



Gateway Controller Basics

What's new in SN07

The following release SN07 features are documented in the Gateway Controller (GWC) Nortel technical publication (NTP) suite. In addition, other changes and enhancements to this NTP for SN07 are noted in the following list:

- A00002512 - CS 2000 GWC Manager internet transparency VCAC provisioning
- A00002550 - H.323 gatekeeper to gatekeeper inter-operability
- A00002644 - Common topology element for inter-CS 2000 internet transparency solution
- A00003568 - E911 PSAP selection, location, identification
- A00003575, A00003576 - IP Security (IPSec) available for SMALL_LINENA, SMALL_LINEINTL, SMALL_TRUNKNA, SMALL_TRUNKINTL profiles in packet cable solutions
- A00003630 - TGCP for the cable market
- A00003691 - IEMS SNMP OM polling from GWC and SC
- A00003948 - Tri-modal server support on CS 2000 Management Tools and CS 2000 GWC Manager
- A00003995 - CS 2000 Management Tools: H.323 GW change capability
- A00004981 - CS 2000 GWC Manager ITRANS-VCAC support for CICM gateways
- A00006340 - CS 2000 GWC Manager support for MTX_TRUNKNA and MTX_TRUNKINTL GWC profiles
- A00006495 - H.323 flexible carrier sizes
- A00006496 - H.323 multiple D-channel support
- A00007063 - H.323 gateway profiles for SN07
- A00007211 - H.323 GWC600 to adhere to OSS requirements
- DOMAIN_NAME gateway profile (in cable market)

- The APG capability is removed in release SN07, although the CS 2000 GWC Manager still displays APG service profiles and gateway profile names. As a result, this NTP maintains references to APG functionality.
- Simplified navigation of the PDF file for the Gateway Controller Configuration Management NTP, NN10205-511
- Re-organized overview information in the NTP Upgrading the Gateway Controller, NN10196-461. Added a new module “Preparing to upgrade the Gateway Controller”.
- The Integrated Element Management System (EMS) supports Carrier Voice over IP (VoIP) components in SN07, including the GWC.
- PVG naming - The table below lists the names used for certain gateways in Carrier VoIP documentation prior to SN07 and provides the new brand names starting in SN07.

Pre-SN07 name	Brand name starting in SN07
Passport Packet Voice Gateway (PVG)	Media Gateway 7400 or 15000
PVG 7400 or PVG 7K	Media Gateway 7400
PVG 15000 or PVG 15K	Media Gateway 15000
<p>Note: The CS 2000 GWC Manager does not reflect these branding changes in SN07. 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.</p>	

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
- Upgrading the Gateway Controller, NN10196-461

Functional description

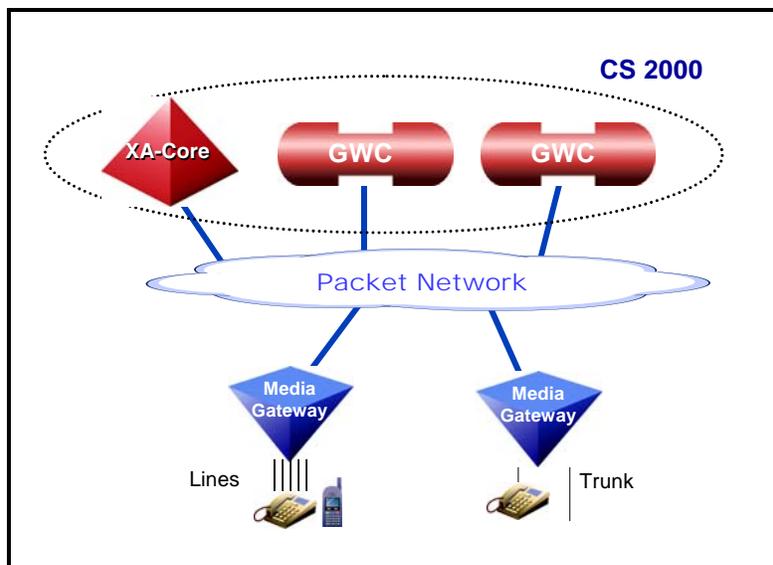
The Gateway Controller (GWC) is a network component in the Communication Server 2000 (CS 2000) and CS 2000 - Compact products. Its function is to manage and manipulate signaling and bearer paths on various types of media gateways. It receives instructions from the CS 2000 XA-Core or Call Agent (CS 2000 - Compact) to perform 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 and the line/trunk Access devices, making the media gateway appear to the XA-Core as an XPM.

Relationship of GWC to other CS 2000 network components



In a sense, the XA-Core 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 view the GWC as a

media gateway controller, or MGC. Therefore, the GWC connects the two views together providing:

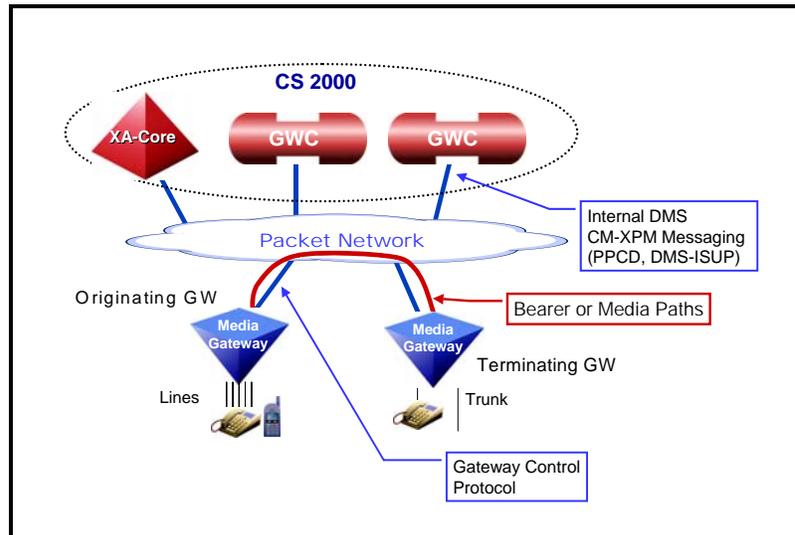
- inter-CS 2000 network calls using the Session Initiation Protocol for Telephony (SIP-T) messaging across the packet network to enable communication between CS 2000s
- intra-CS 2000 network calls using NCS, DSM-CC, MGCP, ASPEN, MEGACO/H.248, H.323 or TGCP signaling protocols to communicate with Nortel 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 IP network environment, the distance between network components is less of an issue than in a TDM environment.

