nortel Carrier VoIP Network entails the distribution of configuration data from a centralized Operation Support System (OSS) to the network elements in the Communication Server and to the CS 2000 Management Tools server. Bulk configuration services can be performed using the OSSGate application, an application in the CS 2000 Management Tools suite.

The following figure shows the interaction of GWC software elements with the OSS in a bulk provisioning activity. For more information about OSSGate and bulk configuration, see *OSSGate User Guide* (NE10004-512).

OSSGate interface to the Carrier VoIP network



GWC nodes and IP addressing

The following list summarizes the physical characteristics of a GWC node (card pair) in a SAM21 shelf:

- Card limit per shelf - A maximum of 16 GWC cards for each SAM21

- Physical interfaces - 2 10/100 Base-T Ethernet ports for each GWC node (1 port per card).
- IP addresses - 4 IP Addresses are used for each GWC node:
  - — 1 physical address for unit (card) 0
  - — 1 physical address for unit (card) 1
  - — 1 logical address for the active unit
  - — 1 logical address for the inactive unit

Four consecutive IP addresses are used for a GWC node (card pair). The physical addresses are provisioned at the CS 2000 SAM21 Manager. The active and inactive IP addresses are determined automatically by the CS 2000 SAM21 Manager. The active unit IP address is required by other network elements such as the Media Server nodes.

Logically, a GWC node is a single entity that can be accessed via a single IP address. Physically, however, a GWC node consists of two separate GWC cards, each of which has its own 10/100 BaseT Ethernet port. At a given moment, one of these cards is active and the other is inactive. The following describes each type of address:

- Active unit - The IP address of the current active unit is used by other network entities. This address is used by the XA-Core or the CCA, media gateways controlled by the GWC, and other GWCs for sending messages related to call-handing. This is the IP address specified when the GWC is datafilled in table SERVRINV.

  The active unit IP address is a floating address: The address is always the same, but the underlying physical unit changes in the event of a SWACT.
- Inactive unit - The IP address of the current inactive unit is used only for synchronization and for heartbeat messaging to and from the corresponding active GWC unit.
- Physical IP addresses - These are the static addresses for OAM&P and physical access to each GWC card (unit 0 and unit 1). These addresses are mapped on to Layer 2 media access control (MAC) addresses, Ethernet physical addresses.

Gateway and network interfaces

The Gateway Controller has an interface application that mediates communication between proprietary XA-Core or CCA peripheral processor virtual machine protocols and the open standard protocols used by media gateways.

This section describes IP addressing characteristics and naming conventions used on media gateways as well as the network interface protocols supported.

IP address management

GWCs simplify IP address management by supporting dynamic IP address allocation for small gateways. When configuring a gateway in the Gateway Category of 2 (small), the gateway IP address field is optional and can be left blank. In this case, the IP address is discovered and assigned dynamically during GWC node provisioning.

Network address and port translator (NAPT) and address discovery

GWCs support the addressing of media gateways behind a network address and port translator (NAPT) device. The GWC performs an internal media gateway database lookup based on IP address and port.

When media gateways are behind NAPT devices they are accessed by the public IP addresses of the NAPT. This means that the GWC sees multiple media gateways sharing the same IP address. To distinguish between individual media gateways in communication with the GWC, user datagram protocol (UDP) or transmission control protocol (TCP) ports are used.

In order to maintain communication between the media gateway and the GWC, the media gateway will send keep alive messages to the GWC throughout its active life. The GWC will use these messages to perform IP address and port discovery.

Naming and provisioning conventions for media gateways

The capacity of a media gateway (MG) is defined in the profiles available for viewing when the MG is associated with the GWC. Therefore, the initial definition of an MG’s capacity is important to get the maximum utilization of your GWC node.

Network interfaces and protocols

Gateway Controllers communicate with each other, or with access devices such as media gateways, using the following industry standard signaling protocols.

Table "Media gateway profiles and characteristics" (page 43) provides information about which gateway profiles support the protocols in this list.

- DSM-CC

  Digital Storage Media - Command and Control is a protocol used by a GWC to manage universal port gateways. This is a trunk gateway which can connect TDM terminations to one of the following:

  — a Real-time Transport Protocol (RTP) termination (for VoIP)

— Network Access Service (NAS) termination for remote access service on a per-call basis

In a Carrier VoIP network, the universal port gateway is the CVX1800 gateway.

The XA-Core and CCA only support Version 5.2 of the DSM-CC protocol. This is the same version that is supported on CVX1800 running the CVX 5.2 software load.

- GCP

  Gateway Controller Protocol used between

  — GWC and the Session Server Lines

  — DPT GWC and the Session Server Trunks

- H.323

  H.323 is a communications protocol used for managing signaling and bearer traffic control. It is composed of an amalgam of other industry standard signaling and control protocols used for controlling

  — video (H.261, H.263)

  — audio (PCMA or PCMU, G.729)

  — media devices (H.245)

  — access and connection activities (H.225)

- Megaco/H.248

  Media Gateway Control (Megaco) from the Internet Engineering Task Force (IETF) is the standard for peripheral messaging protocols. Megaco is promulgated as H.248 by ITU-T (Megaco/H.248) and is used to provide inter-communication server communication using GWCs.

- MGCP

  Media Gateway Control Protocol is used to manipulate terminations in Media Gateways.

- NCS

  Network-based Call Signaling standard is a variant of MGCP and is used in packet cable solutions for controlling small line gateways.

- SIP-T

  SIP-T is an ITU-based standard that encapsulates ISUP messaging as payload within SIP messages. SIP-T allows calls to be delivered between VoIP call servers, like the CS 2000, without any dependency on an SS7 network for call control signaling. In a Carrier VoIP network, SIP-T is used to provide communication between GWCs on different call servers for inter-CS 2000 functionality.

- TGCP

  Trunk Gateway Control Protocol, an extension to MGCP, is used in packet cable networks for the control of public switched telephone network (PSTN) media gateways.

Gateway Controller service profiles

GWCs are usually used to host trunks, lines or other devices through gateways. Gateway Controller service profiles, such as trunk, line, audio, DPT, or VRDN, are used to define the type of GWC being configured. For example, Gateway Controller service profiles TRUNKNA and TRUNKINTL have the same generic service profile: TRUNK.

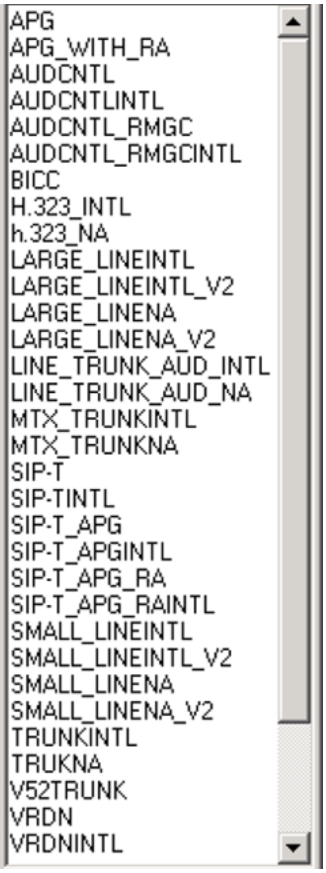
The figure "List of Gateway Controller service profiles" (page 25) lists all Gateway Controller service profiles supported.

Gateway Controller service profiles are not the same as the media gateway profiles. Gateway Controller service profiles, configured when adding a GWC, determine the general capabilities of GWC. A media gateway profile, configured when associating a gateway with a GWC, configures a GWC to support a specific gateway or category of gateways. Table "Media gateway profiles and characteristics" (page 43) lists gateway profiles supported on a Gateway Controller.

There are also GWCs which are not associated with media gateways supporting lines or trunks. The virtual router distribution node (VRDN) GWC is an example of this type of GWC.

In some cases, Gateway Controller service profiles are also reflected in the service type of media gateway profiles supported on a GWC. For example, PVG7K, PVG15K, CVX1800_2688 and CVX1800_612 all have the same service type: TRUNK.