Call flow, signaling and messaging with the GWC



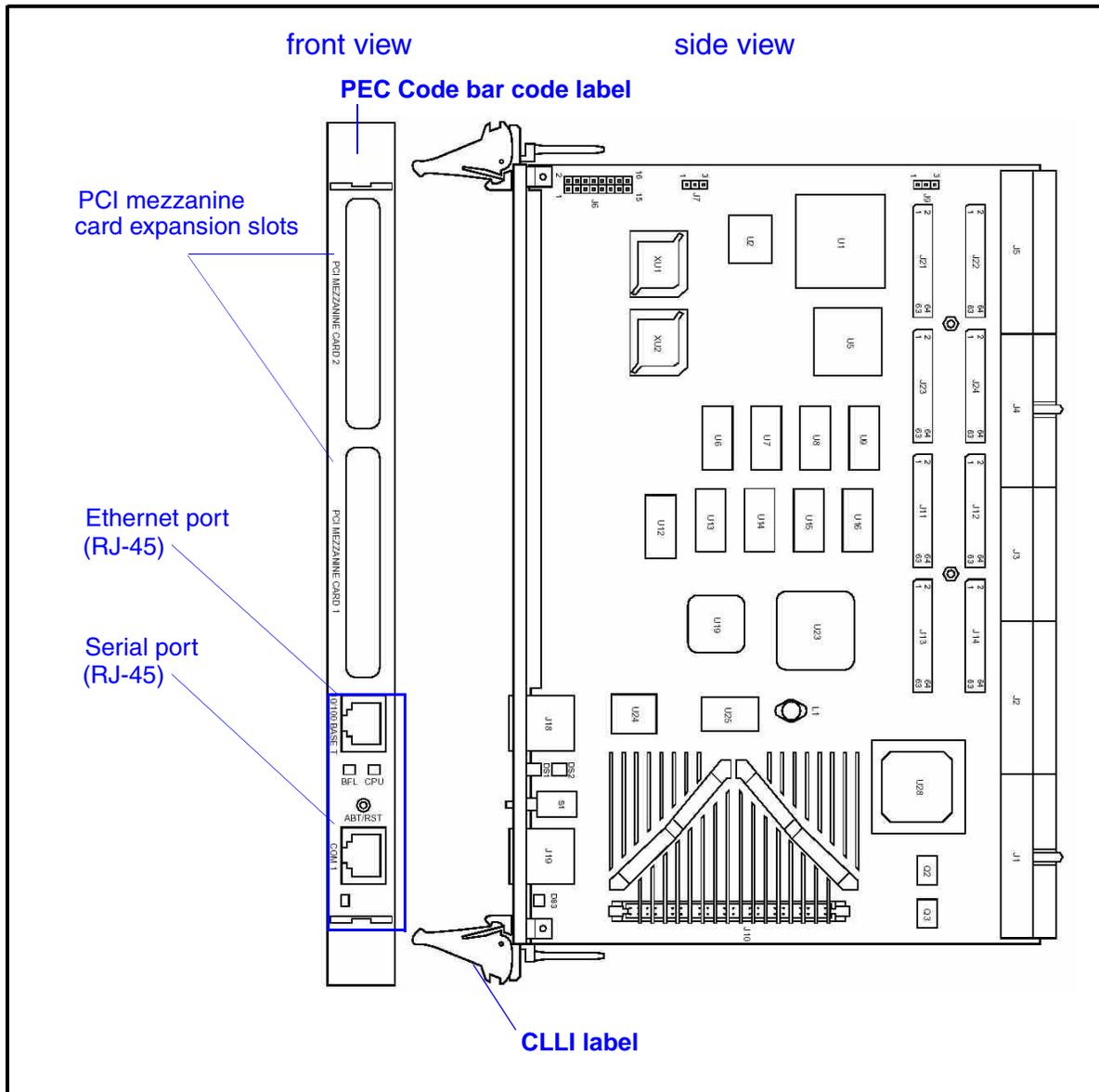
Call flow messages from the GWC to the gateways trigger the set up of the bearer path which carries the call content, whether voice or data. Using gateway control messages from the XA-Core, a GWC can then exchange connection information with another GWC allowing the two to handshake with the correct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

GWC hardware platform

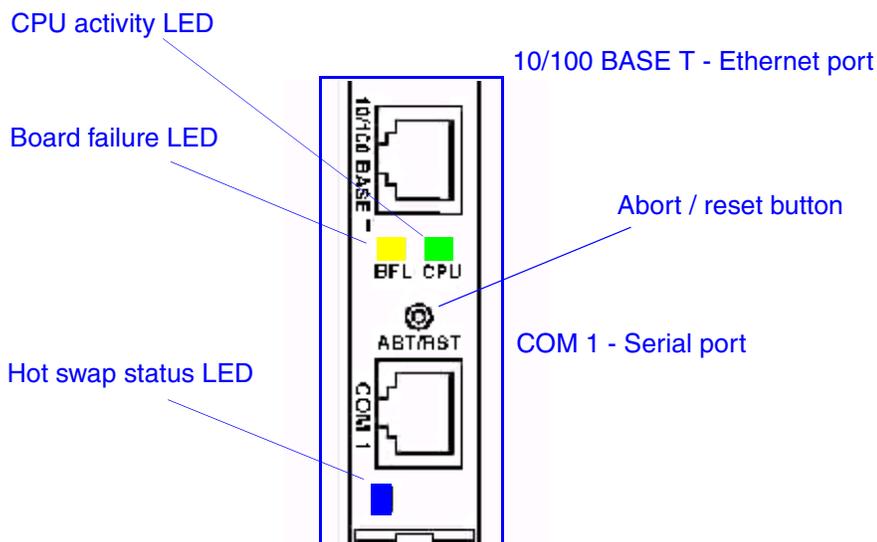
The GWC card hardware runs on a Motorola N750 NSS board. The following figure highlights some physical attributes of the GWC card.

For card identification, refer to the PEC code bar code label at the top of the card edge (front view), and the common language location identifier (CLLI) on the bottom ejector lever.

GWC card (Motorola N750 NSS board)



Ethernet port and serial port details



The ethernet port is an RJ-45 connector labelled 10/100 Base-T located on the front panel, above the connector labelled 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 (SDM) or Core and Billing Manager (CBM) - bootp/load server (same subnet)

Note: GWC cards are normally located on the same subnet as other call processing components such as the CS 2000 Core Manager (SDM) or Core and Billing Manager (CBM), and the Ethernet or High Speed Input/Output Processor (EIOP/HIOP) XA-Core components. Refer to section [GWC hardware platform on page 6](#) for details about

An RJ-45 connector labelled 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 a GWC card:

- BFL (Board failure) LED (yellow) - Lights when a system failure occurs on the card.
- CPU activity LED (green) - Lights when the card's processor is currently active.
- Hot swap status LED (blue) - Lights when it is permissible to remove the card from the shelf.

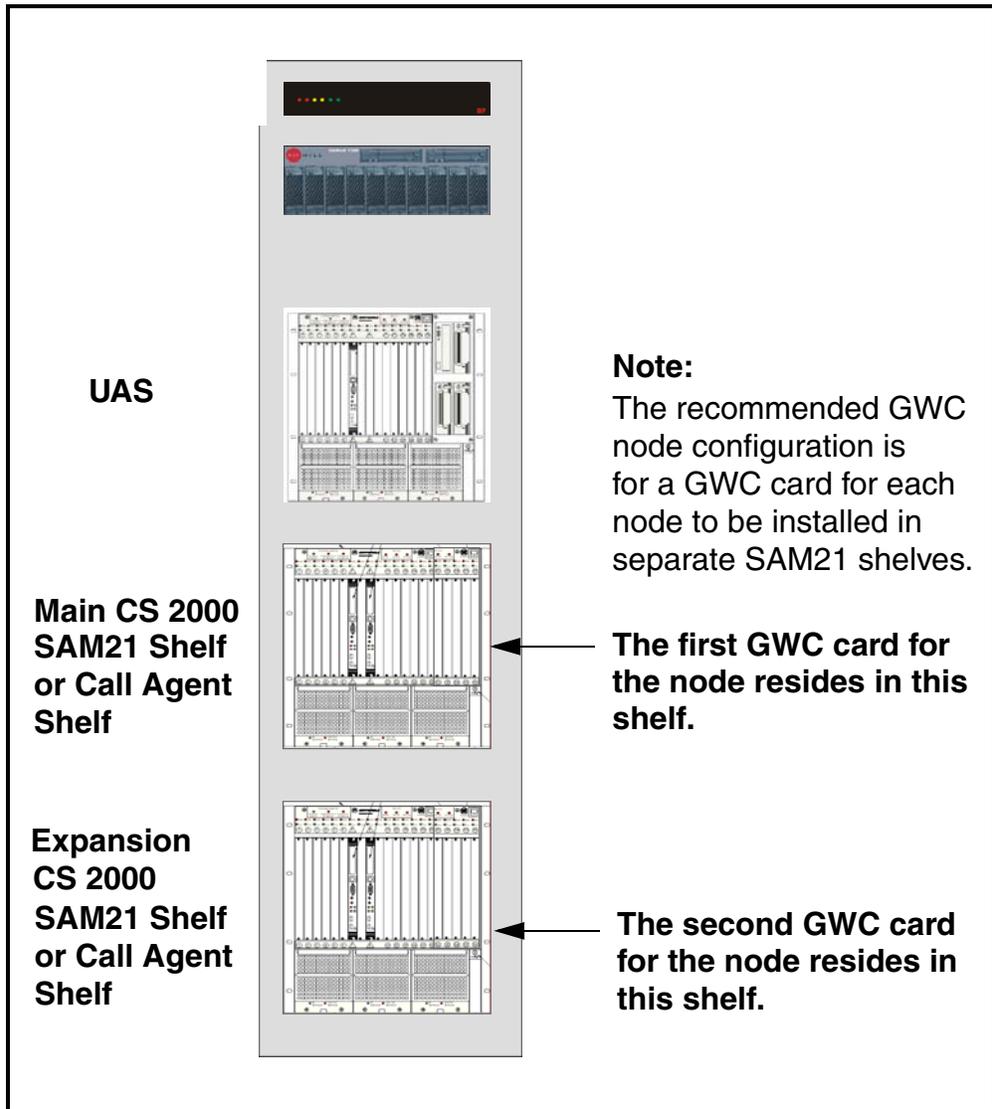
In addition to the LEDs, there is also an ABT/RST (abort / reset) button on the front of GWC card. To abort the CPU's current process, press this button briefly (for less than three seconds). To reset the card, press and hold this button (for more than three seconds).

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 Networks Carrier voice over IP (VoIP) network.

GWC card locations in SAM21 or Call Agent shelves

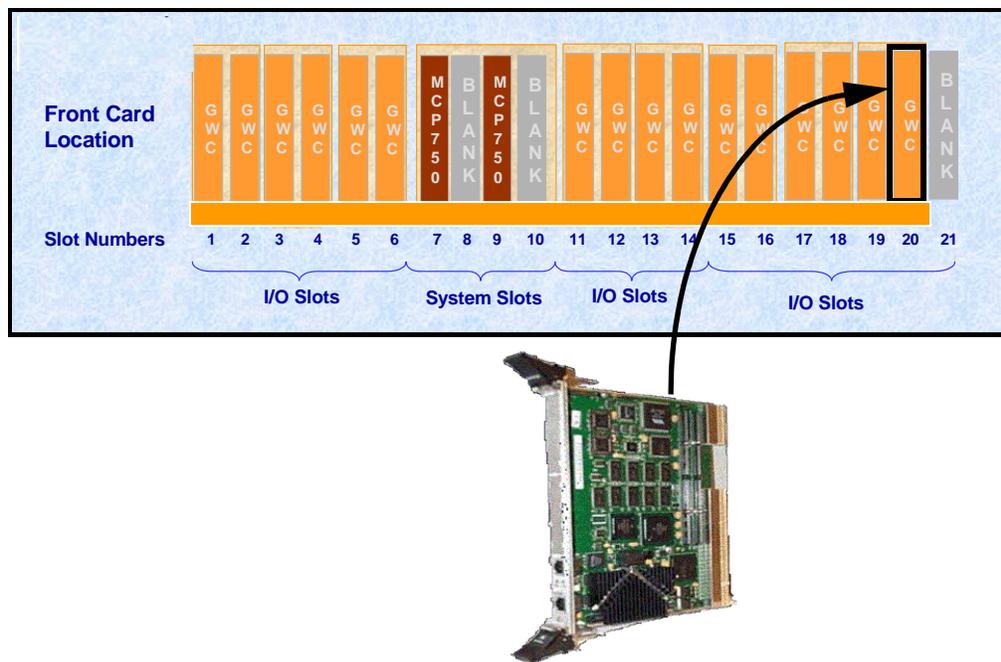


GWC cards and the SAM21 shelf

The CS 2000 SAM21 shelf accommodates a maximum of 16 GWC cards. The 21st slot (front and rear) should always be empty. 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 16 I/O slots in the SAM21 shelf can be filled with GWC cards, as shown in the following figure.

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 (SDM) 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 table lists the software loads used to provision and maintain GWC firmware.

GWC software loads required for SN07

Filename	Description
sitka.flash	GWC Flash file (for manual firmware upgrades)
GN070xx	NA GWC Software Load for SN07
GI070xx	Intl GWC Software Load for SN07

Software ordering and delivery

Refer to the Basics NTP for your solution for more information about ordering software and support options.

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 details, refer to one of the following end-to-end upgrades NTPs:

- IP Solutions Upgrades, NN10344-450
- ATM Solutions Upgrades, NN10261-450

The CS 2000 GWC Manager is designed to handle backward compatibility for up to two (2) major GWC releases. The following diagram illustrates the CS 2000 GWC Manager multi-version compatibility with GWC card software loads.

Versions of GWC card software supported by the CS 2000 GWC Manager

CS 2000 GWC Manager		GWC card software versions supported	
Release	Included in load name	Release	Load name
SN07	CS2M0007, SESM0007	SN07	GN070, GI070
		SN06.2	PGC93, PGT93 PGC92
		SN06.1	PGC91, PGT91
		SN06	PGC09, PGT09
		SN05	PGC08, PGT08
SN06.2	CS2M06.2, SESM06.2	SN06.2	PGC93, PGT93 PGC92
		SN06.1	PGC91, PGT91
		SN06	PGC09, PGT09
		SN05	PGC08, PGT08
SN06.1	CS2M06.1, SESM06.1	SN06.1	PGC91, PGT91
SN06	CS2M06, SESM06	SN06	PGC09, PGT09
		SN05	PGC08, PGT08
SN05	PTM10	SN05	PGC08, PGT08

Note: For information on the contents of the CS 2000 Management Tools software packages, including CS2M and SESM, refer to the Basics NTP for 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 Networks 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 on how to access the CS 2000 GWC Manager and the CS 2000 SAM21 Manager, refer to the CS 2000 Management Tools information in the Security and Administration NTP for your solution, NN10402-600.

Integrated Element Management System

Many FCAPS activities may now be performed using the Integrated Element Management System (EMS). 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 Integrated EMS. For more information, refer to the Integrated EMS Basics NTP, NN10329-111.

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

- “Launching GWC Manager”
- “Launching SAM21 Manager”

Configuration

Initial configuration of a Gateway Controllers is completed by Nortel Networks 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) or policy enforcement point (PEP) middleboxes 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.

Note: For information on alarms and logs on the CS 2000 Management Tools server, refer to the Fault Management NTP for your solution, 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 (EMS)

For details on GWC alarms and for procedures on viewing alarms, refer to the Gateway Controller Fault Management NTP, 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 Integrated EMS.

For details on GWC logs and for procedures on viewing logs, refer to the Gateway Controller Fault Management NTP, NN10202-911.

Performance management

CS 2000 captures performance metrics through OM (operational measurement) registers. The OMs collect operational statistics that are reported to the XA-Core, and stored in the XA-Core 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. To retrieve these OM statistics about gateways, refer to the CS 2000 Performance Management NTP, NN10149-711.

In addition to OMs, the GWC also uses Management Information Base (MIB) based performance measurements (PMs) 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.

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.

Note: 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.