List of Gateway Controller service profiles



APG
APG_WITH_RA
AUDCNTL
AUDCNTLINTL
AUDCNTL_RMGC
AUDCNTL_RMGCINTL
BICC
H.323_INTL
h.323_NA
LARGE_LINEINTL
LARGE_LINEINTL_V2
LARGE_LINENA
LARGE_LINENA_V2
LINE_TRUNK_AUD_INTL
LINE_TRUNK_AUD_NA
MTX_TRUNKINTL
MTX_TRUNKNA
SIP-T
SIP-TINTL
SIP-T_APG
SIP-T_APGINTL
SIP-T_APG_RA
SIP-T_APG_RAINTL
SMALL_LINEINTL
SMALL_LINEINTL_V2
SMALL_LINENA
SMALL_LINENA_V2
TRUNKINTL
TRUKNA
V52TRUNK
VRDN
VRDNINTL

Anchor packet gateway (APG) - obsolete in (I)SN07

ATTENTION

The APG functionality has been removed in the (I)SN07 release. All GWC service profiles that were required to support the APG functionality (all profiles with "APG" in their names, such as, SIP_T_APG) are obsolete. These profiles are still present in the GWC Manager GUI, but to ensure that resources are not allocated for obsolete functionality, do not use these profiles. It is recommended that the existing DPT GWCs that still use these profiles migrate to SIP-T or SIP_TINTL profile to optimize resource utilization (resources previously reserved for APG will be released for other tasks).

The Packet Media Anchor (in IP network solutions) is the replacement device for the APG functionality. For more information, see section "Packet Media Anchor for DPT" (page 26).

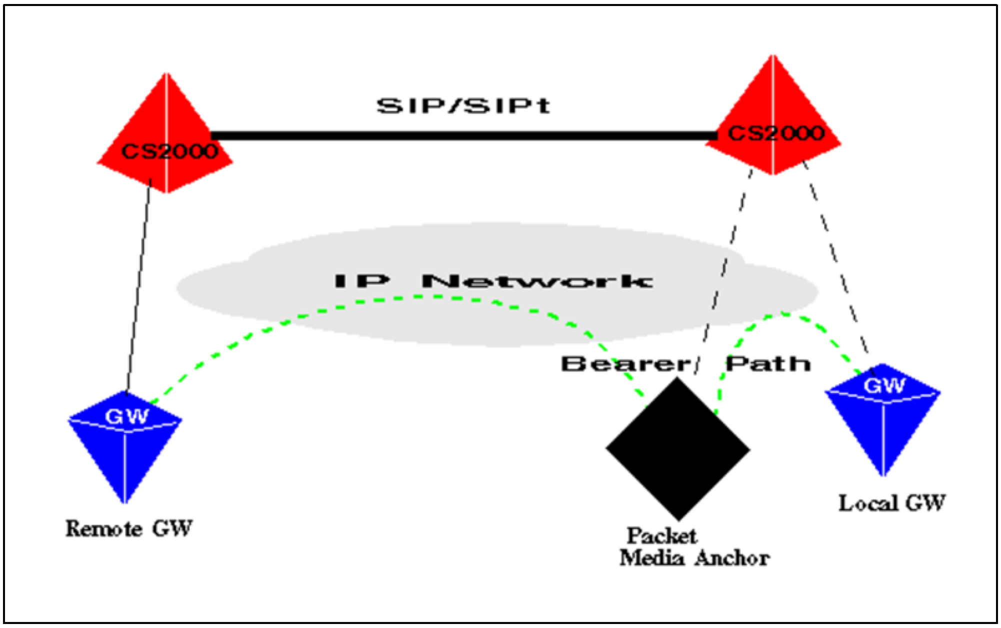
Audio controller

An audio controller service profile is used to support audio server gateways (including any Media Server 2000 Series gateways) within a Carrier VoIP network.

Packet Media Anchor for DPT

The audio controller GWC service profiles support the Packet Media Anchor device in IP network solutions. This device provides tone, digit collection, and bearer path anchoring services for SIP/SIP-T calls. DPTs do not have a physical device for playing tones or collecting digits locally, so the Packet Media Anchor is inserted into the bearer path to inject tones or extract digits from the bearer path. The following figure illustrates the Packet Media Anchor call topology.

Packet Media Anchor call topology



Media Server 2010 gateways supply the media anchoring functionality, using the bearer channel tandeming (BCT) capability. The media anchor is directed by an audio controller GWC, which manages call topology, resource allocation and de-allocation, and resource usage.

Bearer independent call control (BICC)

The BICC service profile enables a GWC to support the CS 2000 network in hosting inter-office DPT trunk calls using Bearer independent call control (BICC) for the bearer path in an ATM network.

Dynamic packet trunk (DPT)

In a CS 2000 network, dynamic packet trunks (DPT) are virtual trunks across a packet network that enable the connection of DPT trunks through the CS 2000. Services that are normally available on ISUP

trunks in the legacy DMS PSTN are fully supported on DPTs across the packet network.

The DPT GWC is responsible for managing calls over dynamic packet trunks. With this GWC service profile, DPT calls are implemented using the SIP-T protocol as the inter-Communication Server protocol. When the DPT GWC is instructed by the XA-Core or the CCA to manage connections that are DPT connections, the DPT GWC formulates and sends SIP-T messages rather than media gateway control messages. In a sense, it serves as a proxy for the real media gateway that resides on a different Communication Server.

In a network configuration with Session Server Trunks, the DPT GWC sends GCP messages to the Session Server, and the Session Server sends SIP-T or SIP messages to the other call server.

H.323

The H.323 service profile enables a GWC to support the H.323 gateways in a Carrier VoIP network. The H.323 gateway type provides virtual private network (VPN) and PSTN connectivity for multiple enterprise networks within the network.

MTX

The MTX_TRUNK service profile allows a GWC to support the packet serving mobile switching center (MSC) solution for mobile telephone exchange (MTX) users.

In order to use either MTX profile, the CS 2000 XA-Core must be upgraded to the (I)SN07 (or higher) MTX software load.

Redirecting media gateway controller (RMGC)

The redirecting media gateway controller (RMGC) service profile is used to enable initializing gateways to obtain the IP address of their associated GWC from a registration agent in the network. The RMGC GWC service profile enables MGCP- or NCS-controlled small line media gateways connected to customer LANs to dynamically obtain the fully qualified domain name (FQDN) of their Media Gateway Controller (MGC) dynamically from the RMGC. This process avoids the task of pre-provisioning the IP address. The RMGC performs this task using a registration agent application. Cable multimedia terminal adapters (MTA) and integrated access devices (IAD) are examples of media gateways that can take advantage of the RMGC service profile.

A dynamic host configuration protocol (DHCP) server provides an RMGC FQDN address to each gateway when the gateway is turned on. Once the gateway registers with the RMGC, the RMGC queries a database and returns the correct GWC FQDN address to the registering gateway. The gateway can then register with its GWC.

The RMGC service profile is applicable only to cable and wireline solutions for (North American or International markets). This service profile combines the audio controller and RMGC capabilities. These capabilities are not inter-related. You may use a GWC node with this profile to perform the RMGC function, as well as an audio controller function.

Resource allocator (RA)

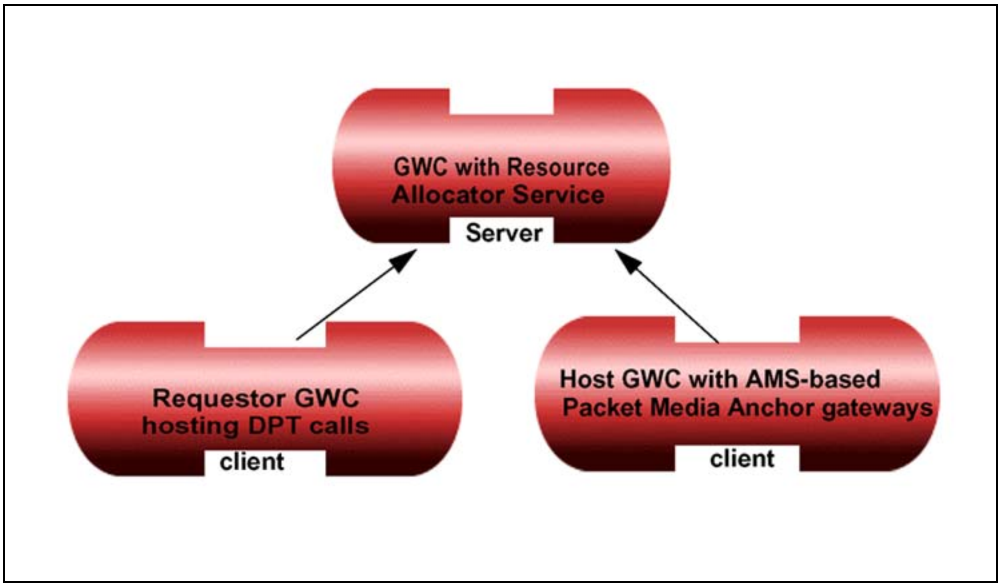
The resource allocator (RA) is responsible for allocating Packet Media Anchor contexts. The RA server tracks the number of available or call-processing-busy resources. The server allocates media anchor resources to DPT clients requesting access to the service. The RA server is provisioned from resources auto-discovered on the audio controller GWC. These resources are reported by the various Media Server gateways as they come into service. The CS 2000 Core partitions these auto-discovered resources and informs the RA server of the number of resources available.