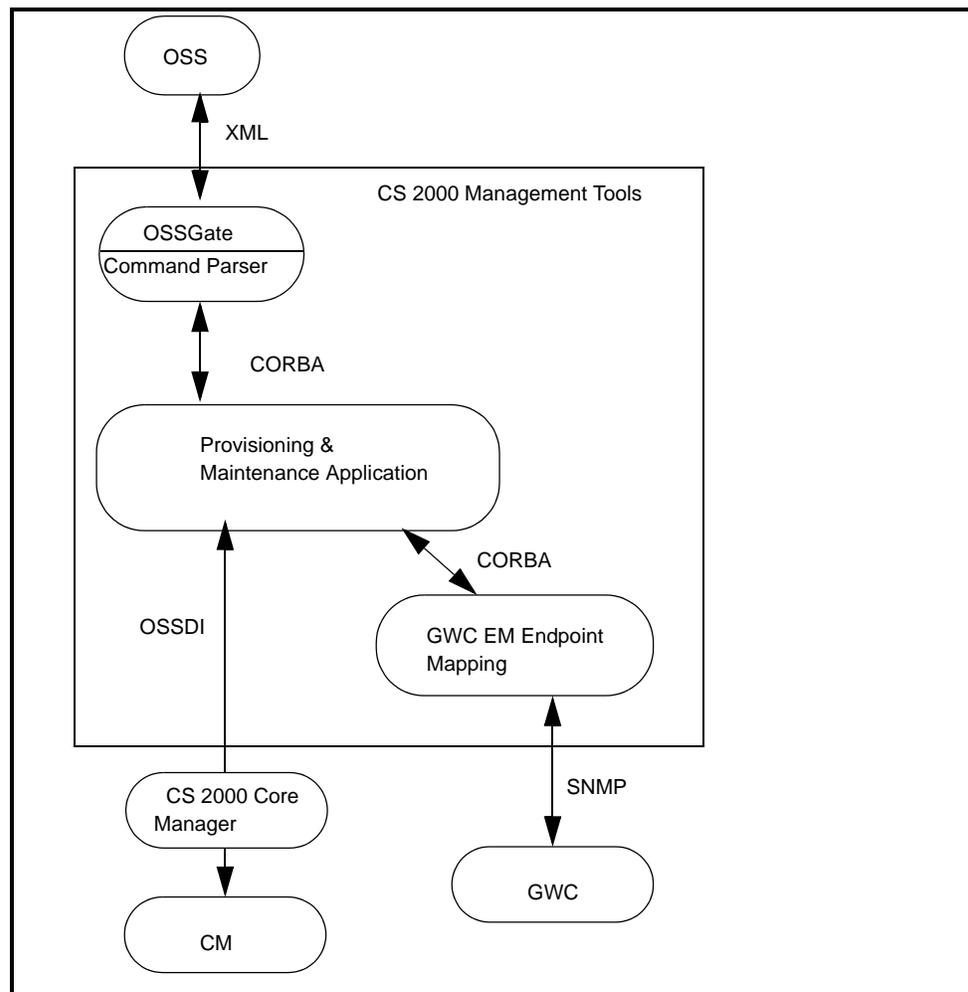
Bulk provisioning using OSSGate

Bulk provisioning (configuration) of GWCs in a Nortel Networks 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, refer to the 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. Although the active IP address is determined automatically, it must also be configured at the CS 2000 GWC Manager. The active unit IP address is required by other network elements such as UAS 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, 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 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

Starting in release SN06, 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, UDP or 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.

For example, a trunk GWC supports a maximum of 4094 datafilled ports. However, some PVG VSP configurations support a maximum of 1120 ports. Therefore, for maximum utilization of the GWC, one would provision three 1120-port VSPs and one 624-port VSP.

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:

Note: Refer to [Table of media gateway profiles and characteristics on page 38](#) for information about which gateway profiles support the protocols in this list.

- ASPEN

ASPEN is based on the Simple Gateway Controller Protocol (SGCP) and includes modifications to support extensions that SGCP does not support. ASPEN 2.1 call control to GWCs for ISUP trunk agencies is also supported.

- 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.

Note: The XA-Core only supports 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.

- 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 (G.711, 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 PSTN media gateways.

Gateway Controller service profiles

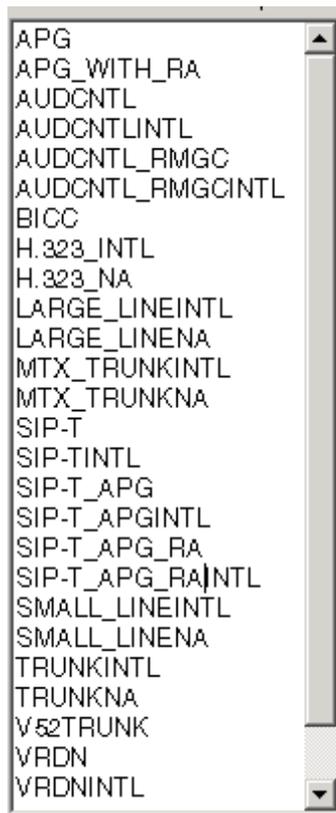
GWCs are usually used to host trunks, lines or other devices through gateways. Gateway Controller service profiles, such as trunk, line, audio, DPT, VRDN or RA, are used to define the type of GWC being configured. For example, Gateway Controller service profiles TRUNKNA and TRUNKINTL have the same generic service profile: TRUNK. The figure [List of Gateway Controller service profiles supported on page 23](#) 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. Refer to [Table of media gateway profiles and characteristics on page 38](#) to view the full list of gateway profiles that may be supported on a Gateway Controller.

Note 1: 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.

Note 2: In some cases, Gateway Controller service profiles are also reflected in the service type of media gateway profiles supported on a GWC. For example, PVG 7K, PVG 15K, CVX1800_2688 and CVX1800_612 all have the same service type: TRUNK.

List of Gateway Controller service profiles supported



Anchor packet gateway (APG)

The APG GWC service profile is responsible for managing dynamic packet trunk calls that require an Anchor packet gateway (APG). In this GWC configuration, DPT calls are implemented using the SIP-T protocol as the inter-Communication Server protocol. When a service requires manipulation of the bearer path, there are several options available, such as remote bearer control or bearer channel proxy. If these options cannot be used, the user may attempt to anchor the bearer connection using an APG. The GWC that controls the APG communicates with the DPT GWC to set up and manage the connections. The APG GWC does not get this type of instruction from the XA-Core as do the DPT GWC and the TDM trunk GWC.

Note: The APG capability is removed in release SN07, although the CS 2000 GWC Manager still displays APG service profiles.

Audio controller

The Audio Controller service profile is used to support UAS gateways (including any Nortel Media Server 2000 Series media gateways) within a Carrier VoIP network.

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 (DPTs) 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 to manage connections that are DPT connections, the DPT GWC formulates and sends SIP-T messages rather than media gateway control messages (such as, ASPEN 2.1). In a sense, it serves as a proxy for the real media gateway that resides on a different Communication 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 public switched telephone network (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.

Note: In order to use either MTX profile, the CS 2000 XA-Core must be upgraded to the SN07 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-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. Mediatrix and ASKEY 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) GWC service profile is responsible for Anchor Packet Gateway (APG) contexts. The RA server application runs on one of the APG GWCs. It is important for requestor GWCs and host GWCs to know where the resource allocator service is. In general, the GWCs which host APG-type gateways are used to associate the RA service. This type of GWC uses the APG_WITH_RA profile category, so a separate GWC is not required to run the RA.

You may also use a SIP-T_APG_RA service profile to add SIP-T based DPT trunk services that will host an APG with an associated RA server for your market. Only one RA server should be configured for each communication server.