The RA is only initialized on audio controller GWCs that host Media Server 2010 gateways configured with the Packet Media Anchor functionality. Multiple audio controller GWCs provisioned within a single CS 2000 LAN will negotiate to determine which RA server will provide service. Once the system chooses a particular RA server, the other audio controller GWCs running RA servers will de-commission their servers.

The following figure illustrates the logical relationship between a resource allocator and its clients. The GWC with which a resource allocator is associated acts as the server for the GWCs that host the Packet Media Anchor gateways. The same GWC also acts as a server for the requestor GWCs that host DPT gateways.

The RA server is physically located on the same GWC as the host GWC.

Resource allocator server and clients


GWC with Resource Allocator Service
Server
Requestor GWC hosting DPT calls
client
Host GWC with AMS-based Packet Media Anchor gateways
client

Session initiation protocol (SIP)

This section pertains to both RFC compliant SIP and SIP-T, but only the SIP acronym will be used.

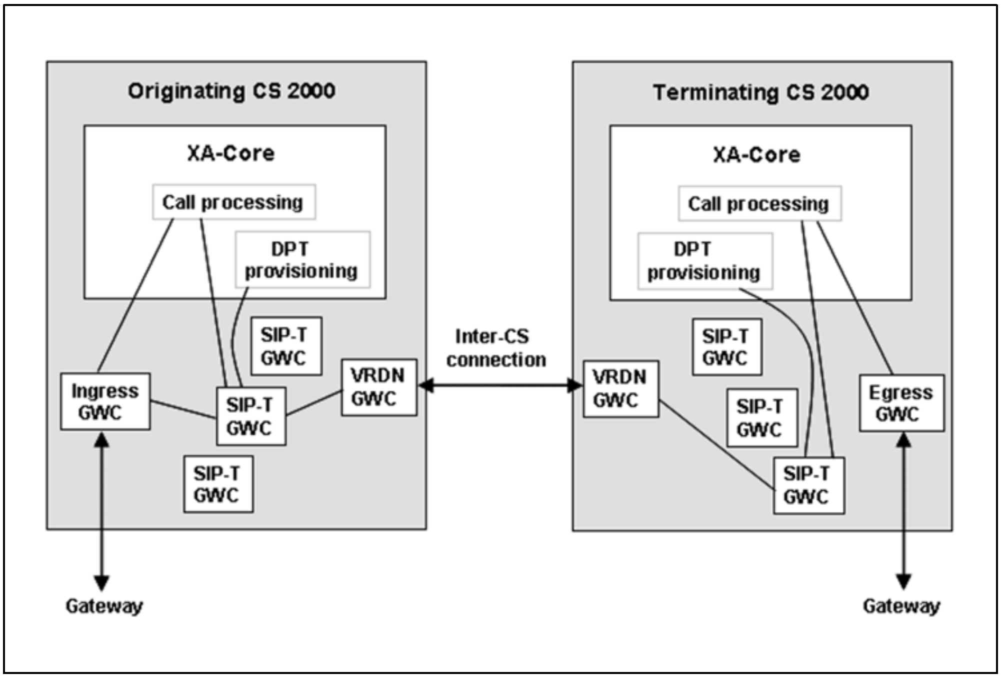
The DPT-type GWC service profile supports SIP messaging using DPT trunking to handle calls delivered between Communication Servers from inside or outside a central office network. SIP replaces the dependency on an SS7 network for call control signaling. SIP uses UDP over IP to transport SIP protocol messages between the Communication Servers.

When two or more CS 2000s are brought together in a network, SIP and VRDN GWCs interact with each other to provide call processing support that spans two servers. In this case, a call ingressing into one Communication Server egresses from another Communication Server.

Starting in (I)SN07, Session Server Trunks hardware and software platform can be used instead of the VRDN GWC.

The following figure provides more information about the role of the DPT and VRDN GWCs in this type of call processor network.

Role of DPT and VRDN GWCs in a CS 2000 network



In a CS 2000 - Compact environment, the Compact Call Agent (CCA) provides the XA-Core functionality.

In summary, the VRDN and DPT GWCs in an inter-CS 2000 network interact as follows:

- The XA-Core or the CCA selects the DPT served by the DPT GWC from the DPT pool and allocates that DPT for the duration of the call.
- The Trunk group data for the selected DPT, including CCS7 protocol and destination hostname and associated VRDN or SST, is downloaded to its DPT GWC when the DPT is selected and allocated. For outgoing calls, the downloaded trunk group data reflects translations, routing, trunk selection, and the telephony profile associated with the destination. For incoming calls, it reflects the telephony profile conveyed in the first SIP message.
- Once a DPT served by a DPT-type GWC has been selected and configured, that GWC can communicate directly with:
  - VRDN (for coordination of messages with the GWC is through call ID)

    or

    Session Server Trunks
  - The appropriate ingress/egress GWC

Call processing can identify the trunk via a standard terminal ID (as if it had been statically provisioned).

Session Server Trunks (SST) can replace VRDN GWC.

Small and large line gateway

The small and large line gateway GWC service profile adds support for a variety of line gateways available around the world, including many non-packet based, legacy line devices.

Support for the SIP Lines functionality

Starting in (I)SN09, GWCs support the implementation of the Session Server SIP Lines functionality. The following GWC service profiles support SIP Lines:

- LARGE_LINENA_V2
- LARGE_LINEINTL_V2
- LINE_TRUNK_AUD_NA
- LINE_TRUNK_AUD_INTL

SIP Lines is an application of capabilities across various elements within the CS 2000 solution. The CS 2000 Session Server Lines (SSL) provides the SIP interface to various clients and provides SIP-oriented multimedia services. The SSL communicates with the CS 2000 Core through the GWC. For more information about the SIP Lines program, see *Session Server Lines Fundamentals* (NN10437-111). For information about SIP Lines configuration requirements on the GWC, see *Gateway Controller Configuration Management* (NN10205-511).

Combined service profiles

GWC nodes configured on two MCPN905 cards support the following combined service profiles:

- LINE_TRUNK_AUD_NA
- LINE_TRUNK_AUD_INTL

These profiles combine the SMALL_LINE, LARGE_LINE, TRUNK, and AUDCNTL profiles and support all gateway types and capabilities supported by those individual service profiles (at capacities provided by the MCPN750 cards). The combined profiles also support the SIP Lines functionality.

The combined profiles do not support DMS-250 PTS and DMS-250 PRI trunks, but do support DMS-250 ISUP trunks.

V5.2 trunk

The V5.2 trunk service profile allows a GWC to host V5.2 protocol based line services, and is often used in cable IP markets. The V5.2 protocol is an international lines concentration protocol defined by the European Telecommunications Standards Institute (ETSI) standards committee and is widely deployed in the international markets including Europe, South America and Asia Pacific.

The V5.2 ETSI specification describes the requirements for connecting a V5.2 interface between a remote access network and a local exchange. Access network (AN) refers to the system implemented between the end user and the local exchange. In the context of V5.2, it describes an active system that replaces some or all of the local line distribution network. The V5.2 interface specifies the electrical, physical, procedural and protocol requirements for this interconnection to support various types of digital and analog access.

A V5.2 interface is similar to a group of E1 (similar to T1) carriers, but with specific V5.2 characteristics such as primary and secondary signaling links and timeslots, on which V5.2 lines are carried.

Carrier VoIP architecture splits the V5.2 System over the GWC and the gateway. High layers (V5.2 system management and V5.2 layer 3 protocols) are located on the GWC. Low layers (V5.2 layer 2 and layer 1) are located on the gateway. V5.2 signaling is tunneled over a V5UA/SCTP/IP protocol stack between the GWC and the signaling gateway.

The media gateway part of the gateway is responsible for applying audio tones (for example, dial tone, ringback tone, call waiting tone), applying V.23 modem tones, recognition of DTMF tones and control of bearer path. Megaco H.248 protocol is used as the gateway control protocol. H.248 signaling is implemented via an H.248/UDP/IP protocol stack between the gateway and GWC.

The access node (AN) is connected to the gateway over a V5.2 interface which may consist of up to 16 E1-links (2048 kbit/sec carriers). The AN is responsible for power, recognition of line signals (for example, off-hook, on-hook, hook-flash, dial-pulses) and applying line signals (for example, cadence ringing, reverse polarity, reduced battery).

To ensure near carrier grade service using the V5.2 protocol, ANs are connected via protected V5.2 interfaces. A protected V5.2 interface consists of at least two V5.2 links housed on two different active VSP cards.

- Connecting ANs over only one VSP card is not recommended, because VSP card failure results in complete loss of service.
- Connecting ANs with an unprotected V5.2 interface is not recommended, because primary E1 link failure results in complete loss of service.

Virtual router distribution node (VRDN)

The virtual router distribution node (VRDN) service profile is used to route SIP-T signaling messages to other CS 2000 nodes. A VRDN can support signaling to a number of other CS 2000 nodes, but only a single VRDN can be used in the signaling path between any two specific nodes.

The VRDN GWC service profile provides a SIP-T interface to the Communication Server. It distributes SIP-T call processing messages between SIP-T GWCs. The VRDN GWC is responsible for aggregating SIP-T messaging and provides a single IP address for routing messages that are destined for any GWC associated with the CS 2000. This aggregation prevents each individual DPT GWC from having to maintain the IP addresses of all the other DPT GWCs across the network. The VRDN GWC maintains the IP address of the other VRDN GWCs in the network.

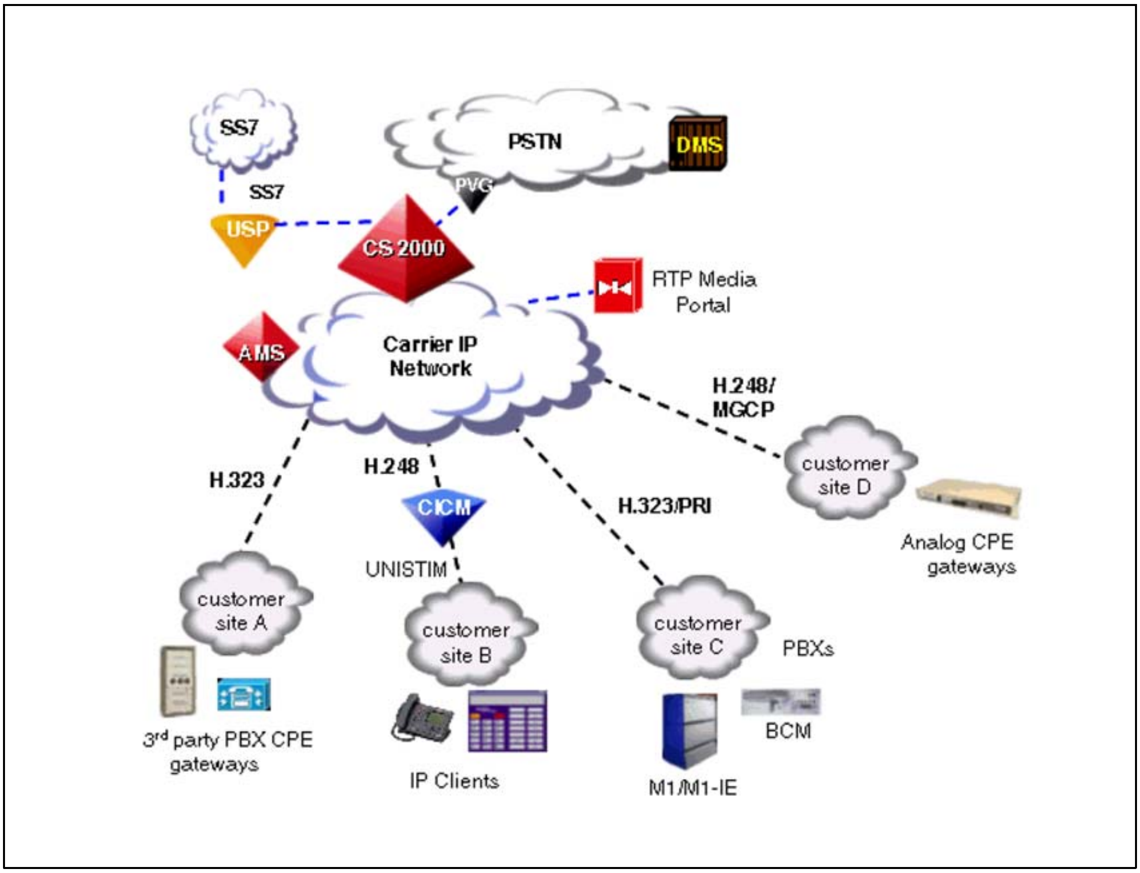
The VRDN architecture allows significant increases in capacity by changing from stream control transmission protocol (SCTP) over IP to user datagram protocol (UDP) over IP. This allows the VRDN to take advantage of UDP transport redirection, which is only supported over a UDP interface. This allows the SIP-T messages to be sent directly between the GWCs after the initial INVITE message, thus bypassing the VRDN and increasing its capacity.

Starting in (I)SN07, the VRDN can be replaced by the Session Server Trunks. The Session Server Trunks platform is the recommended configuration for all new installations. For information about the Session Server Trunks configuration, see *Session Server Trunks Basics* (NN10333-111).

Carrier VoIP virtual private networking

Starting in release SN06.2, the CS 2000 supports VoIP virtual private network (VPN) configurations. The following figure illustrates the different customer networks that can be brought together in a Carrier VoIP VPN. It offers network level services for enterprises, including translations and routing, Centrex groups, and PSTN connectivity in support of features such as Carrier Hosted Services (CHS).

Carrier VoIP VPN



The VPN supports network access via H.323 and H.248, incorporating the following:

- Multiple IP-based networks with interworking to trunks and lines.
- Inter-operability with third-party PBX gateways over H.323; see customer site A.

  Starting in (I)SN09, an alternative direct interconnection between PBX and a CS 2000 is provided in international markets, using Digital Private Network Signaling System (DPNSS) carried over E1 carrier.

  Two solutions are available:

  — DPNSS tunneling over H.323 using Westell gateway. This solution uses H.323 protocol (H.225 signaling, H.245 media control protocol).

  — DPNSS interface on CS 2000 using MG 3200 gateway. This solution uses DPNSS User Adaptation (DUA) protocol (DUA signaling, H.248 media control protocol).

- IP clients over H.248 using Centrex IP Client Manager (CICM); see customer site B.

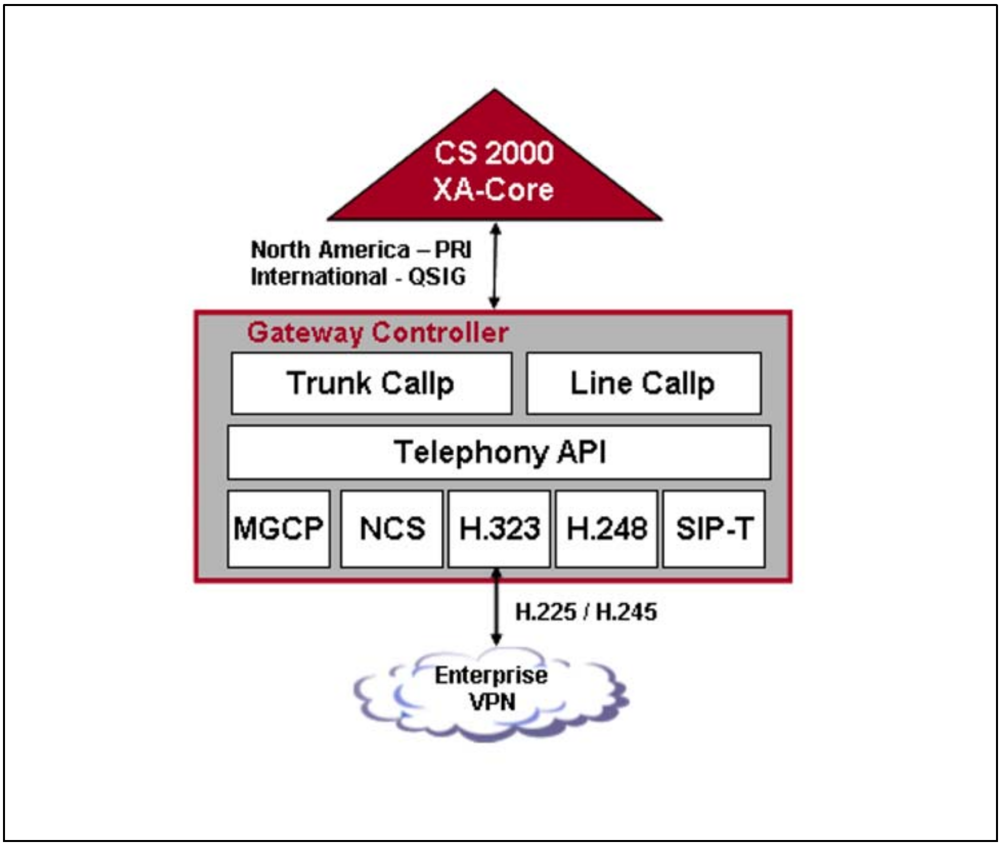
- Connectivity with Nortel gateways over H.323/PRI, including Meridian 1 - IP Enabled and Business Communications Manager (BCM); see customer site C.
- Analog gateways using IAD over H.248/MGCP; see customer site D.