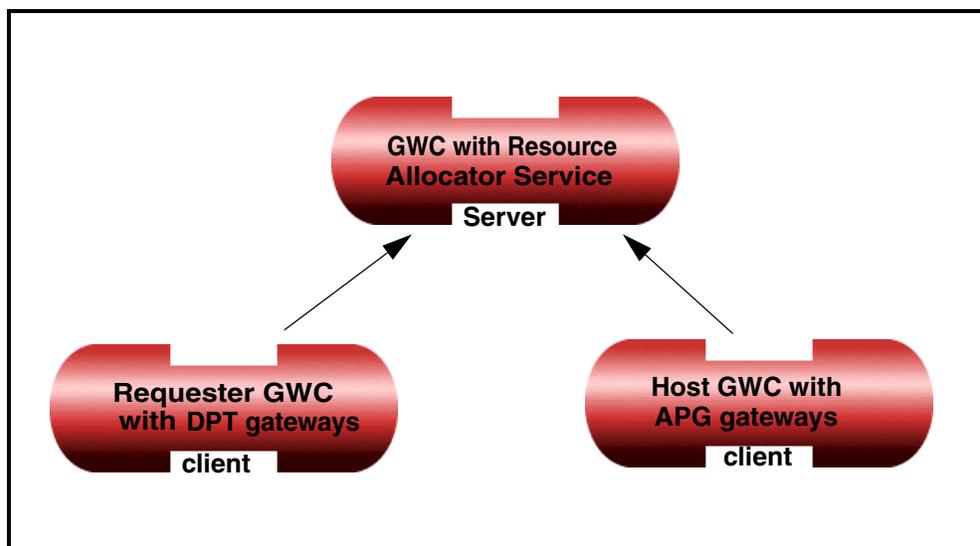
In order to support services on DPT calls, the DPT GWC needs to anchor the bearer path of the call. It uses an APG to do this. The RA is a resource management function that manages contexts (that is, bearer endpoints) on the APGs available to the Communication Server. When the DPT GWC decides that it needs to insert an APG into the call, it queries the RA GWC. The RA GWC responds with the location of an APG GWC that controls an available APG context. The DPT GWC then begins messaging to the APG GWC to set-up the APG connections. The RA GWC maintains the availability of the APG contexts. It does this by having the associated APG GWC inform the RA GWC when the APG contexts become available or unavailable. Starting in SN05 any DPT GWC can optionally perform APG and/or RA server functions, thus requiring fewer GWCs to support the APG function.

The following figure illustrates the 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 APG gateways.

The same GWC also acts as a server for the requester GWCs that host DPT gateways.

Note: The APG capability is removed in release SN07, although the CS 2000 GWC Manager still displays APG service profiles.

Figure 1 Resource allocator server and clients

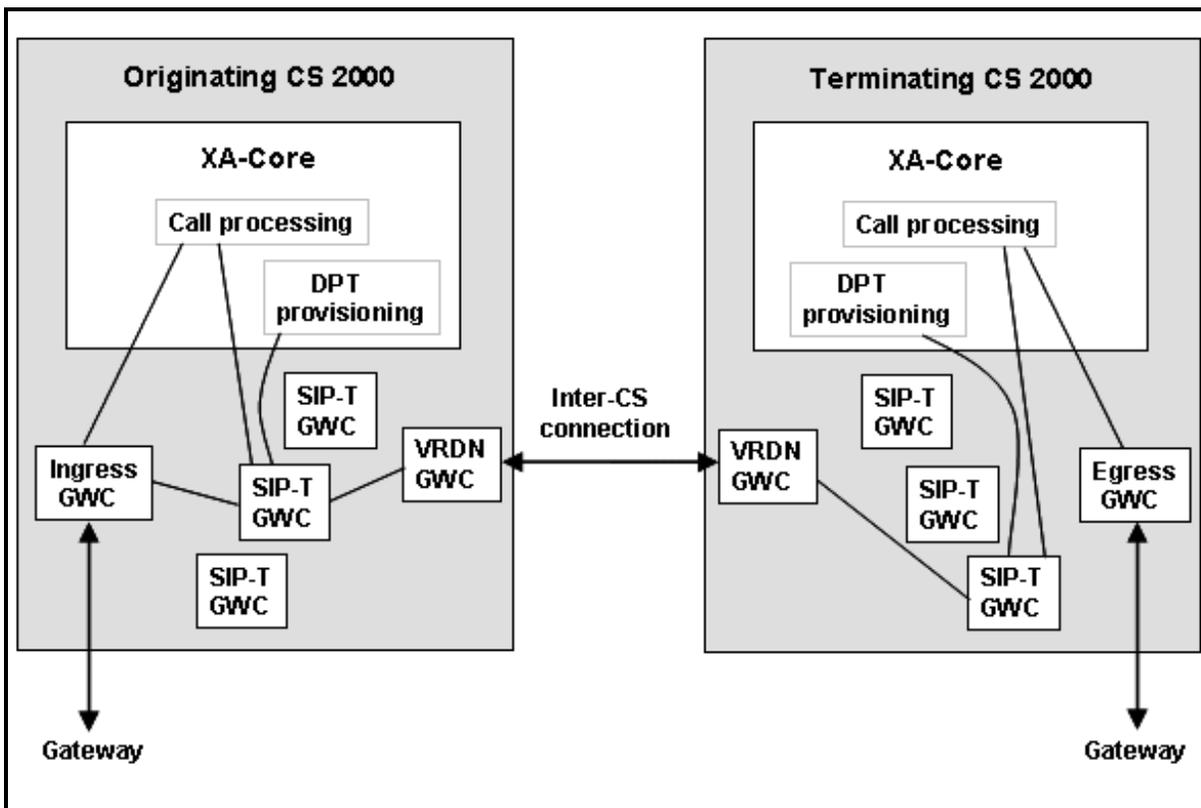


Session initiation protocol for telephony (SIP-T)

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

When two or more CS 2000s are brought together in a network, SIP-T 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. The following figure provides more information about the role of the SIP-T and VRDN GWCs in this type of call processor network.

Role of SIP-T and VRDN GWCs in a CS 2000 network



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

- The XA-Core selects the DPT served by the SIP-T 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, is downloaded to its SIP-T 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-T message.
- Once a DPT served by a SIP-T GWC has been selected and configured, that GWC can communicate directly with:
 - VRDN (for coordination of messages with the GWC is via call ID)
 - The appropriate ingress / egress GWC

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

Small / 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.

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.

Note: Starting in SN06, ASPEN protocol will no longer be supported. Only H.248 /Megaco signaling protocol is supported. H.248 and ASPEN protocol cannot co-exist on one VSP card or on one V5.2 Interface.

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.