The CS 2000 uses real-time transport protocol (RFC 1889), or Border Control Point (BCP), to establish media paths that span the address space of individual enterprise networks. The CS 2000 uses the media portal as required to bridge the RTP paths between endpoints for Centrex IP NAT traversal. The BCP is needed if the endpoints of the media path are not in the same IP address space. This would be the case for calls between two enterprises, or calls from an enterprise H.323 gateway to a gateway on the carrier IP network, such as the PVG.

H.323 support on the GWC

The GWC integrates gateway control protocols into the existing line and trunk call processing engines, as shown in the following figure. The GWC includes H.323 as a peer with the other protocols it supports. H.225 signaling is sent to PRI or QSIG for processing by the XA-Core or the CCA, integrating PRI service and Centrex capabilities across many international variants. H.245 signaling is sent to the H.323 gateways or mapped to Session Description Protocol (SDP - RFC 2327) for media inter-operability with other VoIP gateways.

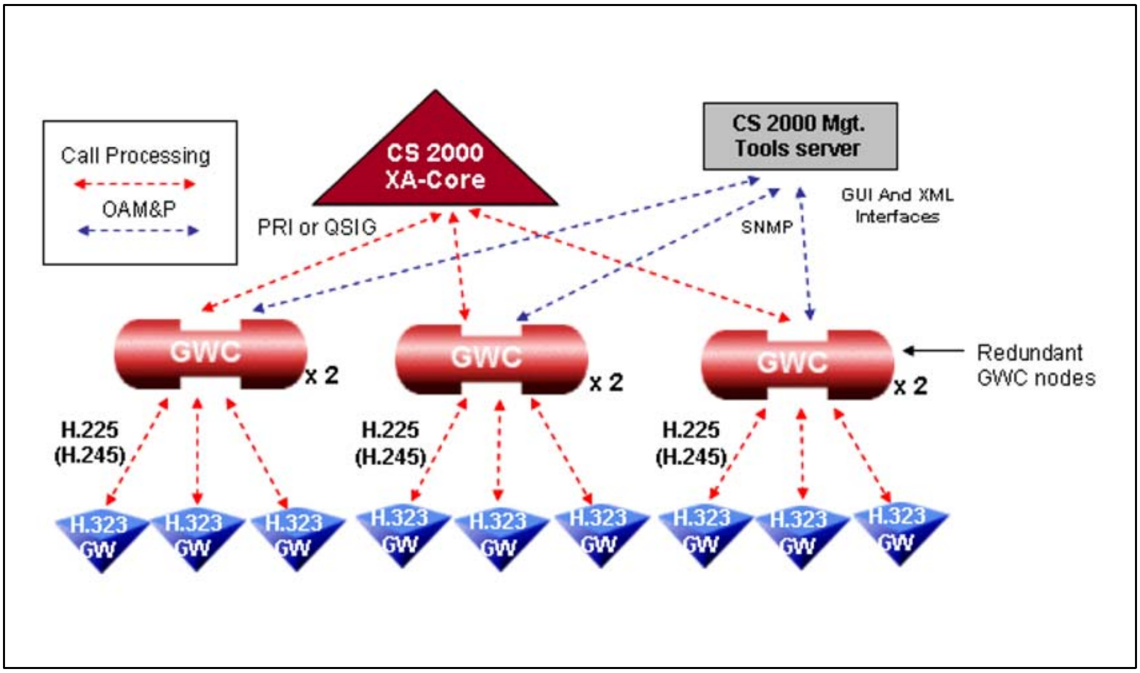
GWC architecture



In a CS 2000 - Compact environment, the Compact Call Agent (CCA) provides the XA-Core functionality.

Each H.323 gateway is associated with a GWC configured for H.323, as indicated in the following figure. A gateway always interacts with the same GWC. One or more PRI or QSIG trunk groups are defined on the XA-Core or the CCA for each H.323 GWC. These trunk groups are used for all traffic to or from the gateway. The number of trunk groups required depends on the number of simultaneous calls that must be supported.

H.323 gateway associations



In a CS 2000 - Compact environment, the Compact Call Agent (CCA) provides the XA-Core functionality.

Virtual call admissions control

Virtual call admissions control (VCAC) is a quality of service (QoS) mechanism that allows the Communication Server 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, starting with the service provider's core packet network and points of bandwidth concentration. These concentration points could occur at customer enterprises that are composed of a collection of sites, or at a regional broadband aggregation point. These sites are connected by a mix of limited bandwidth links (LBL) and network address translators (NAT). The VoIP gateways and the lines are located within the different sites (zones) in each enterprise.

For information about configuring VCAC on a GWC, see *Gateway Controller Configuration Management* (NN10205-511).

Starting in (I)SN08, GWCs can operate in one of the following VCAC modes:

- Network VCAC status: OFF

  In this mode, each GWC counts internally resource usage across LBLs and makes the connection admission decisions.

- Network VCAC status: ON

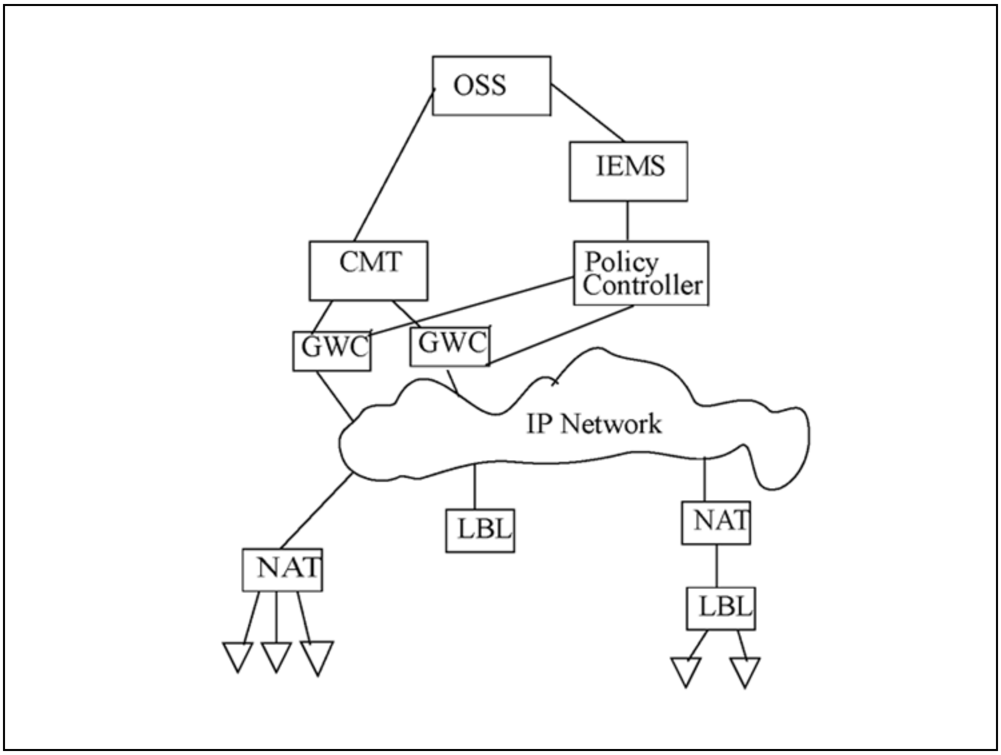
In this mode, the Policy Controller counts resource usage and makes the connection admission decisions, so VCAC GWCs are not required.

Network configuration with the Policy Controller

Network VCAC implementation requires the Policy Controller - a network component that counts available resources across LBLs and makes the connection admission decisions. GWCs communicate with the Policy Controller to determine whether a call can be set up. This process allows LBLs to be shared across different GWCs. Also, Network VCAC supports composite zones (zones comprising the attributes of both NAT and LBL network zones).

The following figure shows an example of network configuration with the Policy Controller.

Network configuration with the Policy Controller



For information about the Network VCAC and the Policy Controller configuration, see *Policy Controller Configuration Management* (NN10432-511).

Trimodal functionality on the CS 2000

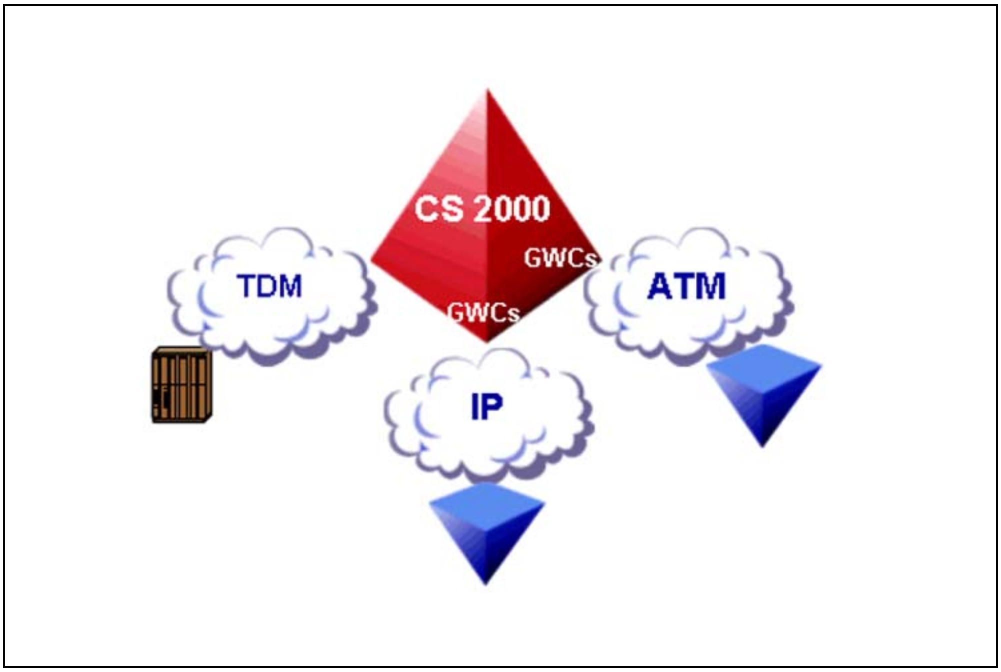
CS 2000 supports the concurrent implementation of multiple bearer networks. Trimodal operation includes IP and ATM packet bearer networks as well as the TDM Enhanced Network (ENET).

The focus is on supporting three bearer networks:

- IP packet network
- ATM Adaptation Layer 1 (AAL1) packet network
- TDM ENET

AAL2 packet networks can be configured, but will not be fully tested in a multiple bearer network configuration.

Trimodal operation



GWC support for Trimodal operation

Starting in (I)SN07, it is possible to configure and use network codec profiles with multiple packet bearer network fabric types on a CS 2000. You can configure individual codecs that use any of the following bearer network fabric types to be used concurrently:

- IP
- AAL1
- AAL2

Each GWC node in a CS 2000 must be configured to use one of the available network codec profiles. GWC nodes in a CS 2000 can use different codec profiles configured to operate over different bearer network fabrics. You can define multiple network codec profiles in the system, and then select the desired profile while adding a GWC node to the network.

For Centrex IP Client Manager (CICM) gateway configured with an audio profile, the GWC codecs combination supersedes the gateway codec configuration. The GWC controls the codec selection order of preference, based on the network codec profile assigned to the GWC node.

Example
If a CICM gateway profile defines G.729 as the primary codec and PCMU as secondary, but the GWC codec profile lists PCMU as primary and G.729 as secondary, the GWC node first attempts to communicate with a CICM gateway using the PCMU codec, then the G.729.
For more information, see section “CODEC negotiation rules” in the *CICM Configuration Management* (NN10240-511).

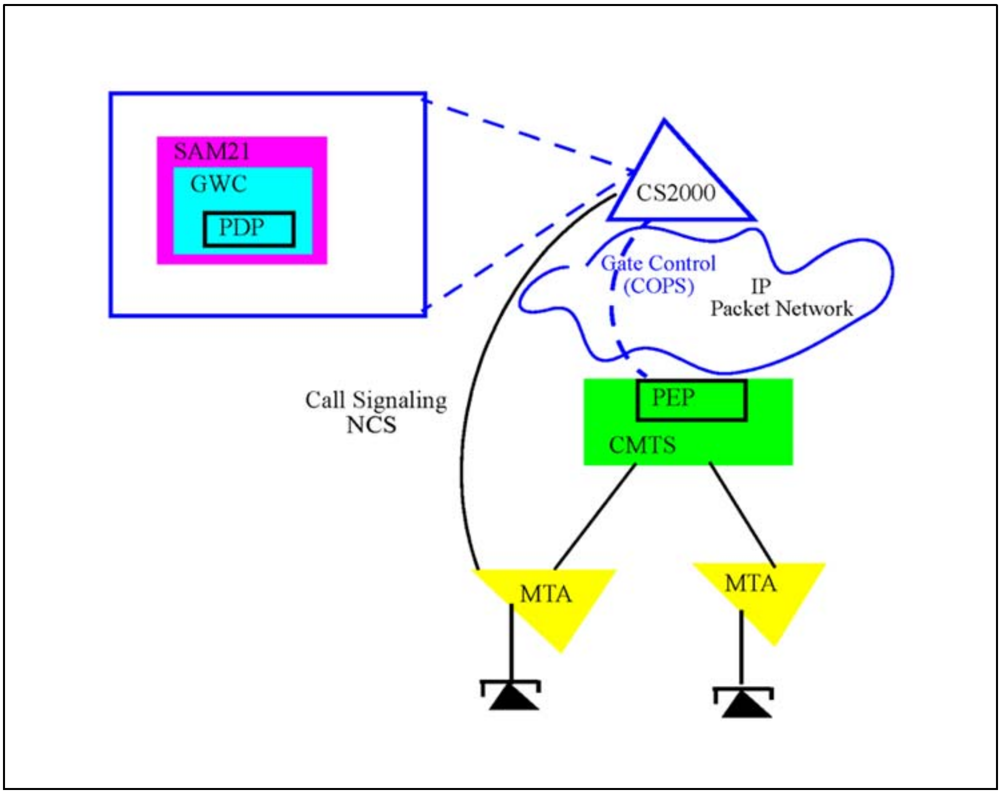
Dynamic quality of service

GWC supports dynamic quality of service (DQoS), a feature used in Nortel Carrier VoIP solutions such as packet cable. It is used to control quality of service in the access portion of a packet cable network. The packet cable multimedia terminal adaptor (MTA) line gateway can negotiate quality of service (QoS) with the cable modem termination system (CMTS) up to the QoS level authorized by the GWC. The MTA supports access to an IP backbone network for analog subscriber lines.

The responsibility of DQoS is shared between a policy decision point (PDP) which resides in the CS 2000 GWC and the policy enforcement point (PEP), or middlebox, which resides in the CMTS or on another server. The PDP authorizes QoS on a per-call basis by sending a common open policy service (COPS) decision message to the PEP when a call is made. The PEP enforces the policy contained in the decision message.

All DQoS/COPS links are managed by the GWC to remain up at all times. If a link fails, the GWC automatically attempts to recover the link by reconnecting to the PEP server. Attempts to reconnect continue at a fixed interval until the connection is successfully re-established, or until the PEP server is deleted. The following figure shows an example of DQoS for a derived lines cable network.

DQoS in a Carrier VoIP network



Access to DQoS and PEP servers is configured using the CS 2000 GWC Manager, usually when setting up the Carrier VoIP network. However, DQoS and PEP server access can be added later, once the network has been made operational.

For instructions about configuring DQoS and PEP server access, see *Gateway Controller Configuration Management* (NN10205-511).

Internet Protocol security

The Internet Protocol security (IPSec) is a standard for implementing security measures at the IP level. IPSec offers a set of security services that provide data integrity, authentication, and confidentiality.

IPSec implementation is optional. Starting in (I)SN08, all Gateway Controller (GWC) service profiles support the IPSec functionality.

For more information about some basic IPSec concepts and the implementation of the IPSec on the GWC component, see *Gateway Controller Security and Administration* (NN10213-611). For detailed IPSec information, see the appropriate Internet Engineering Task Force (IETF) RFC documentation, which can be found at http://www.ietf.org.

In packet cable solutions, IPSec can be used to protect all signaling traffic between the call server and the following network components:

- Multimedia terminal adapter (MTA) line gateway - IPSec with Kerberos key management

  If an application layer gateway (ALG) middlebox is associated with an MTA gateway, IPSec between the GWC, ALG, and MTA gateway is not supported.

  MTA authentication with the CS 2000 requires an integrated third-party key distribution center (KDC), which grants Kerberos call server tickets to the MTA. For more information, see the *Nortel ATM/IP Solution-level Administration and Security* (NN10402-600).
- Cable modem termination system (CMTS) - IPSec with Internet Key Exchange (IKE) management system (with pre-shared keys)

  IPSec protects the dynamic quality of service (DQoS) messages - Common Open Policy Service (COPS) protocol.
- Third-party Trunk Gateway Control Protocol (TGCP) gateways - IPSec with IKE management system (with pre-shared keys)

For a complete list of network paths and devices supporting IPSec, as well as an overview of the IPSec implementation in a network, see *Nortel ATM/IP Solution-level Administration and Security* (NN10402-600).