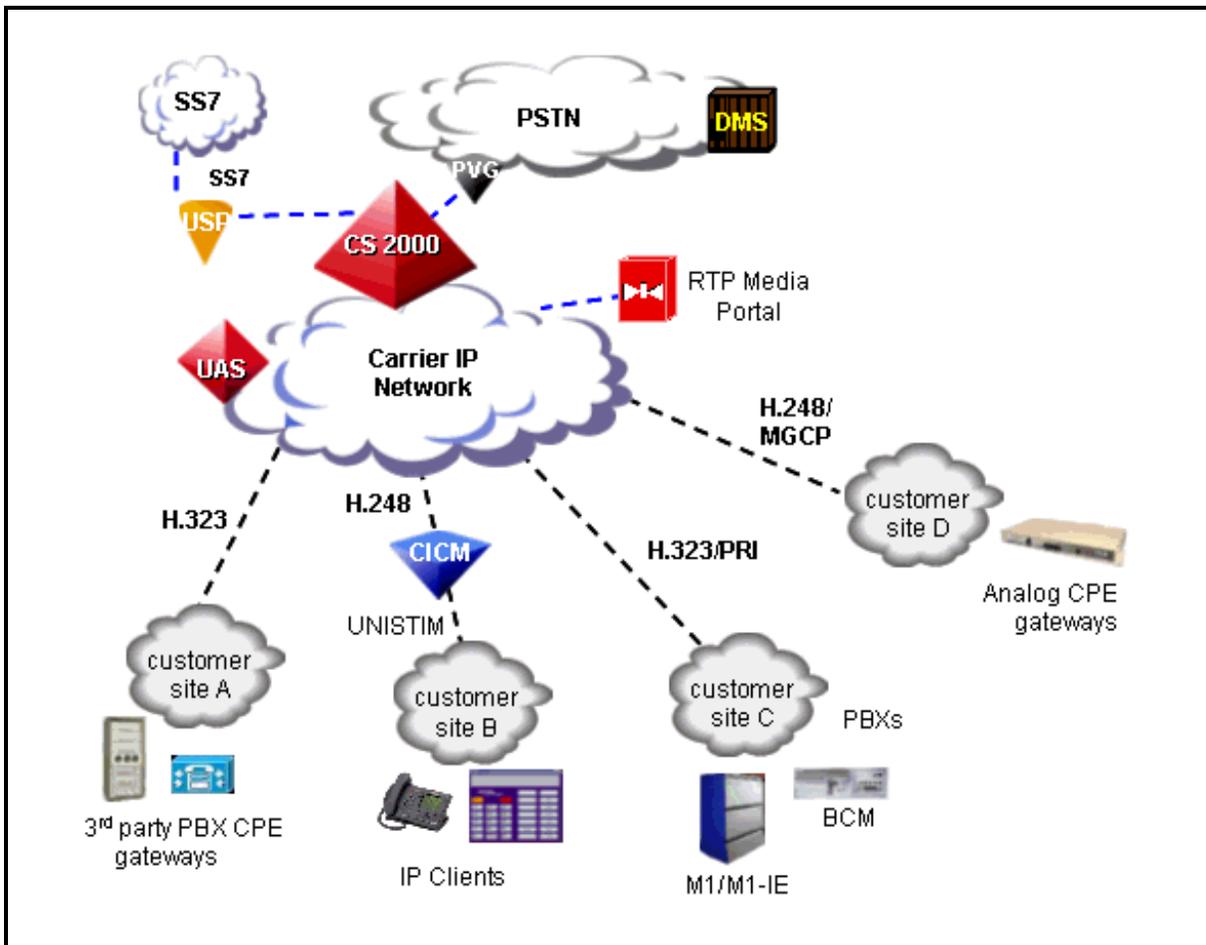
The VRDN GWC service profile provides a SIP-T interface to the Communication Server. It distributes SIP-T call processing messages between SIP-T GWCs. The VRDN GWC is responsible for aggregating SIP-T messaging and provides a single IP address for routing messages that are destined for any GWC associated 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.

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:

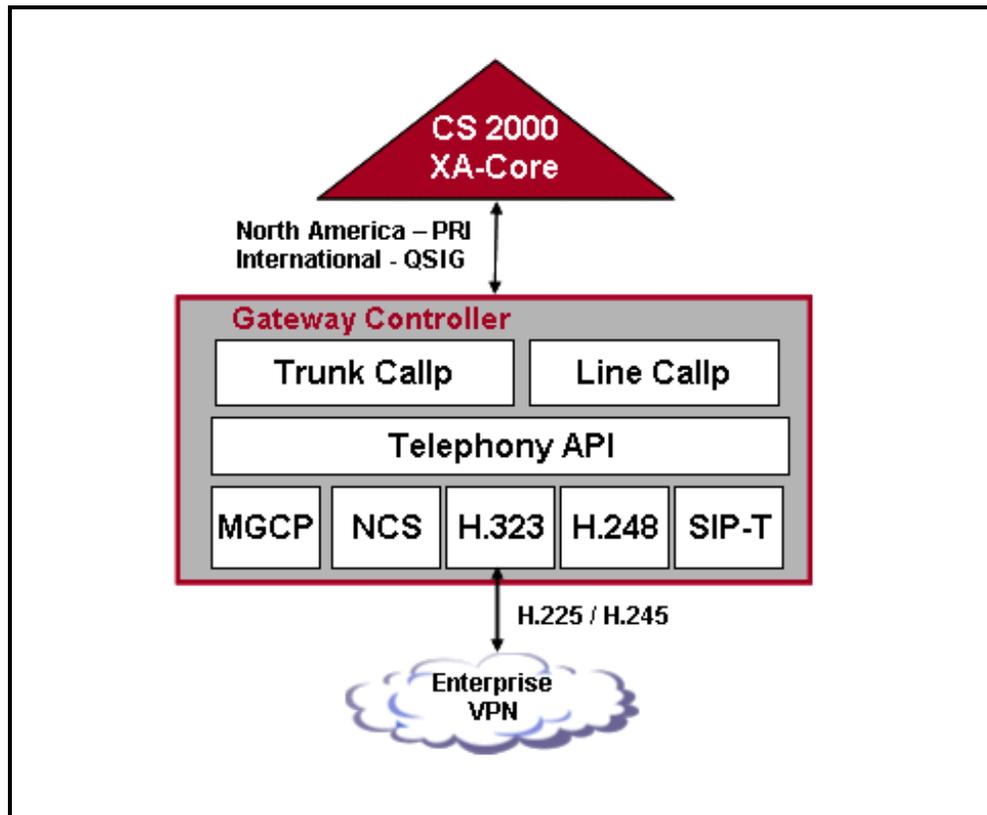
- Multiple IP-based networks with interworking to trunks and lines.
- Inter-operability with third-party PBX gateways over H.323; see customer site A.
- IP clients over H.248 using Centrex IP Client Manager (CICM); see customer site B.
- Connectivity with Nortel Networks gateways over H.323/PRI, including Meridian 1 - IP Enabled and Business Communications Manager (BCM); see customer site C.
- Analog gateways using integrated access devices (IADs) over H.248/MGCP; see customer site D.

The CS 2000 uses real-time transport protocol (RFC 1889), or RTP Media Portal, 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 RTP Media Portal 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

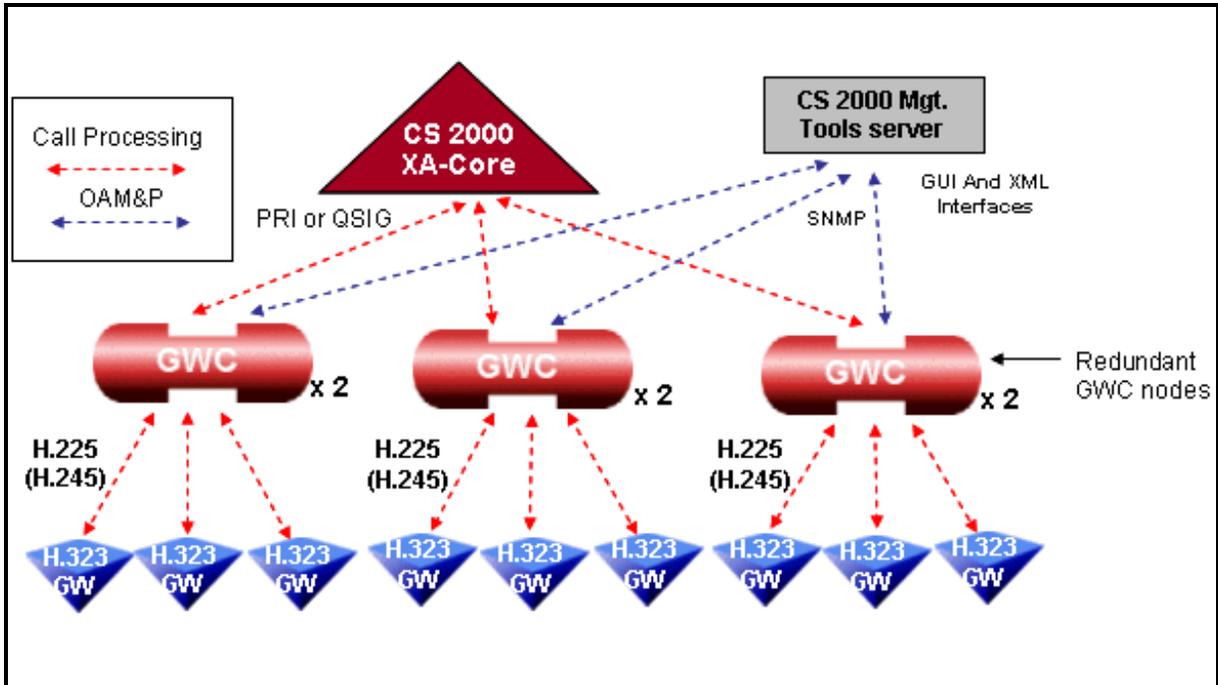
The GWC integrates gateway control protocols into the existing line and trunk call processing engines, as shown in the following figure. The GWC includes H.323 as a peer with the other protocols it supports. H.225 signaling is sent to PRI or QSIG for processing by the XA-Core, integrating PRI service 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



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 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



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 (LBLs) and network address translators (NATs). The VoIP gateways and the lines are located within the different sites in each enterprise.