Media gateway profiles

Table "Media gateway profiles and characteristics" (page 43) contains information about the different profiles supported on a Gateway Controller.

Some profiles support multiple gateways. Contact your Nortel account prime for the gateways supported using a profile.

The media gateway profiles supported depend on the Gateway Controller service profile configured for a GWC node. For details, see "Gateway Controller service profiles" (page 24).

Newly supported gateways may be added to the list and are not shown in this procedure. Not all gateways are supported for every solution and release.

OLD_SN06_CICM and DOMAIN_NAME profiles are present in the GWC Manager GUI, but are not supported.

Changing a profile

Starting in (I)SN08, you can modify an existing gateway profile by creating a new certificate (profile), which will include new values for the selected attributes. Once the new profile is added, you can complete a Change Profile operation to associate the gateway with the new profile. For information about how to change a profile, see procedure "Change gateway attributes" in the *Gateway Controller Configuration Management* (NN10205-511).

For information about how to create, add, and remove a certificate, see procedure "Add a certificate file for a third-party gateway" in the *Gateway Controller Configuration Management* (NN10205-511).

Media gateway profiles and characteristics

Gateway Profile Name	Gateway Category	Signaling Protocol Type	Protocol Version	Default Protocol Port	Service Type	Max. Port/ Endpoint Capacity
Audio gateways						
UAS (includes Media Server 2000 Series)	Audio	MEGACO	1.0	2944	Audio	n/a
AMS	Audio	MEGACO	1.0	2944	Audio	120
Media Server 2010 gateways associated with the AMS (Media Server 2000 series) profile supply the Packet Media Anchor functionality.						
H.323 gateways						
For H.323 gateways, use the following guidelines:						
Protocol port values						
• Use a value of **0** for auto-discovery. This enables the system to discover the protocol port when the gateway registers. Use this value for all CISCO profiles and for H.323_PROXY. or • Use the specific port value of the static bind that has been configured on the NAT for the H.323 gateway. Do not use the port value of 1719. • For gateways in RAS-less mode, use a non-zero value. This value must match the gateway’s call signaling (CS) port value (for gateways without a NAT) or must be mapped through the NAT to the gateway’s CS port value (for gateways behind a NAT in a 1:1 configuration)						
Endpoint capacity values						
The indicated endpoint capacity is a recommended value based on the GWC capacity. The actual endpoint capacity supported depends on the details of your specific installation. For the following H.323 profiles, see the corresponding product documentation to determine the recommended endpoint maximum supported on a specific gateway.						
For all H.323 gateway profiles, the recommended endpoint capacity values are: • 1032 (NA) • 1024 (Intl)						

Gateway Profile Name	Gateway Category	Signaling Protocol Type	Protocol Version	Default Protocol Port	Service Type	Max. Port/ Endpoint Capacity
CISCO_2600	large	H.323	4.0	n/a	H.323, ITRANS	See the preceding guidelines for H.323 gateways.
CISCO_3600	large	H.323	4.0	n/a	H.323, ITRANS	
CISCO_AS5300	large	H.323	4.0	n/a	H.323, ITRANS	
CISCO_H323_IOS	large	H.323	4.0	n/a	H.323, ITRANS	
H323_PROXY	large	H.323	4.0	n/a	H.323, ITRANS	
NORTEL _BCM	large	H.323	4.0	n/a	H.323, ITRANS	
SUCCESSION_1000	large	H.323	4.0	1719	H.323, ITRANS	
WESTELL	large	H.323	4.0	1719	H.323, ITRANS	
Line gateways (wireline market)						
Note: For (I)SN09U, profile AUDIOCODES_6310_LINE is present in the GWC Manager GUI but is not supported.						
AMBIT_LINE_GW_16	Small	MGCP	1.0	2427	Line, ITRANS	16
ASKEY_LINE_GW_4	Small	MGCP	1.0	2427	Line, ITRANS	4
ASKEY_LINE_GW_12	Small	MGCP	1.0	2427	Line, ITRANS	12
ASKEY_LINE_GW_30	Small	MGCP	1.0	2427	Line, ITRANS	30
AUDCDSMG32LN	Large	MEGACO	1.0	2944	Line	384
CALIX_C7	Large	MEGACO	1.0	2944	Line	1023
CICM	Large	MEGACO	1.0	2944	Line, ITRANS_ROAM	3069
KEYMILE_UMUX	Large	MEGACO	1.0	2944	Line	480
MEDIATRIX_GW_4	Small	MGCP	1.0	2427	Line, ITRANS	4

Gateway Profile Name	Gateway Category	Signaling Protocol Type	Protocol Version	Default Protocol Port	Service Type	Max. Port/ Endpoint Capacity
MEDIATRIX_GW_24	Small	MGCP	1.0	2427	Line, ITRANS	24
MGCP_IAD_40	Small	MGCP	1.0	2427	Line, ITRANS	40
MGCP_LINE_GW_1	Small	MGCP	1.0	2427	Line, ITRANS	1
SIPVOICE	Large	GCP	0.0	7060	Line	12 276
The SIPVOICE profile supports a Session Server Virtual Media Gateway (VMG). Associating a VMG with a GWC is necessary to establish a link between the Session Server Lines and the GWC for SIP Lines processing. For more information, see procedure "Associate a Session Server virtual gateway for SIP Lines" in the *Gateway Controller Configuration Management* (NN10205-511).						
Line gateways (cable market)						
ARRIS_TOUCHTONE_NN01_4	Small	NCS	1.0	2427	Line, DQoS	4
ARRIS_TOUCHTONE_NN02_4	Small	NCS	1.0	2427	Line, DQoS	4
MOTOROLA MTA_1	Small	NCS	1.0	2427	Line, DQoS	1
MOTOROLA MTA_2	Small	NCS	1.0	2427	Line, DQoS	2
MOTOROLA MTA_4	Small	NCS	1.0	2427	Line, DQoS	4
TOUCHTONE_NN01_1	Small	NCS	1.0	2427	Line, DQoS	1
TOUCHTONE_NN01_2	Small	NCS	1.0	2427	Line, DQoS	2
TOUCHTONE_NN01_3	Small	NCS	1.0	2427	Line, DQoS	3
TOUCHTONE_NN01_4	Small	NCS	1.0	2427	Line, DQoS	4
Trunk gateways						
Note: The NUERA_GX_ASPEN profile is obsolete. For (I)SN09U, it is still present in the GWC Manager GUI but is not supported						

Gateway Profile Name	Gateway Category	Signaling Protocol Type	Protocol Version	Default Protocol Port	Service Type	Max. Port/ Endpoint Capacity
AUDIOCODES (Nortel Media Gateway 3200 and Nortel Media Gateway 3500)	Large	MEGACO	1.0	2944	Trunk	280
AUDIOCODES _6310_ TRUNK (Nortel Media Gateway 3500 using TP-6310 card and configured as a trunk gateway)	Large	MEGACO	1.0	2944	Trunk	2016
CVX1800 _2688	Large	DSM-CC	5.2	13818	Trunk	2688
CVX600_612	Large	DSM-CC	5.2	13818	Trunk	612
NUERA _BTX4K	Large	TGCP	1.0	2427	Trunk	4032
NUERA_GX _MEGACO	Large	MEGACO	1.0	2944	Trunk	2108
PVG7K _MEGACO	Large	MEGACO	1.0	2944	Trunk	1008
PVG15K _MEGACO	Large	MEGACO	1.0	2944	Trunk	1120
PVG15K_1000 _MEGACO	Large	MEGACO	1.0	2944	Trunk	1000
PVG15K _PARTIAL _MEGACO	Large	MEGACO	1.0	2944	Trunk	624
PVG_VSP3 _MEGACO	Large	MEGACO	1.0	2944	Trunk	2016
PVG_VSP4E	Large	MEGACO	1.0	2944	Trunk	4032
TGCP	Large	TGCP	1.0	2427	Trunk	4032

PVG_ASPEN profiles - obsolete in the (I)SN09 release

Starting in (I)SN09, all PVG_ASPEN profiles are obsolete. These profiles are still present in the GWC Manager GUI but are not supported. Before upgrading the GWC to (I)SN09, make sure that all gateways configured with one of these profiles are changed to a compatible profile with the MEGACO protocol. For example, PVG7K_ASPEN to PVG7K_MEGACO.

Customer support

For information about support options and to order software, see *Basics* NTP applicable to your solution.

Glossary of acronyms and initialisms

This section defines acronyms and initialisms applicable to Carrier Voice over IP (VoIP) networks and the GWC component.