For information on configuring VCAC, refer to the Gateway Controller Configuration Management NTP, NN10205-511.

Trimodal functionality on the CS 2000

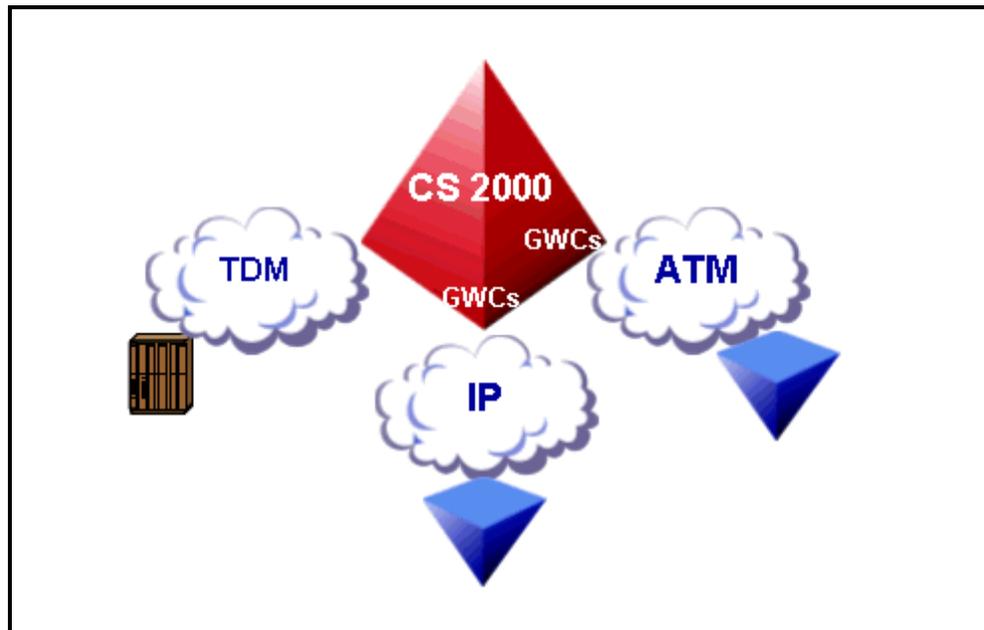
Starting in release SN07, CS 2000 supports the concurrent implementation of multiple bearer networks. Trimodal operation includes IP and ATM packet bearer networks as well as the TDM Enhanced Network (ENET).

In SN07, the focus is on supporting three bearer networks:

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

Note: AAL2 packet networks can be configured, but will not be fully tested in a multiple bearer network configuration in SN07.

Trimodal operation



GWC support for Trimodal operation

Prior to SN07, CS 2000 GWC Manager supported the configuration of only one bearer network fabric type on a CS 2000. Starting in SN07, it is possible to configure and use network codec profiles with multiple 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.

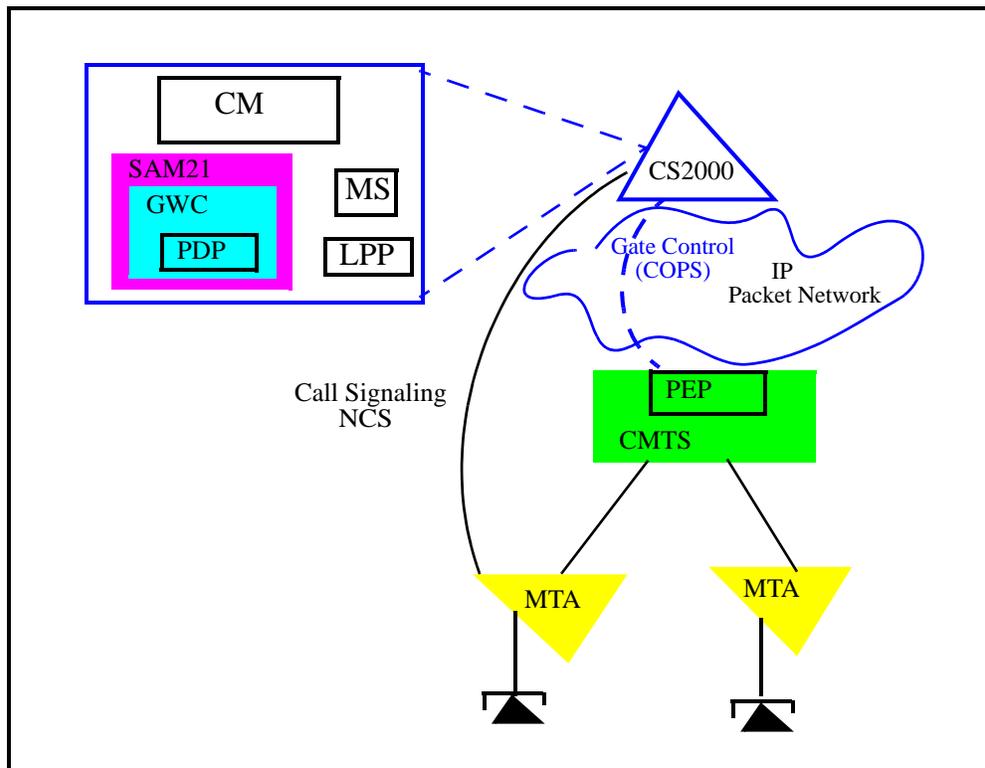
Dynamic quality of service

GWC supports dynamic quality of service (DQoS), a feature used in Nortel Networks 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.

QoS parameters such as packet loss, latency and jitter can be reported on a call-by-call basis for the purpose of network optimization, trend analysis, troubleshooting and service-level agreement (SLA) validation.

Note: QoS reporting is applicable to ATM and hybrid networks as well as to VoIP networks. Currently, QoS reporting has only been tested using GWC-driven gateways in cable solutions.

If you would like to use QoS reporting in a non-cable solution, please contact your Nortel Networks account prime for more information.

For instructions about configuring DQoS and PEP server access, refer to the Gateway Controller Configuration Management NTP, 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.

Note: For more information on basic IPSec concepts, refer to the Gateway Controller Security and Administration NTP, NN10213-611. For detailed IPSec information, refer to the appropriate Internet Engineering Task Force (IETF) RFC documentation, which can be found at <http://www.ietf.org>.

Starting in SN07, IPSec implementation is optional and supported only in packet cable solutions, where 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
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, refer to the ATM/IP Solution-level Security and Administration NTP, 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)

Note: For an overview of the IPSec implementation in a packet cable network, refer to the ATM/IP Solution-level Security and Administration NTP, NN10402-600.

Media gateway profiles

The [Table of media gateway profiles and characteristics](#) contains information about the different profiles supported on a Gateway Controller.

Note 1: Some profiles support multiple gateways. Contact your Nortel Networks account prime for the gateways supported using a profile.

Note 2: The media gateway profiles supported depend on the Gateway Controller service profile configured for a GWC node. Refer to [Gateway Controller service profiles on page 22](#) for details.

Table of media gateway profiles and characteristics (Sheet 1 of 4)

Gateway Profile Name	Gateway Category	Signaling Protocol Type	Protocol Version	Default Protocol Port	Service Type	Max. Port/Endpoint Capacity
<i>Anchor packet gateways</i>						
PVG_APG	APG	ASPEN MEGACO	2.1 1.0	2427 2944	APG	1120
PVG_APG_VSP3	APG	ASPEN MEGACO	2.1 1.0	2427 2944	APG	2016
Note: The APG capability is removed in release SN07, although the CS 2000 GWC Manager still displays APG gateway profile names.						
<i>Audio gateways</i>						
UAS (includes Nortel Media Server 2000 Series)	Audio	MEGACO	1.0	2944	Audio	n/a
<i>H.323 gateways</i> (See Note 1 and Note 2)						
CISCO_2600	large	H.323	4.0	n/a	H.323, ITRANS	1032 (NA) 1024 (Intl)
CISCO_3600	large	H.323	4.0	n/a	H.323, ITRANS	1032 (NA) 1024 (Intl)
CISCO_AS5300	large	H.323	4.0	n/a	H.323, ITRANS	1032 (NA) 1024 (Intl)
CISCO_H323_IOS	large	H.323	4.0	n/a	H.323, ITRANS	1032 (NA) 1024 (Intl)
H323_PROXY	large	H.323	4.0	n/a	H.323, ITRANS	1032 (NA) 1024 (Intl)

Table of media gateway profiles and characteristics (Sheet 2 of 4)

Gateway Profile Name	Gateway Category	Signaling Protocol Type	Protocol Version	Default Protocol Port	Service Type	Max. Port/Endpoint Capacity
NORTEL_BCM	large	H.323	4.0	n/a	H.323, ITRANS	1032 (Intl) 1024 (Intl)
SUCCESSION_1000	large	H.323	4.0	1719	H.323, ITRANS	1032 (NA) 1024 (Intl)
WESTELL	large	H.323	4.0	1719	H.323, ITRANS	1032 (NA) 1024 (Intl)
<i>Line gateways (wireline market)</i>						
AFC	Large	MEGACO	1.0	2944	Line	1023
AMBIT_LINE_GW_1	Small	MGCP	1.0	2427	Line, ITRANS	1
AMBIT_LINE_GW_16	Small	MGCP	1.0	2427	Line, ITRANS	16
AMBIT_LINE_GW_32	Small	MGCP	1.0	2427	Line, ITRANS	32
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
CICM	Large	MEGACO	1.0	2944	Line, ITRANS_ROAM	1024
MEDIATRIX_GW_4	Small	MGCP	1.0	2427	Line, ITRANS	4
MEDIATRIX_GW_24	Small	MGCP	1.0	2427	Line, ITRANS	24
MGCP_LINE_GW_1	Small	MGCP	1.0	2427	Line, ITRANS	1
<i>Line gateways (cable market)</i>						
ARRIS_TOUCHTONE_NN01_4	Small	NCS	1.0	2427	Line, DQoS	4
ARRIS_TOUCHTONE_NN02_4	Small	NCS	1.0	2427	Line, DQoS	4
DOMAIN_NAME	Small	NCS	1.0	2427	Line, DQoS	1
Note: The DOMAIN_NAME profile provides the capability to configure a common domain name for all MTA gateways associated with the selected GWC. For more information, refer to procedure "Configure the domain name for MTA gateways (cable market) in the Gateway Controller Configuration Management NTP, NN10205-511.						

Table of media gateway profiles and characteristics (Sheet 3 of 4)

Gateway Profile Name	Gateway Category	Signaling Protocol Type	Protocol Version	Default Protocol Port	Service Type	Max. Port/Endpoint Capacity
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
<i>Trunk gateways</i>						
AUDIOCODES (Mediant 2000)	Large	MEGACO	1.0	2944	Trunk	280
CVX1800_2688	Large	DSM-CC	5.2	13818	Trunk	2688
CVX600_612	Large	DSM-CC	5.2	13818	Trunk	612
NUERA_GX	Large	ASPEN MEGACO	2.1 1.0	2427 2944	Trunk	2108
PVG7K	Large	ASPEN MEGACO	2.1 1.0	2427 2944	Trunk	1008
PVG15K	Large	ASPEN MEGACO	2.1 1.0	2427 2944	Trunk	1120
PVG15K_1000	Large	ASPEN MEGACO	2.1 1.0	2427 2944	Trunk	1000
PVG15K_PARTIAL	Large	ASPEN MEGACO	2.1 1.0	2427 2944	Trunk	624
PVG_VSP3	Large	ASPEN MEGACO	2.1 1.0	2427 2944	Trunk	2016
TGCP	Large	TGCP	1.0	2427	Trunk	2047

Table of media gateway profiles and characteristics (Sheet 4 of 4)

Gateway Profile Name	Gateway Category	Signaling Protocol Type	Protocol Version	Default Protocol Port	Service Type	Max. Port/Endpoint Capacity
<p>Note 1: When associating an H.323 gateway with a GWC, the protocol port must be set as follows:</p> <ul style="list-style-type: none">• 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. <p>Note 2: For H.323 gateways, the endpoint capacity indicated is a recommended value based on the GWC capacity. The actual endpoint capacity supported depends on the details of your specific installation. For the H.323 profiles listed above, refer to the corresponding product documentation to determine the recommended endpoint maximum supported on a specific gateway.</p>						

Customer support

Refer to the Basics NTP for your solution for information about support options and to order software.

Glossary of acronyms and initialisms

Acronyms and initialisms applicable to Carrier Voice over IP (VoIP) networks and the GWC component are defined below:

AC

Audio controller

AH

Authentication header protocol

ANSI

American National Standards Institute

APG

Anchor packet gateway

APS

Audio Provisioning Server

ARP

Address resolution protocol

ASPEN

A proprietary call control protocol

ATM

Asynchronous transfer mode

BICC

Bearer independent call control

CCF

Call control frame

CISM

Cabinetized integrated service module

CLLI

Common-language location identifier

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

CSAM

Cabinetized services application module

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 Networks Succession 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.

CSV

Comma separated values

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 Kbps) is repeated 20, 10, or 5 times respectively to make a 64 kbps 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

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

FCAPS

Fault, configuration, accounting, performance, security

FCM

Fabric control message

FLPP

fiberized link peripheral processor

FTP

file transfer protocol

GUI

graphical user interface

GWCEM

CS 2000 Gateway Controller (element) manager

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

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

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

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

Java™ Web Start

Kerberos

Network authentication protocol; provides key exchange mechanism for IPSec

KDC

Key distribution center

LAN

Local area network

LBL

Limited bandwidth link

LMM

Line maintenance manager

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

MAPCI

Maintenance and administration position command interface

MCS

Multimedia Communication Server

Media Gateway 7400

Formerly the Passport 7400 PVG

Media Gateway 15000

Formerly the Passport 15000 PVG

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

MTA

Multimedia terminal adapter

NA

North American (market)

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

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 Succession

Passport 7400 PVG

Passport 7400 packet voice gateway

Passport 8600

CS 2000 LAN router

Passport 15000 PVG

Passport 15000 packet voice gateway

PM Poller

Performance measurements poller

Preside MDM

Preside multiservice data manager

Preside MSS

Preside management for Succession solutions; Preside MSS is a suite of element management software that runs on approved hardware platforms. Preside MSS provides the overall OAM&P functionality for Succession solutions.

PDF

Adobe (TM) portable document format

PEP

Policy enforcement point

PRI

Primary rate interface

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

SDM

SuperNode data manager

SDP

Signaling distribution point; also, session descriptor protocol

SESM

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

SFT

Secure file transfer

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.

SSPFS

Succession 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

SWIM

SDM Software Inventory Manager

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

VDRN

Virtual router destination node; a type of Succession GWC

VoIP

Voice over Internet Protocol

VPN

virtual private network

VSP

Voice services processor card in the Passport 15000 PVG or the Passport 7400 PVG

XA-Core

Extended architecture core

XML

Extensible markup language