AAB

Automatic answerback

AAL1

ATM Adaptation Layer 1

AAL2

ATM Adaptation Layer 2

AC

Audio controller

ACD

Automatic call distribution

AH

Authentication header protocol

ALG

Application layer gateway

ANSI

American National Standards Institute

APS

Audio Provisioning Server

ARP

Address resolution protocol

ATM

Asynchronous transfer mode

BCM

Business communications manager

BCP

Border Control Point

BCT

Bearer channel tandeming

BICC

Bearer independent call control

BRI

Basic-rate interface

CBM

Core and Billing Manager

CCA

Compact Call Agent

CCF

Call control frame

CICM

Centrex IP Client Manager

CKLN

Change keyset LEN

CLEI

Common-language equipment identifier

CLLI

Common-language location identifier

CM

Computing module

CMTS

Cable modem termination system

CODEC

Compressor - decompressor

Contivity 600 VPN switch

Contivity 600 virtual private network switch

COPS

Common open policy service

CORBA

Common object request broker architecture

cPCI

Compact peripheral component interconnect

CS 2000

Communication Server 2000:

CS 2000-Compact

Communication Server 2000-Compact

CS 2000 Core Manager

Communication Server 2000 Core Manager is the device manager of the CS 2000.

CS 2000 GWC

CS 2000 Gateway Controller

CS 2000 SAM21

CS 2000 Services Application Module 21

CS LAN

Communication Server local area network: is the integrated component within Nortel Carrier Voice over IP CS 2000 and CS 2000-Compact that provides a secure environment for mission critical processing of message traffic between the CS 2000 components and other key network elements.

CSM

CS 2000 Services Application Module 21

CSV

Channel supervision messages

DHCP

Dynamic host configuration protocol

DLH

Distributed line hunt

DN

Directory number

DNH

Directory number hunt

DNS

Domain name service

DPL

Dynamic packet line

DPNSS

Digital Private Network Signaling System No. 1

DPT

Dynamic packet trunking

DSM-CC

Digital storage media - command and control; used to manage universal port gateways, such as a trunk gateway which can connect TDM terminations.

DQoS

Dynamic quality of service feature: assigns (on demand) resources for each communication, depending on the QoS requested

DS0

Digital signal level 0: the 64 kbit/s channel that is the basic building block for a North American T1 transmission line

DS0A

Refers to a process where a sub-rate signal (2.4, 4.8, or 9.6 kbit/s) is repeated 20, 10, or 5 times respectively to make a 64 kbit/s DS0 channel

DS1

Digital signal level 1: the North American Digital Hierarchy signaling standard for transmission at 1.544 Mbit/s.

DS30

Digital signal level 30: is the equivalent of 30 DS1s

DSL

Digital subscriber line

DTMF

Dual-tone multifrequency

EIOP

Ethernet Input/Output Processor

ENET

Enhanced network (using TDM)

ESP

IPSec encapsulating security payload; protocol that provides both IP packet encryption and optional message integrity, not covering the IP packet header

Ethernet Routing Switch 8600

CS 2000 LAN router

ETSI

European Telecommunications Standards Institute

FCAPS

Fault, configuration, accounting, performance, security

FCM

Fabric control message

FLPP

Fiberized link peripheral processor

FQDN

Fully qualified domain name

FTP

File transfer protocol

GCP

Gateway Controller Protocol

GUI

Graphical user interface

GWC

Gateway Controller

HIOP

High performance input output processor; provides the XA-Core with ethernet access to the IP-based telco network and supports communication between the core and the GWC

HMAC

Hashed message authentication code

IAD

Integrated access device

ICMP

Internet control message protocol

IETF

Internet Engineering Task Force

IKE

Internet key exchange; a key management mechanism used to negotiate and derive keys for security associations (SA) in IPSec

IEMS

Integrated Element Management System

Intl

International (market)

I/O

Input/output

IP

Internet protocol

IPSec

IP Security; a collection of internet standards for protecting IP packets with encryption and authentication

IPSec SA

IPSec security association; a one-way relationship between sender and receiver offering security services on the communication flow

ISDN

Integrated services digital network

ISUP

Integrated services digital network user part

ITRANS

Internet transparency

ITU

International Telecommunications Union

IW SPM-IP

Inter-working spectrum peripheral module

JAAS

Java authentication authorization service

JWS

JavaTM Web Start

Kerberos

Network authentication protocol; provides key exchange mechanism for IPSec

KDC

Key distribution center

LAN

Local area network

LCC

Line class code

LEN

Line equipment number

LBL

Limited bandwidth link

LMM

Line maintenance manager

LGRP

Logical groups

LPP

Link peripheral processor; the core switch’s link to the SS7 network. In the IP topology, works with the GWC to supply signaling to the destination switch

MAC

Media access control

MADN

Multiple appearance directory number

MAPCI

Maintenance and administration position command interface

MDM

Multiservice data manager

MEGACO

Media gateway control; an IETF standard for peripheral messaging protocols promulgated originally as H.248

MG 9000

Media Gateway 9000

MG 9000 Manager

Media Gateway 9000 manager

MGC

Media gateway controller

MGCP

Media gateway control protocol

MIB

Management Information Base

MLH

Multiline hunt

MSC

Mobile switching center

MTA

Multimedia terminal adapter

MTX
Mobile telephone exchange

NA
North American (market)

NAPT
Network address and port translator

NAS
Network access service

NAT
Network address translator or translation

NCS
Network-based call signaling

NEBS
North American new equipment building standard

NFS
Network file system

NOCs
Network operations centers

Nortel Media Gateway 7480
Formerly the Passport 7400 PVG

Nortel Media Gateway 15000
Formerly the Passport 15000 PVG

NPM
Network patch manager

NTP
Network time protocol

NTP
Nortel technical publication

OAM&P
Operations, administration, maintenance, and provisioning

OC-3
Optical carrier level 3 is the SONET transmission rate of 155.52 Mbit/s

OM
Operational measurement

OSI
Open systems interconnection

OSS
Operations support system

OSSGate
An application that provides a machine interface for provisioning components within Carrier Voice over IP

PDF
Adobe (TM) portable document format

PDP
Policy decision point

PEC
Product engineering code

PEP
Policy enforcement point

PFS
Perfect Forward Secrecy

PM Poller
Performance measurements poller

POTS
Plain old telephone service

PRI
Primary rate interface

PSTN
Public switched telephone network

PVG
Passport packet voice gateway

QCA

Quality of service collector application

QoS

Quality of service

RA

Resource allocator

RAID

Redundant array of inexpensive disks

RAS

Remote access server

RMGC

Redirecting media gateway controller

RMON

Remote monitoring specification (simple network management protocol)

RTCP

Real time control protocol

RTP

Real-time transport protocol

SC

Shelf controller

SCCP

Signaling connection control part protocol

SCTP

Simple control transmission protocol

SDP

Signaling distribution point; also, session descriptor protocol

SecMM tool

Security Monitoring and Maintenance tool

SESM

Solution element sub-element manager; a software package that includes several CS 2000 Management Tools applications

SFT

Secure file transfer

SGCP

Simple Gateway Controller Protocol

SIP-T

Session initiation protocol for telephony

SNMP

Simple network management protocol

SPM

Spectrum peripheral module

SS7

Signaling system number 7: is a family of signaling protocols used to set up, manage, and tear down connections, as well as to exchange non-connection associated information.

SSL

Session Server Lines

SST

Session Server Trunks

SPFS

Server platform foundation software; the NCL software package that contains base operating system and common tools, libraries and server functions used by element-management-level applications.

STORM

Storage management

STP

signaling transfer point; a node in the SS7 network

SWACT or SwAct

Switch activity; switch call processing from one card to another in a node

TCP

Transmission control protocol

TDM

Time division multiplexing

TFTP

Trivial file transfer protocol

TGCP

Trunk gateway control protocol

TMM

Trunk maintenance manager

UAS

Universal audio server

UAS Manager

Universal audio server manager

UDP

User datagram protocol

USP

Universal signaling point

USP-Compact

Universal signaling point-compact

USP-Manager

Universal signaling point-manager

VCAC

Virtual call admissions control

VMG

Virtual media gateway

VRDN

Virtual router distribution node; a type of Carrier Voice over IP GWC

VoIP

Voice over Internet Protocol

VPN

Virtual private network

VSP

Voice services processor card in the Nortel Media Gateway 7480 or 15000

XA-Core

Extended architecture core

XML

Extensible markup language

XPM

Extended Peripheral Module

Carrier VoIP

Gateway Controller Basics

Publication: NN10189-111
Document status: Standard
Document version: 08.02
Document date: 20 October 2006

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

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